Manual de Control Panel para administradores

Contents

Información general.....7

Acerca de este manual.....7
Información básica sobre Control Panel.....8
Introducción.....8
Requisitos.....9
Información de versión.....9
Consultar el número de versión.....9
Primeros pasos en Control Panel.....10
Iniciar sesión.....10
Configuración de usuario.....22
Administración de derechos en Control Panel.....53

Email Live Tracking.....63

Estructura de Email Live Tracking.....64
Configurar la vista de correos.....66
Seleccionar las columnas mostradas.....66
Modificar tamaños de campos.....68
Modificar posición de campos de correo.....70
Filtrar correos.....71
Filtrar correos por categorías.....71
Barra de búsqueda.....72
Filtros de campos.....75
Descartar y repetir búsquedas.....77
Detalles de correo.....78
Ejecutar una acción sobre un correo.....78
Iniciar el escaneo ATP.....80
Informe ATP.....82
Información avanzada de correos.....84
Campos de correo.....86
Categorías de correo electrónico.....90
Seleccionar una acción para varios correos.....92
Acciones para correos.....95

Vista previa de correos....99
Exportar datos de correos en formato CSV....103

Dashboard de servicios....106

Acerca del Dashboard de servicios....106
Gestión de roles y contactos....107
Contactos....108
Asignar roles....109
Añadir datos de contacto....110
Filtrar roles y contactos....114
Eliminar asignaciones de roles o contactos....117
Eliminar un cliente propio....119
Entornos secundarios....120
Tipos de entornos secundarios....121
Sincronización de entornos secundarios....121
Crear un entorno secundario....123
Editar un entorno secundario....125
Eliminar un entorno secundario....127
Conexión mediante LDAP....129
Configurar atributos de LDAP....130
Añadir una conexión LDAP....132
Limitar el servicio de directorio a nuestro rango de direcciones IP....141
Configurar el acceso a Control Panel mediante LDAP....142
Editar una conexión LDAP....146
Desactivar la conexión mediante LDAP....148
Activar la conexión mediante LDAP....150
Eliminar una conexión LDAP....151
Ajustar zona horaria e idioma por defecto....153
Condiciones Generales....155
Habilitar la función Condiciones Generales....157
Hacer obligatoria para el contrato de tratamiento de datos....158
Crear un contrato de licencia de usuario final y un contrato de tratamiento de datos....159
Exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos....168
Desactivar la función Condiciones Generales....169

Informes y conformidad....172

Informes y conformidad ... 172
Estadística de correos ... 172
Threat Live Report ... 188
Registro de auditorías 2.0 ... 203

Configuración de clientes ... 230
Configuración de cliente ... 230
Buzones de correo ... 230
Grupos ... 288
Dominios ... 307
Autenticación ... 319

Listas blancas y negras ... 335
Acerca de las listas blancas y negras ... 335
Crear un registro de lista negra para un usuario ... 337
Crear un registro de lista blanca para un usuario ... 340
Crear un registro de lista negra para un dominio ... 342
Crear un registro de lista blanca para un dominio ... 344
Importar registros de listas blancas y negras en formato CSV ... 351
Archivos CSV para la importación de registros de listas blancas y negras ... 356
Archivos CSV para importar registros de lista blanca para un dominio ... 356
Editar un registro de lista blanca para un dominio ... 371
Exportar registros de lista blanca o negra en formato CSV ... 373
Eliminar un registro de lista blanca o negra ... 375
Buscar registros de listas blancas o negras ... 378
Procesamiento de registros de listas blancas y negras ... 379

Configuración de seguridad ... 381
Configuración de seguridad ... 381
Advanced Threat Protection (ATP) ... 381
Estructura y funcionamiento de ATP ... 381
Configuración básica ... 389
Escaneo ATP ... 402
Informe ATP ... 405
Email Authentication ... 407
Acerca de Email Authentication ... 407

Comprobar la configuración de DNS de dominios propios....407
Métodos de autenticación de remitentes....409
Quarantine Report....445
Acerca de Quarantine Report....445
Diseños para informes de cuarentena....447
Acciones para correos en informes de cuarentena....451
Activar Quarantine Report para un dominio....455
Configurar Quarantine Report para un dominio....456
Configurar Quarantine Report para un buzón de correo....463
Crear un texto personalizado para informes de cuarentena....466
Desactivar Quarantine Report para un dominio....472
Entregar un correo de un informe de cuarentena....473
Ver vista previa de correos....476
Spam and Malware Protection....477
Spam and Malware Protection....477
Orden de las reglas de todos los servicios....478
Activar Spam and Malware Protection....480
Configuración del entorno primario....483
Configuración del filtro de correo....489
Permitir o prohibir acciones de usuarios....496
Desactivar Spam and Malware Protection....498
Content Control....500
Acerca de Content Control....500
Lista de categorías....501
Activar Content Control....502
Añadir un grupo a Content Control....503
Configurar Content Control....506
Modificar prioridades de grupos....511
Eliminar un grupo de Content Control....513
Desactivar Content Control....514
Compliance Filter....516
Acerca de Compliance Filter....516
Orden de las reglas de todos los servicios....517
Activar Compliance Filter....519
Reglas de filtrado....520
Diccionarios....562
Expresiones regulares....570
Desactivar Compliance Filter....584

Signature and Disclaimer....586
Acerca de Signature and Disclaimer....586
Uso móvil de Signature and Disclaimer....587
Acceso al módulo Signature and Disclaimer....587
Activar Signature and Disclaimer....588
Crear firmas y notas legales....589
Modificar prioridades de grupos....594
Editar o eliminar una firma o nota legal....597
Desactivar Signature and Disclaimer....598
Editor WYSIWYG....600
Solución de problemas....632
Continuity Service....636
Sobre Continuity Service....636
Añadir todos los usuarios de un dominio a Continuity Service....637
Añadir usuarios sueltos a Continuity Service....638
Excluir usuarios de Continuity Service....640

Personalización.... 642
Personalización de Control Panel....642
Añadir datos de soporte técnico a Control Panel....643
Personalizar correos electrónicos de Control Panel....645
Personalizar Control Panel....653
Modificar los módulos mostrados en User Panel....660

Motivos de clasificación de correos....663
Motivos de clasificación....663

Índice.... 681

Información general

Acerca de este manual

Este manual está dirigido a administradores de Control Panel. Contiene información sobre su uso, así como sobre funciones administrativas.

Los derechos de administración están divididos en dos niveles:

- Administrador a nivel de cliente: Es responsable de un dominio principal y todos los dominios alias y direcciones de correo electrónico correspondientes.
- Administrador a nivel de partner: Es responsable de varios clientes. Cada cliente equivale a un dominio principal y todos los dominios alias y direcciones de correo electrónico correspondientes.

Nota:

Los módulos a los que tiene acceso cada usuario dependen de los derechos de éste. Por eso, puede ocurrir que no estén disponibles algunos de los módulos y funciones descritos para algunos usuarios.

Este manual incluye, en primer lugar, la siguiente información general sobre Control Panel: Control Panel es una interfaz gráfica que permite utilizar y configurar nuestros servicios (véase Introducción en la página 8) y es compatible con diversos navegadores (véase Requisitos en la página 9).

Control Panel se actualiza de modo continuo para introducir nuevas funciones y mejoras. Es posible consultar el número de versión actual de Control Panel (véase Consultar el número de versión en la página 9). Los cambios introducidos en cada versión se describen en notas de publicación (véase Información de versión en la página 9). Además, Control Panel permite a los usuarios ponerse en contacto con nuestro servicio técnico (véase Consultar al soporte técnico por chat).

A continuación, este manual describe los primeros pasos necesarios para utilizar Control Panel. Para poder acceder a Control Panel, los usuarios deben iniciar sesión previamente (véase Iniciar sesión en la página 10). Cada usuario dispone de su propia configuración de usuario y puede modificarla (véase Configuración de usuario en la página 22). Aparte de esto, los administradores pueden

administrar los derechos de los usuarios (véase Administración de derechos en Control Panel en la página 53) en Control Panel.

Más adelante, este manual contiene descripciones detalladas de cada uno de los módulos de Control Panel:

- **Dashboard** (véase Acerca de Dashboard)
- **Email Live Tracking** (véase Email Live Tracking en la página 63)
- **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106)
- **Informes y conformidad** (véase Informes y conformidad en la página 172)
- **Web Filter** (véase Descargar Web Filter)
- **Configuración de cliente** (véase Configuración de cliente en la página 230)
- **Copia de seguridad** (véase Servicios de copia de seguridad)
- **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335)
- **Security Awareness Service** (véase Acerca de Security Awareness Service)
- **Configuración de seguridad** (véase Configuración de seguridad)
- **Personalización** (véase Personalización de Control Panel en la página 642)

Finalmente se presentan las razones de clasificación en base a las cuales se asignan las diversas categorías a los correos en Control Panel (véase Motivos de clasificación en la página 663).

Información básica sobre Control Panel

Introducción

Control Panel es una interfaz gráfica que le permite emplear y configurar nuestros servicios. La función principal de Control Panel es permitirle supervisar y controlar sus correos electrónicos.

Control Panel asiste a los usuarios en el tratamiento de los correos recibidos y analiza su tráfico de correo electrónico.Así, por ejemplo, permite a los usuarios marcar correos como spam o efectuar la entrega de correos marcados como spam.También permite a los usuarios añadir remitentes a listas blancas y negras (véase Acciones para correos en la página 95).

Control Panel es una aplicación web con diseño dinámico y, por tanto, puede emplearse tanto desde dispositivos móviles como desde ordenadores de sobremesa.

Requisitos

Control Panel es compatible con los siguientes navegadores:

- Google Chrome, a partir de la versión 55
- Mozilla Firefox, a partir de la versión 50
- Microsoft Edge a partir de la versión 38
- Apple Safari a partir de la versión 9

> **Importante:**
>
> No es compatible con el modo de navegación privada de los navegadores indicados.

Información de versión

Control Panel se actualiza de modo continuo para introducir nuevas funciones y mejoras. Cada versión tiene asignado un número de versión (véase Consultar el número de versión en la página 9). Las novedades y mejoras de cada versión se describen en notas de publicación. Las notas de publicación actuales pueden consultarse aquí. También puede accederse a ellas mediante un enlace incluido bajo el número de versión de Control Panel.

Consultar el número de versión

En Control Panel, puede consultar el número de versión actual del propio Control Panel. Bajo el número de versión hay un enlace a las notas de publicación (véase Información de versión en la página 9).

1. Inicie sesión en Control Panel con sus datos de acceso.

2. En la esquina superior derecha de la página, haga clic en el símbolo , junto a la configuración de usuario.

   El número de versión actual se muestra en la esquina inferior derecha de Control Panel. Bajo el número de versión hay un enlace a las notas de publicación.

3. Opcional: Si desea abrir las notas de publicación, haga clic en el enlace bajo el número de versión.

   Las notas de publicación se abren.

Se ha consultado el número de versión.

Primeros pasos en Control Panel

Iniciar sesión

Su administrador ha añadido su buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237).

> **Nota:**
>
> Los administradores pueden desactivar buzones de correo de usuarios (véase Activar o desactivar un buzón de correo en la página 260) en Control Panel. Los usuarios con buzones de correo desactivados no pueden iniciar sesión en Control Panel.

Para acceder a Control Panel, es necesario iniciar sesión.

Nota:

Por motivos de seguridad, los usuarios reciben notificaciones por correo electrónico en caso de que se hayan producido varios intentos de inicio de sesión fallidos con su cuenta. La primera notificación se envía al cabo de 5 intentos de inicio de sesión fallidos. Al cabo de 8 intentos de inicio sesión fallidos se envía una nueva notificación y se bloquea el acceso a la cuenta durante 24 horas. Tras cada intento de inicio de sesión fallido posterior se envía una notificación y se vuelve a bloquear la cuenta durante 24 horas.

1. Introduzca el URL de la página web de Control Panel en su navegador para iniciar sesión en Control Panel.

   Se muestra la página de inicio de sesión.

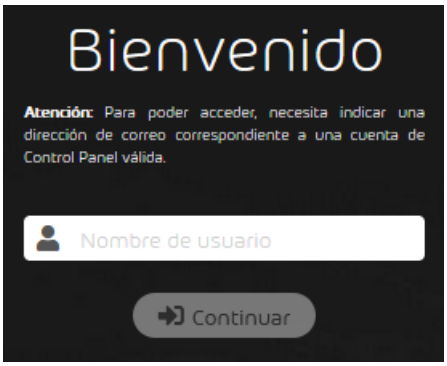


Figura 1: Acceso a Control Panel

2. Introduzca su nombre de usuario en el campo **Nombre de usuario**.

   Nota:

   Indique su dirección de correo electrónico personal como nombre de usuario. Tras registrarse obtendrá los datos de acceso de su partner o del departamento de soporte técnico.

3. Haga clic en **Continuar**.

> **Nota:**
>
> Si ha olvidado su contraseña y su buzón de correo no está sincronizado en Control Panel con un servicio de directorio mediante LDAP, puede solicitar el restablecimiento de la misma (véase Restablecer la contraseña en la página 19).

4. Siga los siguientes pasos si su contraseña se administra en Control Panel o si inicia sesión en Control Panel con sus datos de acceso de un servicio de directorio mediante LDAP.

a) Introduzca su contraseña en el campo **Contraseña**.

Figura 2: Introducir contraseña

b) Haga clic en **Iniciar sesión**.

Si la autenticación multifactor no está configurada para la cuenta, Control Panel se abre. Cuando se inicie sesión en Control Panel por primera vez, se muestra una ventana de selección de la zona horaria, del idioma, del formato de fecha y del formato de hora.

Si se inicia sesión para una cuenta de administrador y se fuerza la autenticación multifactor para los administradores (véase «Forzar la autenticación multifactor para

los administradores» en el manual de Control Panel), el administrador debe configurar la

autenticación multifactor para su cuenta (véase Configurar la autenticación multifactor a partir del paso 7 en la página 30).

Si la autenticación multifactor está configurada para la cuenta (véase Configurar la autenticación multifactor en la página 28), se muestra el campo **Contraseña de uso único**. Se requieren más pasos para iniciar sesión utilizando la autenticación multifactor.

c) Si la autenticación multifactor está configurada para su cuenta, abra su aplicación de autenticación en su dispositivo móvil.

d) Introduzca la contraseña de uso único actual de la aplicación de autenticación en el campo **Contraseña de uso único**.

Figura 3: Introducir la contraseña de uso único

e) Haga clic en **Iniciar sesión**.

> **Nota:**
>
> Si hay problemas con la autenticación multifactor, el administrador puede reiniciar la autenticación multifactor para la cuenta (véase Solución de problemas: Problemas con la autenticación multifactor en la página 21 y "Reiniciar la autenticación multifactor" en el manual de Control Panel).

Control Panel se abre. Si el partner ha publicado un contrato de licencia de usuario final y un contrato de tratamiento de datos, dichos contratos se muestran. Cuando se inicie sesión en Control Panel por primera vez, se muestra una ventana de selección de la zona horaria, del idioma, del formato de fecha y del formato de hora.

5. Si se le pide que defina una contraseña de emergencia, introdúzcala en el campo **Contraseña de emergencia**. Con esta contraseña podrá iniciar sesión en nuestro servicio de correo web si fallase el servidor de correo de su organización. Una vez definida la

contraseña de emergencia, puede cambiarla en su configuración de usuario (véase Cambiar la contraseña de emergencia en la página 26).

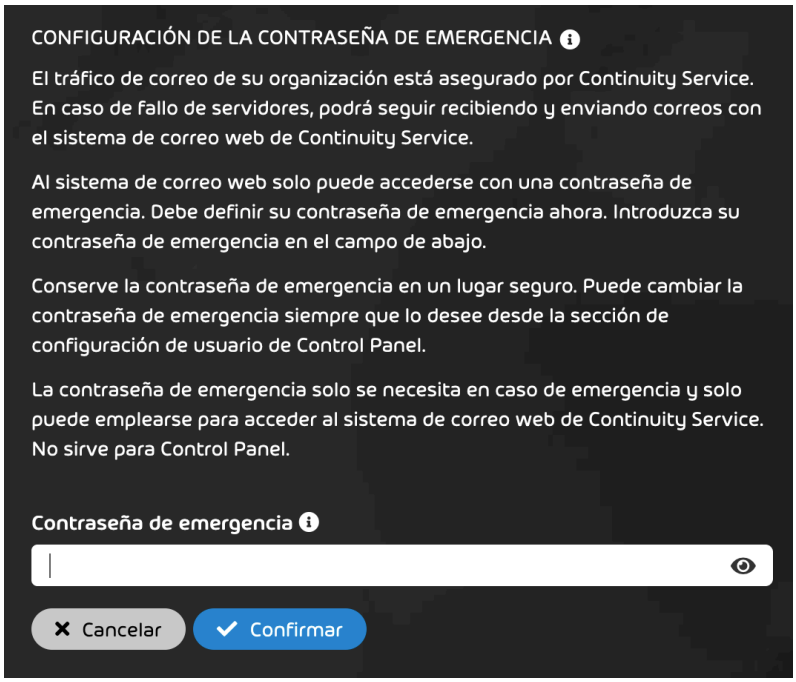


Figura 4: Definir una contraseña de emergencia

6. **Importante:**

   Los partners pueden publicar un contrato de licencia de usuario final y un contrato de tratamiento de datos en Control Panel (véase "Condiciones Generales" en el manual de Control Panel). Para acceder a Control Panel, todos los usuarios deben aceptar el contrato de licencia de usuario final una vez.

   Si se le muestran un contrato de licencia de usuario final y un contrato de tratamiento de datos, acepte sus condiciones.

   a) Marque la casilla **Acepto las condiciones del contrato de licencia de usuario final.**

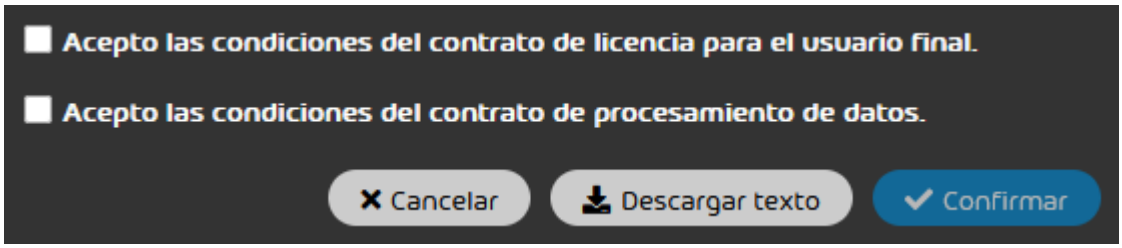


Figura 5: Aceptar el contrato de licencia de usuario final

   b) **Importante:**

   Una vez aceptados por el usuario, los contratos no vuelven a mostrársele en Control Panel.

   Opcional: Si desea guardar el texto de los contratos, haga clic en **Descargar texto**.

   Los contratos se exportan en formato .txt y se facilitan para su descarga.

   c) Opcional: Si ha descargado el texto de los contratos, guarde el archivo .txt en su sistema de archivos.

   d) Haga clic en **Confirmar**.

   Las condiciones de contrato se aceptan.

7. Si inicia sesión en Control Panel por primera vez, seleccione una zona horaria, un idioma, un formato de fecha y un formato de hora en los menús desplegables y haga clic en **Confirmar**.

Figura 6: Seleccionar ajustes

Nota:

Para más información sobre los ajustes, véase Cambiar la zona horaria y el idioma en la página 37. Puede modificar los ajustes en todo momento en su configuración de usuario.

Se ha efectuado el inicio de sesión en Control Panel.

Nota:

Su sesión se cerrará al cabo de 24 horas de inactividad si no la cierra usted antes.

Restablecer la contraseña

Su cuenta no está sincronizada con LDAP.

> **Nota:**
>
> Si su cuenta está sincronizada con LDAP, no podrá restablecer su contraseña por sí mismo. Si desea restablecer su contraseña, consulte a su administrador.

Si ha olvidado su contraseña para Control Panel, puede restablecerla.

1. Abra la página de acceso de Control Panel.
2. Introduzca su dirección de correo electrónico.
3. Haga clic en **¿Restablecer contraseña?**.

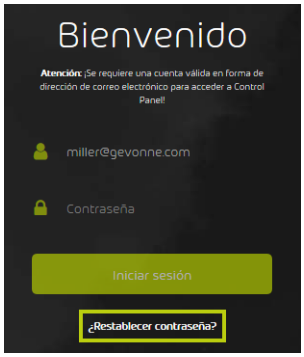


Figura 7: Restablecer la contraseña

4. Haga clic en **Enviar**.

Figura 8: Confirmar el restablecimiento de contraseña

Recibirá un correo electrónico con un enlace para restablecer su contraseña.

> **Nota:**
>
> El enlace será válido durante una hora.

5. Abra el correo y haga clic en el enlace.

Se abre una pantalla con el formulario de inicio de sesión en Control Panel.

6.

> **Importante:**
>
> Por razones de seguridad, la nueva contraseña no debe ser idéntica a la anterior.

Introduzca la nueva contraseña y repítala.

7. Haga clic en **Enviar**.

Figura 9: Confirmar nueva contraseña

Se ha modificado la contraseña. Ahora puede iniciar sesión en Control Panel con su nueva contraseña.

- Si el enlace de restablecimiento de contraseña ha caducado, vuelva a hacer clic en **Enviar**. Recibirá un nuevo enlace.

Solución de problemas: Problemas con la autenticación multifactor

Problema

La autenticación multifactor está configurada para su cuenta de Control Panel (véase Configurar la autenticación multifactor en la página 28). No puede iniciar sesión en Control Panel.

Causa

No puede recuperar la contraseña requerida para el inicio de sesión en Control Panel de su aplicación de autenticación porque ya no tiene acceso a la aplicación o al dispositivo móvil.

Solución

Póngase en contacto con su administrador.

El administrador reinicia la autenticación multifactor para la cuenta (véase el capítulo "Reiniciar la autenticación multifactor" en el manual de Control Panel). La configuración de la autenticación multifactor de la cuenta se elimina. A partir de ahora, solo se necesita la contraseña de Control Panel para iniciar sesión en Control Panel. Es posible reconfigurar la autenticación multifactor (véase Configurar la autenticación multifactor en la página 28).

Configuración de usuario

En la configuración de usuario, los usuarios pueden administrar su configuración personal. La configuración de usuario puede abrirse mediante el icono con forma de rueda dentada en la esquina superior derecha de Control Panel (véase Abrir la configuración de usuario en la página 23).
La configuración de usuario contiene ajustes generales relativos a la contraseña, la contraseña de emergencia del servicio de correo web de Continuity Service (véase Sobre Continuity Service en la página 636), la autenticación multifactor, los datos básicos, la zona horaria y el idioma de un usuario. También permite administrar tokens de API, notas de "fuera de la oficina" y ajustes relativos a informes de cuarentena.

Los usuarios cuyas contraseñas se administren en Control Panel pueden cambiar su contraseña (véase Cambiar la contraseña en la página 24). Si el administrador lo permite (véase "Habilitar la autenticación multifactor" en el manual de Control Panel), los usuarios cuyas contraseñas se administren en Control Panel o en un servicio de directorio mediante LDAP pueden configurar la autenticación multifactor para su cuenta (véase Configurar la autenticación multifactor en la página 28). De este modo se aumenta la seguridad al iniciar sesión en Control Panel. Si lo desean, los usuarios también pueden volver a desactivar la autenticación multifactor para su cuenta (véase Desactivar la autenticación multifactor en la página 33).

Los usuarios cuyos buzones de correo no se sincronicen ni con un servicio de directorio mediante LDAP en Control Panel pueden editar sus datos básicos (véase Editar datos básicos en la página 39). En el caso de los buzones LDAP (véase Tipos de buzón de correo en la página 235), los

datos básicos se sincronizan con el servicio de directorio. Los usuarios de estos buzones de correo pueden consultar sus datos básicos pero no editarlos.

Cada usuario puede seleccionar una zona horaria, un idioma, un formato de fecha y un formato de hora (véase Cambiar la zona horaria y el idioma en la página 37). Los ajustes se aplican a la visualización en Control Panel y a los correos automáticos de Control Panel.

Los administradores y usuarios con el rol **Service Desk** pueden crear tokens de API con los que permitir a aplicaciones acceder a Control Panel a través de la API (véase Crear un token de API en la página 43). Los tokens de API pueden después eliminarse de Control Panel (véase Eliminar un token de API en la página 46), quedando de este modo invalidados.

Además, los usuarios pueden crear notas de "fuera de la oficina" (véase Crear una nota de "fuera de la oficina" en la página 47) para informar automáticamente a los remitentes de sus correos entrantes sobre sus ausencias. Si su administrador se lo permite, los usuarios pueden además editar la configuración de sus propios informes de cuarentena (véase Configurar los informes de cuarentena en la página 48).

Abrir la configuración de usuario

Puede abrir su configuración de usuario (véase Configuración de usuario en la página 22) en Control Panel. En la configuración de usuario puede administrar ajustes generales como, por ejemplo, su zona horaria o su idioma (véase Cambiar la zona horaria y el idioma en la página 37), así como tokens de API (véanse Crear un token de API en la página 43 y Eliminar un token de API en la página 46), notas de fuera de oficina (véase Crear una nota de "fuera de la oficina" en la página 47) y la configuración de sus informes de cuarentena (véase Configurar los informes de cuarentena en la página 48).

1. Inicie sesión en Control Panel con sus datos de acceso.

2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

Se muestra la configuración de usuario.

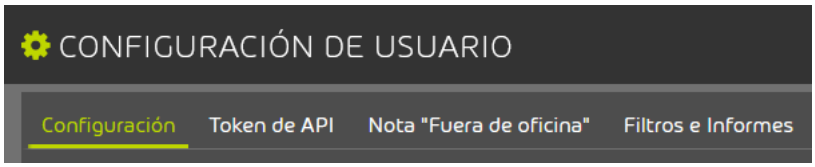


Figura 10: Configuración de usuario

Se ha abierto la configuración de usuario.

configuración

Cambiar la contraseña

Si su buzón de correo no se sincroniza con un servicio de directorio mediante LDAP, puede cambiar su contraseña de Control Panel desde su configuración de usuario (véase Configuración de usuario en la página 22).

Nota:

Los usuarios con buzones de correo LDAP (véase Tipos de buzón de correo en la página 235) pueden acceder a Control Panel con sus datos de acceso del servicio de directorio. Por tanto, dichos usuarios no pueden cambiar sus contraseñas en Control Panel. Los ajustes de contraseña no se muestran a dichos usuarios.

1. Inicie sesión en Control Panel con sus datos de acceso.

2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

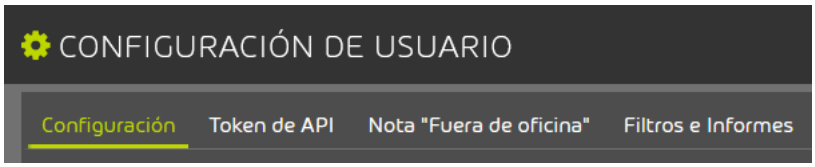


Figura 11: Configuración de usuario

3. Seleccione la pestaña **Configuración**.
4. Introduzca su contraseña actual en el campo **Contraseña antigua**.

Figura 12: Introducir la contraseña antigua

5. **Importante:**

   Las contraseñas nuevas deben contener al menos una letra mayúscula, una letra minúscula, una cifra y un carácter especial. Además, las nuevas contraseñas deben tener una longitud mínima establecida por un administrador a nivel de cliente o de partner. En cualquier caso, las contraseñas deben contener un mínimo de 8 caracteres.

   Importante:

   Por razones de seguridad, la nueva contraseña no debe ser idéntica a la anterior.

   Introduzca la nueva contraseña en el campo **Contraseña nueva**.
6. Repita la nueva contraseña en el campo **Confirmar**.
7. Haga clic en **Guardar**.

La contraseña nueva se guarda. Por motivos de seguridad, el usuario recibe una notificación acerca del cambio de contraseña por correo electrónico.

Se ha cambiado la contraseña.

Cambiar la contraseña de emergencia

1. Inicie sesión en Control Panel con sus datos de acceso.

2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

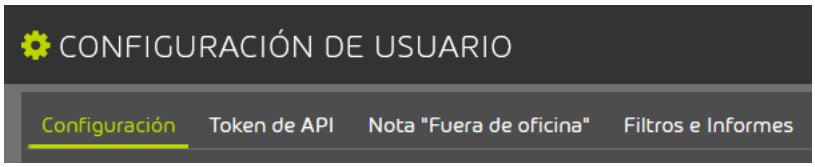


Figura 13: Configuración de usuario

3. Seleccione la pestaña **Configuración**.
4. Introduzca su nueva contraseña de emergencia en el campo **Contraseña de emergencia**.

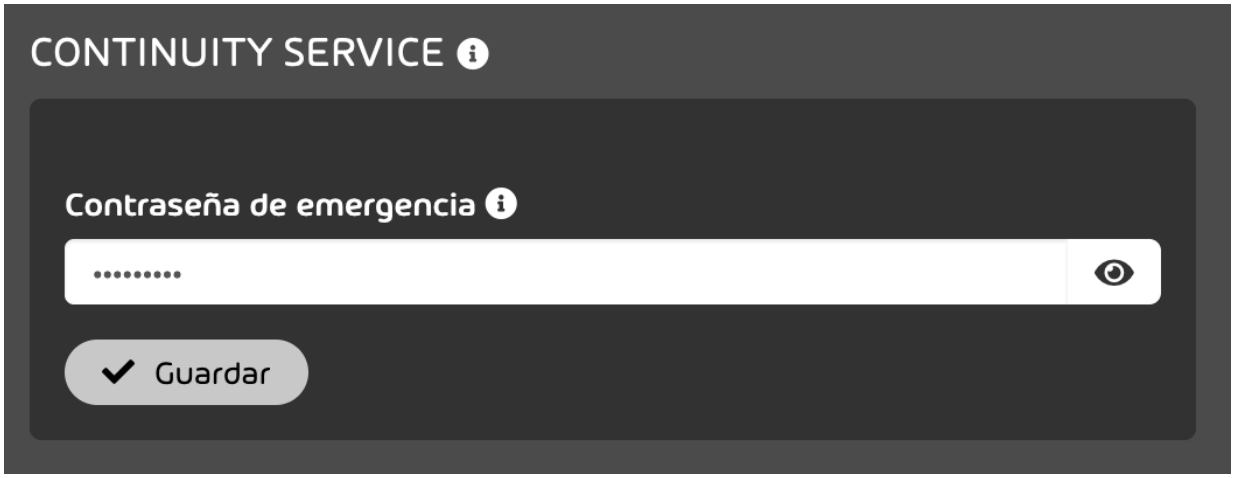


Figura 14: Cambiar la contraseña de emergencia

5. Haga clic en **Guardar**.

   La nueva contraseña de emergencia se guarda.

Se ha cambiado la contraseña de emergencia.

Configurar la autenticación multifactor

Sus datos de acceso de Control Panel se administran en Control Panel o en un servicio de directorio mediante LDAP. Su administrador ha habilitado la autenticación multifactor para los usuarios de su dominio (véase "Habilitar la autenticación multifactor" en el manual de Control Panel). Ha instalado una aplicación de autenticación TOTP (p. ej., Microsoft Authenticator, Google Authenticator) en su dispositivo móvil.

Puede configurar la autenticación multifactor para su cuenta de Control Panel. La autenticación multifactor aumenta la seguridad al iniciar sesión en Control Panel.Recomendamos especialmente que los administradores utilicen la autenticación multifactor.

La autenticación multifactor en Control Panel utiliza el método TOTP. TOTP significa contraseñas de uso único basadas en el tiempo. Para iniciar sesión en Control Panel utilizando la autenticación multifactor, debe introducir una contraseña de uso único de una aplicación de autenticación además de la contraseña de Control Panel (véase Iniciar sesión en la página 10).

1. Inicie sesión en Control Panel.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

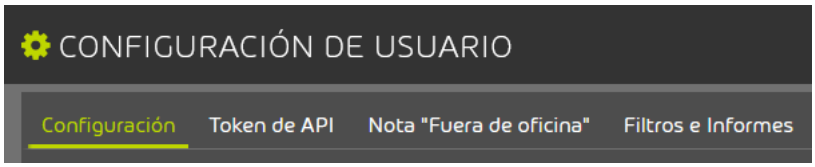


Figura 15: Configuración de usuario

3. Seleccione la pestaña **Configuración**.

4. Accione el interruptor **Autenticación multifactor** de **Activar la autenticación multifactor**.

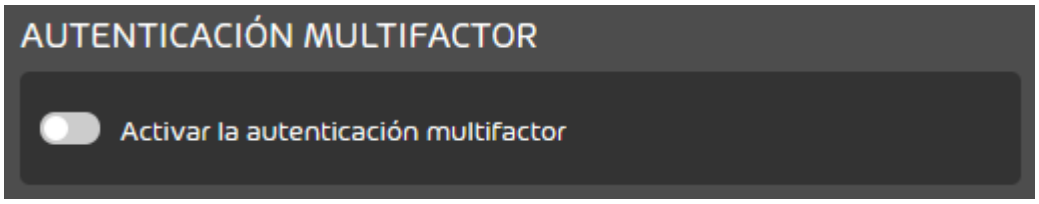


Figura 16: Activar la autenticación multifactor

El interruptor se pone verde y se abre una ventana de confirmación.

5. Haga clic en **Confirmar**.

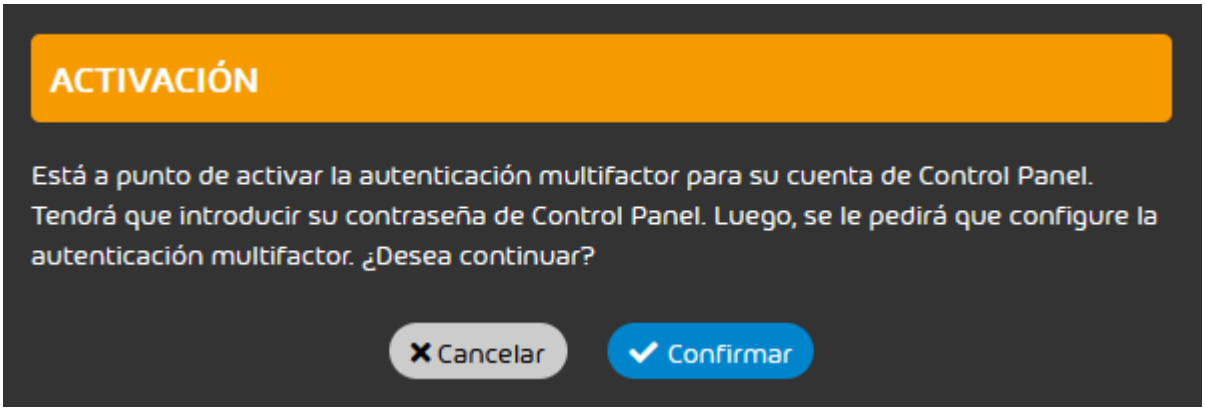


Figura 17: Confirmar

Se muestra la página **Configuración de la autenticación multifactor**.

6. Introduzca su contraseña de Control Panel en el campo de introducción.

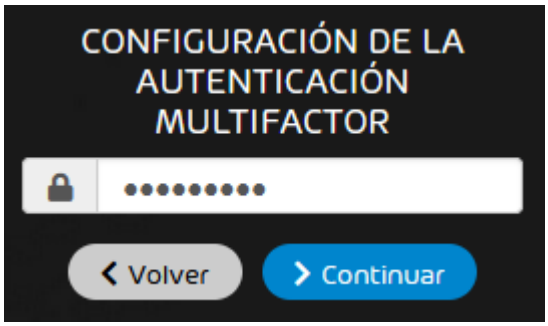


Figura 18: Introducir contraseña

7. Haga clic en **Continuar**.

Se muestra una página con instrucciones sobre cómo configurar la autenticación multifactor.

Figura 19: Configuración de la autenticación multifactor

8. Abra su aplicación de autenticación en su dispositivo móvil.

> **Nota:**
>
> Algunos navegadores son compatibles con complementos de autenticación. Los usuarios que no dispongan de un dispositivo móvil pueden utilizar un complemento de autenticación en el navegador en su ordenador en lugar de una aplicación de autenticación.

9. Añada una nueva cuenta a su aplicación de autenticación.

10.

> **Importante:**
>
> La configuración de la autenticación multifactor requiere un código QR o una clave secreta. El código QR solo se muestra una vez. También la clave secreta se muestra una única vez.
>
> Si la autenticación multifactor se configura para un buzón de correo compartido, todos los propietarios del buzón de correo deben utilizar el mismo código QR o la misma clave secreta para configurar la autenticación multifactor en su aplicación de autenticación. Por tanto, la primera persona en configurar la autenticación multifactor para el buzón de correo debe realizar una captura de pantalla del código QR o guardar la clave secreta y compartirlas con los demás propietarios del buzón de correo.

Opcional: Si desea configurar la autenticación multifactor con el código QR, proceda del siguiente modo:

a) Si su buzón de correo es un buzón de correo compartido, realice una captura de pantalla del código QR en Control Panel y guárdela de modo seguro.

b) Escanee el código QR en Control Panel con la aplicación de autenticación.

La aplicación de autenticación genera una nueva contraseña de seis dígitos cada 30 segundos.

11. Opcional: Si desea configurar la autenticación multifactor con la clave secreta, proceda del siguiente modo:

a) Haga clic en **Mostrar clave secreta**.

La clave secreta se muestra.

Figura 20: Clave secreta

b) Haga clic en **Copiar**.

La clave secreta se copia en el portapapeles.

c) Si su buzón de correo es un buzón de correo compartido, guarde la clave secreta de modo seguro.

d) Introduzca la clave secreta en la aplicación de autenticación.

La aplicación de autenticación genera una nueva contraseña de seis dígitos cada 30 segundos.

12. Introduzca la contraseña de uso único actual de la aplicación de autenticación en la máscara de entrada en Control Panel.

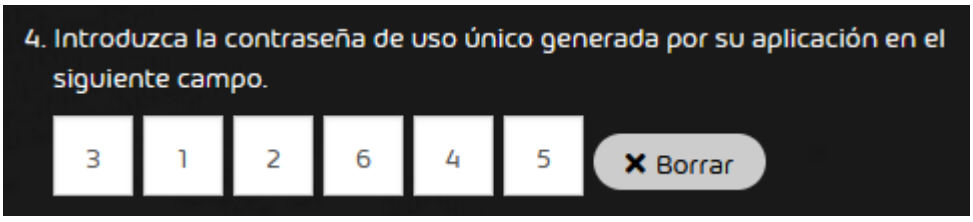


Figura 21: Introducir la contraseña de uso único

13. Opcional: Si desea vaciar la máscara de entrada para poder introducir otra contraseña de uso único, haga clic en **Borrar**.

    La máscara de entrada se vacía.

14. Haga clic en **Confirmar**.

    La autenticación multifactor se configura. A partir de ahora, se utiliza la autenticación multifactor para iniciar sesión en Control Panel.

La autenticación multifactor se ha configurado.

A continuación puede iniciar sesión en Control Panel utilizando la autenticación multifactor (véase Iniciar sesión en la página 10). Si ya no desea utilizar la autenticación multifactor, puede desactivarla para su cuenta (véase Desactivar la autenticación multifactor en la página 33). Si tiene problemas con la autenticación multifactor, puede ponerse en contacto con su administrador (véase Solución de problemas: Problemas con la autenticación multifactor en la página 21).

Desactivar la autenticación multifactor

Ha configurado la autenticación multifactor para su cuenta de Control Panel (véase Configurar la autenticación multifactor en la página 28).

Si ya no desea utilizar la autenticación multifactor, puede desactivarla para su cuenta de Control Panel. La autenticación multifactor aumenta la seguridad al iniciar sesión en Control Panel ya que se requiere una contraseña de uso único de una aplicación de autenticación además de la contraseña de Control Panel.

Nota:

Recomendamos especialmente que los administradores utilicen la autenticación multifactor.

1. Inicie sesión en Control Panel.

2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

Se muestra la configuración de usuario.

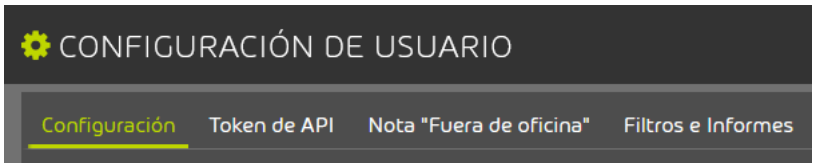


Figura 22: Configuración de usuario

3. Seleccione la pestaña **Configuración**.
4. Accione el interruptor **Autenticación multifactor** de **Activar la autenticación multifactor**.

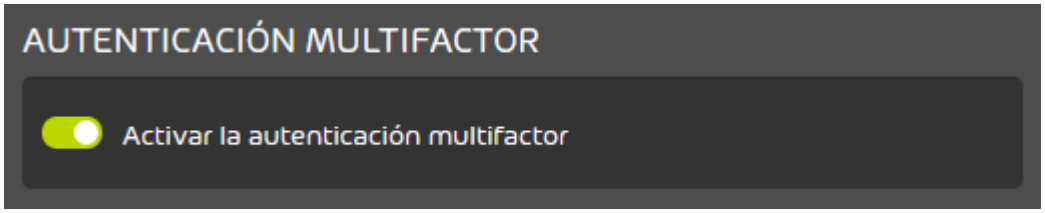


Figura 23: Desactivar la autenticación multifactor

El interruptor se pone gris y se abre una ventana de confirmación.

5. Haga clic en **Confirmar**.

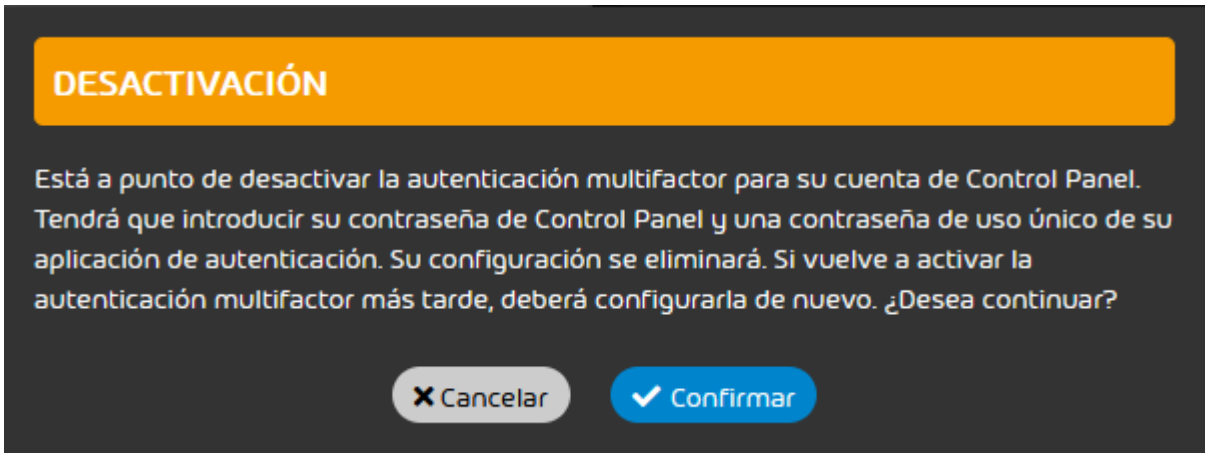


Figura 24: Confirmar

Se muestra la página **Configuración de la autenticación multifactor**.

6. Introduzca su contraseña de Control Panel en el campo superior.

Figura 25: Introducir contraseña

7. Abra su aplicación de autenticación en su dispositivo móvil.

8. Introduzca la contraseña de uso único actual de la aplicación de autenticación en el campo inferior.

Figura 26: Introducir la contraseña de uso único

El botón **Continuar** se habilita.

9. Haga clic en **Continuar**.

La autenticación multifactor se desactiva para la cuenta. La configuración de la autenticación multifactor de la cuenta se elimina. A partir de ahora, ya no se necesita ninguna contraseña de uso único de una aplicación de autenticación para iniciar sesión en Control Panel.

10. Opcional: Elimine la cuenta para la autenticación multifactor de su aplicación de autenticación.

La autenticación multifactor se ha desactivado para la cuenta.

A continuación puede iniciar sesión en Control Panel sin utilizar la autenticación multifactor (véase Iniciar sesión en la página 10). Si desea volver a utilizar la autenticación multifactor más tarde, puede reconfigurarla (véase Configurar la autenticación multifactor en la página 28).

Cambiar la zona horaria y el idioma

En su configuración de usuario (véase Configuración de usuario en la página 22) puede cambiar la zona horaria, el idioma, el formato de fecha y el formato de hora. Estos ajustes se aplican a la visualización en Control Panel y a los correos automáticos de Control Panel.

Nota:

La primera vez que accede a Control Panel, cada usuario selecciona una zona horaria, un idioma, un formato de fecha y un formato de hora. Los usuarios pueden modificar estos ajustes en todo momento en la configuración de usuario.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

Se muestra la configuración de usuario.

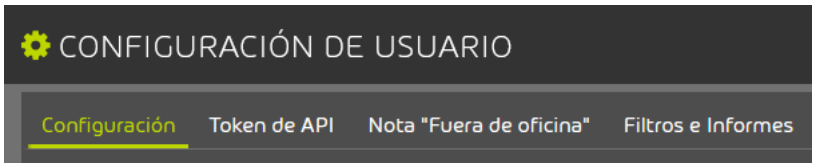


Figura 27: Configuración de usuario

3. Seleccione la pestaña **Configuración**.

En la sección **Zona horaria e idioma** se muestra la configuración de la zona horaria, del idioma, del formato de fecha y del formato de hora.

Figura 28: Zona horaria e idioma

4. Seleccione una zona horaria en el menú desplegable **Zona horaria**.

> **Nota:**
>
> La zona horaria determina el formato de número en Control Panel y en los correos automáticos de Control Panel.

5. Seleccione un idioma en el menú desplegable **Idioma**.

6. Seleccione un formato de fecha en el menú desplegable **Formato de fecha**.

> **Nota:**
>
> El formato de fecha determina el orden en el que se muestran los datos que estén disponibles para una fecha. Si no hay informaciones disponibles para todos los datos, no se muestran los datos que faltan.

7. Seleccione un formato de hora en el menú desplegable **Formato de hora**.

> **Nota:**
>
> El formato de hora determina el orden en el que se muestran los datos que estén disponibles para una hora. Si no hay informaciones disponibles para todos los datos, no se muestran los datos que faltan.

8. Haga clic en **Guardar**.

Los cambios se guardan.

Se han cambiado la zona horaria, el idioma, el formato de fecha y el formato de hora.

Editar datos básicos

En **Configuración de usuario** (véase Configuración de usuario en la página 22) puede editar los datos básicos de su buzón de correo. Los datos básicos son datos relativos al propietario de un buzón de correo.

> **Nota:**
>
> Los usuarios de buzones de correo de tipo LDAP (véase Tipos de buzón de correo en la página 235) no pueden editar sus datos básicos en Control Panel. Si hay datos básicos para estos buzones de correo en el servicio de directorio, éstos se mostrarán en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

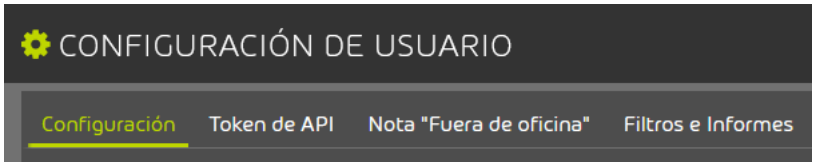


Figura 29: Configuración de usuario

3. Seleccione la pestaña **Configuración**.

   En la parte superior de la página se muestra la sección **Datos básicos**.

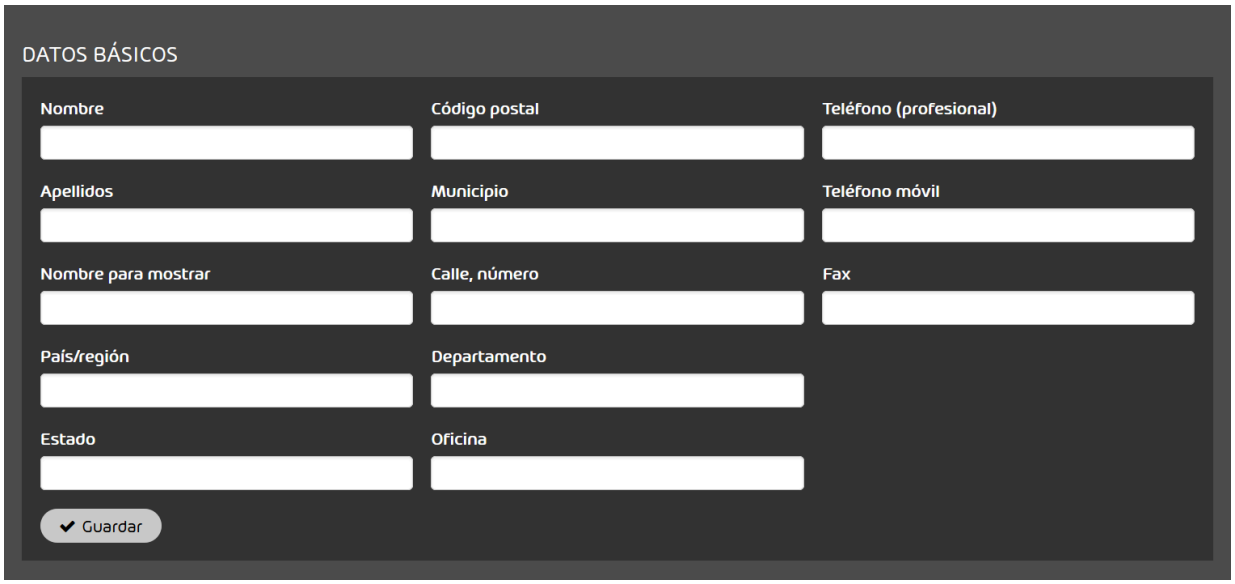


Figura 30: Datos básicos

4. **Nota:**

   Todos los campos son opcionales.

   Introduzca su datos en los campos. Los campos tienen los siguientes significados:

   - **Nombre**: Su nombre
   - **Apellidos**: Su apellido
   - **Nombre para mostrar**: Su nombre mostrado en Control Panel
   - **País/región**: País o región en el que tiene su domicilio su empresa
   - **Estado**: Estado federado o cantón en el que tiene su domicilio su empresa
   - **Código postal**: Código postal de su empresa
   - **Municipio**: Localidad en que tiene su domicilio su empresa
   - **Calle, número**: Calle y número en la que tiene su domicilio su empresa
   - **Departamento**: Departamento al que pertenece
   - **Oficina**: Oficina en la que trabaja
   - **Teléfono (profesional)**: Su número de teléfono profesional
   - **Teléfono móvil**: Su número de teléfono móvil
   - **Fax**: Su número de fax

5. Haga clic en **Guardar**.

   Los cambios se guardan.

Los datos básicos se han editado.

Activar o desactivar **Simulacro de suplantación de identidad** como usuario

Puede desactivar el simulacro de suplantación de identidad para que no se envíen correos del simulacro de phishing en su nombre o reactivarlo si estaba desactivado.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

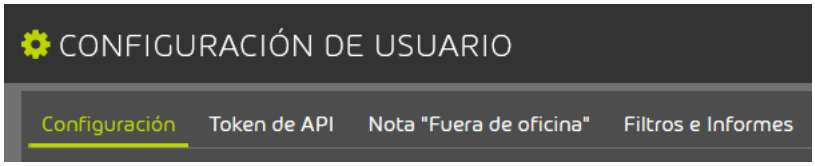


Figura 31: Configuración de usuario

3. Seleccione la pestaña **Configuración**.

   En la sección **Security Awareness Service** se muestra la opción **Enviar correos del simulacro de phishing en mi nombre**.

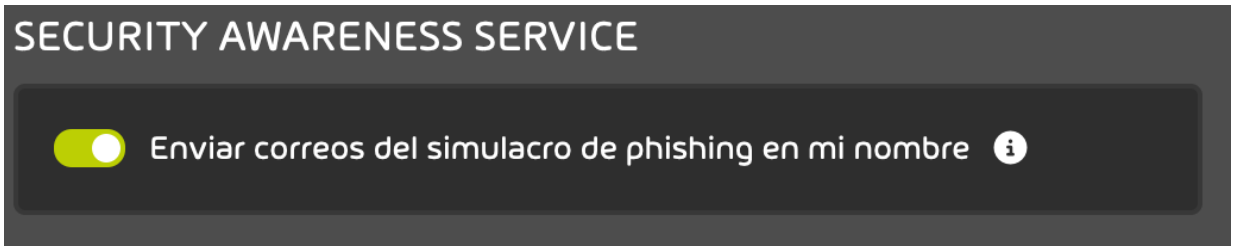


Figura 32: Enviar correos del simulacro de phishing en mi nombre

4. Accione el interruptor **Enviar correos del simulacro de phishing en mi nombre** para desactivar o activar el envío de correos del simulacro de phishing en su nombre.

   Dependiendo de si ha desactivado o activado el envío de correos del simulacro de phishing en su nombre, el interruptor se pone gris o verde.

Se ha desactivado o activado el envío de correos del simulacro de phishing en su nombre.

Crear un token de API

Los tokens de API le permiten conceder a aplicaciones acceso a la API de Control Panel. Cada aplicación necesita su propio token. En su configuración de usuario (véase Configuración de usuario en la página 22) puede crear tokens de API para que se autoricen en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

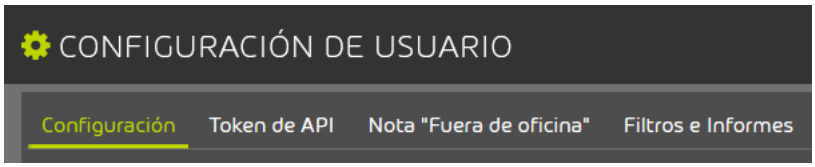


Figura 33: Configuración de usuario

3. Seleccione la pestaña **Token de API**.
4. Haga clic en **Crear token**.

Figura 34: Crear token

Se muestran ajustes adicionales.

5. En el campo **Nombre de la aplicación**, introduzca el nombre de la aplicación que empleará el token.

> **Nota:**
>
> Las acciones ejecutadas con dicho token se mostrarán en el módulo **Registro de auditorías 2.0** a nombre del usuario que crease el token.

Figura 35: Introducir el nombre de la aplicación

6. Opcional: En **Caduca el**, seleccione la fecha de caducidad del token.

> **Nota:**
>
> El valor por defecto es **Nunca**.

7. **PRECAUCIÓN:**

   Por motivos de seguridad, el token solo se muestra una vez. Si no guarda el token, se perderá. Guarde el token inmediatamente.

   Haga clic en **Crear**.

   El token de API se crea y se muestra.

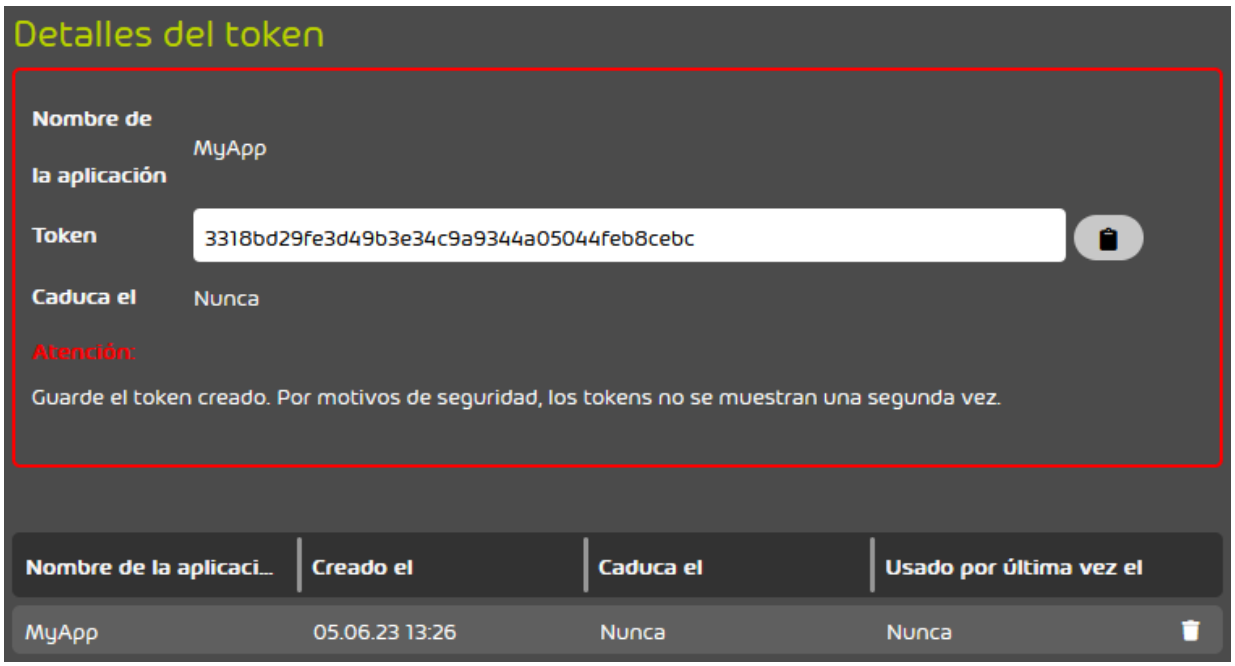


Figura 36: Token creado

Se ha creado un token de API.

Si un token de API deja de serle necesario, puede eliminarlo de Control Panel (véase Eliminar un token de API en la página 46).

Eliminar un token de API

Ha creado un token de API (véase Crear un token de API en la página 43).

Si un token de API deja de serle necesario antes de caducar, puede eliminarlo de Control Panel desde su configuración de usuario (véase Configuración de usuario en la página 22). De este modo, el token de API quedará invalidado. Una vez invalidado, ya no será posible utilizarlo para acceder a la API de Control Panel.

1. Acceda a Control Panel con los datos de acceso del usuario que creó el token.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

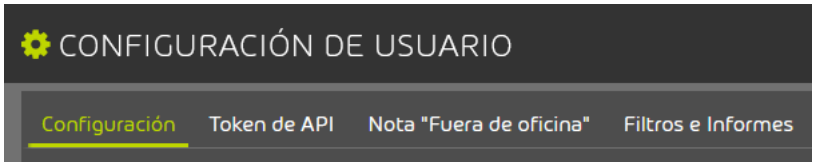


Figura 37: Configuración de usuario

3. Seleccione la pestaña **Token de API**.
4. Seleccione en la lista el token que desee eliminar.

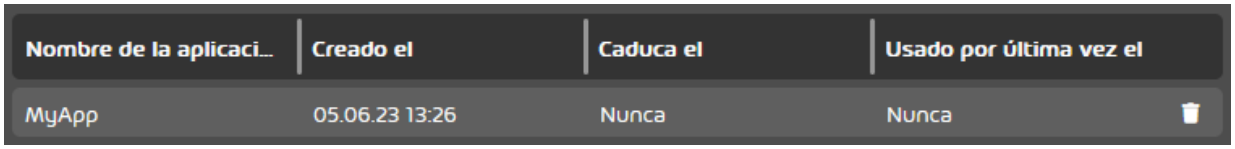


Figura 38: Seleccionar el token

5. Haga clic en la cruz junto al token.

   El token se elimina del sistema.

Un token de API se ha eliminado del sistema e invalidado.

Crear una nota de "fuera de la oficina"

En su configuración de usuario (véase Configuración de usuario en la página 22) puede añadir una nota de "fuera de la oficina" personal a su cuenta de correo. Puede redactar un texto personalizado para su nota de "fuera de la oficina" y activar y desactivar la misma en cualquier momento. Una vez activada la nota de "fuera de la oficina", todos los remitentes de sus correos entrantes recibirán una respuesta automática informándoles de su ausencia.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

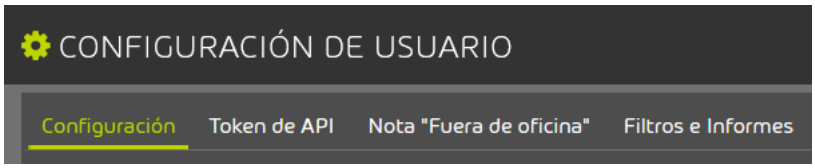


Figura 39: Configuración de usuario

3. Seleccione la pestaña **Nota "Fuera de oficina"**.

4. Introduzca el texto de su nota de 'fuera de la oficina' en el campo de texto libre.

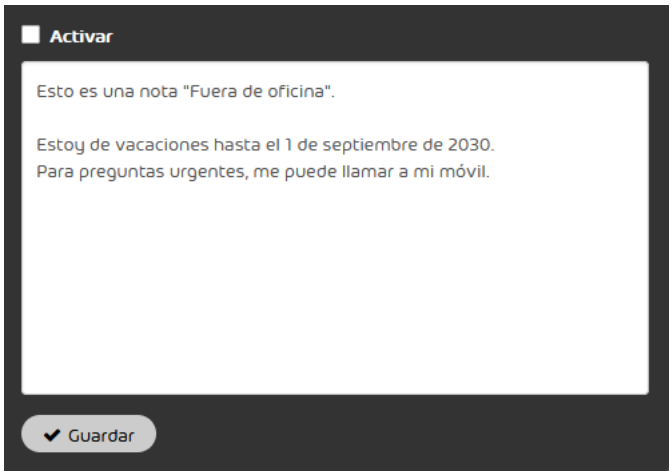


Figura 40: Introducir texto

5. Haga clic en **Guardar**.

   El texto de la nota de "fuera de la oficina" se guarda.

6. Opcional: Para activar la nota de 'fuera de la oficina', marque la casilla **Activar**.

   La nota de "fuera de la oficina" se activa. A partir de este momento, los remitentes de sus correos entrantes recibirán su nota de "fuera de la oficina" a modo de respuesta automática.

Se ha creado una nota de "fuera de la oficina".

Configurar los informes de cuarentena

Si su administrador lo permite, usted podrá, como usuario, activar o desactivar el filtro de infomail para su propio buzón de correo, así como modificar la configuración de sus informes de cuarentena. Puede modificar estos ajustes en su configuración de usuario (véase Configuración de usuario en la página 22).

Si el filtro de infomail está activado, los correos internos de la categoría **Infomail** se pondrán en cuarentena y se le mostrarán en sus informes de cuarentena o bien se marcarán y se le entregarán directamente, según haya establecido el administrador. La categoría **Infomail** incluye correos publicitarios y particularmente boletines de noticias.

Puede modificar las horas de entrega de sus informes de cuarentena. También puede excluir de sus informes de cuarentena correos cuyos remitentes figuren en su lista negra o en la lista negra de su dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Haga clic en el icono , situado en la esquina superior derecha de Control Panel.

   Se muestra la configuración de usuario.

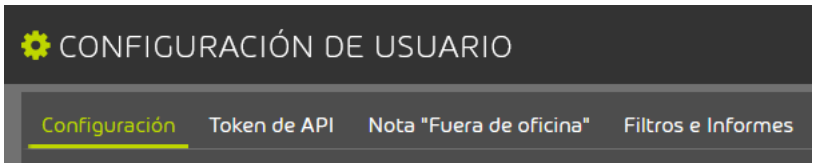


Figura 41: Configuración de usuario

3. Seleccione la pestaña **Filtros e Informes**.

   Se abre la configuración de informes de cuarentena.Por defecto, se aplica la configuración del administrador.

4. **Nota:**

   Los usuarios solo pueden modificar la configuración si su administrador se lo permite.

   Accione el interruptor para activar o desactivar el filtro de infomail.

Figura 42: Activar el filtro de infomail

Si el interruptor está en verde, el filtro de infomail estará activado, y los correos clasificados como **Infomail** bien se pondrán en cuarentena y mostrarán en informes de cuarentena o bien se marcarán y se le entregarán directamente. El administrador es quien decide cómo se deben tratar dichos correos.

5. Para modificar la configuración de sus informes de cuarentena, accione el interruptor **Definir horas de entrega propias**.

Figura 43: Definir horas de entrega individuales

Se habilita la configuración de informes de cuarentena.

Nota:

El módulo Quarantine Report se configura a nivel de buzón principal. Los informes de cuarentena se generan y entregan por buzón de correos principal. Si un buzón principal tiene asignados buzones de correo alias, los correos dirigidos a éstos se mostrarán en un único informe de cuarentena junto con los correos dirigidos al buzón de correo principal.

6.

Importante:

Este ajuste solo puede modificarse si hay definidas horas de entrega de informes de cuarentena.

Si desea excluir de los informes de cuarentena correos de remitentes que se encuentren en su lista negra o en la lista negra del dominio, accione el interruptor **Excluir de los informes de cuarentena remitentes en la lista negra.**.

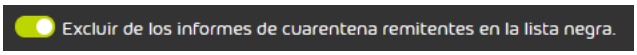


Figura 44: Excluir de los informes de cuarentena remitentes en la lista negra.

Nota:

Si esta opción está activada, los correos de remitentes que se encuentren en la lista negra (véase el capítulo "Acerca de las listas blancas y negras" en el manual de Control Panel) del usuario o del dominio no se muestran en los informes de cuarentena del usuario.

Si el administrador ha seleccionado el diseño **Inbox Manager con vista previa de los correos electrónicos y opción de exclusión** para los informes de cuarentena de sus usuarios (véase "Diseños para informes de cuarentena" en el manual de Control Panel), esta opción está activada y no puede desactivarse. Los informes de cuarentena con este diseño contienen el botón **No mostrar nunca el remitente**. Con este botón, los usuarios pueden añadir un remitente a su propia lista negra para que los correos de este remitente no se muestren en futuros informes de cuarentena. Los usuarios no pueden seleccionar el diseño para sus informes de cuarentena por sí mismos.

El interruptor se pone verde. Los próximos informes de cuarentena ya no contendrán correos cuyos destinatarios figuren en la lista negra del buzón de correo o del dominio.

7. Si desea desactivar los informes de cuarentena para su buzón de correo, accione el botón **Desactivar**.

Figura 45: Desactivar Quarantine Report

Todos los días y horas de entrega se desactivan para el buzón de correo. No se envían informes de cuarentena. No es necesario hacer más ajustes.

8. Si los informes de cuarentena siguen activados para su buzón de correo, seleccione los días en los que entregarlos. Seleccione al menos un día.

   - Para hacer entregar los informes de cuarentena cada día, marque el botón **Cada día**.
   - Para hacer entregar los informes de cuarentena de lunes a viernes, marque el botón **En días laborables**.
   - Marque las casillas de los días deseados.

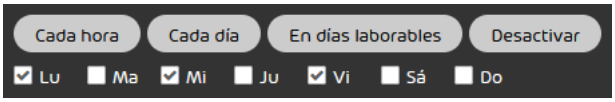


Figura 46: Seleccionar días

9. Elija las horas a las que entregar los informes de cuarentena. Seleccione al menos una hora.
   - Para hacer entregar los informes de cuarentena cada hora, active el botón **Cada hora**.
   - Marque las casillas de las horas deseadas.

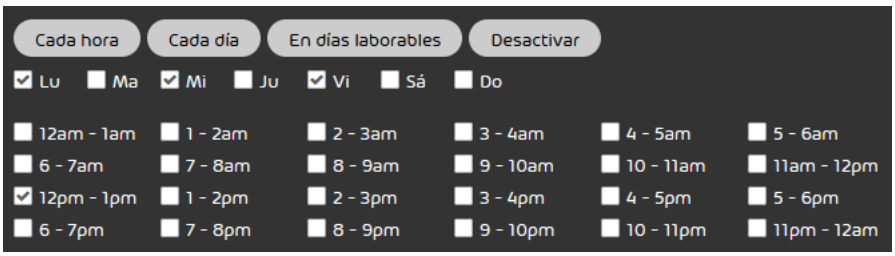


Figura 47: Seleccionar horas

> **Nota:**
>
> Solo se enviará un informe de cuarentena a las horas de entrega seleccionadas si nuevos correos se han puesto en cuarentena desde el último informe de cuarentena.

El filtro de infomail y los informes de cuarentena se han configurado para el buzón de correo.

Administración de derechos en Control Panel

En Control Panel, cada usuario tiene asignado un rol. Cada rol (véase Roles en la página 53) posee determinados derechos en Control Panel. Los derechos se otorgan sobre diversos ámbitos que los usuarios autorizados pueden seleccionar en la selección de ámbitos (véase Selección de ámbitos en la página 58).

Roles

En Control Panel, cada usuario tiene asignado un rol. Cada rol posee determinados derechos en Control Panel. En función de sus derechos, los usuarios tienen acceso a diversas secciones de Control Panel (véase Selección de ámbitos en la página 58).

En Control Panel están definidos los siguientes roles:

- **Usuario**: Este rol se asigna automáticamente si no se ha asignado ningún otro rol. Este rol no puede asignarse manualmente.
- **Administrador**: Este rol dispone de amplios derechos administrativos.
- **Service Desk**: Este rol es para empleados de soporte técnico.
- **Reporting**: Este rol solo tiene acceso a las estadísticas.
- **Marketing**: Este rol está destinado a empleados que elaboran y editan firmas y notas legales. Puede asignarse de modo adicional junto a otro de los roles para conceder a un empleado acceso al módulo **Signature and Disclaimer**. No es preciso asignar este rol a un usuario con el rol **Administrador**, ya que los administradores ya tienen acceso a dicho módulo. Este rol solo está disponible a nivel de cliente.
- **Security Awareness**: Este rol está destinado a empleados encargados de la configuración y la administración de Security Awareness Service para un cliente. Puede asignarse de modo adicional junto a otro de los roles predefinidos para conceder a un empleado acceso al módulo **Security Awareness Service**. No es preciso asignar este rol a un usuario con el rol **Administrador**, ya que los administradores ya tienen acceso a dicho módulo. Este rol solo está disponible a nivel de cliente.

La siguiente tabla muestra los módulos de Control Panel a los que tiene acceso cada rol. **x** indica que el rol correspondiente tiene acceso al módulo.

Tabla 1: Roles y módulos

MÓDULO	USUARIO	ADMINISTRADOR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Email Live Tracking	x	x	x			
Dashboard de servicios		x				

MÓDULO	USUARIO	ADMINISTRADOR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Informes y conformidad	x	x	x	x		
Web Filter		x				
Configuración de cliente		x				
Copia de seguridad		x Los administradores a nivel de cliente solo tienen acceso a este módulo si los administradores a nivel de partner se lo han concedido.				
Listas blancas y negras	x	x	x			
Security Awareness Service		x				x

MÓDULO	USUARIO ADMINISTRADOR	SERVICE DESK	REPORTING	MARKETING	SECURITY AWARENESS
Configuración de seguridad	x			Este rol solo tiene acceso al módulo **Signature and Disclaimer**.	
Personalización	x				
Configuración de usuario	x				

Los roles con acceso al módulo **Email Live Tracking** disponen de distintas acciones para correos electrónicos. La siguiente tabla muestra qué acciones para correos (véase Acciones para correos en la página 95) puede ejecutar cada uno de estos roles.

Nota:

La siguiente tabla incluye algunas acciones que solo están disponibles tras la contratación de servicios adicionales y que, por tanto, no se mencionan en el capítulo Acciones para correos en la página 95.

Tabla 2: Roles y acciones para correos

ACCIÓN PARA CORREOS	USUARIO	ADMINISTRADOR	SERVICE DESK
Entregar correo	x Los usuarios pueden hacerse entregar correos de la categoría **Limpio**. El administrador puede permitir al usuario hacerse entregar correos de otras categorías.	x	x
Restaurar correo	x	x	x
Reportar spam	x	x	x
Reportar infomail	x	x	x
Añadir remitente a lista negra	x	x	x
Añadir remitente a lista blanca y entregar correo	x	x	x
Añadir a lista negra de todos los usuarios		x	
Añadir a lista blanca de todos los usuarios		x	

ACCIÓN PARA CORREOS	USUARIO	ADMINISTRADOR	SERVICE DESK
Enviar correo al administrador	x	x	x
Enviar correo a soporte	x	x	
Marcar como privado	x	x	x
Ver correo	x	Esta acción solo está disponible para correos del propio usuario una vez elegido en la selección de ámbitos.	Esta acción solo está disponible para correos del propio usuario una vez elegido en la selección de ámbitos.
Escaneo ATP		x	x
Informe ATP		x	x
Información	x	x	x

Para más información sobre la administración de los roles, véase el capítulo "Gestión de roles y contactos" del manual de Control Panel.

Selección de ámbitos

Por defecto, cada usuario ve en Control Panel únicamente su propia configuración y sus propios correos electrónicos. Sin embargo, los administradores y otros usuarios provistos de un rol con permisos a nivel de cliente o de partner (véase Roles en la página 53) pueden cambiar su ámbito de aplicación en la selección de ámbitos de Control Panel (véase Uso de la selección de ámbitos en la página 60) para acceder a las configuraciones de otros ámbitos. La selección de ámbitos es un menú desplegable situado en la esquina superior derecha de Control Panel.

Nota:

Los usuarios normales no pueden cambiar el ámbito de aplica

Figura 48: Selección de ámbitos

Si no hay seleccionado ningún ámbito en la selección de ámbitos, se mostrarán en Control Panel la configuración y los correos del usuario activo, y el usuario podrá administrar la configuración de su propio buzón de correo.

Los administradores y otros usuarios provistos de un rol con permisos a nivel de cliente o partner pueden acceder a diversos ámbitos de aplicación en función de sus permisos. Los ámbitos de aplicación están ordenados jerárquicamente.

Tabla 3: Ámbitos de aplicación

ÁMBITO DE APLICACIÓN	EXPLICACIÓN
Partner	El ámbito de partner es el ámbito de aplicación superior en Control Panel. Un partner puede contener, a su vez, partners subordinados o clientes. **Nota:** Bajo partner subordinados no es posible crear nuevos partners, sino solo clientes. En este ámbito de aplicación, los administradores pueden añadir o eliminar partners subordinados o clientes. Además, en este ámbito de aplicación es posible administrar ajustes de orden superior que, a su vez, los partner subordinados y clientes heredan.

ÁMBITO DE APLICACIÓN	EXPLICACIÓN
Cliente	Los clientes son empresas que emplean nuestros servicios. Cada cliente está subordinado a un partner. Los clientes se administran en Control Panel mediante dominios principales. En este ámbito de aplicación, los administradores pueden observar el tráfico de correo de un cliente. Además, los administradores pueden administrar los buzones de correos, grupos y dominios alias del cliente, así como configurar nuestros servicios para el cliente. Desde este ámbito de aplicación también es posible administrar la lista blanca y negra del cliente. Cada cliente tiene subordinados los buzones de correo pertenecientes a su dominio principal y a sus dominios alias.
Usuario	El de usuario es el ámbito de aplicación más bajo de Control Panel. Los usuarios equivalen a buzones de correo. Cada usuario está subordinado al cliente a cuyo dominio principal o alias pertenezca el buzón de correo. En este ámbito de aplicación, los administradores pueden observar el tráfico de correo del usuario correspondiente. Además, los administradores pueden administrar las listas blanca y negra de dicho usuario.

Uso de la selección de ámbitos

Si un usuario tiene asignado un rol distinto al de usuario, Control Panel le permite cambiar fácilmente el ámbito de aplicación de su rol.

En la zona superior de la ventana se encuentra la **Selección de ámbitos**:

Figura 49: Selección de ámbitos

La selección de ámbitos contiene todos los ámbitos de aplicación de los roles asignados al usuario activo. Existen dos opciones para seleccionar el ámbito de aplicación: La primera opción consiste en seleccionar el partner, cliente o usuario directamente del menú desplegable:

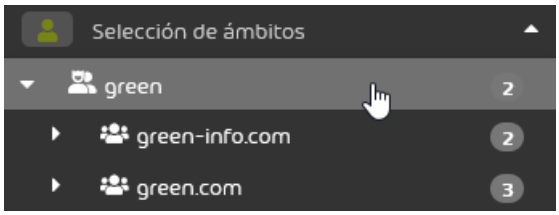


Figura 50: Selección del ámbito de aplicación

La segunda opción consiste en introducir el nombre del partner, cliente o usuario en la barra de búsqueda.

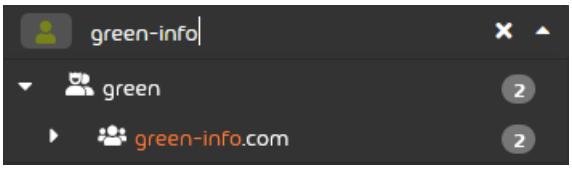


Figura 51: Búsqueda en la selección de ámbitos

No es preciso introducir el nombre completo del ámbito buscado: basta con escribir una parte del nombre para limitar la lista de selección a los elementos que contengan dicha cadena de caracteres.

Por defecto, el ámbito de búsqueda se encuentra limitado a partners y clientes. Para incluir también usuarios en la búsqueda, es preciso activar la búsqueda de usuarios.

Figura 52: Activar la búsqueda de usuarios

Nota:

La búsqueda de usuarios se activa automáticamente al introducir la arroba (@) en la barra de búsqueda.

Para limitar la búsqueda a partners y clientes es preciso desactivar la búsqueda de usuarios.

Figura 53: Desactivar la búsqueda de usuarios

Email Live Tracking

En el módulo **Email Live Tracking**, los usuarios pueden supervisar su propio tráfico de correo electrónico. Los administradores, además, pueden supervisar el de un cliente. Independientemente de sus permisos, cada usuario puede consultar datos sobre sus correos entrantes y salientes y efectuar acciones sobre los mismos.Además de los correos del buzón de correo principal, se muestran los correos de direcciones alias.

También los administradores ven sus propios correos en el módulo **Email Live Tracking** al iniciar sesión. Sin embargo, a diferencia de los usuarios normales, los administradores pueden cambiar de vista. Los administradores a nivel de cliente pueden observar el tráfico de correo de su dominio principal y sus dominios alias.

Nota:

Para cambiar de vista, los administradores pueden seleccionar el dominio o partner deseado en la selección de ámbitos, situada en la esquina superior derecha de Control Panel. Si no han seleccionado nada en la selección de ámbitos, los administradores verán solo sus propios correos en el módulo **Email Live Tracking**.

En este módulo solo se muestran correos de dominios que han sido verificados para un cliente (véase Verificación de dominios en la página 316).

El módulo **Email Live Tracking** se divide en las áreas de filtros, vista de correos y estadística de categorías (véase Estructura de Email Live Tracking en la página 64).

Los usuarios pueden ajustar la vista de correos en el módulo (véase Configurar la vista de correos en la página 66), así como buscar entre los correos mostrados y filtrarlos (véase Filtrar correos en la página 71). El módulo **Email Live Tracking** contiene información detallada (véase Detalles de correo en la página 78) y general sobre los correos (véase Campos de correo en la página 86). Además, los correos pertenecen a diversas categorías (véase Categorías de correo electrónico en la página 90). Es posible efectuar diversas acciones sobre los correos (véase Acciones para correos en la página 95). También es posible exportar datos de todos los correos o una selección de los mismos en formato CSV (véase Exportar datos de correos en formato CSV en la página 103).

Estructura de Email Live Tracking

Estas áreas se describen a continuación.

Filtros

Puede filtrar sus correos de distintos modos (véase Filtrar correos en la página 71).

Figura 54: Selección de filtros

vista de correos

La vista de correos es la ventana principal del módulo Email Live Tracking. En ella se muestran todos los correos electrónicos. Los correos mostrados dependen de los filtros seleccionados previamente.

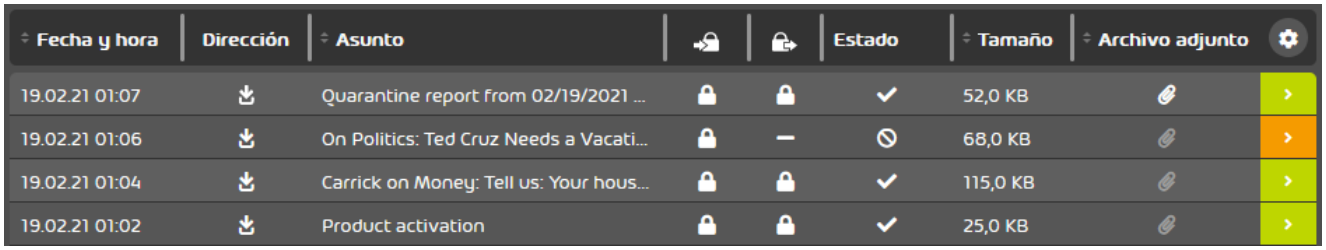


Figura 55: Vista de correos

Puede configurar la vista de modo individual (véase Configurar la vista de correos en la página 66).

Todos los correos que cumplan las condiciones del filtro definido pueden exportarse con la función

. Esta función permite seleccionar los campos a exportar (véase Exportar datos de correos en formato CSV en la página 103).

Las listas de correos largas pueden hojearse con el menú de navegación de páginas. Dicho menú se encuentra en el centro de la parte inferior de la pantalla. La cantidad de elementos mostrados por página puede seleccionarse en el menú desplegable de la derecha. Para acceder directamente a una página concreta, es posible introducir el número de la página en el campo de introducción de datos y confirmar con la tecla Intro. A la derecha del campo de introducción de datos se muestra la cantidad de páginas disponibles. Con los iconos de flechas simples a derecha e izquierda del campo de introducción de datos es posible pasar a la página anterior o a la siguiente. Los iconos de flechas dobles permiten acceder a la primera o a la última página.

Figura 56: Menú de navegación de páginas

Nota:

La vista está limitada a 10000 registros, lo cual equivale a 200 páginas según la configuración por defecto. Si una búsqueda obtiene más resultados, se mostrará un símbolo de suma tras la cantidad de páginas disponibles. Para obtener resultados más precisos es posible limitar los correos mostrados con ayuda de las funciones de filtro (véase Filtrar correos en la página 71).

Estadística de categorías

Los correos de la vista de correos se analizan en cuanto a su categoría y se muestran en la estadística. La estadística puede visualizarse u ocultarse pulsando la flecha de la esquina inferior derecha de la vista de correos.

Nota:

Los filtros aplicados se aplican a en la estadística.

Figura 57: Estadística de categorías

Configurar la vista de correos

Los usuarios tienen las siguientes opciones para personalizar la vista de correos:

- Seleccionar los campos mostrados (véase Seleccionar las columnas mostradas en la página 66).
- Modificar los tamaños de los campos (véase Modificar tamaños de campos en la página 68).
- Modificar las posiciones de los campos (véase Modificar posición de campos de correo en la página 70).

Seleccionar las columnas mostradas

El módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) contiene una vista general de todos los correos entrantes y salientes.

Nota:

Además de sus propios correos, los administradores a nivel de cliente pueden ver los correos de su dominio principal y sus dominios alias eligiendo dichos dominios en la selección de ámbitos situada en la esquina superior derecha de Control Panel.

Los correos se muestran en una tabla. La tabla contiene datos sobre los correos. Puede seleccionar los datos a mostrar en el módulo **Email Live Tracking**. Para más información acerca de las columnas disponibles, véase Campos de correo en la página 86.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Vaya al módulo **Email Live Tracking**.

3. Haga clic en el icono de tabla situado en la esquina superior derecha de la misma.

Figura 58: Abrir campos de correo.

Se muestra una lista de campos de correo disponibles.

4. Seleccione los campos deseados.

Nota: Los campos seleccionados se muestran con el fondo azul.

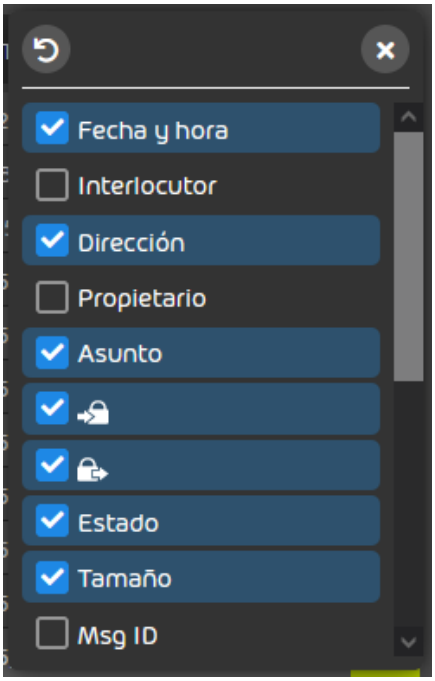


Figura 59: Seleccionar campos de correo

Se han seleccionado los campos de correo a mostrar.

A continuación puede modificar el tamaño de los campos mostrados (véase Modificar tamaños de campos en la página 68) así como su orden (véase Modificar posición de campos de correo en la página 70).

Modificar tamaños de campos

Ha personalizado con éxito los datos de correo mostrados (véase Seleccionar las columnas mostradas en la página 66).

Puede modificar el tamaño de los campos del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63).

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Vaya al módulo **Email Live Tracking**.
3. Sitúe el puntero del ratón entre dos campos.

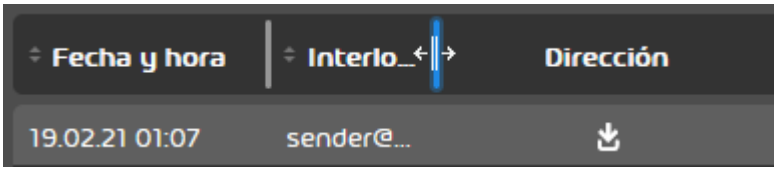


Figura 60: Ajustar el tamaño

Se muestra una línea azul entre los campos.

4. Tire de la línea hacia la izquierda o hacia la derecha hasta obtener el tamaño de campo deseado.

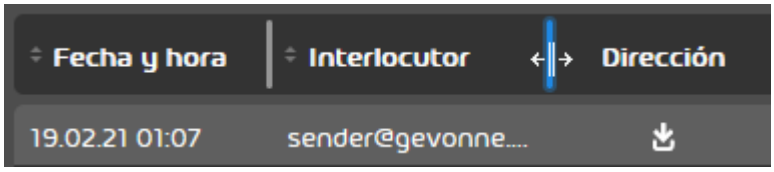


Figura 61: Ajustar el tamaño

Se ha modificado el tamaño de los campos.

A continuación puede ajustar el orden de los campos (véase Modificar posición de campos de correo en la página 70).

Modificar posición de campos de correo

Ha personalizado con éxito los datos de correo mostrados (véase Seleccionar las columnas mostradas en la página 66).

Puede modificar la posición de los campos de correo en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63).

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Vaya al módulo **Email Live Tracking**.
3. Haga clic en un campo y mantenga pulsado el botón del ratón.

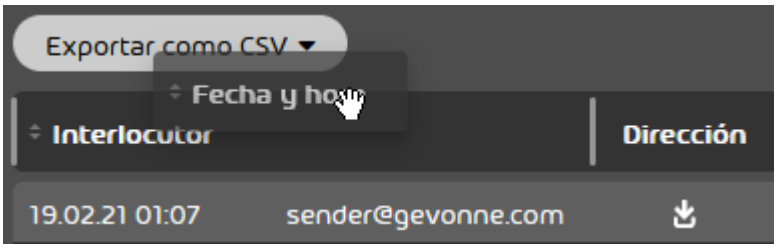


Figura 62: Modificar la posición, 1

4. Desplace el campo hasta la posición deseada y suelte el botón del ratón.

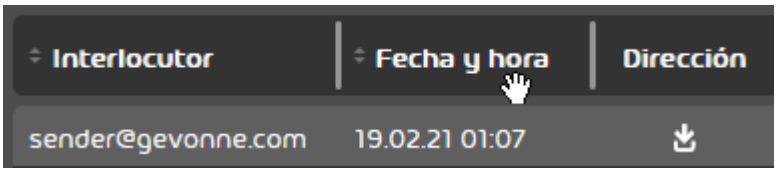


Figura 63: Modificar la posición, 2

Se ha modificado la posición de los campos de correo.

A continuación puede ajustar el tamaño de los campos (véase Modificar tamaños de campos en la página 68).

Filtrar correos

La búsqueda de correos le permite filtrar los correos mostrados en la vista de correos y buscar determinados correos. Están disponibles las siguientes opciones:

- Filtrar correos por categorías (véase Filtrar correos por categorías en la página 71).
- Emplear otros filtros de correo (véase Filtros de campos en la página 75).
- Buscar correos mediante la barra de búsqueda y limitar la búsqueda a determinados campos (véase Barra de búsqueda en la página 72).
- Descartar o repetir la búsqueda (véase Descartar y repetir búsquedas en la página 77).
- Emplear la función de búsqueda avanzada (véase Función de búsqueda avanzada en la página 74)

Filtrar correos por categorías

Puede filtrar los correos del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) por categorías.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. En la selección de ámbitos, seleccione el dominio cuyos correos desee visualizar.
3. Vaya al módulo **Email Live Tracking**.

4. Active o desactive las categorías deseadas en el menú de filtros.

> **Nota:**
>
> Para visualizar únicamente correos de una categoría determinada, haga doble clic sobre la categoría deseada. Todas las demás categorías se desactivarán.

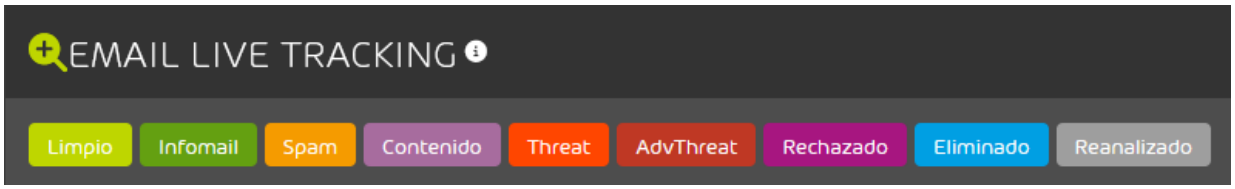


Figura 64: Activar y desactivar categorías de correo

En la tabla se muestran solo correos de las categorías activas.

Los correos se han filtrado por categorías en el módulo **Email Live Tracking**.

Barra de búsqueda

Introduciendo palabras en la barra de búsqueda del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63), los usuarios pueden buscar correos (véase Buscar correos en la página 72). Opcionalmente, es posible limitar la búsqueda a determinados campos (véase Limitar la búsqueda a determinados campos en la página 73). Además, la barra de búsqueda contiene una función de búsqueda avanzada que completa los términos introducidos (véase Función de búsqueda avanzada en la página 74).

Buscar correos

Puede buscar correos en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63).

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Opcional: Si, en lugar de entre sus propios correos, desea buscar entre los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.
4. Introduzca una cadena de caracteres en el campo de búsqueda.

> **Importante:**
>
> Se necesitan al menos tres caracteres para poder emplear la búsqueda.

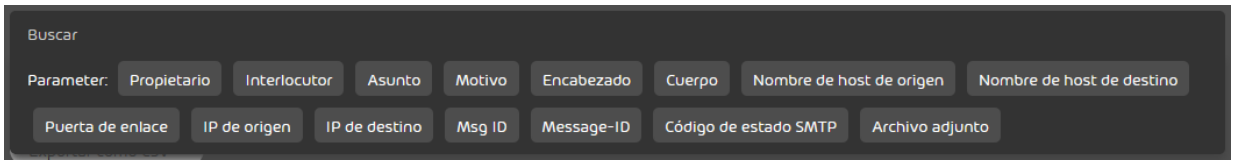


Figura 65: Barra de búsqueda

Los resultados se actualizan en tiempo real.

Se han buscado correos en el módulo **Email Live Tracking**.

Limitar la búsqueda a determinados campos

Puede limitar la búsqueda en el módulo **Email Live Tracking** (véase Buscar correos en la página 72) a determinados campos, de modo que el término de búsqueda introducido se busque solo dentro de dichos campos.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Opcional: Si, en lugar de entre sus propios correos, desea buscar entre los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.
4. Seleccione un campo entre las sugerencias de búsqueda.

5. Introduzca la cadena de caracteres que desee buscar en el campo seleccionado.

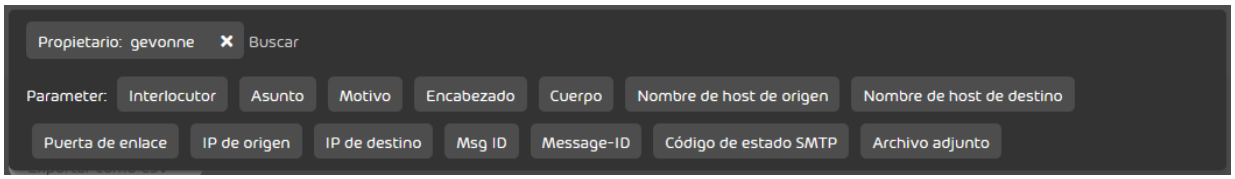


Figura 66: Limitar la búsqueda a determinados campos

La búsqueda de correos se ha limitado a determinados campos.

Función de búsqueda avanzada

Con la función de búsqueda a texto completo del módulo es posible buscar en todos los campos de correo. También existe la opción de buscar en combinaciones de campos de correo.

La función de búsqueda del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) completa los términos introducidos. Esto permite a los usuarios introducir solamente las primeras letras de cada palabra. No es posible buscar texto dentro de palabras.

En los campos de correo se emplean diversos separadores para separar unas palabras de otras.

En la siguiente tabla se muestran ejemplos de búsquedas correctas e incorrectas. También se describen los separadores para los campos de correo indicados.

Nota:

Los archivos adjuntos solo se buscan si la búsqueda se limita al campo **Archivo adjunto** (véase Limitar la búsqueda a determinados campos en la página 73).

Tabla 4: Ejemplos de búsquedas complejas

TIPO	SEPARADOR	EJEMPLO	BÚSQUEDA CORRECTA	BÚSQUEDA INCORRECTA
Dirección de correo	"@" y "." final	info@test.de	info; test; de	o@test; nfo@
Hostname	"-" y "."	gateway07-rz01.test.de	gate; rz01; test; de	eway; 07; 01;
Archivos adjuntos	";"	text.txt; image.jpg	text.txt; image.jpg	text; txt; xt; mage; image; jpg; pg
Texto corrido	Caracteres especiales	Nos ocupamos de la seguridad informática de nuestros clientes: con Cloud Security Services, por todo el mundo y las 24 horas.	nos; ocupamos; segur; hora	curity; ervices; las
Causa	":"	linktag: lt_exprx_15_10_442: auto	linktag; lt_exprx; auto	tag; exprx; 10_442

Filtros de campos

En el módulo **Email Live Tracking** es posible aplicar los filtros **Fecha y hora**, **Dirección**, **Cifrado**, **Estado de envío** y **Tamaño** a correos. Éstos se describen en la tabla de abajo.

Tabla 5: Filtros

PROPIEDAD	DESCRIPCIÓN
Fecha y hora	Seleccione un intervalo de tiempo en el menú desplegable o limite los correos mostrados a un rango concreto. El valor por defecto es **Hoy**. Si se selecciona un intervalo de tiempo (**El mes pasado**, **Este año** etc.), se aplicará la zona horaria UTC independientemente de la configuración del usuario. Por tanto, si el usuario tiene configurada una zona horaria distinta a UTC, pueden aparecerle también correos del día anterior al comienzo del intervalo de tiempo seleccionado en la vista de correos. **Nota:** El intervalo de tiempo no debe superar los 365 días. No es posible seleccionar intervalos más largos en el menú desplegable. Si introduce manualmente un intervalo de tiempo mayor, se emitirá un mensaje de error.
Dirección	Seleccione la dirección de los correos a visualizar. Por defecto se muestran correos en ambas direcciones.
Cifrado	Limite su vista de correos a correos con un tipo de cifrado concreto. También puede seleccionar varios tipos de cifrado.

PROPIEDAD	DESCRIPCIÓN
Estado de envío	Determine el estado de envío de los correos que se mostrarán. Existen las siguientes opciones: **Entregado**, **Aplazado**, **Rechazado** y **Sin estado**.
Tamaño	Limite los correos a diversos tamaños. Seleccione el tamaño en el menú desplegable.

Descartar y repetir búsquedas

Ha efectuado una búsqueda en el módulo **Email Live Tracking** (véase Buscar correos en la página 72 o Limitar la búsqueda a determinados campos en la página 73) y/o aplicado determinados filtros (véase Filtros de campos en la página 75) y continúa en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63).

Después de buscar correos en el módulo **Email Live Tracking**, puede descartar sus ajustes de búsqueda (véanse Buscar correos en la página 72, Limitar la búsqueda a determinados campos en la página 73 y Filtros de campos en la página 75) o bien realizar una nueva búsqueda con los mismos para actualizar la lista de resultados.

Descarte los ajustes de búsqueda o efectúe una nueva búsqueda con los mismos. Haga clic en uno de los siguientes botones:

- **Borrar**: Los ajustes de búsqueda se descartan.
- **Actualizar**: Se realiza una nueva búsqueda con los ajustes de búsqueda actuales.

Figura 67: Descartar ajustes de búsqueda o repetir búsqueda

Se han descartado los ajustes de búsqueda o se ha repetido la búsqueda con los ajustes actuales.

Detalles de correo

La vista de correos **Email Live Tracking**de (véase Email Live Tracking en la página 63) muestra los detalles de correos individuales.

Además, desde la sección de detalles de correo es posible ejecutar acciones para el correo seleccionado (véase Ejecutar una acción sobre un correo en la página 78).Por regla general es posible efectuar las siguientes acciones:

- Reportar el correo como spam (véase **Reportar spam**)
- Reportar el correo como infomail (véase**Reportar infomail**)
- Entregar el correo (véase **Entregar correo**)
- Efectuar un escaneo ATP (véase Iniciar el escaneo ATP en la página 80)

En función de los productos que haya activados y las acciones que haya habilitado el administrador, puede haber disponibles otras acciones (véase Acciones para correos en la página 95).

En la información de correos pueden consultarse metadatos, encabezados y el diálogo SMTP de los correos (véase Información avanzada de correos en la página 84).

Ejecutar una acción sobre un correo

Si desea ejecutar una acción sobre un solo correo, proceda del siguiente modo.

Nota:

Otra opción consiste en ejecutar una acción sobre varios correos al mismo tiempo (véase Seleccionar una acción para varios correos en la página 92).

1. Inicie sesión en Control Panel.
2. Opcional: Si, en lugar de sus propios correos, desea ver los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.

4. Haga clic en la flecha al extremo de la fila del correo deseado.

> **Nota:**
>
> El color muestra la categoría del correo.

Se abre un menú.

5. Haga clic en la acción que desee efectuar.

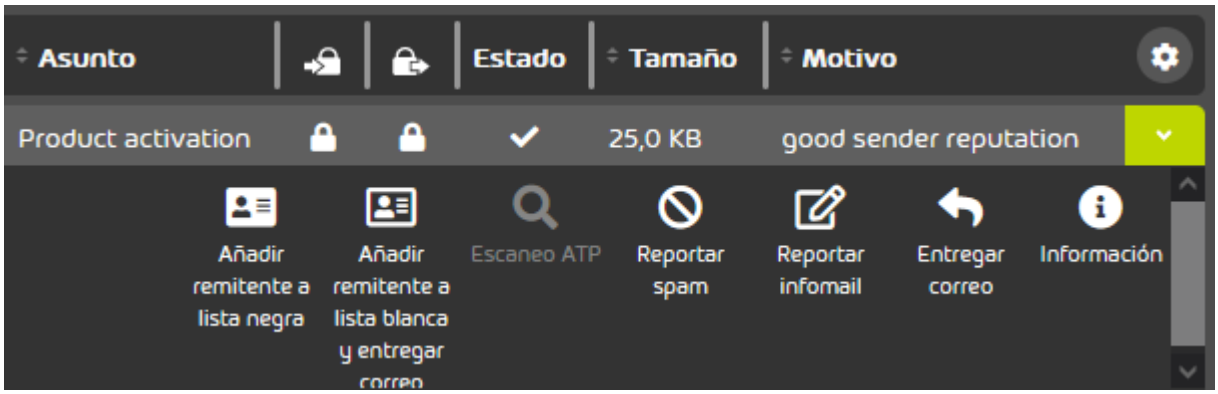


Figura 68: acciones para correos

> **Nota:**
>
> En la selección de correos encontrará acciones adicionales (véase Seleccionar una acción para varios correos en la página 92).

> **Nota:**
>
> En Acciones para correos en la página 95 encontrará una explicación de las acciones para correos.

Se ha ejecutado una acción sobre un correo interno.

Iniciar el escaneo ATP

Ha activado Advanced Threat Protection (véase Activar ATP en la página 389).

Con el escaneo ATP (véase el capítulo "Escaneo ATP" del manual de Control Panel) puede comprobar manualmente correos con archivos adjuntos ejecutables en cuanto a contenidos perjudiciales en el módulo **Email Live Tracking** (véase el capítulo "Email Live Tracking" del manual de Control Panel).

Nota:

El escaneo ATP solo está disponible para correos con archivos adjuntos ejecutables (p. ej., archivos .exe).

Atención:

Si no ha contratado Advanced Threat Protection (siehe das Kapitel "Estructura y funcionamiento de ATP" im Control-Panel-Handbuch), podrá realizar dos escaneos ATP gratuitos al mes. Solo podrá efectuar más escaneos ATP después de contratar el servicio de pago de ATP.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Si, en lugar de sus propios correos, desea ver los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.

4. Haga clic en la flecha a la derecha de la fila del correo deseado.

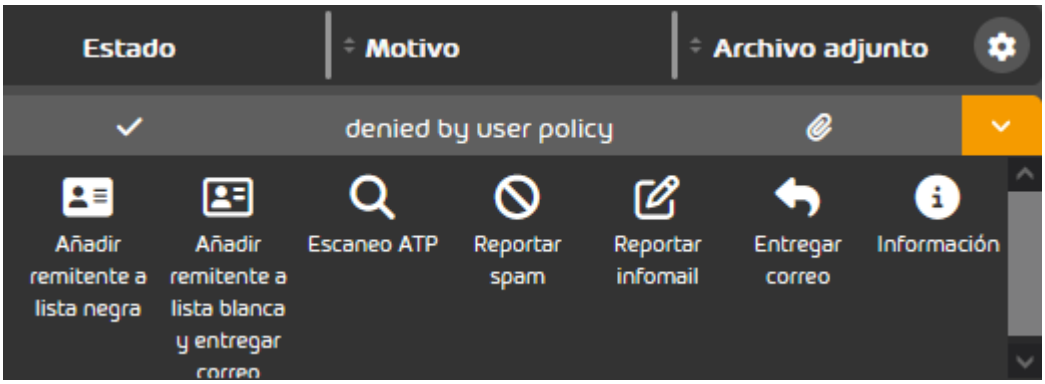


Figura 69: Análisis ATP en Email Live Tracking

La vista de opciones avanzadas se abre.

5. Haga clic en **Escaneo ATP** para iniciar el escaneo.

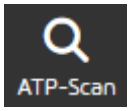


Figura 70: Iniciar el escaneo ATP

Se ha iniciado el escaneo ATP para el correo.

Tan pronto como finalice el escaneo ATP, podrá consultar el informe ATP en la vista de opciones avanzadas del correo (véase Informe ATP en la página 82) desde **Escaneo ATP**.

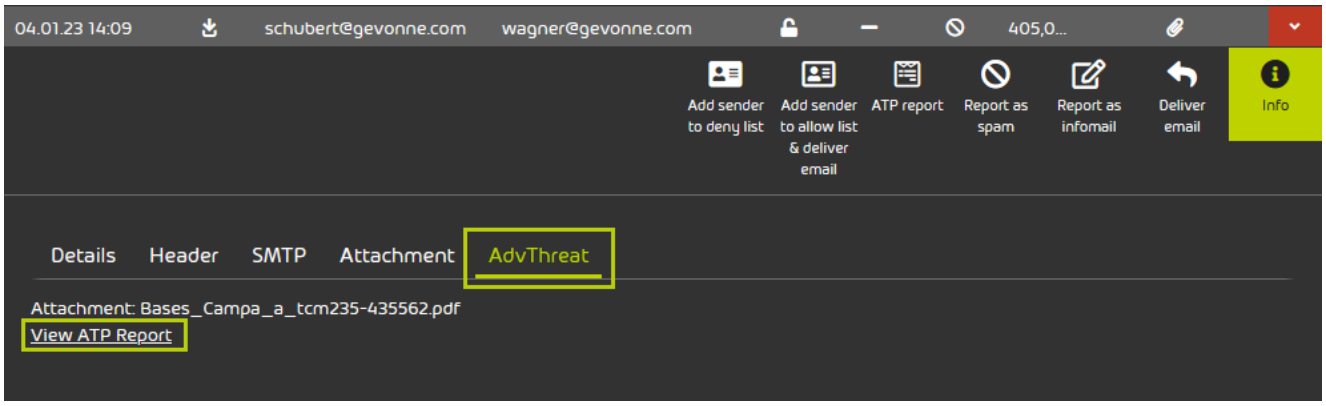


Figura 71: Consultar el informe ATP

Informe ATP

El informe ATP es un informe detallado que se genera tras analizarse un correo con el escaneo ATP (véase el capítulo "Escaneo ATP" del manual de Control Panel y Iniciar el escaneo ATP en la página 80). El informe ATP informa acerca del correo analizado. Los informes ATP están disponibles para los correos analizados en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63). El informe ATP de un correo puede consultarse desde el punto de menú **Informe ATP** o **Información** de la pestaña **AdvThreat**.

El informe ATP se divide en cuatro ventanas principales:

Summary

Aquí se muestra un resumen del archivo analizado. También se asigna al archivo una puntuación (**Score**) de 0 a 10. 0 significa que el archivo no comporta ningún riesgo, mientras que 10 es el nivel de riesgo más alto.

En la sección **Signatures** (firmas), el archivo se asigna a una de las siguientes categorías en función de su comportamiento:

- Información (verde)
- Atención (amarillo)
- Advertencia (rojo)

Si hace clic en una firma, se le mostrará información avanzada sobre el proceso.

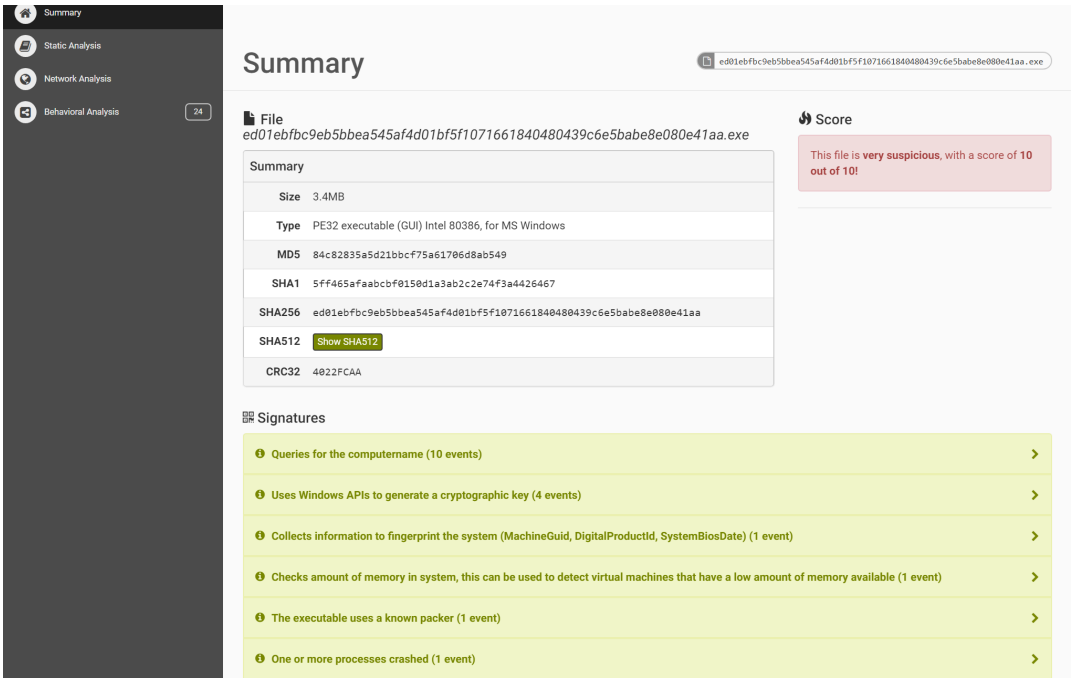


Figura 72: Resumen del informe ATP

Static Analysis

El análisis estadístico se divide, a su vez, en tres subcategorías:

- Static Analysis – Análisis estadístico del archivo. Depende del formato del archivo.
- Strings – Reproducción de las cadenas de caracteres del archivo.
- Antivirus – Análisis del archivo mediante diversos antivirus.

Network Analysis

En este análisis de red se analiza todo el tráfico de la red y se enumera por protocolos (p. ej., HTTP, TCP, UDP).

Behavioral Analysis

En el análisis de comportamiento se analiza el archivo en tiempo de ejecución.

Se muestran todas las llamadas a APIs y recursos del sistema registrados durante un análisis dinámico en sandbox.

Los resultados se dividen en dos secciones:

- Process Tree – Aquí se muestran los procesos en sucesión jerárquica.
- Process Contents – Si selecciona un proceso del "Process Tree", se le mostrarán aquí las llamadas a APIs ejecutadas en orden cronológico.

Información avanzada de correos

En la sección **Información** del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) encontrará datos sobre el correo electrónico seleccionado. La información detallada de un correo se divide en las secciones **Detalles**, **Encabezado**, **SMTP** y, si aplica, **Archivo adjunto**.

Detalles

Esta sección contiene los siguientes datos sobre el correo seleccionado:

- **Propietario**: Usuario de Control Panel que ha enviado o recibido el correo
- **Interlocutor**: Interlocutor del propietario del correo, que puede ser su remitente o destinatario
- **Cifrado de entrada**: Método de cifrado de correos entrantes desde el punto de vista de nuestros servidores. Se trata de correos que llegan a nuestros servidores enviados por usuarios de Control Panel o sus interlocutores.
- **Cifrado de salida**: Método de cifrado de correos salientes desde el punto de vista de nuestros servidores. Se trata de correos enviados por nuestros servidores a usuarios de Control Panel o sus interlocutores.
- **Clasificación**: Categoría asignada al correo en Control Panel (véase Categorías de correo electrónico en la página 90)
- **Asunto**: Asunto del correo
- **Motivo**: Motivo de clasificación del correo (véase Motivos de clasificación en la página 663)
- **Nombre de host de origen**: Nombre de servidor del remitente
- **Message-ID**: Identificador del correo asignado por el servidor de origen del remitente.

- **Código de estado SMTP**: Datos sobre la última respuesta de nuestro servidor en el diálogo SMTP. Dichos datos se muestran para correos con los estados de entrega **Entregado** y **Aplazado** (véase Filtros de campos en la página 75). Se incluyen los siguientes detalles:
  - Sello de tiempo de la transacción
  - Protocolo empleado (SMTP, TLS o EMIG)
  - Nombre de host y dirección IPv4 del servidor que ha recibido el correo
  - Código SMTP y, de haberlo, mensaje SMTP
  - **END-SEND**: Este valor indica que el cliente de SMTP ha emitido la orden SMTP **QUIT**. Esto significa que la comunicación ha finalizado correctamente.
  - **CIPHER**: Este campo solo se muestra en caso de que se haya empleado TLS, y se refiere a la fuerza de los algoritmos de cifrado utilizados. Valores posibles: **NONE** (si la comunicación se ha efectuado a través de un canal sin cifrar), **WEAK** (si la comunicación se ha efectuado con una versión de TLS anterior a la 1.2 o con un algoritmo de cifrado que consideremos débil) y **STRONG** (en cualquier otro caso).
  - **IDENTITY**: Este campo solo se muestra en caso de que se haya empleado TLS, y se refiere al método de autenticación. El valor **NONE** indica que la comunicación se ha efectuado a través de un canal sin cifrar. El valor **EMIG_VERIFIED** indica que la autenticación se ha efectuado mediante EmiG. El valor **CA_VERIFIED** indica que el certificado TLS del interlocutor se ha validado. El valor **SELF_ISSUED** indica que el certificado TLS del interlocutor no se ha validado, bien por ser autofirmado o por no haberse realizado la validación completa. **En casos excepcionales, el valor indica que se ha producido un error.**
- **Dominio del propietario**: Dominio del usuario que ha enviado o recibido el correo.

> **Nota:**
>
> Este campo está vacío para correos antiguos, enviados o recibidos antes de haberse implementado el proceso de verificación de dominios (véase "Verificación de dominios" en el manual de Control Panel).

Encabezado

Aquí se muestra la sección de encabezado del correo seleccionado. No es posible mostrar el encabezado de correos rechazados.

SMTP

En esta sección se muestra el resultado de la transmisión del correo. Para más información, véase la explicación sobre **Detalles** > **Código de estado SMTP**. Si ha habido varios intentos de entrega, se mostrarán aquí varios mensajes.

Archivo adjunto

Aquí se muestran los archivos adjuntos del correo en una tabla. En la columna **Archivo adjunto** se muestra el nombre de archivo y, en la columna **Hash de archivo adjunto**, el valor hash de cada archivo adjunto.

Campos de correo

En la siguiente tabla se describen las columnas que pueden mostrarse en la tabla de correos del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63). Los nombres y significados de las columnas coinciden en gran parte con los de los campos de datos de correos electrónicos (véase Información avanzada de correos en la página 84).

Tabla 6: Campos de correo

CAMPO	DESCRIPCIÓN
Puerta de enlace	Pasarela empleada
Asunto	Asunto del correo
Motivo	Motivo de clasificación del correo (véase Motivos de clasificación en la página 663)

CAMPO	DESCRIPCIÓN
Interlocutor	Interlocutor del propietario del correo, que puede ser su remitente o destinatario **Nota:** El campo contiene, para los correos entrantes, la información del campo From y, para los correos salientes, la información del campo To del encabezado del correo. Para los correos entrantes de la categoría **Rechazado**, el campo contiene la información del campo From del sobre del correo. El campo From del sobre puede contener una cadena de caracteres que no sea una dirección de correo.
Nombre de host de origen	Nombre de servidor del remitente

CAMPO	DESCRIPCIÓN
Propietario	Usuario de Control Panel que ha enviado o recibido el correo **Nota:** El campo contiene, para los correos entrantes, la información del campo To y, para los correos salientes, la información del campo From del encabezado del correo. Para los correos entrantes de la categoría **Rechazado**, el campo contiene la información del campo To del sobre del correo.
Nombre de host de destino	Nombre del servidor del destinatario
IP de destino	Dirección IP del destinatario (solo para mensajes entregados)
Message-ID	Identificador del correo asignado por el servidor de origen del remitente.
IP de origen	Dirección IP del remitente
Msg ID	Identificador del correo asignado por nuestros servidores.
Fecha y hora	Fecha y hora del correo

CAMPO	DESCRIPCIÓN
Dirección	Sentido de envío del correo desde el punto de vista del propietario. Significa "entrante" y significa "saliente".
	Método de cifrado de correos entrantes desde el punto de vista de nuestros servidores. Se trata de correos que llegan a nuestros servidores enviados por usuarios de Control Panel o sus interlocutores. Un icono de un candado indica que el correo entrante está cifrado. Para averiguar el método de cifrado del correo, sitúe el ratón sobre el candado o abra la información del correo.
	Método de cifrado de correos salientes desde el punto de vista de nuestros servidores. Se trata de correos enviados por nuestros servidores a usuarios de Control Panel o sus interlocutores. El estado y el método de cifrado se muestran del modo descrito en
Estado	Estado de entrega del correo (véase Filtros de campos en la página 75)
Tamaño	Tamaño del correo, incluidos sus archivos adjuntos
Archivo adjunto	Un icono indica si el correo contiene archivos adjuntos.

Categorías de correo electrónico

En el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63), los correos de los usuarios se dividen en las siguientes categorías:

Tabla 7: Categorías de correo electrónico

CATEGORÍA	DESCRIPCIÓN
Limpio	Se supone que los correos electrónicos son deseados por el destinatario y que no representan ningún peligro para él.
Infomail	Estos correos electrónicos son publicitarios. Infomail incluye boletines informativos enviados por correo electrónico. Puede clasificar los correos electrónicos de esta categoría como **Spam** o **Limpio**. En los siguientes casos, un correo electrónico no se clasifica directamente como **Limpio**, sino como **Infomail**. • Este correo electrónico viene de un remitente de boletines informativos conocido. • Se envían regularmente boletines informativos desde el rango IP del remitente. • El correo electrónico contiene una palabra clave o una cadena que indica un boletín informativo. • El correo electrónico tiene varias características que, en combinación, indican un boletín informativo.

CATEGORÍA	DESCRIPCIÓN
Spam	Estos correos electrónicos no son deseados y suelen tener un carácter publicitario o fraudulento. Estos correos electrónicos se envían a la vez a un gran número de destinatarios.
Contenido	Estos correos electrónicos tienen un archivo adjunto inválido. Los administradores determinan en el módulo **Content Control** qué archivos adjuntos son inválidos.
Threat	Estos correos electrónicos contienen contenido peligroso, como archivos adjuntos o enlaces maliciosos, o se envían para cometer delitos como la suplantación de identidad (phishing).
AdvThreat	Advanced Threat Protection ha detectado una amenaza en estos correos electrónicos. Los correos electrónicos se utilizan con fines ilícitos y emplean medios técnicos sofisticados que solo se pueden afrontar con procedimientos dinámicos avanzados.
Rechazado	Nuestro servidor de correo rechaza estos correos electrónicos directamente durante el diálogo SMTP debido a características externas, p. ej. relacionadas con la identidad del remitente, sin que los correos electrónicos se analicen más.

CATEGORÍA	DESCRIPCIÓN
Reanalizado	En el improbable caso de que algunos correos se pongan en cuarentena tras haber sido clasificados incorrectamente (p. ej., debido a filtros demasiado estrictos), nuestros administradores pueden ordenar el reanálisis de los correos afectados una vez resuelta la causa. Si dichos correos dejan de considerarse una amenaza, se entregan a sus destinatarios y se clasifican como **Reanalizado**.

Seleccionar una acción para varios correos

Si desea ejecutar una misma acción sobre varios correos al mismo tiempo en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63), proceda del siguiente modo.

> **Nota:**
>
> Otra opción consiste en ejecutar una acción sobre un solo correo (véase Ejecutar una acción sobre un correo en la página 78).

1. Inicie sesión en Control Panel.
2. Si, en lugar de sus propios correos, desea ver los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.

4. Haga clic en el botón que hay debajo de los filtros para abrir una lista de acciones.

Figura 73: Abrir acciones

5. Haga clic en los correos deseados para seleccionarlos.

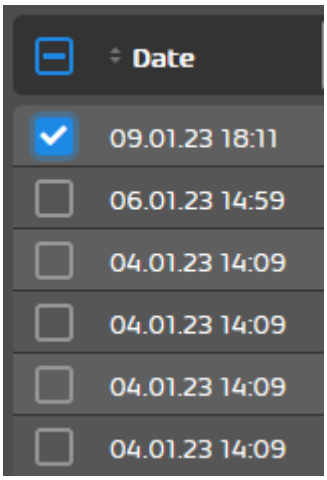


Figura 74: Seleccionar un correo

Nota:

También puede seleccionar todos los mensajes mostrados al mismo tiempo.

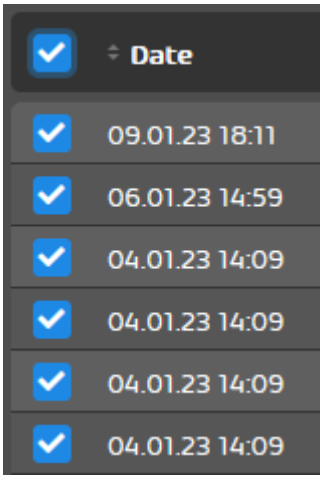


Figura 75: Seleccionar todos los correos mostrados

6. Haga clic en una acción para aplicarla a los correos seleccionados.

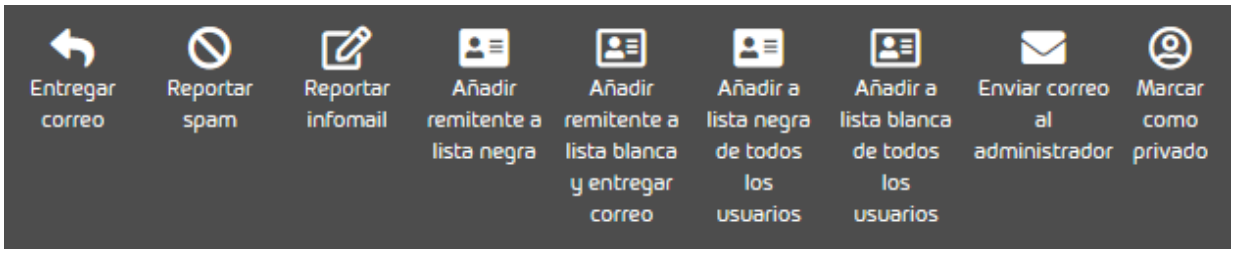


Figura 76: Seleccionar una acción

La acción se aplica sobre los correos seleccionados.

Se ha ejecutado una acción sobre varios correos al mismo tiempo.

Acciones para correos

En el módulo **Email Live Tracking** es posible efectuar diversas acciones sobre los correos, tales como, por ejemplo, añadir sus remitentes a una lista negra. En la siguiente tabla se describen las acciones que pueden efectuarse sobre los correos en el módulo **Email Live Tracking**

Nota:

La disponibilidad de acciones para correos depende de las acciones que el administrador haya habilitado y de los productos que estén activados.

Tabla 8: Acciones para correos

ACCIÓN	DESCRIPCIÓN
Entregar correo	Los correos seleccionados se entregan al destinatario. Esta acción está disponible para correos clasificados como **Limpio**, **Infomail**, **Spam**, **Contenido**, **Threat** o **AdvThreat**. Los correos clasificados como **Spam**, **Contenido**, **Threat** o **AdvThreat**, además de entregarse, se someten a un proceso de reevaluación de su categoría. Sin embargo, para los usuarios, esta acción solo estará disponible para correos de las categorías **Infomail**, **Spam**, **Contenido** y **Threat** si el administrador ha habilitado su entrega (véase Permitir o prohibir acciones de usuarios en la página 496). Solo los administradores y usuarios con el rol **Service Desk** pueden entregar correos de la categoría **AdvThreat**. A los correos entregados se les añade una línea extra en el encabezado con el texto **x-hornetsecurity-delivered:** e información sobre el rol del usuario que ha efectuado la acción. Los empleados de soporte técnico, administradores a nivel de partner, administradores a nivel de usuario y usuarios normales se indican con las palabras **support**, **reseller**, **admin** y **user**.

ACCIÓN	DESCRIPCIÓN
Ver correo	Mediante un enlace cifrado, se accede a un servicio online en una nueva ventana en la que el contenido del correo seleccionado se muestra de modo seguro. Las imágenes, enlaces y otros contenidos activos del correo se desactivan o sustituyen mediante sustitutivos seguros. Cuando sea preciso y posible, se modificarán ligeramente el diseño y la codificación para poder mostrar el contenido del correo. **Nota:** Esta acción solo es visible si no hay ningún ámbito de aplicación seleccionado en la selección de ámbitos y en Email Live Tracking se muestran los correos del buzón del usuario activo (véase Selección de ámbitos en la página 58). **Nota:** Los usuarios de Control Panel pueden efectuar esta acción sobre correos de los cuales sean propietarios. Los delegados también pueden ver vistas previas de correos de los buzones de correo para los que estén registrados como delegados (véase Designar un delegado en la página 263). **Nota:** Esta acción solo puede ejecutarse para un único correo (véase Ejecutar una acción sobre un correo en la página

ACCIÓN	DESCRIPCIÓN
Reportar spam	Los correos seleccionados se reportan al sistema de soporte técnico y gestión de calidad y se reclasifican. Éste es el método preferido para tratar correos mal clasificados. **Nota:** La acción para correos **Reportar spam** permite reportar todos los correos mal clasificados (falsos negativos).
Reportar infomail	Los correos seleccionados se clasifican como infomail. Es posible definir individualmente qué hacer con los correos de este tipo.
Añadir remitente a lista negra	Los remitentes de los correos seleccionados se añaden a la lista negra del usuario. Los correos enviados por estos remitentes que se reciban a partir de ahora se clasificarán automáticamente como spam.
Añadir remitente a lista blanca y entregar correo	Los remitentes de los correos seleccionados se añaden a la lista blanca del usuario y los correos se entregan. Los correos enviados por estos remitentes que se reciban a partir de ahora se entregarán automáticamente.
Añadir a lista negra de todos los usuarios	Los remitentes de los correos seleccionados se añaden a la lista negra para todos los usuarios del dominio, y los correos que se reciban se clasificarán como spam.

ACCIÓN	DESCRIPCIÓN
Añadir a lista blanca de todos los usuarios	Los remitentes de los correos seleccionados se añaden a la lista blanca para todos los usuarios. Todos los correos enviados por estos remitentes que se reciban se entregarán automáticamente.
Enviar correo al administrador	Los correos seleccionados se envían a la dirección de correo de la persona asignada al contacto **send_email_to_admin** bajo **Dashboard de servicios** > **Gestión de roles y contactos** (véase Asignar un contacto para la entrega de correos en la página 113).

Nota:

Los registros de listas blancas y negras se procesan del siguiente modo:

- Lista negra de administrador
- Lista blanca de administrador
- Lista negra de usuario
- Lista blanca de usuario

Un administrador añade la cuenta example@example.com a la lista negra global. Un usuario añade la misma cuenta de correo a su lista blanca. El usuario recibe todos los correos de dicha cuenta. A los usuarios que no tengan la cuenta añadida a sus listas blancas no se les entregarán.

Vista previa de correos

La vista previa del módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) permite a los usuarios y delegados visualizar el contenido de correos de las siguientes categorías (véase Categorías de correo electrónico en la página 90):

- **Spam**

- **Threat**
- **AdvThreat**
- **Contenido**
- **Infomail**
- **Limpio**

La vista previa de correos es compatible con las versiones más recientes de los siguientes navegadores:

- Edge
- Chrome
- Firefox
- Safari

La vista previa de correos puede abrirse en el módulo **Email Live Tracking** y en los informes de cuarentena (véase el capítulo "Acerca de Quarantine Report" del manual de Control Panel). En el módulo **Email Live Tracking**, la vista previa de correos de un usuario solo está disponible para correos que, o bien pertenezcan al usuario, o bien hayan pertenecido a un buzón de correo que se haya eliminado y asignado posteriormente al usuario. Los delegados también pueden ver vistas previas de correos de los buzones de correo para los que estén registrados como delegados (véase Designar un delegado en la página 263). Para más información, véase Acciones para correos en la página 95. En los informes de cuarentena, la vista previa de correos solo está disponible si el administrador ha seleccionado un diseño que la contenga y se generan informes de cuarentena propios para cada usuario del dominio (véase Configurar Quarantine Report para un dominio en la página 456).

La vista previa de correos puede abrirse en el módulo **Email Live Tracking** y en los informes de cuarentena. Al solicitar una vista previa de correos, un servicio web se abre en una nueva ventana de su navegador mediante un enlace cifrado.

El enlace cifrado solo es válido por tiempo limitado. En el módulo **Email Live Tracking** se genera el enlace cifrado tan pronto como el usuario solicita la vista previa. El enlace puede usarse una sola vez. Desde este módulo, el usuario puede crear tantos enlaces como desee. Por defecto, esta función está disponible durante seis meses. Los enlaces de los informes de cuarentena son válidos durante

14 días y pueden utilizarse tantas veces como se desee durante dicho plazo. No es posible volver a generar los enlaces de los informes de cuarentena.

En el servicio web, el contenido del correo seleccionado se muestra de un modo seguro. Las imágenes del correo se sustituyen mediante una imagen de relleno segura con el texto **Original image has been removed for security reasons.**. Los enlaces y otros contenidos activos se desactivan. Cuando sea preciso y posible, se modificarán ligeramente el diseño y la codificación para poder mostrar el contenido del correo.

> **Importante:**
>
> La vista previa de correos se abre en una ventana emergente. Es posible que su navegador bloquee ventanas emergentes. En la configuración del navegador puede permitir las ventanas emergentes.

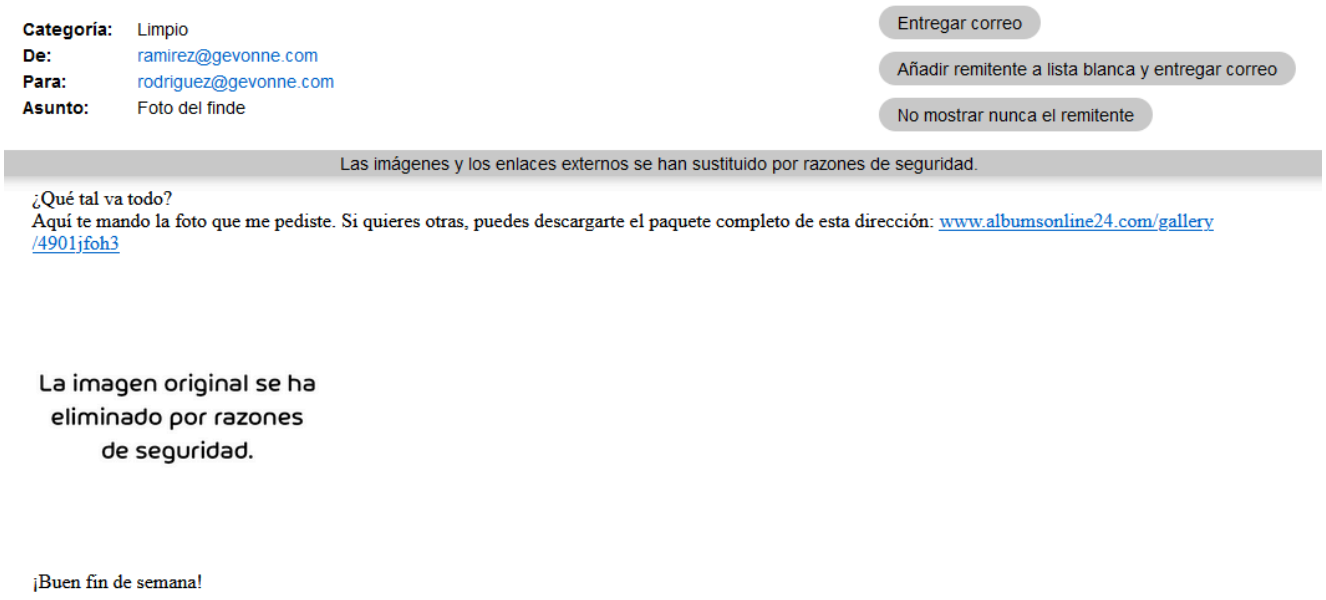


Figura 77: Vista previa de un correo.

Los usuarios pueden hacerse entregar correos desde la vista previa de correos. Para ello disponen de las siguientes opciones que pueden utilizar pulsando botones situados en la parte superior de la vista previa de correos:

- **Entregar correo**: El correo se entrega. Para saber más, véase la explicación de la acción para correos **Entregar correo** en Acciones para correos en la página 95.

> **Nota:**
>
> Esta acción no está disponible para correos enviados a buzones de correo de reenvío (véase el capítulo "Tipos de buzón de correo" del manual de Control Panel). Si intentan ejecutar esta acción, los usuarios reciben un mensaje de error.

- **Añadir remitente a lista blanca y entregar correo**: El remitente del correo se añade a la lista blanca del usuario y el correo se entrega. Los correos enviados por este remitente que se reciban a partir de ahora se entregarán automáticamente.

> **Nota:**
>
> Esta acción no está disponible para correos enviados a buzones de correo de reenvío (véase el capítulo "Tipos de buzón de correo" del manual de Control Panel). Si intentan ejecutar esta acción, los usuarios reciben un mensaje de error.

- **No mostrar nunca el remitente**: El remitente se añade a la lista negra del usuario y los correos que éste envíe en adelante no se mostrarán en informes de cuarentena (véase Acerca de Quarantine Report en la página 445).

> **Nota:**
>
> Este botón solo se muestra si la opción para informes de cuarentena **Excluir de los informes de cuarentena remitentes en la lista negra.** está activada (véase Configurar Quarantine Report para un buzón de correo en la página 463).

> **Nota:**
>
> Esta acción no está disponible para correos enviados a buzones de correo de reenvío (véase el capítulo "Tipos de buzón de correo" del manual de Control Panel). Si intentan ejecutar esta acción, los usuarios reciben un mensaje de error.

Exportar datos de correos en formato CSV

Puede exportar los resultados de sus búsquedas en el módulo **Email Live Tracking** en formato CSV (véase Email Live Tracking en la página 63). Los resultados de las búsquedas dependen de los filtros empleados (véase Filtros de campos en la página 75). Las filas del archivo de exportación se ordenan del mismo modo que los datos mostrados en el módulo **Email Live Tracking**.

Nota:

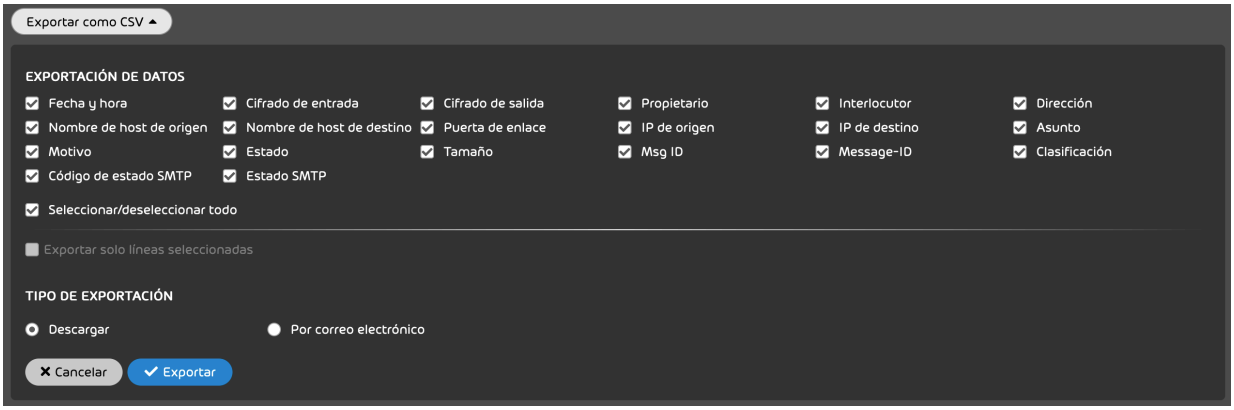
Si se selecciona un intervalo de tiempo (**El mes pasado**, **Este año** etc.), se aplicará la zona horaria UTC independientemente de la configuración del usuario. Por tanto, si el usuario tiene configurada una zona horaria distinta a UTC, pueden exportársele también datos del día anterior al comienzo del intervalo de tiempo seleccionado.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Opcional: Si, en lugar de sus propios correos, desea ver los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.
4. Opcional: Si solo desea exportar determinados correos, filtre los correos mostrados (véase Filtrar correos en la página 71).

   En el módulo **Email Live Tracking** se muestran solo los correos que cumplan las condiciones de la búsqueda.

5. Haga clic en **Exportar como CSV**.

Se abre un submenú de configuración avanzada.



6. Seleccione las columnas de tabla que desee exportar.

> **Nota:**
>
> Para más información acerca de los campos de correo, véase Información avanzada de correos en la página 84.

7. Seleccione el tipo de exportación deseado:
   - **Descargar**
   - **Por correo electrónico**
8. Haga clic en **Exportar** para exportar las columnas de la tabla seleccionadas.

> **Nota:**
>
> Esta función permite exportar un máximo de 10.000 registros por archivo. Si los resultados de la búsqueda contienen más de 10.000 registros solo se mostrarán los 10.000 primeros conforme al orden actual.

Se han exportado datos de correos en formato CSV.

Dashboard de servicios

Acerca del Dashboard de servicios

El Dashboard de servicios permite a los administradores mantener las actividades administrativas bajo control.

El Dashboard de servicios muestra una vista general de todos los roles creados para dominios de usuarios concretos .

En la sección **Gestión de roles y contactos**, los administradores a nivel de partner y cliente pueden crear nuevas asignaciones de roles (véase Roles en la página 53) y administrar asignaciones de roles preexistentes (véase Gestión de roles y contactos en la página 107). Además, los administradores pueden registrar datos de contacto para diversos cargos de su empresa (véase Añadir datos de contacto en la página 110).

En el apartado **Entornos secundarios**, los administradores a nivel de cliente pueden administrar sus entornos secundarios para dirigir el tráfico de correo entrante de determinados buzones de correo de un dominio a otros servidores de destino (véase Entornos secundarios en la página 120).

En la pestaña **Conexión LDAP**, los administradores a nivel de cliente pueden configurar la conexión LDAP de Control Panel (véase Conexión mediante LDAP en la página 129).

Además, los administradores a nivel de partner y cliente pueden definir una zona horaria, un idioma, un formato de fecha y un formato de hora por defecto para todos sus partners subordinados, clientes y usuarios en la pestaña **Zona horaria e idioma por defecto** (véase Ajustar zona horaria e idioma por defecto en la página 153).

Además, los administradores a nivel de partner pueden definir un contrato de licencia de usuario final y un contrato de tratamiento de datos para solicitar su aceptación por parte de los usuarios de sus clientes en la pestaña **Condiciones Generales** (véase Condiciones Generales en la página 155).

Gestión de roles y contactos

En el módulo **Dashboard de servicios**, los administradores pueden administrar las asignaciones de roles de sus usuarios, así como los contactos de su propia organización. Los usuarios con un rol asignado tienen permisos distintos a los de los usuarios normales (véase el capítulo "Roles" en el manual de Control Panel). Los contactos son interlocutores de un departamento o con un cargo concreto en la organización (véase Contactos en la página 108).

En **Gestión de roles y contactos** es posible efectuar las siguientes acciones:

- Asignar un rol a un usuario (véase Asignar roles en la página 109).
- Definir un usuario como contacto (véase Añadir datos de contacto en la página 110)
- Definir un usuario como contacto para la entrega de correos (véase Asignar un contacto para la entrega de correos en la página 113)
- Filtrar roles y contactos (véase Filtrar roles y contactos en la página 114)
- Eliminar una asignación de roles o un contacto (véase Eliminar asignaciones de roles o contactos en la página 117)

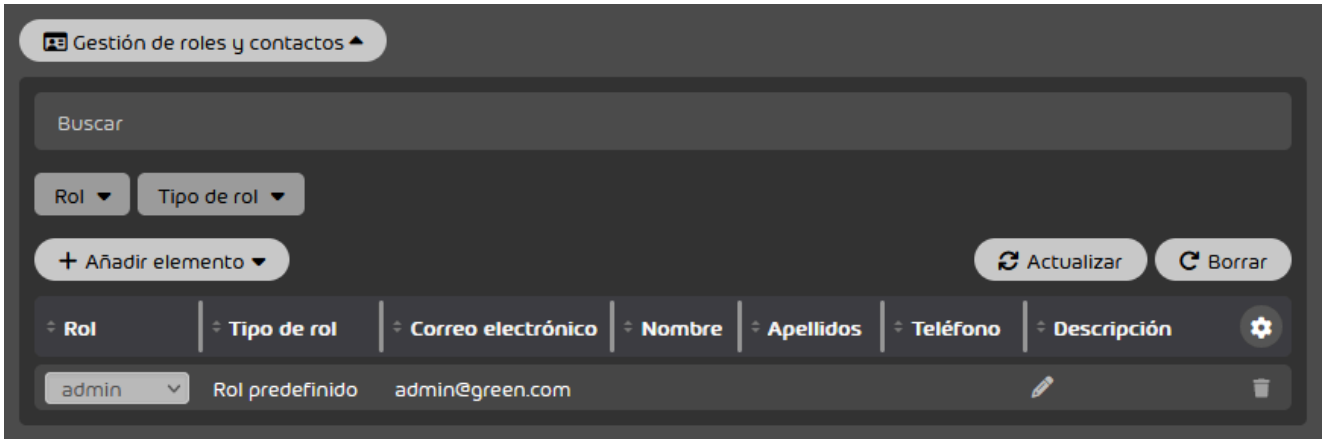


Figura 78: Vista general de gestión de roles y contactos

Contactos

Los administradores a nivel de cliente y partner pueden definir a usuarios como contactos en Control Panel. Los contactos hacen referencia a cargos o departamentos de una organización del cliente o partner. Mediante la asignación de contactos, los administradores pueden ver en todo momento en Control Panel quién es la persona de contacto para determinada función de una organización.

A diferencia de los roles (véase el capítulo "Roles" del manual de Control Panel), los contactos asignados no afectan a los derechos de los usuarios en Control Panel. La mayoría de contactos no afectan a las funciones de Control Panel. Solo el contacto **send_email_to_admin** está asociado a una acción dentro de Control Panel.

Los contactos se explican en la siguiente tabla.

Tabla 9: Contactos

CONTACTO	EXPLICACIÓN
it_director	Dirección del departamento de informática
helpdesk	Empleado de soporte técnico
sales	Empleado de ventas
license_management	Empleado responsable de la administración de licencias
emergency	Contacto para emergencias
personal_contact	Contacto personal
send_email_to_admin	Empleados que recibirán correos mediante la acción **Enviar correo al administrador** del módulo **Email Live Tracking**

Asignar roles

Los usuarios con roles asignados (véase Roles en la página 53) tienen permisos distintos a los de los usuarios normales. En el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106), puede asignar roles a sus usuarios para concederles permisos adicionales.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos a cuyos usuarios desee asignar roles.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.
5. Haga clic en **Gestión de roles y contactos** > **Añadir elemento**.

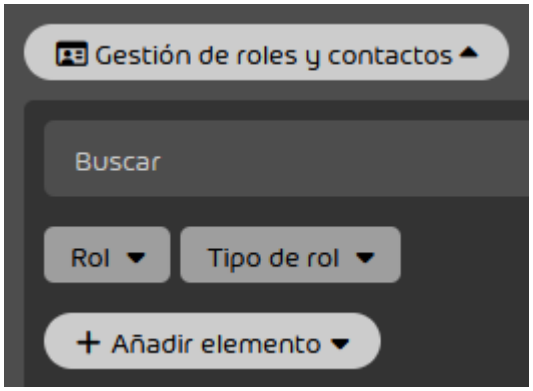


Figura 79: Añadir registro

6. En **Seleccionar usuario**, introduzca el usuario al cual desee asignar un rol nuevo.

7. Seleccione en el menú desplegable el rol que desee asignar al usuario.

> **Nota:**
>
> Los roles se detallan en el capítulo Roles en la página 53.

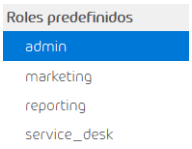


Figura 80: Seleccionar rol

8. Haga clic en **Confirmar**.

El rol se asigna al usuario. El usuario se muestra en la tabla con el rol asignado.

Se ha asignado un rol a un usuario.

Añadir datos de contacto

En el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede añadir datos de contacto para diversos cargos y departamentos de su organización, definiendo usuarios como personas de contacto con las funciones correspondientes. Los datos de contacto de dichos usuarios quedan asignados a sus cargos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyo usuario desee definir como contacto.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.

5. Haga clic en **Gestión de roles y contactos** > **Añadir elemento**.

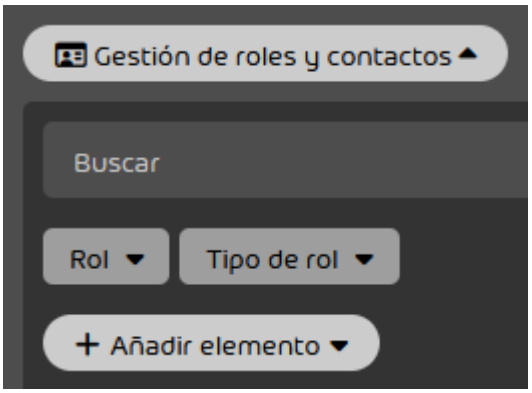


Figura 81: Añadir registro

6. En el menú desplegable, seleccione un cargo al que desee asignar los datos de contacto de un usuario.

   Puede elegir entre los siguientes cargos:

   - it_director
   - helpdesk
   - sales
   - license_management
   - emergency
   - personal_contact
   - send_email_to_admin

   Importante:

   El contacto **send_email_to_admin** es distinto al rol **admin**. Con la acción **Enviar correo al administrador** en **Email Live Tracking**, los correos solo se envían a la persona asignada al contacto **send_email_to_admin** (véase Asignar un contacto para la entrega de correos en la página 113).

   Nota:

   Para más información sobre contactos, véase Contactos en la página 108.

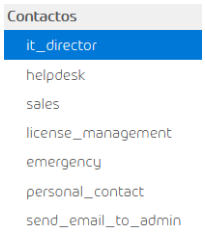


Figura 82: Seleccionar cargo

7. En **Seleccionar usuario**, seleccione un usuario cuyos datos desee registrar como datos de contacto para el cargo seleccionado.

8. Haga clic en **Confirmar**.

   Los datos del usuario seleccionado se asignan al cargo. El registro se muestra en la tabla con la indicación **Tipo de rol** en la columna **Contacto**.

Se ha definido un usuario como persona de contacto para cierto cargo.

Asignar un contacto para la entrega de correos

Puede asignar el contacto **send_email_to_admin** a un usuario para que sus usuarios puedan entregarle correos en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63). Si hay algún usuario con el contacto **send_email_to_admin** asignado, los usuarios pueden entregar correos a dicho usuario mediante la acción **Enviar correo al administrador** en el módulo **Email Live Tracking** (véase Acciones para correos en la página 95). De lo contrario, esta acción para correos no estará disponible para los usuarios del dominio y no se les mostrará en Control Panel.

Nota:

El contacto **send_email_to_admin** se asigna automáticamente al primer administrador definido para un cliente. Sin embargo, los administradores pueden eliminar este contacto si lo desean (véase Eliminar asignaciones de roles o contactos en la página 117).

Puede asignar el contacto **send_email_to_admin** a un usuario de modo manual.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Vaya a **Dashboard de servicios**.
3. Seleccione la pestaña **Administración**.
4. Haga clic en **Gestión de roles y contactos** > **Añadir elemento**.

   Se abre una vista avanzada.

5. Seleccione el contacto **send_email_to_admin** del menú desplegable.

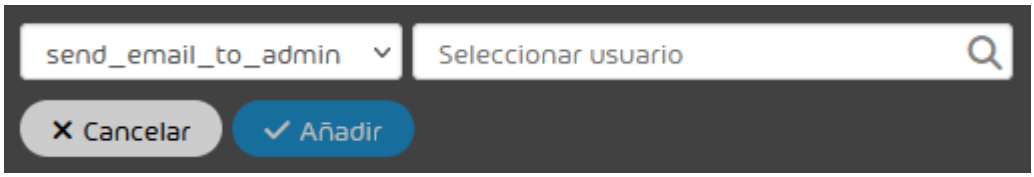


Figura 83: Seleccionar contacto

6. En **Seleccionar usuario**, introduzca el usuario al que desee asignar el contacto.

   El botón **Añadir** se habilita.

7. Haga clic en **Añadir**.

   El contacto se asigna al usuario. La asignación se añade a la tabla de abajo.

> **Nota:**
>
> Si el contacto **send_email_to_admin** no estaba asignado previamente a ningún usuario del dominio, deberá cerrar sesión en Control Panel e iniciar una nueva para que el cambio sea efectivo.

El contacto **send_email_to_admin** se ha asignado a un usuario. A partir de ahora, los usuarios pueden entregar correos al usuario asignado mediante la acción **Enviar correo al administrador** en el módulo **Email Live Tracking**.

Filtrar roles y contactos

Ha asignado roles a usuarios (véase Asignar roles en la página 109) y definido usuarios como contactos (véase Añadir datos de contacto en la página 110).

En el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) es posible filtrar roles (véase Roles en la página 53) y contactos por el rol asignado o el tipo de rol, lo cual simplifica la administración de roles y contactos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos roles y contactos desee filtrar.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.
5. Haga clic en **Gestión de roles y contactos**.

6. Filtre por roles o tipos de roles:
   - Para filtrar por un rol, selecciónelo en el menú desplegable **Rol**.
   - Para filtrar por un tipo de rol, selecciónelo en el menú desplegable **Tipo de rol**.

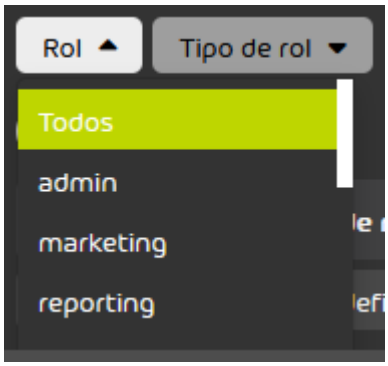


Figura 84: Filtrar por rol

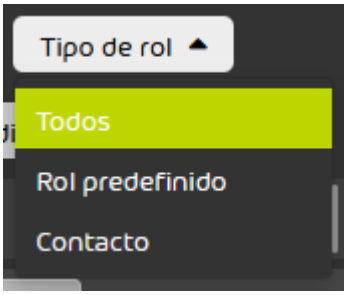


Figura 85: Filtrar por tipo de rol

Los registros filtrados se muestran en la tabla.

Se han filtrado roles y contactos.

Eliminar asignaciones de roles o contactos

Ha asignado un rol a un usuario (véase Asignar roles en la página 109) o ha definido un usuario como contacto (véase Añadir datos de contacto en la página 110).

En el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) es posible asignar roles a usuarios (véase Roles en la página 53) y registrar usuarios como contactos (véase Añadir datos de contacto en la página 110). Los usuarios con roles asignados tienen permisos distintos a los de los usuarios normales. Los contactos son interlocutores de un departamento de la empresa. Si una asignación de roles o un contacto pierde vigencia, es posible eliminarlo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyos usuarios desee eliminar una asignación de roles o un contacto.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.

5.

> **Importante:**
>
> Si se elimina el último contacto de tipo **send_email_to_admin**, la acción para correos **Enviar correo al administrador** dejará de estar disponible para los usuarios y desaparecerá del módulo **Email Live Tracking**.

> **Importante:**
>
> El rol **admin** debe estar asignado al menos a un usuario. Solo puede eliminar la asignación de este rol a un usuario cuando dicho rol esté asignado, al menos, a otro usuario.

> **Nota:**
>
> Los usuarios con el rol **admin** pueden eliminar su propia asignación del rol **admin**.

Haga clic en el icono en el lado derecho de la fila de la asignación de roles o contacto que desee eliminar.

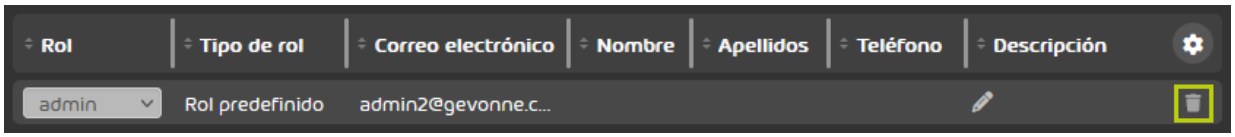


Figura 86: Eliminar un registro

Se muestra un mensaje de advertencia.

Figura 87: Mensaje de advertencia

6. Confirme la eliminación del registro con **Confirmar**.

El registro se elimina.

> **Nota:**
>
> Si se elimina el último contacto de tipo **send_email_to_admin**, los usuarios del dominio deberán cerrar sesión en Control Panel e iniciar una nueva para que el cambio sea efectivo.

Se ha eliminado una asignación de rol o contacto.

Eliminar un cliente propio

Como administrador a nivel de partner puede usted eliminar de Control Panel clientes que usted administre en el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio del cliente que desee eliminar en la selección de ámbitos.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.
5. En **Gestión de roles y contactos**, haga clic en **Eliminar el cliente seleccionado**.

Figura 88: Eliminar clientes

Aparece una ventana de confirmación.

6. Introduzca el nombre del cliente que desee eliminar en el campo de introducción de datos.

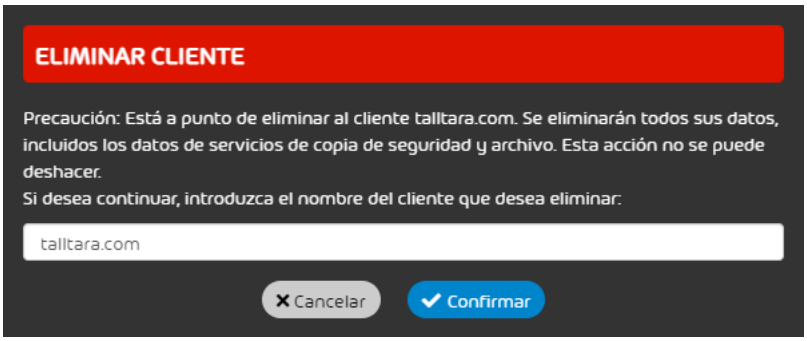


Figura 89: Introducir el nombre del cliente

7. Haga clic en **Confirmar**.

El cliente se elimina.

Se ha eliminado un cliente de Control Panel.

Entornos secundarios

Por defecto, el tráfico de correo entrante de todos los buzones de correo de un dominio se dirige al servidor de destino definido en el módulo **Spam and Malware Protection** (véase Configurar el entorno primario en la página 484). Este servidor de destino se denomina entorno primario.

Es posible dirigir el tráfico de correo entrante de determinados buzones de correo a otros servidores de destino. Estos otros servidores de destino se administran en Control Panel como entornos secundarios. Se distingue entre diversos tipos de entornos secundarios (véase Tipos de entornos secundarios en la página 121). Los entornos secundarios pueden crearse (véase Crear un entorno secundario en la página 123), editarse (véase Editar un entorno secundario en la página 125) y eliminarse (véase Eliminar un entorno secundario en la página 127) en el módulo **Dashboard de servicios**.

Tipos de entornos secundarios

Además del entorno primario (véase "Configuración del entorno primario" en el manual de Control Panel), al cual se dirige por defecto el tráfico de correo entrante de los buzones de correo de un dominio, es posible administrar entornos secundarios en Control Panel. Como entornos secundarios se definen servidores de destino a los cuales dirigir el tráfico de correo entrante de buzones de correo concretos del dominio en lugar del entorno primario. En el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) es posible administrar los siguientes tipos de entornos secundarios:

- **Individual**: Con este tipo de entornos secundarios, los administradores pueden definir sus propios servidores de destino. También pueden definir la dirección IPv4 o el nombre de host de los servidores de destino. Los administradores pueden crear varios entornos secundarios de este tipo.

Sincronización de entornos secundarios

Por defecto, los buzones de correo sincronizados con un servicio de directorio mediante LDAP se asignan al entorno primario de Control Panel (véase "Configuración del entorno primario" en el manual de Control Panel). A diferencia de los buzones de correo no sincronizados, los buzones de correo sincronizados no se pueden asignar manualmente a un entorno secundario (véase Entornos secundarios en la página 120) en Control Panel.

Sin embargo, es posible asignar estos buzones de correo a entornos secundarios de modo automático. Para ello, es preciso que el buzón de correo pertenezca, en el servicio de directorio, a un grupo con el mismo nombre que un entorno secundario de Control Panel. El hecho de que este grupo exista o no en Control Panel no influye en modo alguno.

Durante la sincronización de un buzón de correo en Control Panel, los nombres de sus grupos del servicio de directorio se comparan uno tras otros con los nombres de los entornos secundarios. En cuanto se descubre una coincidencia, el proceso se interrumpe y el buzón de correo se asigna al entorno secundario correspondiente. Por tanto, no se tienen en cuenta coincidencias posteriores.

Nota:

El procesamiento de los grupos se realiza por el orden de sus nombres según la tabla Unicode. A continuación se detalla el orden de algunos caracteres. La siguiente lista contiene tan solo una selección de caracteres y no pretende ser exhaustiva.

1. Signo de exclamación !
2. Almohadilla #
3. Asterisco *
4. Signo más +
5. Signo menos -
6. Cifras
7. Signo menor que <
8. Signo mayor que >
9. Guion bajo _
10. Letras minúsculas
11. Tilde ~
12. Letras minúsculas con signos diacríticos

Todas las letras de los nombres de los grupos y buzones secundarios se tratan como si fueran minúsculas.

Para que un buzón de correo sincronizado se asigne al entorno secundario correcto, recomendamos el siguiente procedimiento: En el servicio de directorio, el administrador asigna el buzón de correo exclusivamente a un grupo cuyo nombre coincida con el nombre del entorno secundario de Control Panel. al que se desee asignar el buzón de correo.

Importante:

Para que un buzón de correo sincronizado se asigne al entorno primario, no deberá pertenecer a ningún grupo o del servicio de directorio cuyo nombre coincida con el nombre de un entorno secundario de Control Panel.

Crear un entorno secundario

Por defecto, el tráfico de correo entrante de todos los buzones de correo de un dominio se dirige al servidor de destino definido (véase Configurar el entorno primario en la página 484) como entorno primario en el módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477). Si desea dirigir el tráfico de correo entrante de determinados buzones de correo del dominio a otros servidores de destino, puede crear entornos secundarios para dichos servidores.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear un entorno secundario.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.
5. En **Entornos secundarios**, haga clic en **Añadir entorno secundario**.

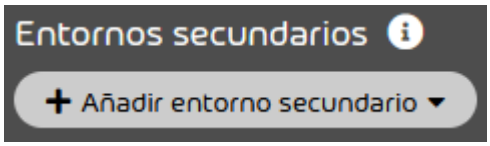


Figura 90: Añadir un entorno secundario

Se abre un menú.

6. Seleccione la pestaña correspondiente al tipo de entorno secundario que desee crear (véase Tipos de entornos secundarios en la página 121). Puede elegir entre los siguientes tipos de entornos secundarios:

   - **Individual**

7. **Importante:**

   Durante su sincronización en Control Panel, los buzones de correo de tipo LDAP (véase el capítulo "Tipos de buzón de correo" en el manual de Control Panel) se asignan automáticamente a un entorno secundario si pertenecen a un grupo del servicio de directorio cuyo nombre coincida con el de dicho entorno secundario de Control Panel. Los buzones de correo se asignan al entorno secundario con dicho nombre.

   Los nombres de los grupos de los grupos se procesan y comparan con los nombres de los entornos secundarios siguiendo el orden de los caracteres de la tabla Unicode. Cada buzón de correo se asigna al primer entorno secundario cuyo nombre coincida con el de uno de sus grupos. Para más información, véase Sincronización de entornos secundarios en la página 121.

   En el campo **Nombre del entorno en Control Panel**, introduzca el nombre asignado al nuevo entorno secundario en Control Panel.

Figura 91: Introducir el nombre del entorno secundario

8. Opcional: Si ha seleccionado la pestaña **Individual**, introduzca la dirección IPv4 o el nombre de host del servidor de destino en el campo **Dirección del servidor de destino**.

Figura 92: Introducir la dirección del servidor de destino

9. Haga clic en **Añadir**.

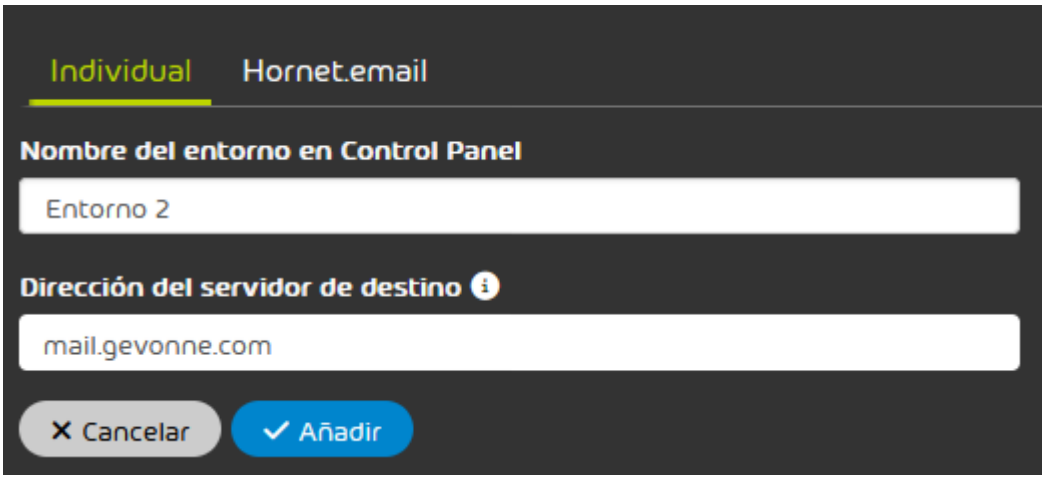


Figura 93: Añadir un entorno secundario

El entorno secundario se crea y se añade a la tabla de **Entornos secundarios**.

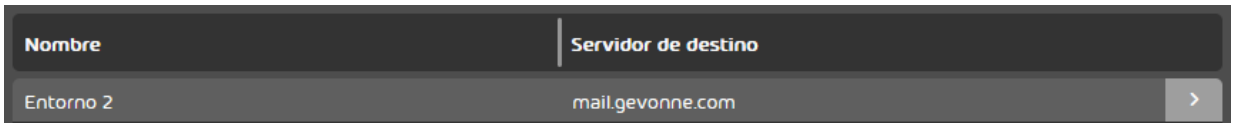


Figura 94: Lista de entornos secundarios

Se ha creado un entorno secundario.

A continuación puede asignar el entorno secundario a buzones de correo de su dominio (véase Cambiar de entorno en la página 276). Puede eliminar el entorno secundario cuando deje de ser necesario (véase Eliminar un entorno secundario en la página 127).

Editar un entorno secundario

Ha creado un entorno secundario (véase Crear un entorno secundario en la página 123).

Puede editar los entornos secundarios disponibles. Sin embargo, no puede cambiar el tipo de entorno secundario (véase Tipos de entornos secundarios en la página 121).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee editar un entorno secundario preexistente.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.
5. Seleccione el entorno secundario de la lista bajo **Entornos secundarios** y haga clic en la flecha de menú junto al entorno secundario.

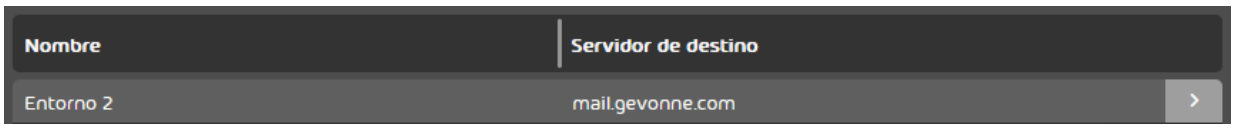


Figura 95: Abrir el menú

Se abre un menú.

6. Haga clic en **Editar registro**.

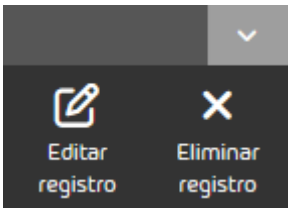


Figura 96: Editar el registro

Se abre un menú con la configuración actual del entorno secundario.

7. Edite la configuración del entorno secundario como desee (véase Crear un entorno secundario en la página 123).

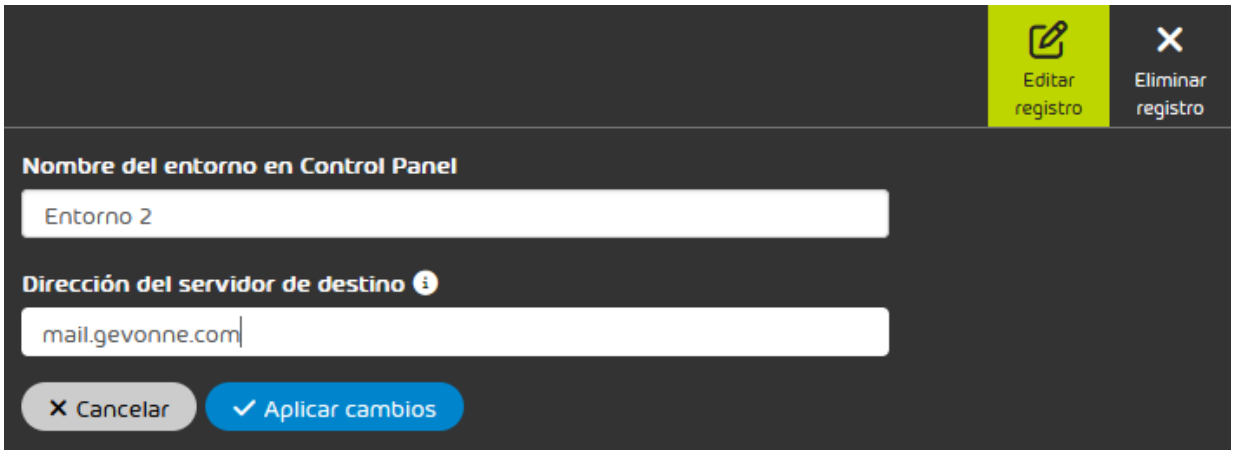


Figura 97: Editar un entorno secundario

8. Haga clic en **Aplicar cambios**.

Los cambios se guardan y se aplican sobre todos los buzones de correo que tengan asignado este entorno secundario.

Se ha editado un entorno secundario.

Eliminar un entorno secundario

Ha creado un entorno secundario (véase Crear un entorno secundario en la página 123).

Puede eliminar un entorno secundario cuando deje de ser necesario. Tras eliminarse un entorno secundario, a los buzones de correo que lo tuviesen asignado se les asigna el entorno primario (véase Configuración del entorno primario en la página 483).

Importante:

Si los buzones de correo del entorno primario se sincronizan con un servicio de directorio mediante LDAP, los buzones de correo del entorno secundario eliminado se asignarán al entorno primario, pero no se sincronizarán.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee eliminar un entorno secundario preexistente.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Administración**.
5. Seleccione el entorno secundario de la lista bajo **Entornos secundarios** y haga clic en la flecha de menú junto al entorno secundario.

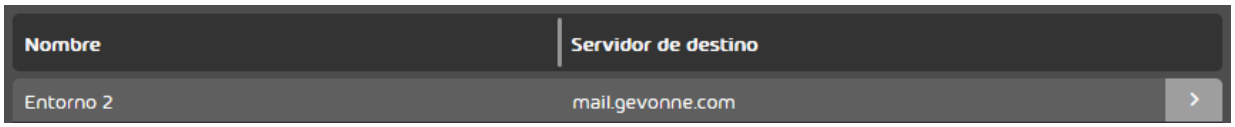


Figura 98: Abrir el menú

Se abre un menú.

6. Haga clic en **Eliminar registro**.

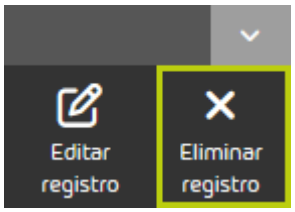


Figura 99: Eliminar un registro

Se muestra un mensaje.

7. Haga clic en **Confirmar**.

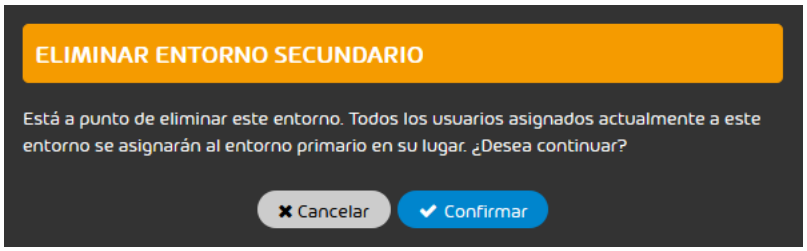


Figura 100: Eliminar un entorno secundario

El entorno secundario se elimina. A los buzones de correo del domino que lo tuviesen asignado se les asigna en su lugar el entorno primario.

Se ha eliminado un entorno secundario.

Conexión mediante LDAP

En la pestaña **Conexión LDAP** del módulo **Dashboard de servicios**, los administradores a nivel de cliente pueden conectar un servicio de directorio, p. ej., Active Directory (AD) de Microsoft, con Control Panel mediante LDAP. La conexión LDAP solo puede aplicarse al entorno primario (véase el capítulo «Configuración del entorno primario» en el manual de Control Panel).

Para conectar un servicio de directorio con Control Panel, los administradores a nivel de cliente deben configurar primero los atributos de LDAP del servicio de directorio en Control Panel (véase Configurar atributos de LDAP en la página 130). Después, los administradores pueden añadir una conexión LDAP (véase Añadir una conexión LDAP en la página 132). De este modo se establece una conexión entre Control Panel y un servicio de directorio. Es posible añadir varias conexiones LDAP para servicios de directorio distintos. Al añadir una conexión LDAP, los administradores pueden además asegurarla configurando LDAPS como protocolo de acceso. Como medida de protección adicional, los administradores pueden limitar el acceso a su servicio de directorio a nuestro rango de direcciones IP (véase Limitar el servicio de directorio a nuestro rango de direcciones IP en

la página 141). Además, los administradores pueden definir si los usuarios y grupos del servicio de directorio deberán sincronizarse en Control Panel. Los administradores pueden comprobar el resultado de la sincronización haciéndose mostrar una lista de los usuarios y grupos a sincronizar.

Cuando haya al menos una conexión LDAP activa, los administradores a nivel de cliente pueden disponer que sus usuarios puedan iniciar sesión en Control Panel con sus datos de acceso del servicio de directorio (véase Configurar el acceso a Control Panel mediante LDAP en la página 142). Los administradores pueden comprobar, mediante una prueba, si realmente es posible efectuar el acceso con datos de acceso del servicio de directorio.

Los administradores a nivel de cliente pueden editar conexiones LDAP existentes a posteriori (véase Editar una conexión LDAP en la página 146). Si una conexión LDAP no se debe utilizar temporalmente, los administradores pueden desactivarla (véase Desactivar la conexión mediante LDAP en la página 148). Si una conexión LDAP deja de ser necesaria, los administradores pueden eliminarla (véase Eliminar una conexión LDAP en la página 151).

Configurar atributos de LDAP

En la pestaña **Conexión LDAP** (véase Conexión mediante LDAP en la página 129) del módulo **Dashboard de servicios** (véase el capítulo «Acerca del Dashboard de servicios» en el manual de Control Panel), los atributos de LDAP contienen valores por defecto para Active Directory de Microsoft. Si los atributos de su directorio tienen otros nombres, puede cambiarlos en **Atributos de LDAP**. Los atributos de LDAP se aplican a todas las conexiones LDAP del cliente en Control Panel (véase Añadir una conexión LDAP en la página 132).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee configurar los atributos de LDAP.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.

5. Cumplimente el formulario bajo **Atributos de LDAP**. Los campos tienen los siguientes significados:

   - **Dirección de correo**: Atributo del servicio de directorio en el que se registran las direcciones de correo electrónico de los usuarios. En un Active Directory de Microsoft se emplea por defecto el atributo **proxyAddresses**.
   - **Direcciones de correo alias**: Atributo del servicio de directorio en el que se registran las direcciones de correo electrónico alias de los usuarios. En un Active Directory se emplea igualmente por defecto el atributo **proxyAddresses**.
   - **Grupo**: Atributo del servicio de directorio en el que se indican los grupos. En un Active Directory de Microsoft se emplea por defecto el atributo **memberOf**.
   - **Nombre de cuenta SAM**: Atributo del servicio de directorio en el que se registra el nombre de la cuenta SAM. En un Active Directory de Microsoft se emplea por defecto el atributo **sAMAccountname**.
   - **Cantidad mínima de usuarios**: Cantidad mínima de usuarios esperada durante la sincronización mediante LDAP. Este valor se refiere al número total de los usuarios sincronizados de todas las conexiones LDAP activas. Este valor puede emplearse como indicador de la calidad de la sincronización. Si no se alcanza este valor durante un proceso de sincronización, se envía un correo a la dirección de correo electrónico indicada en **Dirección de correo para notificaciones** avisando de posibles problemas de sincronización. El valor por defecto es **1**.
   - **Cantidad mínima de grupos**: Análogo a **Cantidad mínima de usuarios**, pero para grupos en lugar de para usuarios. El valor por defecto es **0**.
   - **Dirección de correo para notificaciones**: Dirección de correo electrónico a la que enviar las notificaciones sobre la sincronización LDAP.
   - **ID de objeto**: Atributo del servicio de directorio empleado como identificador externo unívoco de los buzones de correo. En un Active Directory de Microsoft se emplea por defecto el atributo **objectguid**.
   - **Puestos e idiomas para Security Awareness Service**: Atributo personalizado del servicio de directorio que contiene los puestos e idiomas de los usuarios para Security Awareness

Service (véase Sincronizar puestos e idiomas para Security Awareness Service). El atributo deseado puede seleccionarse con un menú desplegable.

Nota:

Este campo solo es visible cuando Security Awareness Service (véase Acerca de Security Awareness Service) está activado.

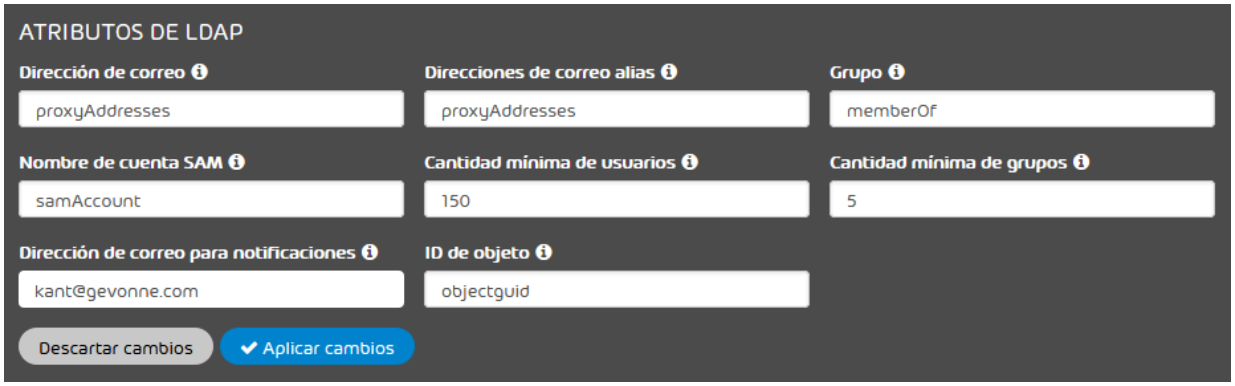


Figura 101: Rellenar el formulario

6. Haga clic en **Aplicar cambios**.

Los cambios se guardan.

Se han configurado los atributos de LDAP del servicio de directorio de un cliente en Control Panel.

A continuación puede añadir una conexión LDAP a Control Panel (véase Añadir una conexión LDAP en la página 132).

Añadir una conexión LDAP

Ha configurado los atributos de LDAP de su servicio de directorio en Control Panel (véase Configurar atributos de LDAP en la página 130).

En la pestaña **Conexión LDAP** (véase Conexión mediante LDAP en la página 129) del módulo **Dashboard de servicios** (véase el capítulo «Acerca del Dashboard de servicios» en el manual de Control Panel) puede añadir una conexión LDAP a Control Panel. De este modo se establece una conexión entre Control Panel y un servicio de directorio. Puede configurar que los usuarios y grupos del servicio de directorio se sincronicen en Control Panel. Puede añadir varias conexiones LDAP para servicios de directorio distintos a Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee añadir una conexión LDAP.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.

5. En **Conexiones LDAP disponibles**, haga clic en **Añadir conexión LDAP**.

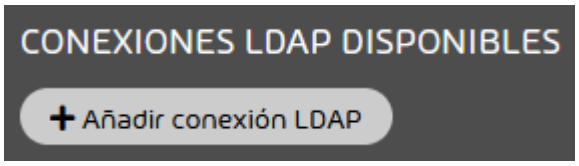


Figura 102: Añadir una conexión LDAP

Se abre una vista avanzada.

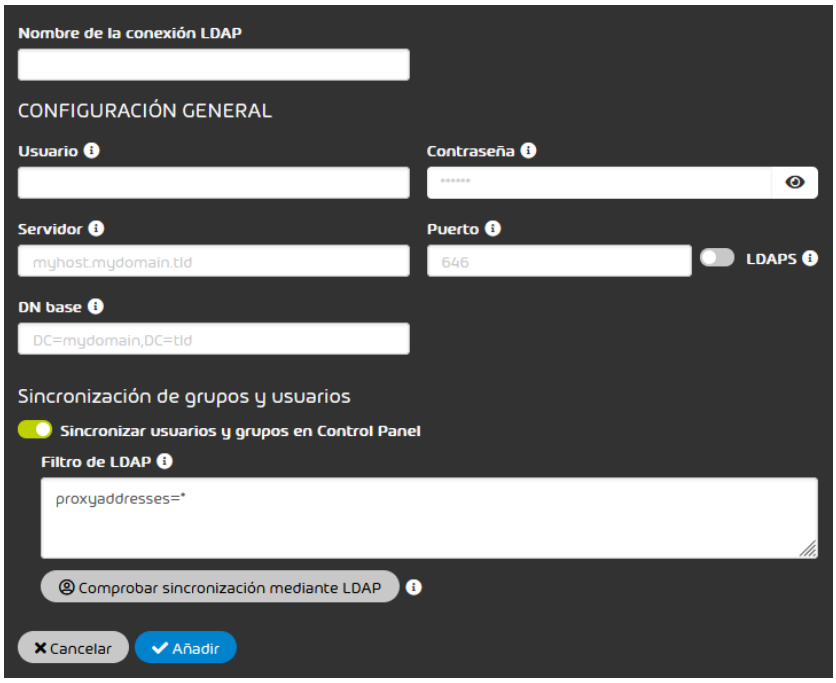


Figura 103: Vista avanzada

6. Introduzca un nombre para la conexión LDAP en el campo **Nombre de la conexión LDAP**.

7. Cumplimente los campos bajo **Configuración general**. Los campos tienen los siguientes significados.

   - **Usuario**. Nombre de usuario de un usuario del directorio con derechos de lectura sobre la estructura del directorio bajo el DN base. También es posible introducir la dirección de correo electrónico o la ruta LDAP del usuario.

     > **Nota:**
     >
     > En Active Directory de Microsoft, es posible conceder los derechos necesarios al usuario asignándolo al grupo **RAS and IAS Servers**.

     > **Nota:**

   - **Contraseña**: Contraseña del usuario
   - **Servidor**: Dirección IPv4 o nombre de host del servidor de destino del servicio de directorio
   - **Puerto**: Puerto del servidor de destino del servicio de directorio. Los puertos estándar para los diversos protocolos LDAP son:
     - LDAP: Puerto 389
     - LDAPS: Puerto 636
     - GC_LDAP: Puerto 3268
     - GC_LDAPS: Puerto 3269
   - **DN base**: La ruta básica de LDAP en la que se encuentra el usuario. Por ejemplo: **DC=myDomain,DC=tld**.

8. Opcional: Si su servicio de directorio se comunica mediante el protocolo LDAPS, accione el interruptor **LDAPS**.

> **Nota:**
>
> El protocolo LDAPS asegura la conexión LDAP mediante TLS/SSL. La conexión LDAP se puede además asegurar limitando el servicio de directorio a nuestro rango de direcciones IP (véase Limitar el servicio de directorio a nuestro rango de direcciones IP en la página 141).

El interruptor se pone verde.

9. Opcional: Si los usuarios y grupos del servicio de directorio no deben sincronizarse en Control Panel, accione el interruptor **Sincronizar usuarios y grupos en Control Panel**.

> **Nota:**
>
> La sincronización de usuarios y grupos está activada por defecto.
>
> Mediante la sincronización de usuarios y grupos, los usuarios y sus pertenencias a grupos del servicio de directorio se transmiten a Control Panel. Si se eliminan o modifican usuarios o pertenencias a grupos en el servicio de directorio, dichos cambios también se aplicarán en Control Panel.
>
> Los buzones de correo creados en Control Panel o no procedentes de LDAP (véase el capítulo "Tipos de buzón de correo" del manual de Control Panel) se mantienen en Control Panel en caso de sincronización con LDAP. Durante la sincronización solo se eliminan buzones de correo de Control Panel que se hayan creado previamente en él mediante sincronización con LDAP pero ya no estén disponibles en el servicio de directorio.

> **Nota:**
>
> La pertenencia a grupos de buzones de correo de tipo LDAP se administra exclusivamente en el servicio de directorio. Por tanto, los buzones de correo de tipo LDAP no pueden añadirse manualmente a grupos ni eliminarse de los mismos en Control Panel. Para que los usuarios en Control Panel se puedan asignar a los grupos del servicio de directorio en Control Panel, se deben crear manualmente grupos con los mismos nombres en Control Panel. Para más información sobre cómo crear grupos, véase «Grupos» en el manual de Control Panel. Sin embargo, a los grupos sincronizados con un servicio de directorio en Control Panel se les pueden añadir buzones de correo de entornos secundarios, que también pueden importarse a los mismos (véanse "Administrar miembros" y "Importar miembros de un grupo desde un archivo CSV" en el manual de Control Panel).

Nota:

Con la sincronización de usuarios del servicio de directorio es posible efectuar una asignación automática de direcciones alias. Esto tiene la ventaja de que solo se envíe un informe de cuarentena (véase "Acerca de Quarantine Report" en el manual de Control Panel) por dirección de correo principal, incluidas todas las direcciones alias correspondientes.

El interruptor se pone gris. El campo **Filtro de LDAP** se oculta.

10. Si la sincronización de usuarios y grupos está activada, introduzca el filtro de LDAP con el cual se encuentren los usuarios y grupos en el servicio de directorio en el campo **Filtro de LDAP**.

Nota:

El filtro de LDAP **proxyaddresses=*** está establecido por defecto. Este filtro de LDAP encuentra por defecto los usuarios y grupos en Active Directory de Microsoft.

Nota:

Si es preciso cambiar el filtro, deberá emplearse la siguiente sintaxis:

(|(xxxxxxxxxx=xxxxxxxxxx)(xxxxxxxxxx=xxxxxxxxxx))

La totalidad del filtro, así como cada pareja de atributos y valores, deben escribirse entre paréntesis. La barra vertical **|** del principio une los parámetros incluidos a continuación entre paréntesis con un operador O. De este modo, debe cumplirse una de las dos condiciones indicadas. Es posible realizar una operación UND entre los parámetros añadiendo un **&** al principio.

Además, al menos uno los parámetros deberá encontrarse entre paréntesis.

Nota:

Con la expresión **(|(sAMAccountType=805306368)(sAMAccountType=268435456)(sAMAccountType=268435457)(objectclass=publicFolder))** se encuentran todos los usuarios de un Active Directory de Microsoft.

11. Opcional: Si desea comprobar qué usuarios y grupos a sincronizar el filtro de LDAP introducido encuentra en el servicio de directorio, proceda del siguiente modo.

a) Haga clic en **Comprobar sincronización mediante LDAP**.

Se abre la pantalla **Prueba de LDAP**.

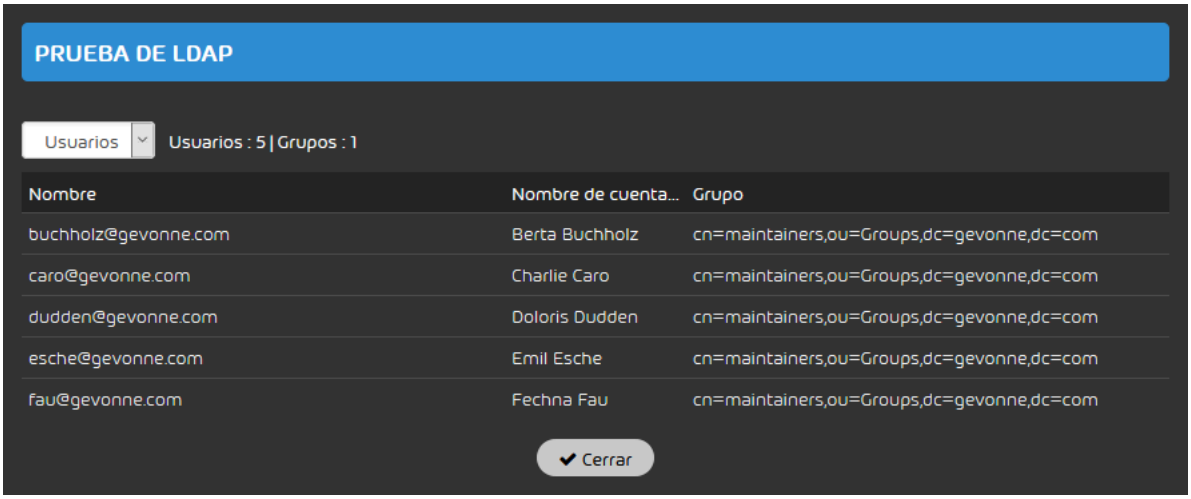


Figura 104: Prueba de LDAP

b) En el menú desplegable, seleccione la opción sobre la cual desee ver más información. Puede elegir entre las siguientes opciones.

- **Usuarios**: Se muestran los usuarios que el filtro de LDAP encuentre en el servicio de directorio y que se puedan sincronizar.
- **Grupos**: Se muestran los grupos que el filtro de LDAP encuentre en el servicio de directorio y que se puedan sincronizar.
- **Registro**: Se muestra el protocolo de la prueba de LDAP.

c) Compruebe si los datos mostrados se corresponden con los esperados en relación al contenido de su servicio de directorio.

d) Haga clic en **Cerrar**.

La ventana se cierra.

12. Haga clic en **Aplicar cambios**.

Los ajustes se guardan. La conexión LDAP se añade a Control Panel y se activa.

> **Nota:**
>
> La sincronización de los datos del servicio de directorio se efectúa una vez cada hora. Por tal motivo, es posible que el resultado de los ajustes no se haga efectivo hasta al cabo de dos horas.

Se ha añadido una conexión LDAP a Control Panel. Si la sincronización de usuarios y grupos está activada, los usuarios y grupos del servicio de directorio se sincronizarán regularmente en Control Panel. Los usuarios sincronizados se añaden a Control Panel como buzones LDAP (véase el capítulo «Tipos de buzón de correo» en el manual de Control Panel).

A continuación puede configurar que los usuarios de buzones LDAP inicien sesión en Control Panel con los datos de acceso del servicio de directorio (véase Configurar el acceso a Control Panel mediante LDAP en la página 142). Puede editar una conexión LDAP existente a posteriori (véase Editar una conexión LDAP en la página 146). Además puede desactivar una conexión LDAP temporalmente (véase Desactivar la conexión mediante LDAP en la página 148) o eliminarla de Control Panel (véase Eliminar una conexión LDAP en la página 151).

Limitar el servicio de directorio a nuestro rango de direcciones IP

Puede limitar el acceso a su servicio de directorio (véase Conexión mediante LDAP en la página 129) a nuestro rango de direcciones IP. Introduciendo nuestros rangos de direcciones en el cortafuegos de su servicio de directorio, puede impedir que éste acepte solicitudes de otras direcciones IP.

Introduzca los siguientes rangos de direcciones IP en el cortafuegos su servicio de directorio.

- Primer rango: **83.246.65.0/24** con la máscara de subred **255.255.255.0**, correspondiente a las direcciones de 83.246.65.1 a 83.246.65.255.
- Segundo rango: **94.100.128.0/20** con la máscara de subred **255.255.240.0**, correspondiente a las direcciones de 94.100.128.1 a 94.100.143.255.
- Tercer rango: **185.140.204.0/22** con la máscara de subred **255.255.252.0**, correspondiente a las direcciones de 185.140.204.1 a 185.140.207.255.
- Cuarto rango: **173.45.18.0/24** con la máscara de subred **255.255.255.0**, correspondiente a las direcciones de 173.45.18.1 a 173.45.18.255.

Nota:

Los clientes canadienses deben registrar adicionalmente los siguientes rangos IP:

- Quinto rango: **108.163.133.224/27** con la máscara de subred **255.255.255.224**, correspondiente a las direcciones de 108.163.133.224 a 108.163.133.255.
- Sexto rango: **199.27.221.64/27** con la máscara de subred **255.255.255.224**, correspondiente a las direcciones de 199.27.221.64 a 199.27.221.95.
- Séptimo rango: **209.172.38.64/27** con la máscara de subred **255.255.255.224**, correspondiente a las direcciones de 209.172.38.64 a 209.172.38.95.
- Octavo rango: **216.46.2.48/29** con la máscara de subred **255.255.255.248**, correspondiente a las direcciones de 216.46.2.48 a 216.46.2.55.
- Noveno rango: **216.46.11.224/27** con la máscara de subred **255.255.255.224**, correspondiente a las direcciones de 216.46.11.224 a 216.46.11.255.

El rango de direcciones IP permitidas de su cortafuegos se ha limitado a nuestros rangos de direcciones IP.

Configurar el acceso a Control Panel mediante LDAP

Ha añadido una conexión LDAP activa a Control Panel (véase Añadir una conexión LDAP en la página 132).

En la pestaña **Conexión LDAP** del módulo **Dashboard de servicios** puede configurar que los usuarios de buzones LDAP (véase el capítulo «Tipos de buzón de correo» en el manual de Control Panel) inicien sesión en Control Panel con los datos de acceso del servicio de directorio.

Nota:

Los usuarios de todas las conexiones LDAP activas pueden iniciar sesión con los datos de acceso del servicio de directorio.

Nota:

Si se emplean datos de acceso del servicio de directorio para el acceso a Control Panel, los usuarios no podrán cambiar su contraseña en Control Panel (véase el capítulo "Cambiar la contraseña" del manual de Control Panel).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyos usuarios desee activar la autenticación con datos de acceso del servicio de directorio.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.

5. Accione el interruptor **Acceso a Control Panel** de **Autenticación en Control Panel con datos de acceso de LDAP**.

   Bajo el interruptor se muestra el campo adicional **Filtro de LDAP**.

Figura 105: Filtro de LDAP para el inicio de sesión en Control Panel

6. Introduzca un filtro para los usuarios y grupos del servicio de directorio que deban iniciar sesión en Control Panel con sus datos de acceso del servicio de directorio en el campo **Filtro de LDAP**.

> **Nota:**
>
> El filtro de LDAP **proxyaddresses=*** está establecido por defecto. Con esta expresión se seleccionan todos los usuarios de un Active Directory de Microsoft.

7. Si desea comprobar si es posible iniciar sesión en Control Panel con los datos de acceso del servicio de directorio, proceda del siguiente modo.

   a) Haga clic en **Comprobar acceso**.

   Se abre la pantalla **Prueba de acceso mediante LDAP**.

Figura 106: Prueba de acceso mediante LDAP

   b) En el campo **Usuario**, introduzca la dirección de correo electrónico del usuario para el cual desee intentar iniciar sesión en Control Panel.

   c) Introduzca la contraseña del usuario del servicio de directorio en el campo **Contraseña**.

   d) Haga clic en **Confirmar**.

   La prueba se efectúa y el resultado se muestra en la parte inferior de la ventana.

   e) Haga clic en **Cerrar**.

   La ventana se cierra.

8. Haga clic en **Aplicar cambios**.

   Los cambios se guardan.

   > **Nota:**
   >
   > La sincronización de los datos del servicio de directorio se efectúa una vez cada hora. Por tal motivo, es posible que el resultado de sus ajustes no se haga efectivo hasta al cabo de dos horas.

Se ha configurado el acceso a Control Panel con los datos de acceso del servicio de directorio.

> **Importante:**
>
> El acceso mediante LDAP solo está disponible para buzones de correo LDAP (véase el capítulo "Tipos de buzón de correo" en el manual de Control Panel). Los usuarios con buzones de correo de un entorno secundario podrán seguir iniciando sesión con sus datos de acceso administrados en Control Panel.

Editar una conexión LDAP

Ha añadido una conexión LDAP a Control Panel (véase Añadir una conexión LDAP en la página 132).

En la pestaña **Conexión LDAP** (véase Conexión mediante LDAP en la página 129) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede editar una conexión LDAP existente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuya conexión LDAP desee editar.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.

5. En **Conexiones LDAP disponibles**, seleccione la conexión LDAP que desee editar y haga clic en la flecha de menú junto a la conexión LDAP.

Figura 107: Abrir el menú

Se abre un menú.

Figura 108: Menú

6. Haga clic en **Editar registro**.

Se muestra la configuración de la conexión LDAP.

7. Ajuste la configuración como desee (véase Añadir una conexión LDAP en la página 132).
8. Haga clic en **Aplicar cambios**.

Los cambios se guardan.

Nota:

La sincronización de los datos del servicio de directorio se efectúa una vez cada hora. Por tal motivo, es posible que el resultado de los ajustes no se haga efectivo hasta al cabo de dos horas.

Se ha editado una conexión LDAP existente.

Desactivar la conexión mediante LDAP

Ha añadido una conexión LDAP activa a Control Panel (véase Añadir una conexión LDAP en la página 132).

En la pestaña **Conexión LDAP** (véase Conexión mediante LDAP en la página 129) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede desactivar una conexión LDAP existente si no desea seguir sincronizando usuarios y pertenencias a grupos del servicio de directorio en Control Panel. Si los usuarios han utilizado sus datos de acceso del servicio de directorio para iniciar sesión en Control Panel, la contraseña sincronizada por última vez sigue almacenada en Control Panel y los usuarios pueden cambiar su contraseña en Control Panel. Los ajustes se guardarán por si desea volver a activar su conexión mediante LDAP con posterioridad.

Nota:

Una vez desactivada la conexión mediante LDAP, los datos de usuarios de Control Panel dejarán de sincronizarse con el servicio de directorio. Tan pronto como se modifiquen datos en el servicio de directorio, se producirá una divergencia respecto a los datos almacenados en Control Panel. Así, por ejemplo, dejarán de actualizarse automáticamente las contraseñas en Control Panel, de añadirse buzones de correo de nuevos usuarios del servicio de directorio y de eliminarse buzones de correo de usuarios eliminados en el servicio de directorio.

Sin embargo, los buzones de correo de Control Panel cuyos datos se hayan sincronizado mediante LDAP seguirán protegidos por nuestros servicios y seguirán siendo de tipo LDAP (véase el capítulo «Tipos de buzón de correo» en el manual de Control Panel).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuya conexión LDAP desee desactivar.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.

5. En **Conexiones LDAP disponibles**, seleccione la conexión LDAP que desee desactivar y haga clic en la flecha de menú junto a la conexión LDAP.

Figura 109: Abrir el menú

Se abre un menú.

Figura 110: Menú

6. Haga clic en **Editar registro**.

Se muestra la configuración de la conexión LDAP.

7. Accione el interruptor **Activar conexión a LDAP**.

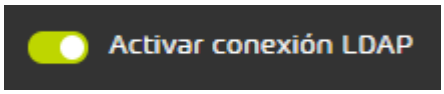


Figura 111: Desactivar la conexión mediante LDAP

El interruptor se pone gris. El botón **Comprobar sincronización mediante LDAP** bajo **Sincronización de grupos y usuarios** se deshabilita.

8. Haga clic en **Aplicar cambios**.

Los ajustes se guardan.

Se ha desactivado una conexión LDAP.

Activar la conexión mediante LDAP

Ha desactivado una conexión LDAP existente (véase Desactivar la conexión mediante LDAP en la página 148).

En la pestaña **Conexión LDAP** (véase Conexión mediante LDAP en la página 129) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede activar una conexión LDAP existente para establecer una conexión entre Control Panel y un servicio de directorio. Después de activar la conexión LDAP, volverá a ser posible sincronizar los usuarios y sus pertenencias a grupos del servicio de directorio en Control Panel (véase Añadir una conexión LDAP en la página 132), así como utilizar los datos de acceso del servicio de directorio para iniciar sesión en Control Panel (véase Configurar el acceso a Control Panel mediante LDAP en la página 142).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuya conexión LDAP desee activar.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.
5. Accione el interruptor **Activar conexión a LDAP**.

Figura 112: Desactivar la conexión mediante LDAP

El interruptor se pone verde. El botón **Comprobar sincronización mediante LDAP** bajo **Sincronización de grupos y usuarios** se habilita.

6. Haga clic en **Aplicar cambios**.

   Los ajustes se guardan.

   > **Nota:**
   >
   > La sincronización de los datos del servicio de directorio se efectúa una vez cada hora. Por tal motivo, es posible que el resultado de los ajustes no se haga efectivo hasta al cabo de dos horas.

Se ha activado una conexión LDAP existente.

Eliminar una conexión LDAP

Ha añadido una conexión LDAP a Control Panel (véase Añadir una conexión LDAP en la página 132).

En la pestaña **Conexión LDAP** (véase Conexión mediante LDAP en la página 129) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede eliminar una conexión LDAP existente si deja de ser necesaria. Después de eliminarla, los usuarios cuyos buzones de correo se hayan sincronizado con el servicio de directorio seguirán existiendo en Control Panel como buzones LDAP. Pero los buzones de correo dejarán de sincronizarse. Si los usuarios han utilizado sus datos de acceso del servicio de directorio para iniciar sesión en Control Panel, la contraseña sincronizada por última vez sigue almacenada en Control Panel y los usuarios pueden cambiar su contraseña en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuya conexión LDAP desee eliminar.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Conexión LDAP**.

5. En **Conexiones LDAP disponibles**, seleccione la conexión LDAP que desee eliminar y haga clic en la flecha de menú junto a la conexión LDAP.

Figura 113: Abrir el menú

Se abre un menú.

Figura 114: Menú

6. Haga clic en **Eliminar**.

Se muestra un mensaje de advertencia.

7. Haga clic en **Confirmar**.

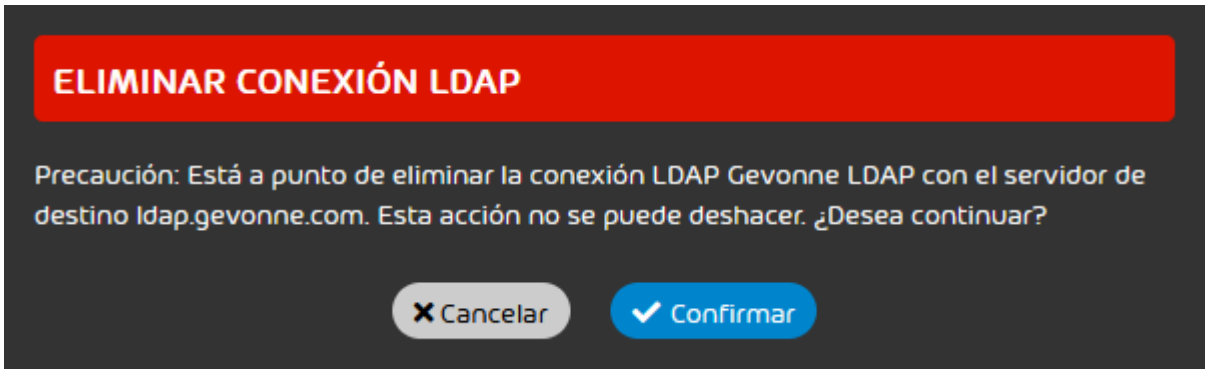


Figura 115: Confirmar la eliminación

La conexión LDAP se elimina de la lista bajo **Conexiones LDAP disponibles**.

Se ha eliminado una conexión LDAP de Control Panel.

Ajustar zona horaria e idioma por defecto

En el módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede definir una zona horaria, un idioma, un formato de fecha y un formato de hora por defecto para un cliente. Los ajustes se aplican a la visualización en Control Panel y a los correos automáticos de Control Panel.

Nota:

Los valores por defecto se transmiten a todos los usuarios subordinados. Cuando un usuario del cliente ajuste su propia configuración, los valores por defecto se sobrescribirán para el usuario. Los usuarios pueden modificar los ajustes en su configuración de usuario (véase el capítulo "Cambiar la zona horaria y el idioma" en el manual de Control Panel).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente para el cual desee definir valores por defecto.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Zona horaria e idioma por defecto**.

   En la sección **Zona horaria e idioma** se muestra la configuración de la zona horaria, del idioma, del formato de fecha y del formato de hora.

Figura 116: Zona horaria e idioma

5. Seleccione una zona horaria en el menú desplegable **Zona horaria**.

   Nota:

   La zona horaria determina el formato de número en Control Panel y en los correos automáticos de Control Panel.

6. Seleccione un idioma en el menú desplegable **Idioma**.

7. Seleccione un formato de fecha en el menú desplegable **Formato de fecha**.

> **Nota:**
>
> El formato de fecha determina el orden en el que se muestran los datos que estén disponibles para una fecha. Si no hay informaciones disponibles para todos los datos, no se muestran los datos que faltan.

8. Seleccione un formato de hora en el menú desplegable **Formato de hora**.

> **Nota:**
>
> El formato de hora determina el orden en el que se muestran los datos que estén disponibles para una hora. Si no hay informaciones disponibles para todos los datos, no se muestran los datos que faltan.

9. Haga clic en **Guardar**.

Los cambios se guardan.

Se han definido una zona horaria, un idioma, un formato de fecha y un formato de hora por defecto para un cliente.

Condiciones Generales

En la pestaña **Condiciones Generales** del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106), los administradores a nivel de partner pueden definir un contrato de licencia de usuario final y un contrato de tratamiento de datos para solicitar su aceptación por parte de los usuarios de sus clientes.

Una vez publicado el contrato de licencia de usuario final y el contrato de tratamiento de datos de un partner, dichos contratos se muestran a los usuarios de los clientes la siguiente vez que inicien sesión en Control Panel. Para poder acceder a Control Panel, los usuarios deben aceptar el contrato

de licencia de usuario final. Los administradores pueden además aceptar el contrato de tratamiento de datos. Por defecto, la aceptación del contrato de tratamiento de datos es opcional. Sin embargo, los administradores a nivel de partner pueden establecer que sea obligatorio aceptar el contrato de tratamiento de datos.

Para poder definir condiciones de contratación, los administradores a nivel de partner deben habilitar previamente la función Condiciones Generales (véase Habilitar la función Condiciones Generales en la página 157). Una vez hecho esto se habilitan los ajustes relativos a las condiciones de contratación del partner. A continuación, los administradores pueden hacer que aceptar el contrato de tratamiento de datos sea obligatorio para los administradores de sus clientes (véase Hacer obligatoria para el contrato de tratamiento de datos en la página 158), así como crear y publicar un contrato de licencia de usuario final y un contrato de tratamiento de datos (véase Crear un contrato de licencia de usuario final y un contrato de tratamiento de datos en la página 159). Los contratos pueden crearse en todos los idiomas de Control Panel. Si se modifican las condiciones de contrato de un partner, sus administradores pueden publicar una nueva versión de los contratos.

Nota:

Las versiones antiguas de los contratos no se almacenan en Control Panel. En la pestaña **Condiciones Generales** del módulo **Dashboard de servicios** se muestra solo la versión actual de los contratos.

Los administradores a nivel de partner pueden exportar la versión actual del contrato de licencia de usuario final y del contrato de tratamiento de datos de Control Panel (véase Exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos en la página 168) para poder acceder a dichos contratos en el futuro. Si un partner no desea seguir utilizando la función Condiciones Generales en Control Panel, los administradores del partner pueden desactivarla (véase Desactivar la función Condiciones Generales en la página 169).

Los cambios relativos a la función Condiciones Generales se registran en el módulo **Informes y conformidad** > **Registro de auditorías 2.0** (véase el capítulo "Registro de auditoría 2.0" del manual de Control Panel).

Habilitar la función Condiciones Generales

Si desea solicitar la aceptación de un contrato de licencia de usuario final y un contrato de tratamiento de datos a los usuarios de sus clientes, debe habilitar previamente las condiciones de contratación para el partner en la pestaña **Condiciones Generales** (véase Condiciones Generales en la página 155) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner para el cual desee habilitar la función Condiciones Generales.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Condiciones Generales**.
5. Accione el interruptor **Habilitar las condiciones generales**.

Figura 117: Habilitar la función Condiciones Generales

El interruptor se pone verde. Se habilitan los ajustes adicionales de la pestaña **Condiciones Generales**.

> **Nota:**
>
> Si en la pestaña **Condiciones Generales** ya se han realizado ajustes con anterioridad, los ajustes vuelven a hacerse efectivos.

La función Condiciones Generales se ha habilitado para un partner.

A continuación puede hacer que los administradores de sus clientes deban aceptar el contrato de tratamiento de datos (véase Hacer obligatoria para el contrato de tratamiento de datos en

la página 158) así como crear y publicar un contrato de licencia de usuario final y un contrato de tratamiento de datos (véase Crear un contrato de licencia de usuario final y un contrato de tratamiento de datos en la página 159).

Hacer obligatoria para el contrato de tratamiento de datos

Ha habilitado la función Condiciones Generales (véase Habilitar la función Condiciones Generales en la página 157).

Si publica usted un contrato de licencia de usuario final y un contrato de tratamiento de datos en la pestaña **Condiciones Generales** (véase Condiciones Generales en la página 155) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106), los usuarios de sus clientes deberán aceptar el contrato de licencia de usuario final la próxima vez que inicien sesión en Control Panel para poder acceder al mismo. Los administradores de sus clientes pueden además aceptar el contrato de tratamiento de datos. Por defecto, la aceptación del contrato de tratamiento de datos es opcional. Sin embargo, puede disponer que sea obligatorio aceptar el contrato de tratamiento de datos para los administradores de sus clientes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner para el cual desee habilitar la función Condiciones Generales.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Condiciones Generales**.
5. Accione el interruptor **Acuerdo de tratamiento de datos obligatorio**.

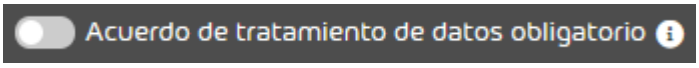


Figura 118: Hacer obligatoria la aceptación del contrato de tratamiento de datos

El interruptor se pone verde. Si se han publicado un contrato de licencia de usuario final y un contrato de tratamiento de datos para un partner, aparte del contrato de licencia de usuario final, los administradores de los clientes subordinados a dicho partner deberán aceptar el contrato de tratamiento de datos para poder acceder a Control Panel.

La aceptación del contrato de tratamiento de datos se ha hecho obligatoria.

A continuación puede crear y publicar un contrato de licencia de usuario final y un contrato de tratamiento de datos (véase Crear un contrato de licencia de usuario final y un contrato de tratamiento de datos en la página 159).

Crear un contrato de licencia de usuario final y un contrato de tratamiento de datos

En la pestaña **Condiciones Generales** (véase Condiciones Generales en la página 155) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede crear y publicar un contrato de licencia de usuario final y un contrato de tratamiento de datos. Dichos contratos se mostrarán a los usuarios de sus clientes la próxima vez que inicien sesión en Control Panel. Para poder acceder a Control Panel, los usuarios deberçam aceptar el contrato de licencia de usuario final una vez. Los administradores de sus clientes pueden además aceptar el contrato de tratamiento de datos. Si cambian las condiciones de contratación, puede crear y publicar una nueva versión de los contratos. En cuanto se publique una versión nueva, los usuarios deberán volver a aceptar las condiciones de contratación.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner para el cual desee habilitar la función Condiciones Generales.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Condiciones Generales**.

5. En **Contenido del contrato de licencia de usuario final y acuerdo de tratamiento de datos**, haga clic en **Crear nueva versión**.

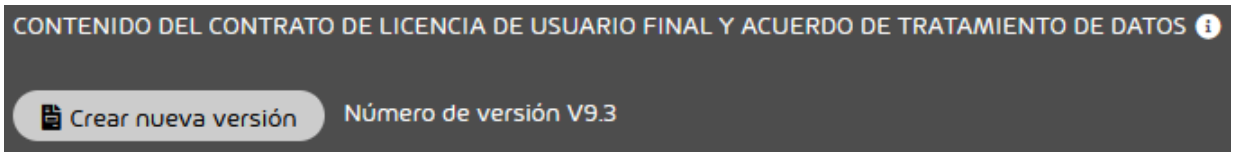


Figura 119: Crear una nueva versión

Nota:

Si ya hay disponible una versión, el número de versión actual se muestra a la derecha junto al botón **Crear nueva versión**.

Se muestra una ventana de confirmación.

6. Haga clic en **Crear nueva versión**.

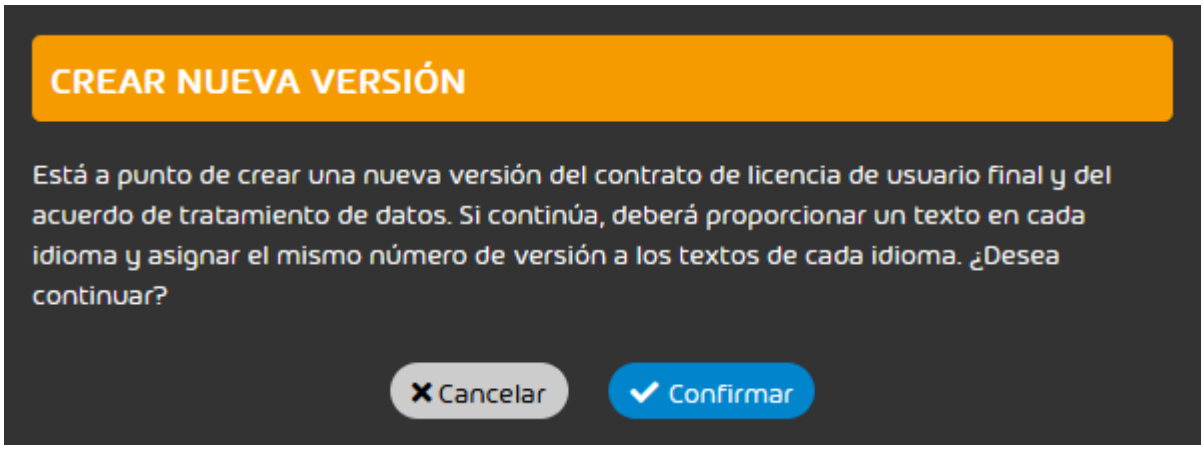


Figura 120: Confirmar la creación de una versión nueva

Junto al número de versión actual se muestra un campo para introducir el nuevo número de versión.

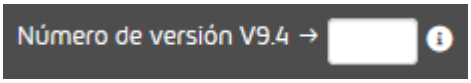


Figura 121: Campo para el nuevo número de versión

7. Introduzca el nuevo número de versión en el campo de números de versión.

Nota:

No se aceptan números de versión que ya se hayan utilizado anteriormente.

Los números de versión pueden contener los siguientes caracteres:

- Puntos
- Letras
- Cifras

Los puntos no están permitidos al principio ni al final. No se permite introducir dos o más puntos seguidos.

8. En el menú desplegable **Idioma**, seleccione el idioma en el que desee crear un texto.

Figura 122: Seleccionar el idioma

Nota:

Los textos del contrato de licencia de usuario final y del contrato de tratamiento de datos pueden redactarse en todos los idiomas de Control Panel. Los contratos se muestran a todos los usuarios de los clientes subordinados, independientemente de si se dispone o no del texto en el idioma de interfaz configurado por cada usuario.

El editor de texto se muestra vacío.

Figura 123: Editor de textos

Nota:

En la parte baja del editor de texto se muestran los idiomas de la interfaz de Control Panel. Los idiomas para los que ya se ha publicado un texto en la versión actual se muestran sobre un fondo blanco. Los idiomas que aún no se han utilizado están bloqueados y se muestran en gris.

9. Opcional: Si desea copiar el texto de la versión actual al editor de texto, haga clic en **Restaurar el contenido de la versión anterior**.

Si se ha publicado un texto en el idioma seleccionado para la versión actual, dicho texto se muestra en el editor de texto.

10. Opcional: Si desea importar un texto de su sistema de archivos al editor de texto, siga los pasos indicados a continuación.

a) Haga clic en **Importar texto**.

Se abre una vista avanzada.

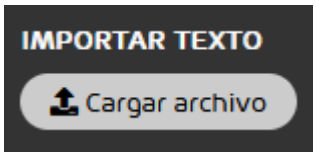


Figura 124: Vista avanzada

b) Haga clic en **Cargar archivo**.

Se abre una ventana de selección de archivos.

c) Seleccione el archivo cuyo contenido desee importar.

> **Nota:**
>
> Solo es posible importar archivos con la extensión .txt.

Control Panel lee el archivo y prepara su contenido para la importación.

d) Haga clic en **Importar**.

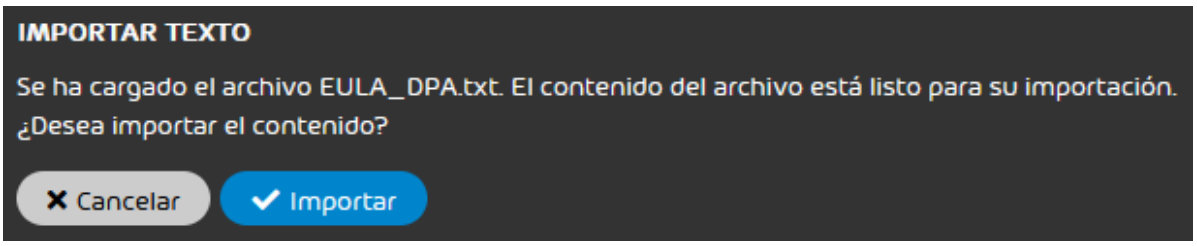


Figura 125: Confirmar la importación

El texto del archivo importado se muestra en el editor de texto.

11. Opcional: Introduzca el texto del contrato de licencia de usuario final y del contrato de tratamiento de datos en el editor de textos o modifique el texto disponible a su gusto.

> **Nota:**
>
> No es posible dar formato al texto.

12. Una vez el texto esté preparado para su publicación, haga clic en el botón **Publicar**, situado bajo el editor de texto.

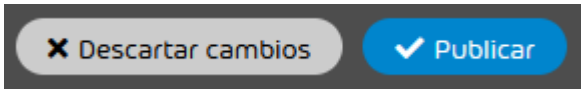


Figura 126: Publicar un texto

Se muestra una ventana de confirmación.

13. Haga clic en **Confirmar**.

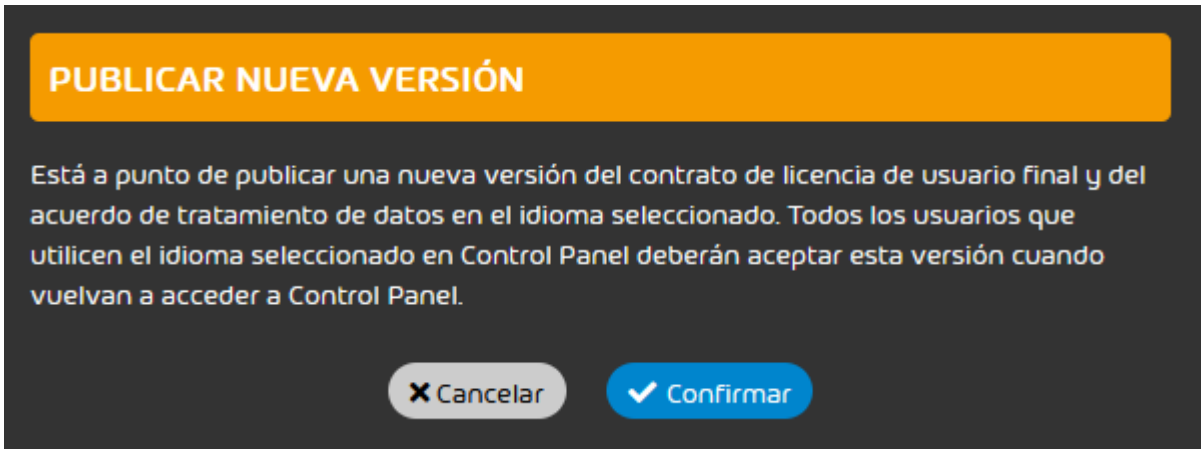


Figura 127: Confirmar la publicación

El texto se publica en el idioma seleccionado. La nueva versión del contrato de licencia de usuario final y del contrato de tratamiento de datos se mostrará a todos los usuarios de los clientes subordinados la próxima vez que éstos inicien sesión en Control Panel. Para poder acceder a Control Panel, los usuarios deben aceptar el contrato de licencia de usuario final una vez. Los administradores de los clientes subordinados pueden aceptar además el contrato de tratamiento de datos.

14. Repita los pasos 8 en la página 163 a 13 en la página 167 para todos los idiomas en los que desee añadir textos de contratos de licencia de usuario final y de tratamiento de datos.

Se ha creado y publicado una nueva versión del contrato de licencia de usuario final y del contrato de tratamiento de datos.

A continuación puede exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos en su versión actual (véase Exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos en la página 168).

Exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos

Ha creado y publicado un contrato de licencia de usuario final y un contrato de tratamiento de datos (véase Crear un contrato de licencia de usuario final y un contrato de tratamiento de datos en la página 159).

En la pestaña **Condiciones Generales** (véase Condiciones Generales en la página 155) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos en sus versiones actuales. Esto le permite guardar los contratos fuera de Control Panel para acceder a ellos con posterioridad.

Nota:

Las versiones antiguas de los contratos no se almacenan en Control Panel. En la pestaña **Condiciones Generales** del módulo **Dashboard de servicios** se muestra solo la versión actual de los contratos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner para el cual desee habilitar la función Condiciones Generales.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Condiciones Generales**.

5. En el menú desplegable **Idioma**, seleccione el idioma en que desee exportar los textos.

Figura 128: Seleccionar el idioma

En el editor de texto se muestran los textos del contrato de licencia de usuario final y del contrato de tratamiento de datos en el idioma seleccionado.

6. Haga clic en el botón **Exportar texto**, situado encima del editor de texto.

Figura 129: Exportar el texto

Los textos del contrato de licencia de usuario final y del contrato de tratamiento de datos se exportan en formato .txt en el idioma seleccionado y se facilitan para su descarga.

7. Guarde el archivo importado en su sistema de archivos.
8. Repita los pasos 7 en la página 169 a para todos los idiomas cuyos textos desee exportar.

Los textos de la versión actual del contrato de licencia de usuario final y del contrato de tratamiento de datos se han exportado.

Desactivar la función Condiciones Generales

Ha habilitado la función Condiciones Generales (véase Habilitar la función Condiciones Generales en la página 157).

En la pestaña **Condiciones Generales** (véase Condiciones Generales en la página 155) del módulo **Dashboard de servicios** (véase Acerca del Dashboard de servicios en la página 106) puede desactivar la función Condiciones Generales. Al desactivar la función Condiciones Generales se bloqueará el resto de ajustes de la pestaña **Condiciones Generales**. Los usuarios de sus clientes ya no verán ningún contrato de licencia de usuario final ni ningún contrato de tratamiento de datos al iniciar sesión en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el partner para el cual desee habilitar la función Condiciones Generales.
3. Vaya a **Dashboard de servicios**.
4. Seleccione la pestaña **Condiciones Generales**.
5. Accione el interruptor **Habilitar las condiciones generales**.

Figura 130: Desactivar la función Condiciones Generales

El interruptor se pone gris. Los ajustes adicionales de la pestaña **Condiciones Generales** se bloquean. Los usuarios de los clientes subordinados ya no verán ningún contrato de licencia de usuario final ni ningún contrato de tratamiento de datos al iniciar sesión en Control Panel.

Nota:

El resto de ajustes de la pestaña **Condiciones Generales** quedan guardados por si la función Condiciones Generales vuelve a habilitarse más tarde (véase Habilitar la función Condiciones Generales en la página 157).

Se ha desactivado la función Condiciones Generales.

A continuación puede volver a habilitar la función Condiciones Generales (véase Habilitar la función Condiciones Generales en la página 157).

Informes y conformidad

Informes y conformidad

El módulo **Informes y conformidad** reúne información sobre el tráfico de correo, sobre ataques contra los usuarios de un dominio y sobre las acciones efectuadas en Control Panel.

En el submódulo **Estadísticas de correo electrónico**, los usuarios pueden consultar estadísticas relativas a su propio tráfico de correo (véase Estadística de correos en la página 172). Allí, los administradores a nivel de cliente y los usuarios con el rol **Service Desk** o **Reporting** (véase Roles en la página 53) pueden también ver estadísticas del tráfico de correo de su dominio o de un usuario de su dominio.

El submódulo **Threat Live Report** está disponible para administradores a nivel de cliente y usuarios con el rol **Service Desk** o **Reporting** si el cliente tiene activado el servicio Advanced Threat Protection. Este submódulo contiene información relativa a ataques perpetrados contra usuarios del dominio (véase Sobre Threat Live Report en la página 188).

El submódulo **Registro de auditorías 2.0** está disponible para administradores a nivel de cliente y de partner. En este submódulo se registran las acciones efectuadas por los usuarios de Control Panel (véase Registro de auditoría 2.0 en la página 203).

Estadística de correos

Los administradores a nivel de cliente pueden ver las estadísticas de su propio tráfico de correo electrónico, del tráfico de correo electrónico de su dominio o de un usuario de su dominio en el módulo **Estadísticas de correo electrónico**.

Los administradores pueden seleccionar el rango de fechas y la dirección del tráfico de correo que incluir en las estadísticas del módulo (véase Filtrar la estadística de correos en la página 173). Las estadísticas se muestran en dos diagramas. El primer diagrama muestra la distribución de los correos por categorías de correo (véase Correos por tipo en la página 176). El segundo diagrama muestra la distribución temporal de los correos (véase Correos por fecha en la página 177). Los datos del

segundo diagrama pueden además exportarse en formato CSV (véase Exportar estadísticas de correos en formato CSV en la página 179). Los administradores a nivel de cliente pueden además ver la distribución de los correos de los usuarios de un dominio por categorías de correo de Control Panel (véase Correos por usuario en la página 180).

También es posible recopilar mensualmente las estadísticas de correo en un informe (véase Informe mensual en la página 181). Los administradores a nivel de cliente pueden determinar los buzones de correo a los que enviar el informe mensual (véase Añadir un destinatario en la página 182). Además de añadir destinatarios uno por uno, los administradores pueden importar listas de destinatarios en formato CSV (véase Importar destinatarios desde archivos CSV en la página 184). Además, los administradores pueden eliminar destinatarios previos (véase Eliminar destinatarios en la página 187).

Filtrar la estadística de correos

En el módulo **Estadísticas de correo electrónico** se muestran estadísticas sobre su tráfico de correo electrónico (véanse Correos por tipo en la página 176 y Correos por fecha en la página 177).Los administradores a nivel de cliente y los clientes con el rol **Service Desk** o **Reporting** pueden ver los datos del dominio de un cliente además de los suyos propios. Para los dominios se muestra también la distribución de los correos de sus usuarios por categorías de correo de Control Panel (véase Correos por usuario en la página 180). En el módulo **Estadísticas de correo electrónico**, puede filtrar los datos por rango de fechas y dirección de tráfico de correo.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Opcional: Si, en lugar de sus propios datos, desea ver los datos de un dominio o de un usuario de un dominio, seleccione dicho dominio o usuario en la selección de ámbitos.
3. Vaya a **Informes y conformidad** > **Estadísticas de correo electrónico**.

4. Haga clic en el rango de fechas.

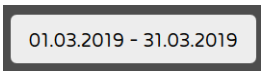


Figura 131: Hacer clic en el rango de fechas

Se muestra un calendario.

5. **Importante:**

   Como máximo, es posible elegir datos de los últimos 3 meses.

Seleccione un rango de fechas.

Figura 132: Seleccionar un periodo

En el módulo **Estadísticas de correo electrónico** se muestran solo datos de correos del ámbito de correos seleccionado.

6. Opcional: En el menú desplegable **Dirección**, seleccione la dirección de los correos a incluir en las estadísticas. Puede elegir entre las siguientes opciones:

   - **Ambas**: Los correos entrantes y salientes se incluyen en las estadísticas.
   - **Entrante**: Solo los correos entrantes se incluyen en las estadísticas.
   - **Saliente**: Solo los correos salientes se incluyen en las estadísticas.

Figura 133: Seleccionar la dirección

En el módulo **Estadísticas de correo electrónico** solo se muestran datos de correos con la dirección seleccionada.

Los datos del módulo **Estadísticas de correo electrónico** se filtran por rango de fechas y dirección de tráfico de correo.

Correos por tipo

El diagrama **Correos por tipo** del módulo **Informes y conformidad** > **Estadísticas de correo electrónico** muestra cómo se distribuyen los correos de un usuario o dominio por categorías de correo en Control Panel (véase Categorías de correo electrónico en la página 90).

Nota:

Los administradores a nivel de cliente y los usuarios con el rol **Service Desk** o **Reporting** (véase Roles en la página 53) también pueden ver los datos de un dominio o de un usuario de un dominio en lugar de sus propios datos. Los datos mostrados pueden filtrarse por rango de fechas y dirección de tráfico de correo (véase Filtrar la estadística de correos en la página 173).

El diagrama muestra el total de correos recibidos y/o enviados dentro del rango de fechas seleccionado. El diagrama también muestra el número y el porcentaje de correos electrónicos que corresponden a cada una de las categorías.

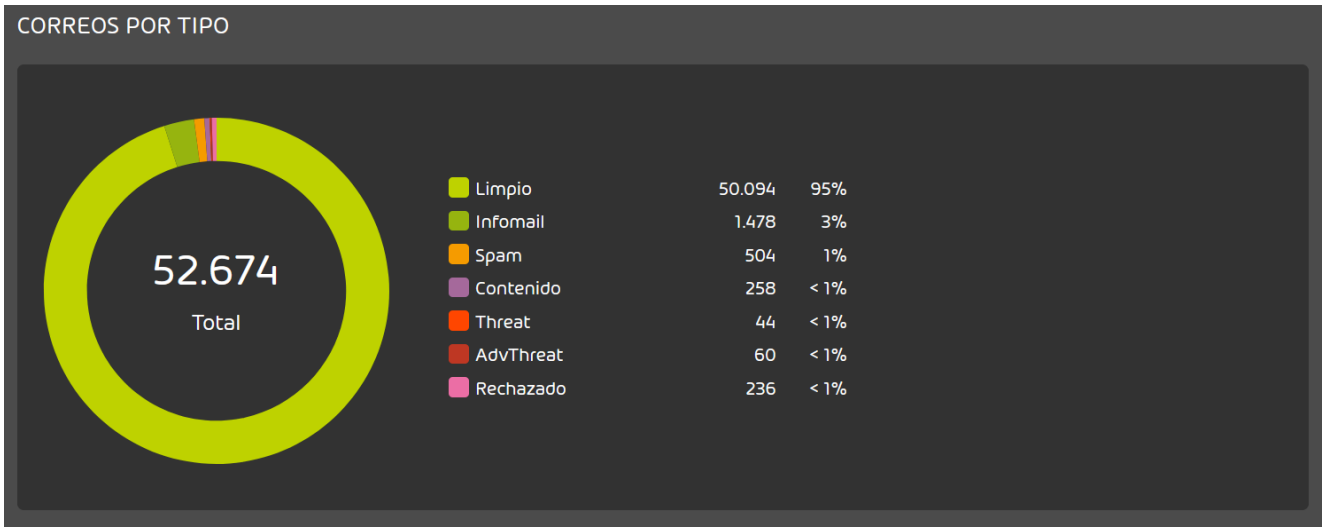


Figura 134: Correos por tipo

Correos por fecha

El diagrama **Correos por fecha** muestra un resumen de todos los correos electrónicos entrantes y/o salientes en el periodo de tiempo seleccionado. En la estadística se muestra la cantidad de correos por categoría en cifras absolutas.

Nota:

Los administradores a nivel de cliente y los usuarios con el rol **Service Desk** o **Reporting** (véase Roles en la página 53) también pueden ver los datos de un dominio o de un usuario de un dominio en lugar de sus propios datos. Los datos mostrados pueden filtrarse por rango de fechas y dirección de tráfico de correo (véase Filtrar la estadística de correos en la página 173).

El diagrama muestra la cantidad de correos recibidos y/o enviados en diversas fechas dentro del rango de fechas seleccionado. El diagrama está subdividido en categorías de correo electrónico (véase Categorías de correo electrónico en la página 90), mostradas en colores distintos.

Al colocar el puntero del ratón sobre un punto del diagrama, se muestra un resumen de correos recibidos y/o entregados por categoría en la fecha más próxima al puntero. Además, se muestra una línea vertical relativa a la fecha en la que se disponen los puntos correspondientes a cada categoría de correo. Al colocar el puntero del ratón sobre uno de esos puntos se muestra la cantidad de correos en dicha categoría.

También es posible exportar datos del diagrama en formato CSV (véase Exportar estadísticas de correos en formato CSV en la página 179).

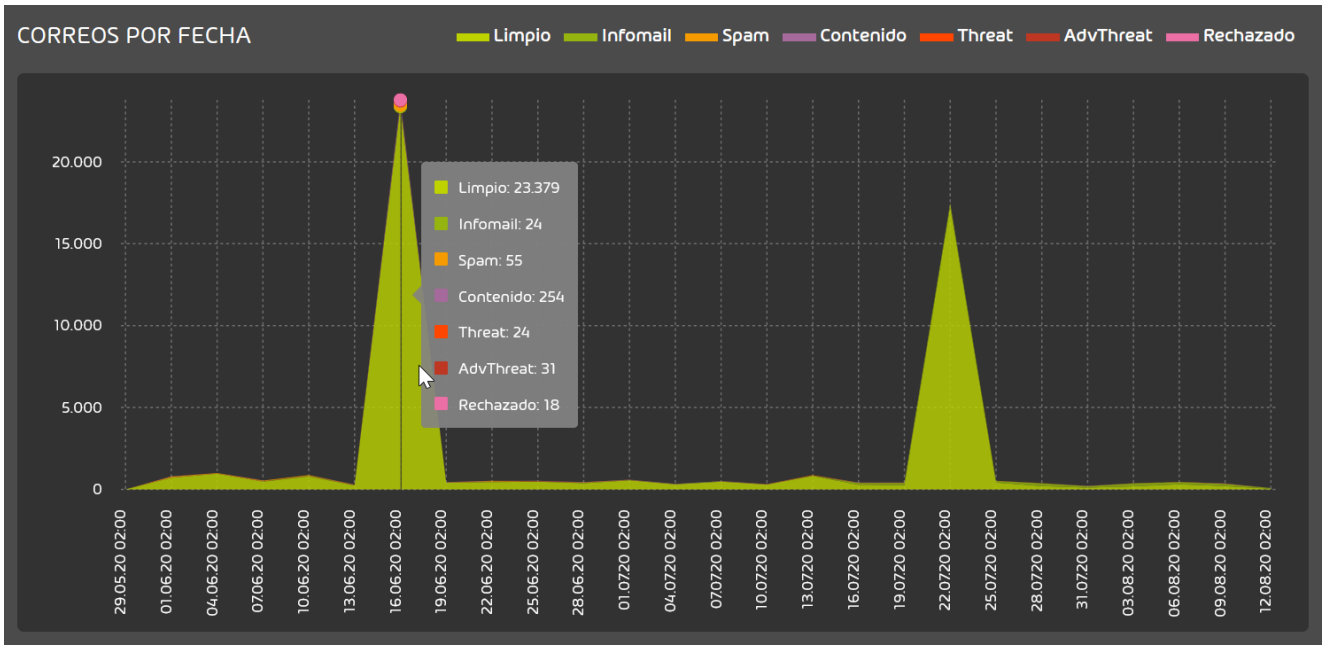


Figura 135: Correos por fecha

Exportar estadísticas de correos en formato CSV

El módulo **Estadísticas de correo electrónico** contiene un diagrama que muestra la distribución temporal de los correos (véase Correos por fecha en la página 177). Puede exportar los datos de este diagrama en formato CSV. Los administradores a nivel de cliente y los usuarios con el rol **Service Desk** o **Reporting** (véase Roles en la página 53), pueden exportar, o bien sus propios datos, o bien los datos de su dominio o de un usuario de su dominio.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Opcional: Si, en lugar de sus propios datos, desea exportar los datos de un dominio o usuario de un dominio, seleccione dicho dominio o usuario en la selección de ámbitos.
3. Vaya a **Informes y conformidad** > **Estadísticas de correo electrónico**.

4. Seleccione un rango de fechas y una dirección de tráfico de correo para la estadística (véase Filtrar la estadística de correos en la página 173).

   En la estadística se incluyen únicamente correos del rango de fechas y la dirección de tráfico de correo seleccionados.

5. Haga clic en **Exportar como CSV**.

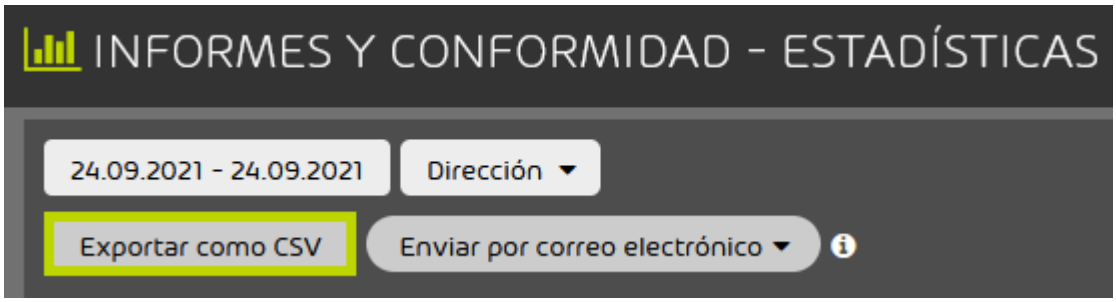


Figura 136: Exportar en formato CSV

   Se prepara para su descarga un archivo CSV con los datos del diagrama de distribución temporal de los correos.

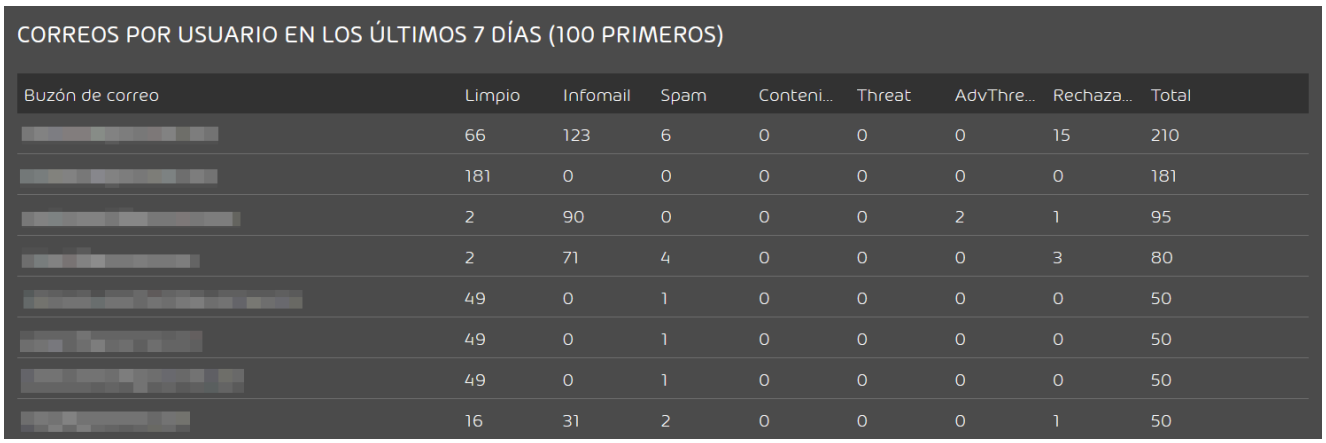
6. Descargue el archivo.

Se han descargado los datos del diagrama de distribución temporal de correos.

Correos por usuario

La estadística **Correos por usuario en los últimos 7 días (100 primeros)** del módulo **Informes y conformidad** > **Estadísticas de correo electrónico** está disponible para administradores a nivel de cliente y para usuarios con el rol **Service Desk** o **Reporting** (véase Roles en la página 53). Esta estadística solo se muestra cuando hay un dominio seleccionado en la selección de ámbitos (véase Filtrar la estadística de correos en la página 173). La estadística puede filtrarse por dirección de correo electrónico (véase Filtrar la estadística de correos en la página 173).

En la estadística se muestran los 100 usuarios del dominio que más correos hayan recibido o entregado durante los últimos 7 días. Los usuarios se ordenan por su número total de correos. También se muestra la cantidad de correos por categoría (véase Categorías de correo electrónico en la página 90).



CORREOS POR USUARIO EN LOS ÚLTIMOS 7 DÍAS (100 PRIMEROS)

Buzón de correo	Limpio	Infomail	Spam	Conteni...	Threat	AdvThre...	Rechaza...	Total
[redacted]	66	123	6	0	0	0	15	210
[redacted]	181	0	0	0	0	0	0	181
[redacted]	2	90	0	0	0	2	1	95
[redacted]	2	71	4	0	0	0	3	80
[redacted]	49	0	1	0	0	0	0	50
[redacted]	49	0	1	0	0	0	0	50
[redacted]	49	0	1	0	0	0	0	50
[redacted]	16	31	2	0	0	0	1	50

Figura 137: correos por usuario

Informe mensual

La estadística de correo de un dominio puede resumirse una vez al mes en un informe. El informe mensual se envía a principios de cada mes a una serie de destinatarios y resume la estadística de correo del mes anterior.

Los administradores a nivel de cliente pueden seleccionar los destinatarios a los que enviar el informe mensual. El informe mensual puede enviarse tanto a usuarios del dominio como a buzones de correo externos. Los administradores pueden, o bien añadir a los destinatarios uno por uno (véase Añadir un destinatario en la página 182) o bien importar una lista de destinatarios en formato CSV (véase Importar destinatarios desde archivos CSV en la página 184). Estos archivos CSV deben cumplir determinados requisitos (véase Archivos CSV para la importación de destinatarios en la página 186). Cuando ya no se necesite algún destinatario, los administradores pueden eliminarlo (véase Eliminar destinatarios en la página 187).

Añadir un destinatario

Una vez al mes se envía, para cada dominio, un informe con estadísticas de correo (véase Estadística de correos en la página 172) del mes pasado a una selección de destinatarios. Puede añadir usuarios de su dominio y buzones de correo individualmente como destinatarios.

Nota:

Los usuarios de Control Panel reciben un informe mensual en el idioma seleccionado en su configuración de usuario (véase el capítulo "Cambiar la zona horaria y el idioma" del manual de Control Panel). Los destinatarios externos reciben el informe mensual en inglés.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyo informe mensual desee definir destinatarios.
3. Vaya a **Informes y conformidad** > **Estadísticas de correo electrónico**.
4. Haga clic en **Enviar por correo electrónico**.

Figura 138: Abrir configuración del informe mensual

Se muestra la configuración del informe mensual.

5. Opcional: Si desea añadir un usuario del dominio como destinatario, proceda del siguiente modo.

   a) Introduzca la dirección de correo del usuario en el campo de búsqueda bajo **Buzones de correo** y pulse "Intro".

   Los resultados de la búsqueda se muestran en la lista bajo el campo de búsqueda.

Figura 139: Resultado de la búsqueda

   b) Haga clic en la lista sobre la dirección de correo del usuario.

   La dirección de correo se añade a la lista de destinatarios.

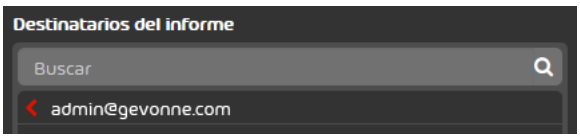


Figura 140: Lista de destinatarios

6. Opcional: Si desea añadir un buzón de correo externo como destinatario, proceda del siguiente modo.

   a) Introduzca la dirección de correo electrónico externa en el campo **Buzón externo**.

   El botón **Añadir** se habilita.

   b) Haga clic en **Añadir**.

Figura 141: Añadir un buzón de correo externo

   La dirección de correo externa se añade a la lista de destinatarios.

7. Haga clic en **Aplicar cambios**.

   Los cambios se aplican.

Se han definido destinatarios individuales para el informe mensual.

Importar destinatarios desde archivos CSV

Una vez al mes se envía, para cada dominio, un informe con estadísticas de correo (véase Estadística de correos en la página 172) del mes pasado a una selección de destinatarios. Puede importar nuevos destinatarios para el informe mensual desde archivos CSV. El archivo CSV puede contener tanto usuarios del dominio como buzones de correo externos.

Nota:

Los usuarios de Control Panel reciben un informe mensual en el idioma seleccionado en su configuración de usuario (véase el capítulo "Cambiar la zona horaria y el idioma" del manual de Control Panel). Los destinatarios externos reciben el informe mensual en inglés.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyo informe mensual desee definir destinatarios.
3. Vaya a **Informes y conformidad** > **Estadísticas de correo electrónico**.
4. Haga clic en **Enviar por correo electrónico**.

Figura 142: Abrir configuración del informe mensual

Se muestra la configuración del informe mensual.

5. Haga clic en **Importar lista desde un archivo CSV**.

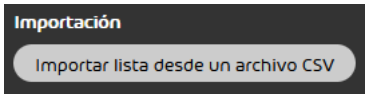


Figura 143: Importar listas desde archivos CSV

Se abre una ventana de selección de archivos.

6. **Importante:**

   Para que un archivo CSV externo pueda importarse correctamente en Control Panel, éste deberá respetar ciertas reglas de formato, estructura interna y sintaxis (véase Archivos CSV para la importación de destinatarios en la página 186).

   Seleccione el archivo CSV deseado.

   Las direcciones de correo electrónico del archivo CSV se añaden a la lista de destinatarios.

Se han importado destinatarios para el informe mensual desde un archivo CSV.

Archivos CSV para la importación de destinatarios

Es posible importar una lista de destinatarios para el informe mensual desde un archivo CSV (véase Importar destinatarios desde archivos CSV en la página 184). Para que un archivo CSV externo con destinatarios del informe mensual pueda importarse correctamente en Control Panel, deberá cumplir reglas respecto a su extensión y su estructura interna. El archivo CSV puede contener direcciones de correo electrónico tanto de usuarios de Control Panel como de buzones de correo externos.

Reglas sobre la extensión

- La extensión del archivo a importar será **.csv**. No se aceptan o extensiones, tales como .txt o .docx.

Reglas sobre columnas y filas

- El archivo CSV contendrá una única columna.
- La primera fila contendrá el nombre de la columna. El nombre de la columna se podrá elegir libremente.
- A partir de la segunda fila, el archivo CSV contendrá una dirección de correo de un destinatario en cada fila.
- Las filas no terminarán en signo de puntuación.

Reglas sobre la estructura de las direcciones de correo

- Las direcciones de correo están bien estructuradas (siguiendo el patrón 'partelocal@nombredehost.dominio-de-nivel-superior').

> **Importante:**
>
> Las direcciones con estructura incorrecta se ignorarán durante la importación.

Regla sobre registros repetidos

- Los registros repetidos no afectan al procesamiento del archivo CVS, pero deberán evitarse.

Eliminar destinatarios

Ha definido destinatarios del informe mensual (véase Añadir un destinatario en la página 182 o Importar destinatarios desde archivos CSV en la página 184).

Si un destinatario no necesita seguir recibiendo el informe mensual, puede eliminarlo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyo informe mensual desee definir destinatarios.
3. Vaya a **Informes y conformidad** > **Estadísticas de correo electrónico**.

4. Haga clic en **Enviar por correo electrónico**.

Figura 144: Abrir configuración del informe mensual

Se muestra la configuración del informe mensual.

5. En la lista de destinatarios, haga clic sobre el destinatario que desee eliminar.

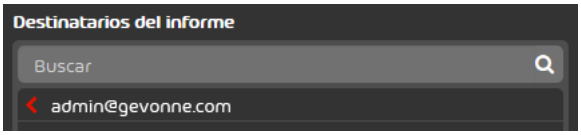


Figura 145: eliminar destinatarios

El destinatario se elimina de la lista.

Se ha eliminado un destinatario del informe mensual.

Threat Live Report

Sobre Threat Live Report

Importante:

Threat Live Report solo está disponible para clientes que han contratado **Advanced Threat Protection**.

Encontrará más información sobre los diagramas directamente en la interfaz. Para consultarla, coloque el puntero del ratón sobre el icono mostrado detrás del nombre de la estadística o diagrama concreto.

Descripción de las estadísticas

Vista general de ataques en vivo

El diagrama **Vista general de ataques en directo** de **Threat Live Report** muestra en tiempo real todos los ataques contra usuarios de Control Panel interceptados por todo el mundo (véase Alternar entre datos globales y de dominio en la página 200). Su origen, destino y tipo de amenaza se muestran en una tabla. En Descripción de los tipos de ataque en la página 195 encontrará una lista de todos los tipos de amenaza.

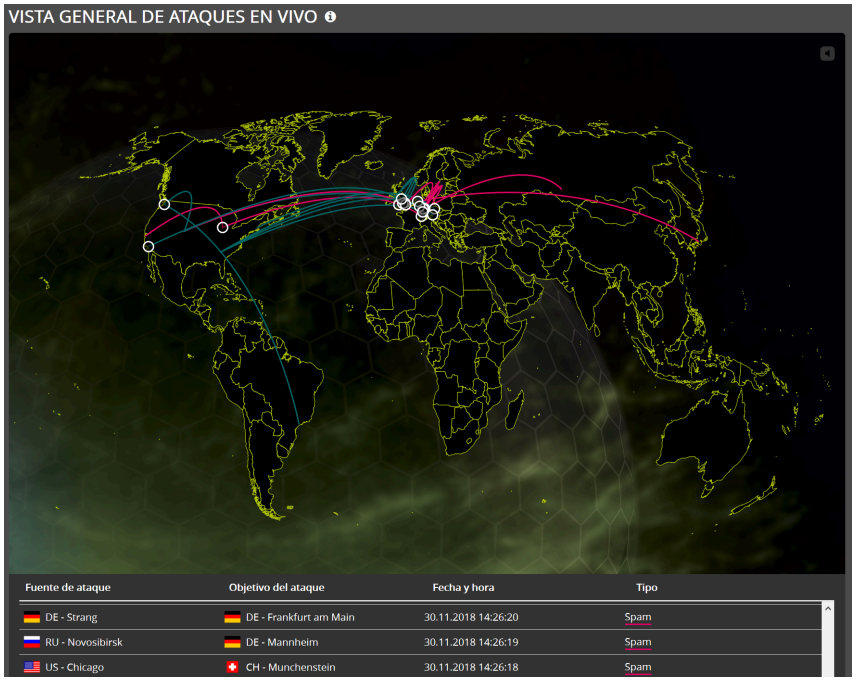


Figura 146: Vista general de ataques en vivo

Intentos de ataque - Tipos de ataque por fecha

La estadística **Tipos de ataque por fecha** de **Threat Live Report** muestra cuántos ataques de cada tipo se produjeron en un momento determinado del periodo seleccionado. Los datos pueden referirse bien al dominio seleccionado actualmente, bien a todos los clientes (véase Alternar entre datos globales y de dominio en la página 200).

Para observar las cifras absolutas de ataques por tipo en un momento determinado, puede pasar el puntero del ratón sobre las líneas verticales. Al posar el puntero sobre un punto correspondiente a un tipo de ataque se muestran solo el diagrama ly los datos sobre la cantidad de ataques correspondientes.

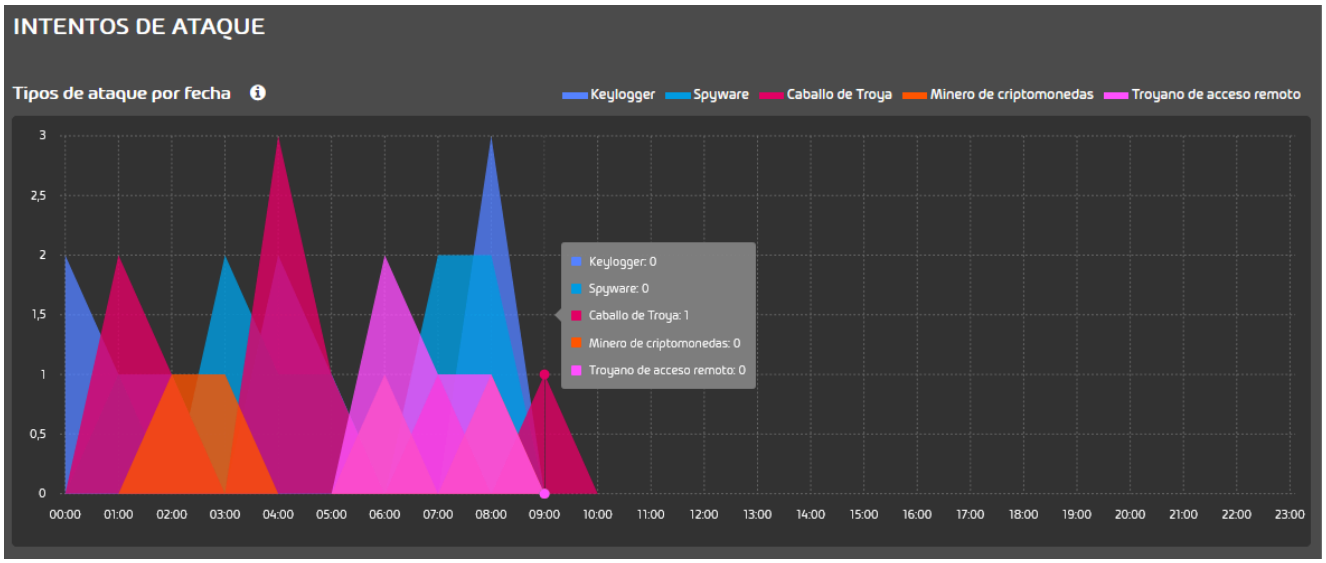


Figura 147: Intentos de ataque - Tipos de ataque por fecha

Estadística de amenazas - Por tipo de ataque

El diagrama **Por tipo de ataque** de **Threat Live Report** muestra la distribución de los ataques por tipo de ataque durante el periodo seleccionado. En el centro se muestra el total de ataques ocurridos durante el periodo seleccionado. Los datos pueden referirse bien al dominio seleccionado actualmente, bien a todos los clientes (véase Alternar entre datos globales y de dominio en la

página 200). Encontrará una descripción de los tipos de ataque en Descripción de los tipos de ataque en la página 195.

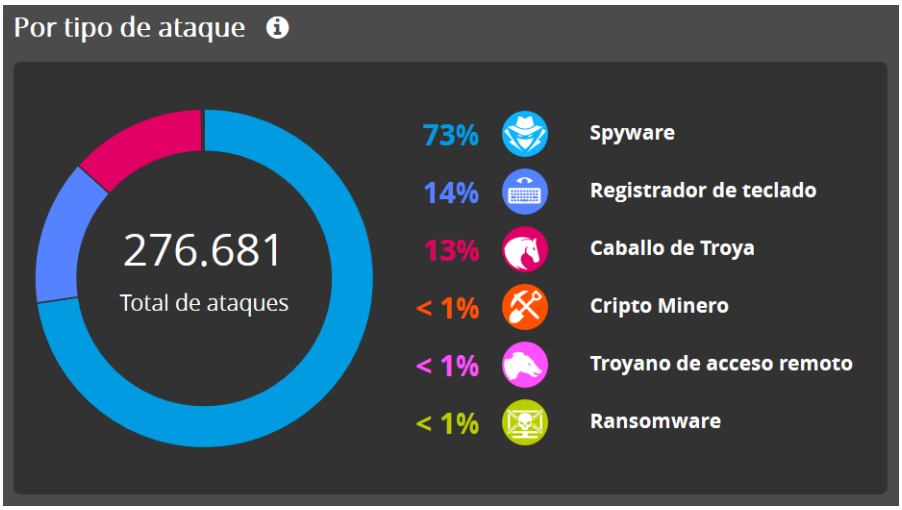


Figura 148: Estadística de amenazas - Por tipo de ataque

Estadística de amenazas - Por vector de ataque

El diagrama **Por vector de ataque** de **Threat Live Report** muestra la distribución de los ataques por vector de ataque durante el periodo seleccionado. En el centro se muestra el total de ataques ocurridos durante el periodo seleccionado. Los datos pueden referirse bien al dominio seleccionado actualmente, bien a todos los clientes (véase Alternar entre datos globales y de dominio en la página 200). En Descripción de los vectores de ataque en la página 198 encontrará una descripción de los vectores de ataque.

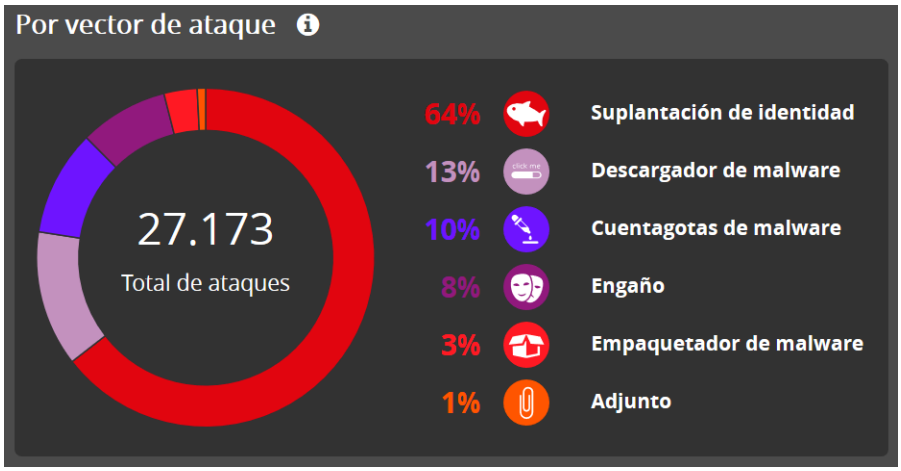


Figura 149: Estadística de amenazas - Por vector de ataque

Intentos de ataque - Vector de ataque por fecha

La estadística **Vectores de ataque por fecha** de **Threat Live Report** muestra cuántos ataques se produjeron en un momento determinado del periodo seleccionado por vector de ataque. Los datos pueden referirse bien al dominio seleccionado actualmente, bien a todos los clientes (véase Alternar entre datos globales y de dominio en la página 200).

Para observar las cifras absolutas de ataques por vector de ataque en un momento determinado, puede pasar el puntero del ratón sobre las líneas verticales. Al posar el puntero sobre un punto correspondiente a un vector de ataque se muestran solo el diagrama y los datos sobre la cantidad de ataques correspondientes.

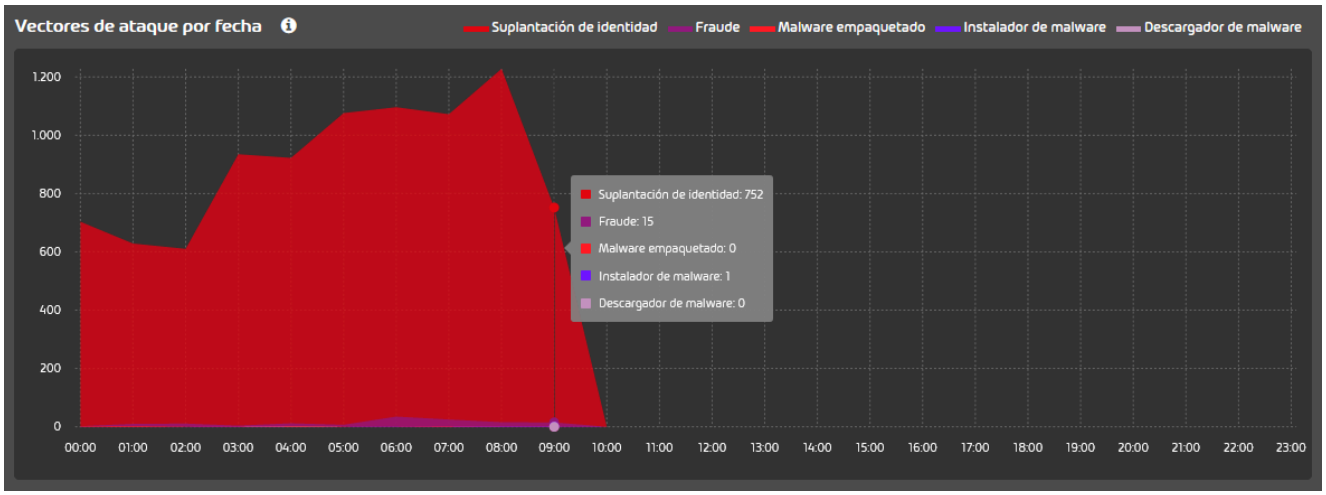


Figura 150: Estadística de amenazas - Vectores de ataque por fecha

Estadística de Secure Links

Las estadísticas y diagramas incluidos en **Estadística de Secure Links** indican la cantidad de enlaces reescritos por el motor Secure Links sobre los que se ha hecho clic en los correos del periodo seleccionado. Se trata de datos globales de todos los clientes y no de datos del dominio seleccionado. En **Estadística de Secure Links** se muestran las siguientes estadísticas y diagramas:

- La estadística **Clics por hora del día** muestra la distribución porcentual de clics sobre enlaces en correos por hora.

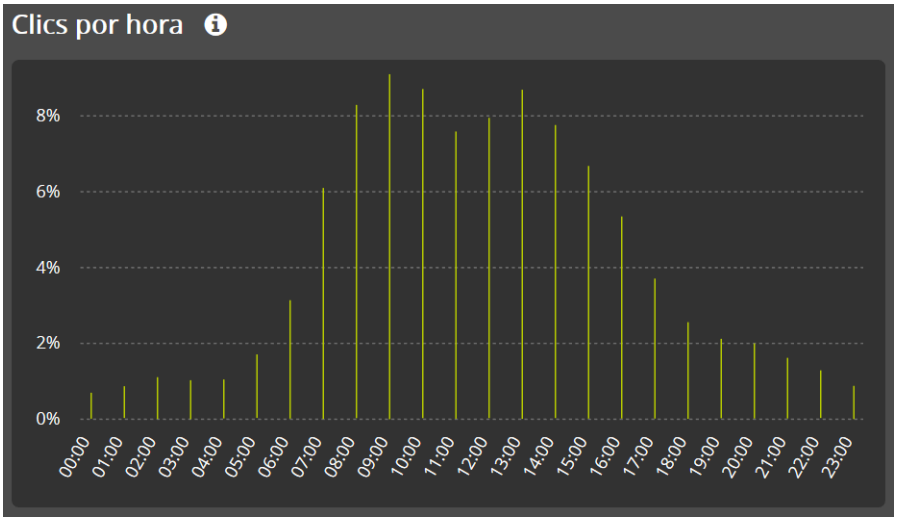


Figura 151: Clics por hora

- La estadística **Clics por dispositivo** muestra la distribución porcentual de los clics por dispositivo.

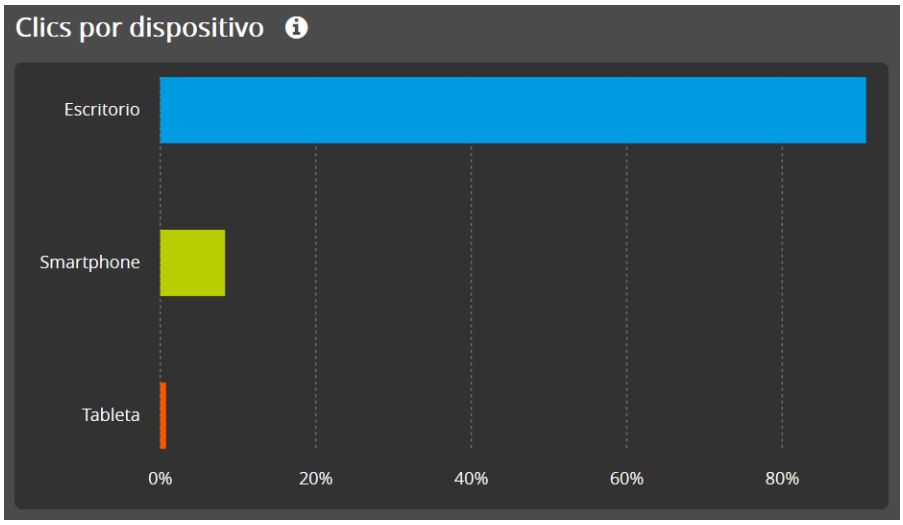


Figura 152: Clics por dispositivo

- El diagrama **Clics por sistema operativo (SO)** muestra la distribución porcentual de los clics por sistema operativo.

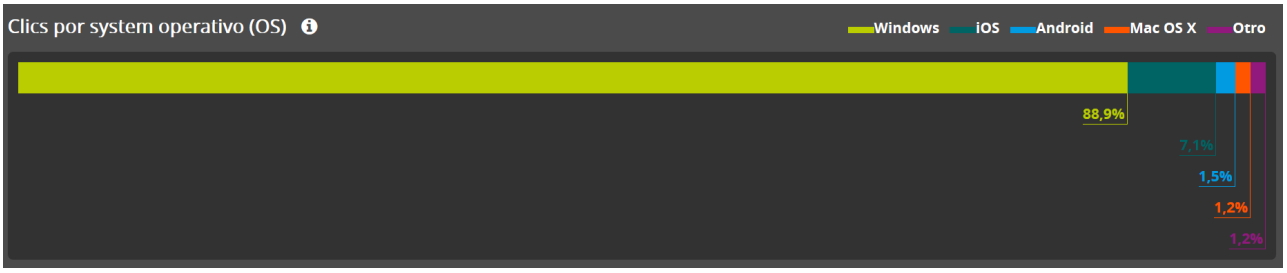


Figura 153: Clics por sistema operativo (OS)

Tipos y vectores de ataque

Descripción de los tipos de ataque

Tabla 10: Tipos de ataque

NOMBRE DEL TIPO DE ATAQUE	EXPLICACIÓN
Puerta trasera	El malware de puerta trasera persigue objetivos similares a los de un troyano de acceso remoto, pero emplea otros medios. En un ataque de puerta trasera, los atacantes utilizan las denominadas "puertas traseras" presentes en programas o sistemas operativos y, en ocasiones, implantadas allí a propósito. Sin embargo, también pueden instalarse en secreto. La peculiaridad de las puertas traseras es que permiten eludir los mecanismos de defensa habituales y, por tanto, son muy atractivas para los ciberdelincuentes. Éstos, por ejemplo, suelen utilizarlas para crear redes de bots.

NOMBRE DEL TIPO DE ATAQUE	EXPLICACIÓN
Troyano bancario	Los troyanos bancarios son un tipo de malware que trata de sustraer datos sensibles tales como datos bancarios o de cuentas de correo electrónico. A menudo, los atacantes lo logran en combinación con ataques de suplantación de identidad en los que una página web finge ser la página web oficial de un banco.
Bot	Un bot no tiene por qué ser siempre malware, pues en principio solo se trata de un programa de ordenador que ejecuta tareas de modo autónomo y automatizado. Cuando varios bots se comunican entre sí, se habla de una red de bots. Los atacantes crean redes de bots infectando gran cantidad de ordenadores. Un atacante puede enviar órdenes a todos los ordenadores al mismo tiempo y, de este modo, ejecutar actividades. Lo peor del asunto es que los propietarios de los ordenadores afectados no suelen saber que forman parte de las redes hasta que éstas ya han efectuado sus actividades por control remoto.
Minero de criptomonedas	Los mineros de criptomonedas son un tipo de malware que se emplea para calcular divisas digitales. Los delincuentes infectan ordenadores con mineros de criptomonedas para aprovecharse de su potencia de cálculo o uso de CPU de servidores. Esto reduce principalmente la potencia del ordenador, pero también su vida útil. Los mineros de criptomonedas pueden inutilizar redes de empresas enteras.
Keylogger	Los keyloggers son un tipo de malware que pueden realizarse mediante hardware o software. Los keyloggers registran las órdenes del teclado y lo que dice un usuario con el fin de acceder a datos sensibles o contraseñas.

NOMBRE DEL TIPO DE ATAQUE	EXPLICACIÓN
Troyano de punto de venta	Los troyanos de punto de venta son un tipo de malware que ataca sistemas de venta en los cuales se producen transacciones con datos de pago sensibles. Los ciberdelincuentes emplean los troyanos de punto de venta para acceder a datos de clientes de tarjetas bancarias y de crédito.
Ransomware	El ransomware es un tipo de ataque en el cual se cifran los archivos del sistema atacado. Sin la clave no es posible abrir los archivos. Los atacantes exigen un elevado rescate por la clave. Aunque a principio solo se encuentre infectado un ordenador, el ransomware puede extenderse por toda la red.
Troyano de acceso remoto	Un troyano de acceso remoto (RAT, por sus siglas en inglés) permite a los atacantes apoderarse de ordenadores y controlarlos a distancia. De este modo pueden ejecutar comandos en los sistemas de la víctima y distribuir RATs a otros ordenadores con el objetivo de crear una red de bots.
Rootkit	Los rootkits permiten encubrir código malicioso para que no sea descubierto. En esta forma de ataque, el atacante penetra profundamente en el sistema del ordenador, accede a los privilegios de raíz y, de este modo, obtiene derechos de acceso generales. A continuación, los ciberdelincuentes modifican el sistema de tal modo que el usuario no pueda ver qué procesos y actividades se inician. Esto hace que los ataques basados en encubrimiento mediante rootkit sean muy difíciles de detectar.

NOMBRE DEL TIPO DE ATAQUE	EXPLICACIÓN
Spyware	El spyware es un tipo de malware que recopila información del ordenador de la víctima. Esta información puede incluir, por ejemplo, datos de acceso de cuentas de usuario, datos bancarios sensibles o datos sobre las páginas visitadas. En la mayoría de ocasiones, los usuarios no saben que han sido víctimas de spyware.
Caballos de troya	Los caballos de troya son programas que fingen ser inofensivos pero albergan código malicioso. El usuario solo percibe sus beneficios, mientras que, en segundo plano, el sistema se va infectando con código malicioso. A partir de este punto, el usuario no tiene ningún control sobre los efectos.
Suplantación de identidad	Un ataque en el que el atacante suplanta la identidad de una persona o institución en la que confía o la cual conoce la víctima para obtener acceso a información sensible, sustraer dinero (p. ej., solicitando una transferencia), obtener acceso a propiedad intelectual, etc.

Descripción de los vectores de ataque

Tabla 11: Vectores de ataque

NOMBRE DEL VECTOR DE ATAQUE	EXPLICACIÓN
Archivo adjunto	Un archivo adjunto de un correo es un archivo que puede contener malware.
Enlace	Los enlaces de los correos conducen a otras páginas web. Los enlaces puede dirigir a malware.

NOMBRE DEL VECTOR DE ATAQUE	EXPLICACIÓN
Enlace de instalación	Los enlaces de instalación son enlaces portadores de malware. El enlace en sí no es perjudicial, pero permite ejecutarse al malware que está detrás.
Enlace de descarga	Los enlaces de descarga son enlaces en correos electrónicos que conducen a malware. Si la víctima hace clic en ellos, el malware se descarga.
Descargador de malware	Los descargadores de malware son un tipo de troyanos, porque descargan archivos perjudiciales desde un servidor remoto.
Instalador de malware	Los instaladores de malware no son software malicioso, sino que transportan malware al sistema. Desde fuera, los instaladores de malware parecen inofensivos y pueden camuflarse como archivos. Sin embargo, los archivos que contienen pueden ejecutarse e infectar el sistema con software malicioso.
Malware comprimido	El malware comprimido es un tipo de malware que ha sido comprimido por los delincuentes con una serie de métodos. De este modo se pretende eludir los análisis de malware.
Engaño	Por "engaño" se entiende en Internet la obtención de datos sensibles, dinero o datos bancarios de los usuarios mediante servicios de Internet. Por ejemplo, puede tratarse de páginas web o de transacciones que fingen ser reales, pero que realmente fueron programadas por ciberdelincuentes. Una variante popular es el fraude del CEO, en el que los criminales se hacen pasar por presidentes de una empresa y se ponen en contacto con el departamento de contabilidad de la misma, por teléfono o por correo electrónico, para ordenar transferencias de importes elevados.

NOMBRE DEL VECTOR DE ATAQUE	EXPLICACIÓN
Phishing	La suplantación de identidad o "phishing", de "passwort" ("contraseña") y "fishing" ("pesca") en inglés, es un método con el que se pretende "pescar contraseñas". Para lograrlo, los ciberdelincuentes hacen pasar direcciones de correo o páginas web falsas como auténticas, incitando de este modo a los usuarios a introducir datos sensibles. De este modo, los usuarios entregan sus datos sin saber que están cayendo en manos de delincuentes.

Acciones en Threat Live Report

Alternar entre datos globales y de dominio

Aún no ha accionado el interruptor **Global** de **Threat Live Report**.

En la sección **Vista general de ataques en directo**, así como en los diagramas y estadísticas de **Intentos de ataque** y **Estadística de amenazas** es posible elegir entre datos globales de todos los clientes o datos del dominio seleccionado actualmente en la selección de ámbitos. Los datos del dominio se muestran por defecto.

Nota:

Por el contrario, los diagramas de **Estadística de Secure Links** muestran siempre datos globales de todos los clientes y no pueden cambiarse por otros.

1. Seleccione un dominio en la selección de ámbitos.

   El módulo **Threat Live Report** se activa en **Informes y conformidad**.
2. Vaya a **Informes y conformidad** > **Threat Live Report**.

3. Accione el interruptor **Global**.

Figura 154: Interruptor Global en verde

El interruptor **Global** se pone verde. Los diagramas y estadísticas de **Vista general de ataques en directo**, **Intentos de ataque** y **Estadística de amenazas** muestran ahora datos globales de todos los clientes.

4. Vuelva a accionar el interruptor **Global**.

El interruptor **Global** se pone gris. Los diagramas y estadísticas de **Vista general de ataques en directo**, **Intentos de ataque** y **Estadística de amenazas** emplean ahora datos del dominio mostrado en la selección de ámbitos.

Se han cambiado los datos mostrados en los diagramas y estadísticas de **Threat Live Report** de datos globales a datos de dominio (o viceversa).

Seleccionar el periodo de visualización

Puede seleccionar el periodo de visualización de los diagramas y estadísticas mostrados en **Intentos de ataque**, **Estadística de amenazas** y **Estadística de Secure Links**.

Nota:

La sección **Vista general de ataques en directo** siempre muestra datos en tiempo real y no se ve afectada por el periodo seleccionado.

1. Seleccione un dominio en la selección de ámbitos.

   El módulo **Threat Live Report** se activa en **Informes y conformidad**.

2. Vaya a **Informes y conformidad** > **Threat Live Report**.
3. Haga clic en el botón de selección de periodos.

Figura 155: Hacer clic en el botón de selección de periodos

   Se muestra calendario para la selección de periodos.

4. Seleccione el periodo seleccionado manualmente.
   a) Haga clic en el primer día del periodo deseado en el calendario.
   b) Haga clic en el último día del periodo deseado.

   El periodo deseado se selecciona.

   Los diagramas y estadísticas arriba indicados solo muestran datos del periodo seleccionado.

5. Seleccione un periodo predefinido. Tiene las siguientes opciones:
   - **Hoy**: El periodo se limita a la fecha actual.
   - **Ayer**: El periodo se limita al día anterior a la fecha actual.
   - **Hace dos días**: El periodo se limita al día dos días antes de la fecha actual.
   - **Este mes**: Se selecciona como periodo el mes natural actual.
   - **El mes pasado**: Se selecciona como periodo el mes natural anterior al actual.
   - **Últimos 3 meses**: Se selecciona como periodo el mes natural actual y los dos anteriores.
   - **Este año**: Se selecciona como periodo el año natural actual.
   - **Últimos 12 meses**: Se seleccionan como periodo los últimos 12 meses.

   Los diagramas y estadísticas arriba indicados solo muestran datos del periodo seleccionado.

Se ha seleccionado el periodo de visualización.

Registro de auditorías 2.0

Registro de auditoría 2.0

En el módulo **Registro de auditorías 2.0** se documentan las actividades de los usuarios en Control Panel en un registro de auditoría. El registro de auditoría permite a los administradores a nivel de cliente y partner seguir las actividades de sus usuarios. Los administradores pueden, por ejemplo, determinar qué usuario fue el que eliminó determinado registro de datos y en qué momento lo hizo. Esto permite a los administradores deshacer tales acciones cuando sea necesario.

Cada registro representa un evento realizado por un usuario en Control Panel. Para cada evento se almacena información sobre varias categorías (véase Categorías en la página 204). Los administradores pueden seleccionar las categorías a mostrar en el registro de auditoría (véase Seleccionar las categorías mostradas en la página 206).

Para facilitar la búsqueda de registros, los administradores pueden filtrar los registros del registro de auditoría. Los administradores pueden determinar el periodo del cual mostrar registros en el registro de auditoría (véase Seleccionar el periodo de visualización en la página 208). Los administradores también pueden filtrar los registros por acciones (véase Filtrar por acciones en la página 209) y eventos (véase Filtrar por eventos en la página 211). Si lo desean, los administradores pueden recuperar la configuración por defecto de los filtros (véase Descartar los ajustes en la página 222). Además, los administradores pueden buscar términos de búsqueda en los registros del registro de auditoría (véase Buscar registros en la página 223).

Para ver qué valores se han modificado debido a un evento en Control Panel, los administradores pueden abrir el registro del evento (véase Abrir un registro en la página 224). Además, los administradores pueden exportar los registros mostrados en formato CSV (véase Exportar registros en la página 226).

Categorías

En el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203) se documentan los eventos provocados por los usuarios de Control Panel en un registro de auditoría. Para cada registro se almacena información sobre varias categorías. Cada columna del registro de auditoría corresponde a una categoría. Las categorías se explican en la tabla de abajo.

Tabla 12: Categorías del registro de auditoría

CATEGORÍA	EXPLICACIÓN
Fecha y hora	Indica el momento en que se ejecutó la acción.
Usuario	Indica el usuario que ejecutó la acción.
Destino	Indica el usuario para el que se ejecutó la acción.
Evento	Indica en qué consistió el evento, p. ej. en una modificación de la configuración del usuario, de la lista negra o blanca o de los datos de acceso, o bien de un inicio de sesión.

CATEGORÍA	EXPLICACIÓN
Acción	Indica si la acción ejecutada creó, actualizó o eliminó algo. "Éxito" y "Error" indican si un inicio de sesión se efectuó con éxito.
Ruta de destino	Indica el dominio al que pertenece el usuario de destino para el que se efectuó la acción.
ID de app	Muestra los números de identificación de las aplicaciones que emplean la API. La API permite a las aplicaciones comunicarse con nuestros servicios. Para más información sobre la API, véase el manual "Interfaz de Programación de Aplicaciones (API)".
Versión de app	Muestra la versión de la aplicación que se comunicó con la API.
IP	Muestra la dirección IPv4 del usuario que efectuó la acción.
URL	Indica la ruta al punto de conexión de la API.

Las siguientes categorías se muestran por defecto en el registro de auditoría:

- **Fecha y hora**
- **Usuario**
- **Destino**
- **Evento**
- **Acción**

Los administradores pueden elegir que se muestren además las siguientes categorías en el registro de auditoría (véase Seleccionar las categorías mostradas en la página 206):

- **Ruta de destino**
- **ID de app**

- **Versión de app**
- **IP**
- **URL**

Seleccionar las categorías mostradas

El registro de auditoría del módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203) contiene información sobre varias categorías (véase Categorías en la página 204). Puede seleccionar las categorías a mostrar en el registro de auditoría. Cada columna de la tabla del registro de auditoría corresponde a una categoría.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente cuyo registro de auditoría desee abrir.
3. Vaya a **Informes y conformidad** > **Registro de auditorías 2.0**.

4. Haga clic en el icono situado en la esquina superior derecha de la tabla.

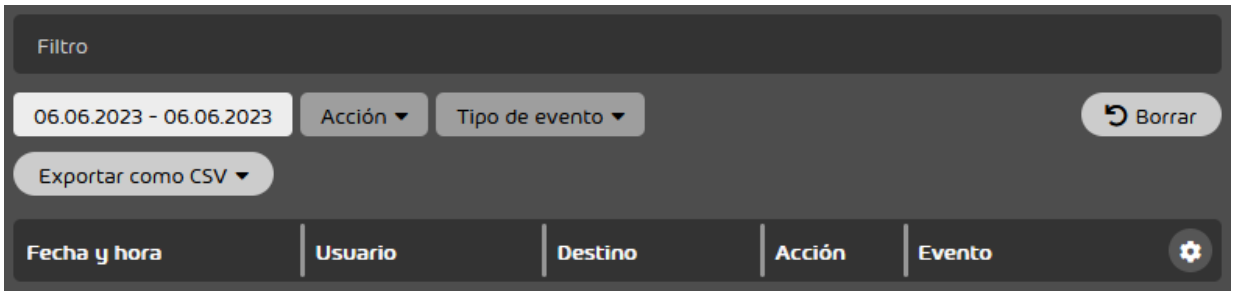


Figura 156: Abrir la lista de las categorías disponibles

Se muestra una lista con todas las categorías disponibles. Las categorías mostradas actualmente en el registro de auditoría se muestran con el fondo azul.

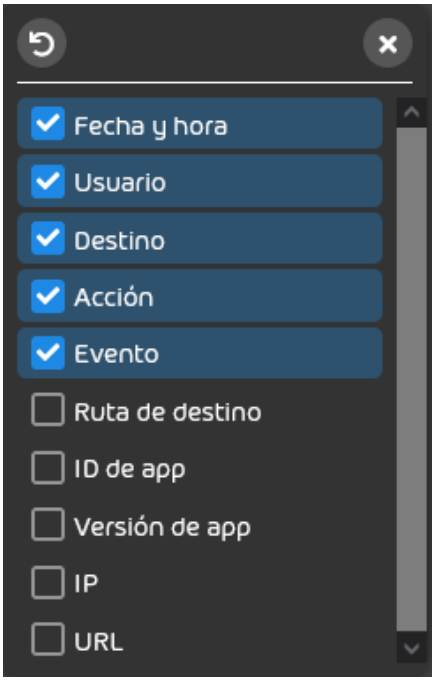


Figura 157: Categorías disponibles

5. Para mostrar una categoría ocultada actualmente en el registro de auditoría, haga clic en la categoría.

   La categoría se pone azul.
6. Para ocultar una categoría mostrada actualmente en el registro de auditoría, haga clic en la categoría.

   La categoría ya no se muestra con el fondo azul.
7. Opcional: Para restaurar la configuración por defecto de las columnas del registro de auditoría, haga clic en **Default**.

   Se recupera la configuración por defecto de las columnas del registro de auditoría.
8. Haga clic en la ventana fuera de la lista para cerrarla.

   La lista se cierra. Las categorías seleccionadas se muestran en el registro de auditoría.

Se han seleccionado las categorías a mostrar en el registro de auditoría.

Filtrado de registros

Seleccionar el periodo de visualización

En el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203) puede seleccionar un periodo de visualización para el registro de auditoría.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente cuyo registro de auditoría desee abrir.
3. Vaya a **Informes y conformidad** > **Registro de auditorías 2.0**.

4. Haga clic en el rango de fechas mostrado.

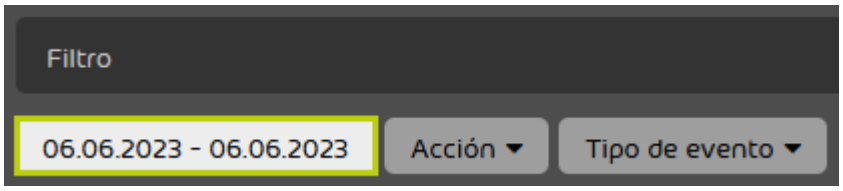


Figura 158: Seleccionar un periodo

Se abre un calendario.

5. En el calendario, seleccione el periodo del cual deben mostrarse los eventos en el registro de auditoría.

Todos los días del periodo seleccionado se marcan en el calendario. La fecha inicial y final se muestran abajo en el calendario.

6. Haga clic en la ventana fuera del calendario para cerrarlo.

El calendario se cierra. El registro de auditoría solo muestra los eventos del periodo seleccionado.

Se ha seleccionado un periodo de visualización para el registro de auditoría.

Filtrar por acciones

Acciones para filtrar

Los administradores pueden filtrar los registros del registro de auditoría en el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203) por acciones. Para ello, los administradores pueden seleccionar una acción en el menú desplegable **Acción**. Tras la selección se mostrarán solo los registros relativos a la acción seleccionada.

Nota:

Solo es posible filtrar por una acción al mismo tiempo.

Figura 159: Filtrar por acciones

En la siguiente tabla se enumeran las acciones por las que los administradores pueden filtrar.

Tabla 13: Acciones

ACCIÓN	EXPLICACIÓN
Todas	Muestra todas las acciones efectuadas en el periodo indicado.
Actualización	Muestra todas las acciones con las que se ha actualizado algo.
Éxito	Muestra todos los inicios de sesión realizados con éxito.
Creación	Muestra todas las acciones con las que se ha creado algo.

ACCIÓN	EXPLICACIÓN
Fallo	Muestra todos los intentos de inicio de sesión fallidos.
Eliminado	Muestra todas las acciones con las que se ha eliminado algo.

Filtrar por eventos

Eventos para filtrar

Los administradores pueden filtrar los registros del registro de auditoría en el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203) por eventos. En el menú desplegable **Tipo de evento**, los administradores pueden seleccionar eventos. Tras seleccionarse un evento se muestran únicamente los registros correspondientes al mismo.

Nota:

Solo es posible filtrar por un evento al mismo tiempo.

En el módulo **Registro de auditorías 2.0**, los administradores pueden ver todos los eventos que se hayan producido al nivel del partner o cliente seleccionado, así como en todos sus ámbitos de aplicación inferiores. Los registros del evento **Acción para correo** se realizan a nivel del ámbito de aplicación más elevado al que tenga acceso el usuario que los haya originado.

Nota:

A excepción del evento **Acción para correo**, todos los registros relativos a eventos se realizan a nivel del ámbito de aplicación que estuviese seleccionado en la selección de ámbitos al producirse el evento correspondiente (véase el capítulo "Selección de ámbitos" del manual de Control Panel).

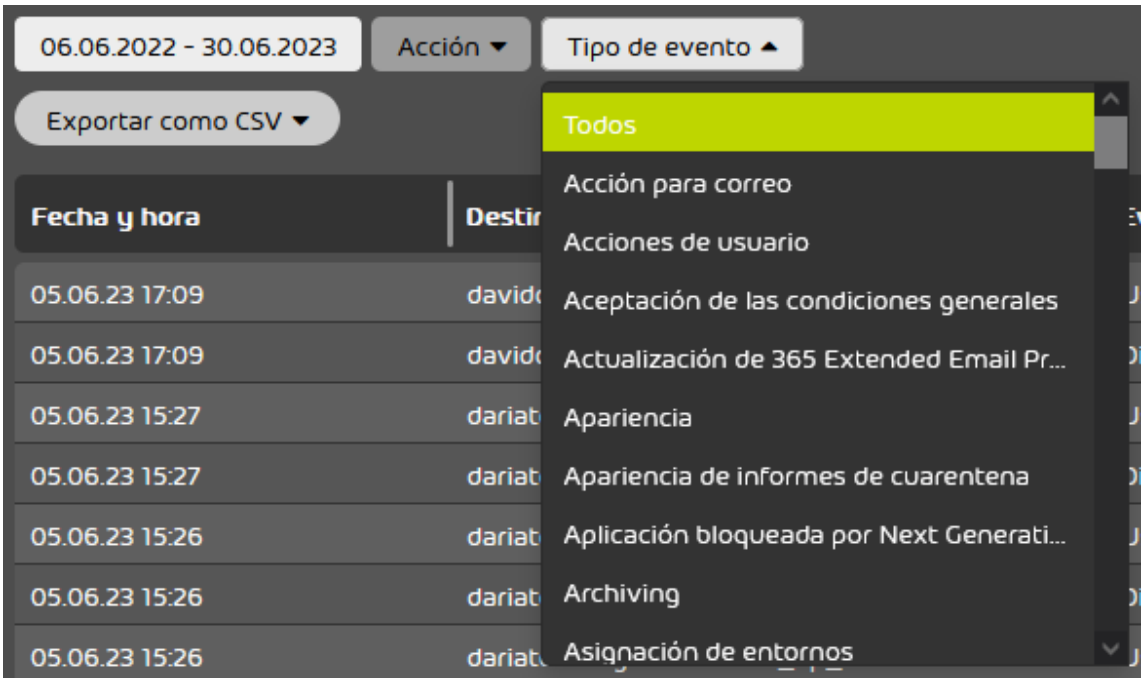


Figura 160: Filtrar por eventos

En la siguiente tabla se enumeran los eventos por los que los administradores pueden filtrar.

Tabla 14: Eventos para filtrar

EVENTO	EXPLICACIÓN
Todos	Muestra todos los cambios realizados en Control Panel.
Configuración general LDAP	Filtra por eventos que han actualizado la configuración general para todas las conexiones LDAP en el módulo **Dashboard de servicios**.
Nota "Fuera de oficina"	Filtra por eventos que han actualizado la configuración relativa a notas de 'fuera de oficina' en el módulo **Configuración de usuario**.

EVENTO	EXPLICACIÓN
Datos de registro	Filtra por eventos que han actualizado los datos de inicio de acceso de un usuario.
Inicio de sesión	Filtra por inicios de sesión en Control Panel fallidos y con éxito.
Token de API	Filtra por eventos que han creado o eliminado tokens de API en la pestaña **Token de API** de **Configuración de usuario**.
Configuración de ATP	Filtra por eventos que han actualizado la configuración del módulo **Advanced Threat Protection**.
Apariencia	Filtra por eventos que han actualizado los ajustes disponibles en la pestaña **Control Panel** del módulo **Personalización**.
Apariencia de informes de cuarentena	Filtra por eventos que han actualizado la apariencia de los informes de cuarentena. Esto incluye cambios realizados en los módulos **Personalización** y **Quarantine Report**.
Cierre de sesión automático: Ajustes	Filtra por eventos que han creado, actualizado o eliminado ajustes personalizados para el cierre de sesión automático de usuarios inactivos en el módulo **Configuración de cliente** > **Autenticación**.

EVENTO	EXPLICACIÓN
Creación automática de usuarios	Filtra por eventos que han actualizado el estado de activación de la opción de creación automática de usuarios en función del método de comprobación de usuarios en el módulo **Spam and Malware Protection**.
Copia de seguridad	Filtra por eventos que han provocado la activación de servicios de copia de seguridad y restauración de datos.
Acciones de usuario	Filtra por eventos que han creado, actualizado o eliminado ajustes relativos a acciones permitidas en la pestaña **Permisos de usuario** del módulo **Spam and Malware Protection**.
Configuración de usuario	Filtra por eventos que han creado, actualizado o eliminado ajustes de **Configuración de usuario**. Como parte de este evento, también se auditan cambios de la zona horaria, del idioma, del formato de fecha y del formato de hora por defecto de un partner o un cliente en el módulo **Dashboard de servicios** (véase el capítulo "Ajustar zona horaria e idioma por defecto" en el manual de Control Panel).
Listas blancas y negras	Filtra por eventos que han actualizado la configuración del módulo **Listas blancas y negras**.
Compliance Filter	Filtra por eventos que han creado, actualizado o eliminado reglas, así como actualizado ajustes en el módulo **Compliance Filter**.

EVENTO	EXPLICACIÓN
Instalación del conector	Filtra por eventos que han provocado la instalación de conectores.
Content Control	Filtra por eventos que han creado o actualizado los ajustes del módulo **Content Control**.
Continuity Service	Filtra por eventos que han actualizado la configuración del módulo **Continuity Service**.
Dominio	Filtra por eventos que han creado, actualizado o eliminado dominios en el módulo **Dominios**.
Dirección de correo	Filtra por eventos que han creado, actualizado o eliminado direcciones de correo electrónico en el módulo **Buzones**.

EVENTO	EXPLICACIÓN
Acción para correo	Filtra por eventos relativos a acciones para correos del módulo **Email Live Tracking**. El estado **Actualización** se refiere a las siguientes acciones: • **Reportar spam** • **Reportar infomail** • **Marcar como privado** La acción para correos **Eliminar correo** se registra con el estado **Eliminado**. El estado **Éxito** se refiere a las siguientes acciones: • **Entregar correo** • **Añadir remitente a lista negra** • **Añadir remitente a lista blanca y entregar correo** • **Añadir a lista negra de todos los usuarios** • **Añadir a lista blanca de todos los usuarios** • **Enviar correo al administrador** • **Escaneo ATP**
Información de correo electrónico	Filtra por eventos que han actualizado los ajustes disponibles en la pestaña **Información de correo electrónico** del módulo **Personalización**.

EVENTO	EXPLICACIÓN
Destinatarios de estadísticas de correos	Filtra por eventos que han provocado la adición o eliminación de buzones de correo de la lista de destinatarios de estadísticas de correo en el módulo **Estadísticas de correo electrónico**.
Previsualización de correos	Filtra por eventos que han creado una vista previa de correos en el módulo **Email Live Tracking**.
Email Authentication	Filtra por eventos que han creado o eliminado excepciones, o bien actualizado ajustes en el módulo **Email Authentication**.
Condiciones Generales	Filtra por eventos que han creado o actualizado los ajustes disponibles en la pestaña **Condiciones Generales** del módulo **Dashboard de servicios**.
Grupo	Filtra por eventos que han creado, actualizado o eliminado grupos en el módulo **Grupos**.
Contenido de las condiciones generales	Filtra por eventos que han creado textos de contratos de licencia de usuario final y de tratamiento de datos en la pestaña **Condiciones Generales** del módulo **Dashboard de servicios**.
Contacto	Filtra por eventos que han creado, actualizado o eliminado contactos en el módulo **Dashboard de servicios**.
Cliente	Filtra por eventos que han creado o eliminado clientes del módulo **Dashboard de servicios**.

EVENTO	EXPLICACIÓN
Conexión LDAP	Filtra por eventos que han creado, actualizado o eliminado la configuración de una conexión LDAP en el módulo **Dashboard de servicios**.
Migración de un solo buzón de correo	Filtra por eventos que han actualizado o eliminado una tarea de migración de datos de un único buzón de correo durante la migración de buzones de correo en el módulo **365 Total Protection**.
Migración de varios buzones de correo	Filtra por eventos que han creado, actualizado o eliminado una tarea de migración de datos de varios buzones de correo durante la migración de buzones de correo en el módulo **365 Total Protection**.

EVENTO	EXPLICACIÓN
Autenticación multifactor	Filtra por eventos que han creado, actualizado o eliminado la configuración de la autenticación multifactor. "Crear" se refiere a habilitar la autenticación multifactor para los usuarios de un dominio en el módulo **Configuración de cliente** > **Autenticación**. "Actualizar" se refiere a que un usuario configura la autenticación multifactor para su propia cuenta en **Configuración de usuario**. "Eliminar" se refiere a que un usuario desactiva la autenticación multifactor para su propia cuenta en **Configuración de usuario**, que un administrador reinicia la autenticación multifactor para un usuario en el módulo **Configuración de cliente** > **Buzones** o que un administrador desactiva la autenticación multifactor para los usuarios de un dominio en el módulo **Configuración de cliente** > **Autenticación**.
Boletín informativo	Filtra por eventos que han creado suscripciones a boletines de noticias para clientes o partners en el módulo **Dashboard de servicios**.
Contraseña de emergencia del cliente	Filtra por eventos que han actualizado la contraseña de emergencia de Continuity Service.
Outlook Add-in	Filtra por eventos que han actualizado la configuración de Outlook Add-in.
Partner	Filtra por eventos que han creado o eliminado partners en el módulo **Dashboard de servicios**.

EVENTO	EXPLICACIÓN
Directiva de contraseñas	Filtra por eventos que han actualizado normas sobre contraseñas en el módulo **Autenticación**.
Buzón de correo	Filtra por eventos que han creado o actualizado buzones de correo en el módulo **Buzones**.
Quarantine Report	Filtra por eventos que han actualizado la configuración del módulo **Quarantine Report**.
Asignación de roles	Filtra por eventos que han creado, actualizado o eliminado asignaciones de roles en el módulo **Dashboard de servicios**.
Spam and Malware Protection	Filtra por eventos que han actualizado la configuración del módulo **Spam and Malware Protection**.
Información de soporte técnico	Filtra por eventos que han actualizado los ajustes disponibles en la pestaña **Información de soporte técnico** del módulo **Personalización**.
Grupos de Targeted Fraud Forensics Filter	Filtra por eventos que han creado o eliminado grupos de Targeted Fraud Forensics Filter en el módulo **Advanced Threat Protection**.
Entorno	Filtra por eventos que han creado, actualizado o eliminado entornos secundarios en el módulo **Dashboard de servicios**.

EVENTO	EXPLICACIÓN
Validación de entorno	Filtra por eventos que han creado o eliminado la validación de un entorno para la migración de buzones de correo en el módulo **365 Total Protection**.
Asignación de entornos	Filtra por eventos que han creado, actualizado o eliminado asignaciones de entornos a buzones de correo en el módulo **Configuración de cliente** > **Buzones**. "Crear" se refiere al momento en que se asigna por primera vez un entorno a un buzón de correo recién creado. "Actualizar" se refiere a asignar a un buzón de correo un entorno distinto al que tenía hasta entonces. "Eliminar" se refiere a la eliminación de una asignación de un buzón de correo que sucede al eliminar dicho buzón de correo.
Diccionario de Compliance Filter	Filtra por eventos que han creado, actualizado o eliminado diccionarios del módulo **Compliance Filter**.
Normas	Filtra por eventos que han actualizado la configuración del módulo **Autenticación**.
Datos de acceso para migración de buzones	Filtra por eventos que han creado o eliminado datos de acceso de un servidor de Exchange local para la migración de buzones de correo en el módulo **365 Total Protection**.

Eventos adicionales

En la siguiente tabla se muestran eventos por los que los administradores no pueden filtrar, pero que se muestran en el módulo **Registro de auditorías 2.0** de todos modos.

Tabla 15: Eventos por los que no es posible filtrar

EVENTO	EXPLICACIÓN
Datos básicos	Corresponde a eventos que han creado, actualizado o eliminado datos básicos de buzones de correos en el módulo **Buzones**.

Descartar los ajustes

Ha modificado los ajustes para la visualización del registro de auditoría en el módulo **Registro de auditorías 2.0** (véanse Seleccionar el periodo de visualización en la página 208, Filtrar por acciones en la página 209 y Filtrar por eventos en la página 211). Todavía está en el módulo **Registro de auditorías 2.0**.

Puede recuperar los ajustes por defecto para la visualización del registro de auditoría en el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203).

Haga clic en **Borrar**.

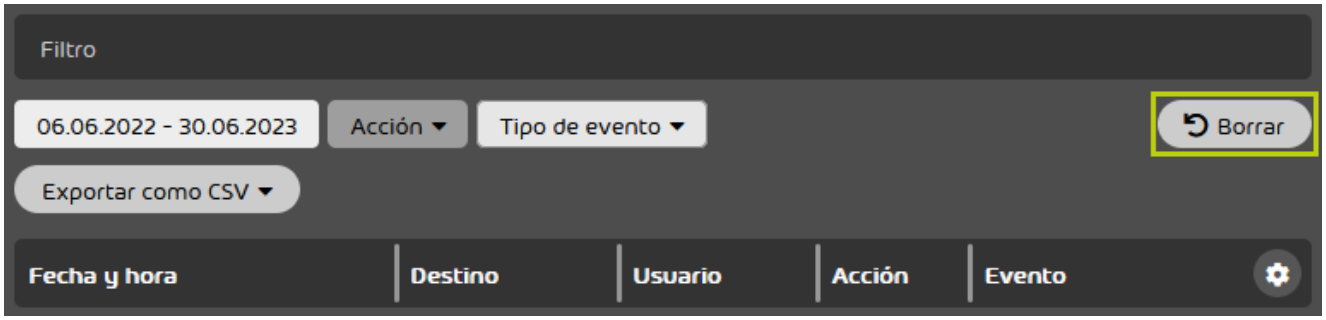


Figura 161: Restaurar los ajustes por defecto

Los ajustes se descartan.

Los ajustes por defecto para la visualización del registro de auditoría se han recuperado.

Buscar registros

Los administradores pueden buscar términos de búsqueda en los registros del registro de auditoría en el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203). Los administradores pueden buscar términos de búsqueda en los siguientes parámetros:

- **Usuario**
- **Ruta de destino**
- **Destino**
- **ID de app**
- **Versión de app**
- **Valores antiguos**
- **Valores nuevos**
- **IP**
- **URL**

Salvo los parámetros **Valores antiguos** y **Valores nuevos**, todos corresponden a categorías del registro de auditoría (véase Categorías en la página 204). En cambio, los parámetros **Valores antiguos** y **Valores nuevos** se refieren a los valores antiguos y nuevos indicados en los registros del registro de auditoría en el punto de menú **Información**.

Los administradores pueden introducir un término de búsqueda en la barra de búsqueda. Para comparar un término de búsqueda con un parámetro determinado, los administradores pueden hacer clic en el parámetro deseado debajo de la barra de búsqueda. De lo contrario, el término de búsqueda se comparará con todos los parámetros. Los administradores pueden iniciar la búsqueda pulsando la tecla Intro. El registro de auditoría solo muestra los registros que cumplan los criterios de búsqueda.

Nota:

Los administradores pueden utilizar varios parámetros al mismo tiempo. Los administradores pueden introducir un término de búsqueda para cada parámetro utilizado. Los resultados de la búsqueda solo contienen registros que cumplan todos los criterios de búsqueda.

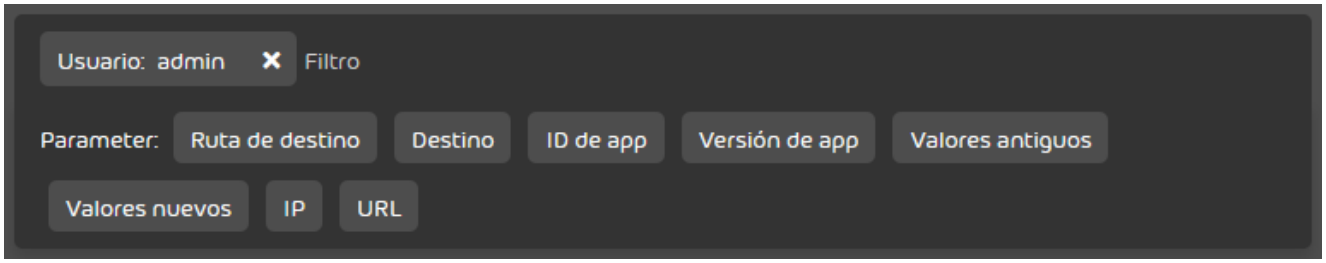


Figura 162: Buscar registros

Abrir un registro

Puede abrir un registro del registro de auditorías en el módulo **Registro de auditorías 2.0** para ver qué valores se aplicaron antes y después de un evento.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente cuyo registro de auditoría desee abrir.
3. Vaya a **Informes y conformidad** > **Registro de auditorías 2.0**.
4. Opcional: Para buscar un registro, filtre los registros del registro de auditoría (véase Seleccionar el periodo de visualización en la página 208, Filtrar por acciones en la página 209, Filtrar por eventos en la página 211 o Buscar registros en la página 223).

5. Haga clic en la flecha de menú junto al registro que desee abrir.

Figura 163: Abrir el menú

Se abre un menú.

6. Haga clic en **Información**.

Figura 164: Abrir informaciones

El registro se abre. En caso de haberlos, se muestran los valores antiguos y nuevos del evento.

Figura 165: Valores del evento

Nota:

El valor modificado por el evento se muestra con el fondo gris.

Se ha abierto un registro del registro de auditoría.

Exportar registros

En el módulo **Registro de auditorías 2.0** (véase Registro de auditoría 2.0 en la página 203) puede usted exportar registros del registro de auditorías en formato CSV. Durante la exportación se exportan todos los registros mostrados en el módulo **Registro de auditorías 2.0**. Puede elegir las columnas cuyos datos desee exportar.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente cuyo registro de auditoría desee abrir.
3. Vaya a **Informes y conformidad** > **Registro de auditorías 2.0**.
4. Seleccione el periodo de visualización cuyos registros desee exportar (véase Seleccionar el periodo de visualización en la página 208).
5. Filtre los registros mostrados por acciones (véase Filtrar por acciones en la página 209).
6. Filtre los registros mostrados por eventos (véase Filtrar por eventos en la página 211).

7. Haga clic en **Exportar como CSV**.

Se abre un formulario para la exportación de registros del registro de auditoría.

Figura 166: Formulario

8. Marque las casillas de las categorías cuyos datos desee exportar del registro de auditorías. Tiene las siguientes opciones:

   - **Fecha y hora**
   - **Usuario**
   - **Ruta de destino**
   - **Destino**
   - **ID de app**
   - **Versión de app**
   - **IP**
   - **Acción**
   - **Evento**
   - **URL**

   Nota:

   Cada categoría se corresponde con una columna del registro de auditoría (véase Categorías en la página 204). Por defecto, todas las categorías del formulario están seleccionadas.

9. En **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o enviarlo por correo electrónico.
   - **Descargar**: El archivo CSV se facilita para su descarga.
   - **Por correo electrónico**: El archivo CSV se envía por correo electrónico.

Figura 167: Seleccionar el tipo de exportación

Si se elige la opción **Por correo electrónico**, se muestra un campo adicional.

10. Opcional: Si elige la opción **Por correo electrónico**, introduzca en el campo la dirección de correo electrónico a la que enviar el archivo CSV.

Figura 168: Introducir una dirección de correo electrónico

11. Haga clic en **Exportar**.

El archivo CSV se presenta para su descarga o se envía por correo electrónico.

Se han exportado registros del registro de auditoría.

Configuración de clientes

Configuración de cliente

El módulo **Configuración de cliente** permite a los administradores consultar y administrar ajustes básicos relativos a buzones de correo, grupos, dominios, reglas para contraseñas y direcciones IP. El módulo **Configuración de cliente** se divide en los siguientes submódulos:

- **Buzones**: En Control Panel, los usuarios se administran mediante buzones de correo. Para poder aplicar nuestros servicios a los buzones de correo, estos deben registrarse en Control Panel. En este módulo, los administradores a nivel de cliente pueden añadir los buzones de correo de sus dominios a Control Panel y administrarlos (véase Buzones de correo en la página 230).
- **Grupos**: En Control Panel, los buzones de correo pueden reunirse en grupos, lo que permite configurar diversos servicios a nivel de grupo. En este módulo, los administradores a nivel de cliente pueden crear y administrar grupos (véase Grupos en la página 288).
- **Dominios**: En Control Panel es posible añadir dominios alias a un dominio principal para poder añadir buzones de correo de dichos dominios alias a Control Panel. En este módulo, los administradores a nivel de cliente pueden añadir dominios alias a Control Panel, exportarlos y eliminarlos (véase Dominios en la página 307).
- **Autenticación**: En este módulo, los administradores a nivel de cliente pueden realizar ajustes relativos a la autenticación de los usuarios en Control Panel (véase Autenticación en la página 319).

Buzones de correo

En el módulo **Configuración de cliente** > **Buzones** se muestran y administran todos los buzones de correo registrados bajo el dominio seleccionado. Este módulo solo está disponible para administradores a nivel de cliente.

Los buzones de correo sirven de base para las licencias de todos los servicios. Cada buzón de correo principal equivale a un usuario. Además de buzones de correo principales es posible crear

varias direcciones alias para los mismos sin coste adicional (véase Añadir una dirección alias en la página 261).

Para poder emplear nuestros servicios para un buzón de correo, éste deberá estar registrado en Control Panel. Los administradores a nivel de cliente pueden añadir buzones de correo a Control Panel uno por uno (véase Añadir un buzón de correo en la página 237) o importar varios al mismo tiempo desde un archivo CSV (véanse Archivos CSV para la importación de buzones de correo en la página 244 y Importar buzones de correo desde un archivo CSV en la página 240). Los buzones de correo también pueden añadirse automáticamente a Control Panel (véase Creación automática de buzones de correo en la página 236).

Además, los administradores a nivel de cliente pueden crear buzones de reenvío (véase Añadir un buzón de reenvío en la página 255) que reenvían sus correos entrantes a otros buzones de correo (véase Tipos de buzón de correo en la página 235). Los destinatarios de correos de buzones de reenvío pueden importarse desde un archivo CSV (véase Archivos CSV para importar destinatarios de buzones de reenvío en la página 267).

Los buzones de correo de Control Panel pueden exportarse en formato CSV (véase Exportar buzones de correo en formato CSV en la página 251) y volver a importarse mediante la función de importación desde archivos CSV.

Si no es preciso seguir aplicando nuestros servicios a determinados buzones de correo, es posible eliminarlos de Control Panel (véanse Quitar un buzón de correo en la página 281 y Eliminar varios buzones de correo en la página 283).

Los buzones de correo disponibles pueden ordenarse por tipo y por entorno en el módulo **Buzones** (véanse Configuración del entorno primario en la página 483 y Entornos secundarios en la página 120). En el menú desplegable **Todos los tipos**, los buzones de correo pueden filtrarse por tipo (véase Tipos de buzón de correo en la página 235).

Figura 169: Filtrado por tipo

En el menú desplegable **Todos los entornos**, los buzones de correo pueden filtrarse por entorno. En el menú desplegable se indican el entorno primario y los entornos secundarios del dominio.

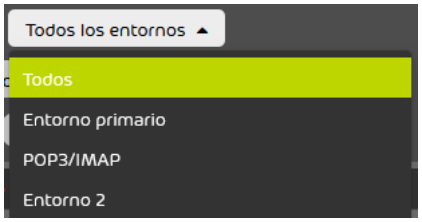


Figura 170: Filtrado por entorno

El menú desplegable **Autenticación multifactor** solo se muestra si un administrador a nivel de cliente ha habilitado la autenticación multifactor para los buzones de correo del cliente (véase Habilitar la autenticación multifactor en la página 323). En este menú desplegable, los buzones de correo pueden filtrarse por su configuración de la autenticación multifactor.

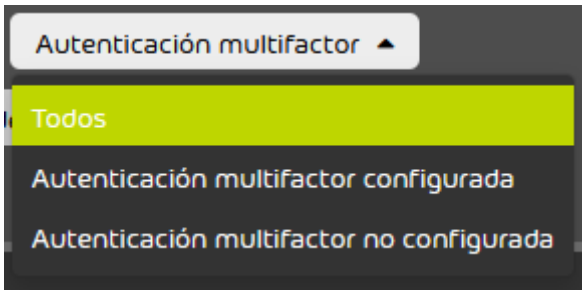


Figura 171: Filtrado por autenticación multifactor

Además, el módulo **Buzones** ofrece las siguientes opciones de administración de buzones de correo individuales a los administradores a nivel de cliente.

Tabla 16: Administrar buzones de correo

SÍMBOLO	TEXTO	DESCRIPCIÓN
	Grupos	Adición del buzón de correo a un grupo (véanse Grupos en la página 288 y Añadir un buzón de correo a un grupo en la página 257), así como eliminación del buzón de correo de un grupo (véase Quitar un buzón de correo de un grupo en la página 258)
	Zona horaria e idioma	Cambio de la zona horaria, del idioma, del formato de fecha y del formato de hora del buzón de correo (véase Configurar la zona horaria y el idioma de un buzón de correo en la página 268)
	Datos básicos	Personalización de los datos básicos del buzón de correo (véase Editar los datos básicos de un buzón de correo en la página 271)
	Cambiar entorno	Cambio del entorno del buzón de correo (véase Cambiar de entorno en la página 276)
	Cambiar contraseña	Cambio de contraseña (véase Cambiar la contraseña en la página 277)

SÍMBOLO	TEXTO	DESCRIPCIÓN
	Reiniciar la autenticación multifactor	Reinicio de la autenticación multifactor para el buzón de correo (véase Reiniciar la autenticación multifactor en la página 279) **Nota:** Esta acción solo es visible si la autenticación multifactor está habilitada para el dominio (véase Habilitar la autenticación multifactor en la página 323).
	Activo o **Inactivo**	Activación o desactivación de buzones de correo (véase Activar o desactivar un buzón de correo en la página 260)
	Alias	Adición de una dirección alias a un buzón de correo principal (véase Añadir una dirección alias en la página 261)
	Delegado	Designación de un delegado para el buzón (véase Designar un delegado en la página 263)
	Quarantine Report	Configuración del informe de cuarentena para el buzón de correo (véase Configurar Quarantine Report para un buzón de correo en la página 463)
	Quitar	Eliminación del buzón de correo (véase Quitar un buzón de correo en la página 281)

Nota:

Algunas de las funciones descritas no pueden aplicarse a buzones de correo LDAP, o solo pueden aplicarse parcialmente. Esto se indica en los capítulos de las funciones correspondientes.

Tipos de buzón de correo

En Control Panel se distingue entre los siguientes tipos de buzón de correo.

Tabla 17: Tipos de buzón de correo

TIPO DE BUZÓN DE CORREO	EXPLICACIÓN
Buzón de correo	Este buzón de correo se ha creado manualmente en Control Panel. El buzón de correo no se sincroniza con un servicio de directorio mediante LDAP. Para más información sobre cómo crear buzones de correo de este tipo, véase Añadir un buzón de correo en la página 237.
Buzón funcional	Los buzones de correo de este tipo no se registran actualmente en Control Panel.
Buzón de reenvío	Un buzón de reenvío es un buzón de correo virtual que está vinculado, como mínimo, a un buzón de correo de Control Panel o a un buzón de correo externo. Los correos entrantes del buzón de reenvío se reenvían a sus buzones de correo vinculados. Para más información sobre cómo crear buzones de reenvío, véase Añadir un buzón de reenvío en la página 255.
Buzón administrativo de Control Panel	Los buzones de correo de este tipo tienen asignados el rol **admin** en Control Panel (véase el capítulo «Roles» en el manual de Control Panel).

TIPO DE BUZÓN DE CORREO	EXPLICACIÓN
Buzón LDAP	Los datos de usuario de este buzón de correo se sincronizan en Control Panel con un servicio de directorio mediante LDAP. Para más información sobre la sincronización de buzones de correo mediante LDAP, véase Sincronizar usuarios y grupos con LDAP.

Creación automática de buzones de correo

Además de añadir buzones de correo manualmente a Control Panel (véase Añadir un buzón de correo en la página 237) o importarlos al mismo (véase Importar buzones de correo desde un archivo CSV en la página 240), es posible crear automáticamente buzones de correo en Control Panel de dos modos distintos:

- Los buzones de correo de tipo LDAP se sincronizan mediante un servicio de directorio.
- A partir de direcciones de destinatarios de correos aceptados por el servidor de correo del cliente se detectan y crean automáticamente buzones de correo. En el proceso se registra un buzón de

correo para cada dirección de destinatario. La creación automática de buzones de correo está activada por defecto.

PRECAUCIÓN:

Para evitar la creación de buzones de correo innecesarios y los costes asociados a los mismos, es preciso configurar una comprobación de usuarios que solo permita aceptar correos a buzones de correo válidos (véase Configurar el entorno primario en la página 484).

PRECAUCIÓN:

Aunque esté activada la comprobación de usuarios, el mecanismo de creación automática de buzones de correo no puede distinguir entre direcciones alias y buzones de correo principales siempre que los datos de los buzones de correo no se sincronicen mediante un servicio de directorio. Para evitar la creación automática de buzones de correo innecesarios a causa de la recepción de correos destinados a direcciones alias válidas, las direcciones alias deberán registrarse manualmente en Control Panel siempre que los datos no se sincronicen automáticamente (véase Añadir una dirección alias en la página 261).

Añadir un buzón de correo

Nuestros servicios pueden aplicarse a buzones de correo registrados bajo su dominio en Control Panel. En el módulo **Configuración de cliente** > **Buzones** puede añadir buzones de correo a su dominio en Control Panel.

Importante:

Los clientes que hayan configurado la sincronización de los buzones de correo de su entorno primario con un servicio de directorio mediante LDAP solo pueden añadir manualmente buzones de correo nuevos cuando hayan creado un entorno secundario (véase Crear un entorno secundario en la página 123). Los buzones de correo añadidos manualmente no se sincronizan mediante LDAP.

Importante:

Si se añade un buzón de correo nuevo con el mismo nombre que un buzón de correo eliminado anteriormente (véase Quitar un buzón de correo en la página 281), este nuevo buzón de correo no tendrá ninguna relación con el buzón eliminado en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que desee añadir un nuevo buzón de correo.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en **Añadir buzón de correo**.

Se abre un formulario.

Figura 172: Formulario

5. Introduzca el nombre del propietario del buzón de correo en el campo **Nombre**.
6. Introduzca los apellidos del propietario del buzón de correo en el campo **Apellidos**.

7. Introduzca la dirección del buzón de correo en el campo **Correo electrónico**.

> **Nota:**
>
> Los siguientes caracteres especiales pueden emplearse en direcciones de correo electrónico:
>
> - Almohadilla #
> - Et &
> - Apóstrofe '
> - Signo más +
> - Barra /
> - Signo igual -
> - Signo de interrogación ?
> - Acento grave `
> - Barra vertical |
>
> Los siguientes caracteres especiales no pueden emplearse:
>
> - Asterisco *
> - Signo de exclamación !
> - Símbolo de porcentaje %
> - Espacio en blanco
> - Coma ,

8. > **Importante:**
>
> La contraseña debe cumplir las normas sobre contraseñas. Las normas sobre contraseñas se muestran al colocar el puntero del ratón sobre el símbolo de encima del campo.

En el campo **Contraseña**, introduzca una contraseña que el propietario del buzón de correo pueda emplear para acceder a Control Panel en calidad de usuario.

9. En el menú desplegable de **Entorno**, seleccione el entorno al que dirigir el tráfico de correo entrante del buzón.

> **Nota:**
>
> El entorno determina el servidor de destino al cual debe dirigirse el tráfico de correo entrante del buzón. El tráfico de correo entrante puede dirigirse al entorno primario (véase Configurar el entorno primario en la página 484) o a un entorno secundario (véase Entornos secundarios en la página 120) del dominio. Los clientes que hayan configurado la sincronización de los buzones de correo de su entorno primario con un servicio de directorio, solo pueden seleccionar entornos secundarios.

10. Haga clic en **Añadir**.

El buzón de correo se crea y se añade a la lista de buzones de correo.

Se ha añadido un buzón de correo al dominio en Control Panel.

Importar buzones de correo desde un archivo CSV

En lugar de introducir buzones de correo manualmente en Control Panel, puede importarlos desde un archivo CSV en el módulo **Configuración de cliente** > **Buzones**. Puede importar buzones de correo tanto inicialmente, antes de que se hayan creado otros buzones de correo en Control Panel, como posteriormente, a modo de complemento. En el proceso es posible actualizar o eliminar los registros presentes en Control Panel, según se desee. Durante la importación, los buzones de correo principales se importan a Control Panel junto con sus direcciones alias, entornos y otros datos.

> **Nota:**
>
> Para más información sobre los datos que se pueden importar, véase Archivos CSV para la importación de buzones de correo en la página 244.

Nota:

Los buzones de correo de tipo LDAP (véase Tipos de buzón de correo en la página 235) no pueden importarse desde un archivo CSV.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al cual desee importar buzones de correo.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en **Importar CSV**.

   Se abre un menú.

Figura 173: Menú de importación de buzones de correo desde archivos CSV

5. **PRECAUCIÓN:**

   Durante una importación con la opción **Conservar solo los usuarios del archivo y eliminar el resto.**, los buzones de correo presentes en Control Panel se eliminan.

   Para evitar la pérdida de datos, exporte los buzones de correo existentes antes de la importación. Aunque el formato de los archivos exportados no es válido para la importación, estos archivos pueden ser útiles con fines informativos.

   Opcional: Para eliminar todos los buzones de correo presentes en el sistema antes de realizar la importación, marque la casilla **Conservar solo los usuarios del archivo y eliminar el resto.**.

6. Haga clic en **Cargar archivo**.

> **Nota:**
>
> Si no se trata de la primera importación, el texto del botón es **Iniciar importación nueva.**.

Se abre una ventana de selección de archivos.

7.

> **Importante:**
>
> Para que un archivo CSV externo pueda importarse correctamente en Control Panel, éste deberá respetar ciertas reglas de formato, estructura interna y sintaxis (véase Archivos CSV para la importación de buzones de correo en la página 244). El archivo CSV debe tener un tamaño máximo de 100 MB.

Seleccione el archivo CSV deseado.

Control Panel lee el archivo. Si el archivo está en formato adecuado, Control Panel analiza los datos de buzones de correo e intenta importarlos. Los buzones de correo que aún no estén disponibles se crean en Control Panel, y aquéllos que ya lo estén se actualizan. A

continuación se muestra un resumen de los buzones de correo añadidos y actualizados, así como, en su caso, de los registros de CSV incorrectos, indicándose el tipo de error.

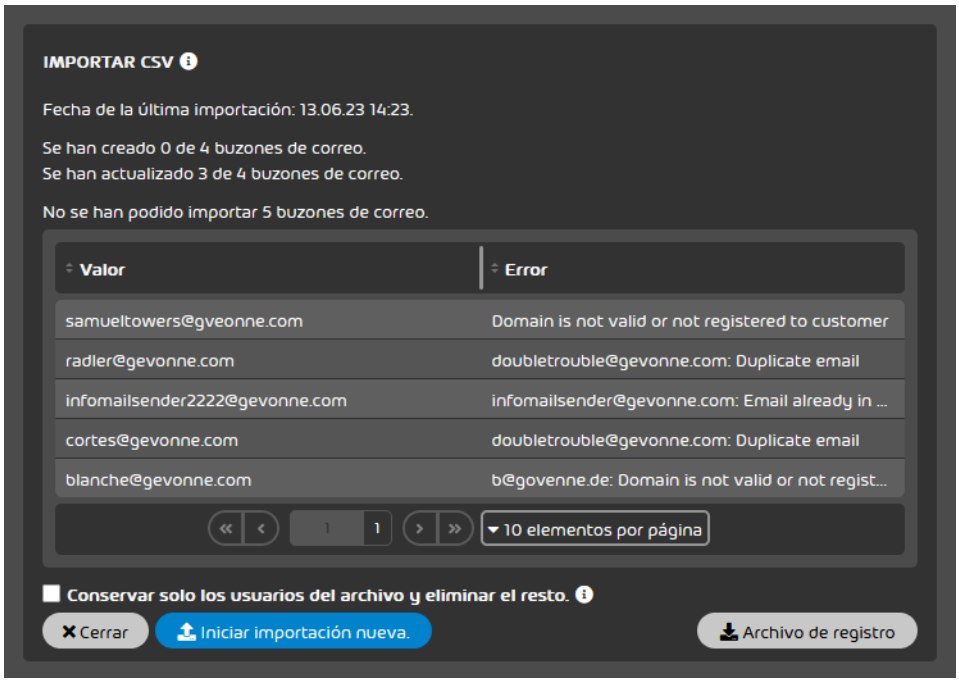


Figura 174: Resultado de la importación

Nota:

Dependiendo del tamaño del archivo, la importación puede tardar un tiempo. Durante la importación, el progreso de la operación se muestra en el módulo **Configuración de cliente** > **Buzones**. Para archivos con más de 1000 registros, el progreso se indica en pasos de 1000 registros. El administrador puede salir del módulo sin que se interrumpa la importación para volver más tarde.

Nota:

Para más información sobre los tipos de errores posibles, véase Errores al importar buzones de correo en la página 249.

8. Opcional: Para conocer más detalles sobre el resultado de la importación, haga clic en **Archivo de registro**.

   Se descarga un archivo de registro llamado **task.log**. El archivo contiene una lista de buzones de correo en la que se indica la hora de procesamiento, el resultado de la importación y los errores que se han producido.

9. Haga clic en **Cerrar**.

   El menú se cierra.

Se han importado buzones de correo desde un archivo CSV y se han añadido al dominio seleccionado en Control Panel.

Nota:

Los resultados de la última importación se mantienen en el sistema. Los administradores pueden ver los resultados en el punto **Importar CSV** del módulo **Configuración de cliente** > **Buzones**.

Archivos CSV para la importación de buzones de correo

Para que un archivo CSV externo con datos de buzones de correo pueda importarse correctamente en Control Panel (véase Importar buzones de correo desde un archivo CSV en la página 240), deberá cumplir reglas respecto a su extensión y su estructura interna.

Requisitos para archivos CSV

- La extensión del archivo a importar será **.csv**. No se aceptan o extensiones, tales como .txt o .docx.
- El archivo CSV debe estar codificado en UTF-8.
- El archivo CSV tiene un tamaño máximo de 100 MB.

Columnas

El archivo CSV contiene 19 columnas separadas entre sí por punto y coma. Estas columnas están reservadas para los siguientes datos:

1. Dirección de correo electrónico primaria del buzón.

   > **Importante:**
   >
   > Esta columna no debe estar vacía en ninguna fila.

2. Dirección alias del buzón de correo
3. Entorno del buzón de correo. El entorno determina el servidor de destino al cual debe dirigirse su tráfico de correo entrante (véase Entornos secundarios en la página 120).

   > **Importante:**
   >
   > Esta columna no debe estar vacía en ninguna fila.

4. Nombre del usuario
5. Apellidos del usuario
6. Nombre de usuario mostrado en Control Panel
7. País o región en que tiene su domicilio la organización del usuario
8. Estado federado o cantón en el que tiene su domicilio la organización del usuario
9. Código postal de la organización del usuario
10. Municipio en que tiene su domicilio la organización del usuario
11. Calle y número en que tiene su domicilio la organización del usuario
12. Departamento al que pertenece el usuario
13. Oficina en que trabaja el usuario

14. Número de teléfono profesional del usuario
15. Número de teléfono móvil del usuario
16. Número de fax del usuario
17.
18.
19. Grupos a los que pertenece el buzón de correo (véase Grupos en la página 288)

> **Importante:**
>
> La primera columna (dirección de correo electrónico primaria) y la tercera (entorno) deben contener datos. El resto de columnas son opcionales y, por tanto, pueden dejarse en blanco. Sin embargo, cada fila debe contener 18 puntos y comas como carácter de separación.

> **Nota:**

Filas

- Las filas de los archivos CSV terminan sin signos de puntuación.
- La primera fila contendrá los nombres de las columnas. Los nombres de la columnas pueden elegirse libremente y no afectan al resultado de la importación. Sin embargo, por mayor claridad, se recomienda utilizar nombres de columna descriptivos.

Direcciones de buzones de correo

- Las direcciones de los buzones de correo deben estar en formato correcto (según el patrón **parte-local@nombre-de-host.domino-de-nivel-superior**).

> **Importante:**
>
> Las direcciones con estructura incorrecta se ignorarán durante la importación.

- Las direcciones de los buzones de correo pertenecen a dominios creados para los clientes en Control Panel.

> **Importante:**
>
> Las direcciones de buzones de correo de otros dominios no se importan a Control Panel.

Direcciones alias

- Las direcciones alias (en la segunda columna) solo pueden indicarse en combinación con la dirección primaria del buzón de correo (en la primera columna). La primera columna no debe dejarse nunca vacía.
- Si la segunda columna de una fila contiene varias direcciones alias, éstas deberán separarse entre sí mediante comas.

Buzón de correo principal sin dirección alias y en el entorno primario (sin datos adicionales):

buzónprincipal@solo.es;;primary;;;;;;;;;;;;;;;;

Buzón de correo principal con una dirección alias y en el entorno primario (sin datos adicionales):

buzónprincipal@ejemplo.es;alias@ejemplo.es;primary;;;;;;;;;;;;;;;;

Buzón de correo principal con varias direcciones alias y en el entorno primario (sin datos adicionales):

buzónprincipal@ejemplo.es;alias1@ejemplo.es,alias2@ejemplo.es;primario;;;;;;;;;;;;;;;;

Entornos

- Los entornos que deben asignarse a los buzones de correo a importar en Control Panel deben indicarse en la tercera columna.
- Para el entorno primario debe emplearse el nombre **primary**. Para los entornos secundarios se emplearán los nombres con los que estén registrados en Control Panel. Los nombres de los entornos no distinguen entre mayúsculas y minúsculas.

> **Importante:**
>
> Los registros con entornos secundarios solo pueden importarse de un archivo CSV si los entornos secundarios se han creado previamente en Control Panel (véase Crear un entorno secundario en la página 123).

Buzón de correo principal con una dirección alias y entorno primario (sin datos adicionales):

buzónprincipal@ejemplo.es;alias@ejemplo.es;primary;;;;;;;;;;;;;;;;

Buzón de correo principal con una dirección alias y entorno secundario (sin datos adicionales):

buzónprincipal@ejemplo.es;alias@ejemplo.es;entorno2;;;;;;;;;;;;;;;;

Grupos

- Los grupos a los que pertenecen los buzones a importar se indican en la columna número 19.
- Si una celda de la columna número 19 contiene varios grupos, éstos deberán separarse entre sí mediante comas.

Registros duplicados

- Los registros duplicados no hacen que la importación falle durante el procesamiento del archivo CSV, pero deben evitarse.
- El archivo no contendrá filas con idéntico contenido en la columna izquierda y distinto contenido en las otras columnas.

Importante:

Las filas con un mismo buzón principal no se importarán si el archivo contiene alguna otra fila con el mismo buzón principal pero direcciones alias diferentes u otro entorno.

Filas incorrectas con el mismo buzón de correo principal, direcciones alias distintas y entorno primario (sin datos adicionales):

buzónprincipal@ejemplo.es;alias1@ejemplo.es,alias2@ejemplo.es;primary;;;;;;;;;;;;;;;;
buzónprincipal@ejemplo.es;alias3@ejemplo.es;primary;;;;;;;;;;;;;;;;

Errores al importar buzones de correo

Durante la importación de buzones de correo (véase Importar buzones de correo desde un archivo CSV en la página 240), Control Panel efectúa diversas comprobaciones consecutivas que pueden resultar en diversos errores. En primer lugar se valida el archivo CSV y, a continuación, se comprueban y procesan los datos de buzones de correo que contiene.

Errores durante la validación de archivos CSV

El archivo CSV se valida en cuanto el usuario lo selecciona para la importación de buzones de correo. Durante la validación se comprueba, entre otras cosas, que el archivo CSV tenga un formato correcto. Pueden producirse los siguientes errores:

- **Ha ocurrido un error al cargar el estado de la importación en curso.**
- **Ha ocurrido un error al validar el archivo.**
- **Ha ocurrido un error al procesar el archivo.**
- **El archivo contiene una línea demasiado larga.**: El archivo contiene una fila con un tamaño superior a 1 MiB (véase Archivos CSV para la importación de buzones de correo en la página 244).
- **La codificación del archivo debe ser {{encodingType}}.**: El archivo no está codificado en UTF-8 (véase Archivos CSV para la importación de buzones de correo en la página 244).
- **El servicio de carga no se encuentra accesible en este momento.**

- **El archivo tiene un número de columnas incorrecto.**: El archivo no contiene 19 columnas en cada fila (véase Archivos CSV para la importación de buzones de correo en la página 244).

Errores durante el procesamiento de buzones de correo

Una vez validado el archivo CSV, sus datos de buzones de correo se comprueban en cuanto a su formato y a la presencia de repeticiones. También se comprueba si los entornos (véanse Configuración del entorno primario en la página 483 y Entornos secundarios en la página 120) y dominios (véase Dominios en la página 307) existen en Control Panel y están asignados al cliente, así como si los buzones de correo pertenecen a un entorno cuyos buzones se sincronicen con un servicio de directorio.

1. **Data is invalid**: Algunos datos de buzones de correo no están en formato correcto, sin más indicación.
2. **Email is not valid**: La dirección de correo electrónico indicada no está en formato correcto.
3. **Domain is not valid or not registered to customer**: El dominio de la dirección de correo electrónico indicada (primaria o alias) no está registrado para el cliente en Control Panel (véase Añadir dominios alias en la página 307).
4. **Email already in use**: Ya existe un buzón de correo con la misma dirección en Control Panel.
5. **Unknown error**: Se ha producido un error desconocido.
6. **User creation failed**: No se ha podido crear un usuario para el buzón de correo en Control Panel.
7. **Failed to import**: Por alguna otra razón, no se ha podido importar el registro.
8. **Synchronized mailboxes needs to be changed in the source system**: El registro afectado se refiere a un buzón de correo que se sincroniza con un servicio de directorio en Control Panel.
9. **Unable to assign the primary environment to the manual mailbox**: Los buzones de correo primarios del entorno primario (véase Configuración del entorno primario en la página 483)

se sincronizan con un servicio de directorio. Por tanto, no es posible asignar un buzón de correo creado manualmente a este entorno.

10. **The primary email appeared on two users in the request at the same time**: El archivo CSV contiene dos registros con la misma dirección de correo en la primera columna (véase Archivos CSV para la importación de buzones de correo en la página 244).

11. **Duplicate email**: La dirección de correo se utiliza en más de un registro, ya sea como dirección primaria o como dirección alias.

Exportar buzones de correo en formato CSV

Ha añadido un buzón de correo a Control Panel (véanse Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

Para evitar la pérdida de datos de los buzones de correo de su dominio, puede exportar dichos datos en formato CSV. Durante la exportación se exportan todos los buzones de correo registrados en el dominio en Control Panel.

Importante:

Los archivos de exportación no están destinados a su importación en Control Panel (véase Importar buzones de correo desde un archivo CSV en la página 240), ya que se encuentran en un formato distinto (véase Archivos CSV para la importación de buzones de correo en la página 244).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyos buzones de correo desee exportar.
3. Vaya a **Configuración de cliente** > **Buzones**.

4. Haga clic en **Exportar como CSV**.

Se muestra un formulario.

Figura 175: Formulario de exportación en formato CSV

5. Marque las casillas de los datos que desee exportar en **Exportación de datos**.

- **Nombre**: Se exportan las direcciones de los buzones de correo principales.
- **Tipo**: Se exportan los tipos de los buzones de correo principales (véase Buzones de correo en la página 230).
- **Alias**: Si los buzones de correo principales tienen asignadas direcciones alias, éstas también se exportan.
- **Entorno**: Se exportan los entornos de los buzones de correo (véase Añadir un buzón de correo en la página 237).
- **Seleccionar/deseleccionar todo**: Se marcan o desmarcan todas las casillas anteriormente descritas.

6. Opcional: Si solo desea exportar datos de una selección de buzones de correo, proceda del siguiente modo:

   a) En el módulo, haga clic en .

   Aparece una columna con casillas en la tabla.

   b) Seleccione las filas cuyos datos desee exportar.

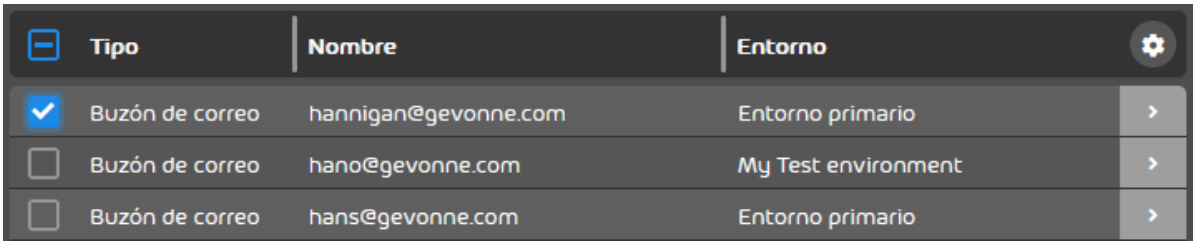


Figura 176: Seleccionar filas

   La casilla **Exportar solo líneas seleccionadas** se habilita en el formulario.

   c) Marque la casilla **Exportar solo líneas seleccionadas**.

Figura 177: Exportar las filas seleccionadas

7. En **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o enviarlo por correo electrónico.
   - **Descargar**: El archivo CSV se facilita para su descarga.
   - **Por correo electrónico**: El archivo CSV se envía por correo electrónico.

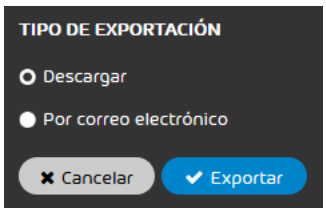


Figura 178: Seleccionar el tipo de exportación

Si se elige la opción **Por correo electrónico**, se muestra un campo adicional.

8. Opcional: Si elige la opción **Por correo electrónico**, introduzca en el campo la dirección de correo electrónico a la que enviar el archivo CSV.

Figura 179: Introducir una dirección de correo electrónico

9. Haga clic en **Exportar**.

El archivo se ofrece para su descarga o se envía por correo electrónico.

Se han exportado buzones de correo en formato CSV.

Añadir un buzón de reenvío

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** puede crear buzones de reenvío para buzones de correo ya registrados. Los buzones de reenvío pueden reenviar su tráfico de correo hasta a un máximo de 100 buzones de correo internos o externos.

Importante:

El tamaño máximo permitido de los correos reenviados mediante buzones de reenvío está limitado y depende de la cantidad de destinatarios del reenvío. La siguiente tabla indica el tamaño permitido por cantidad de destinatarios.

CANTIDAD DE DESTINATARIOS	TAMAÑO MÁXIMO PERMITIDO DE CORREO (MB)
1	100
2-9	50
10-24	25
25-49	15
50-100	10

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al cual desee añadir un buzón de reenvío.
3. Vaya a **Configuración de cliente** > **Buzones**.

4. Haga clic en **Añadir buzón de reenvío**.

Se despliega un menú desplegable.

5. En **Correo electrónico**, indique el buzón de correo al que desee añadir un buzón de reenvío. (1)
6. Para añadir un buzón de correo de reenvío,
   - seleccione un buzón de correo registrado de la lista de (2a) o
   - introduzca una dirección válida en el campo **Buzón externo** (2b) y confirme con **Añadir**.

> **Nota:**
>
> Repita este paso si desea añadir más buzones de reenvío.

Los buzones se muestran en la lista **Reenviado a**.

7. Haga clic en **Añadir** (3) para establecer el reenvío.

Se ha añadido un buzón de reenvío.

Añadir un buzón de correo a un grupo

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240). Ha creado un grupo (véase Crear un grupo en la página 290).

En lugar de añadir buzones de correo a un grupo en el módulo **Grupos** (véase Administrar miembros en la página 297), puede añadir un buzón de correo a un grupo en el módulo **Buzones** (véase Grupos en la página 288).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio a cuyos grupos desee añadir un buzón de correo.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo que desee añadir a un grupo.

   Se abre un menú.

Figura 180: Acciones para buzones de correo

5. Haga clic en **Grupos**.

Se abre un menú para la administración de grupos. Aquí se muestran todos los grupos a los que pertenece el buzón de correo.

Figura 181: Menú de grupos

6. Introduzca en el campo el nombre del grupo al que desee añadir el buzón de correo.
7. Haga clic en **Añadir**.

El buzón de correo se añade al grupo. El grupo se muestra en la lista de grupos.

Se ha añadido un buzón de correo a un grupo.

A continuación puede eliminar el buzón de correo del grupo (véase Quitar un buzón de correo de un grupo en la página 258).

Quitar un buzón de correo de un grupo

Ha creado un buzón y lo ha añadido a un grupo (véase Añadir un buzón de correo a un grupo en la página 257).

En lugar de quitar buzones de correo de un grupo en el módulo **Grupos** (véase Administrar miembros en la página 297), puede quitar un buzón de correo de un grupo en el módulo **Buzones** (véase Grupos en la página 288).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el grupo del cual desee quitar un buzón de correo.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo que desee quitar de un grupo.

   Se abre un menú.

Figura 182: Acciones para buzones de correo

5. Haga clic en **Grupos**.

   Se abre un menú para la administración de grupos. Aquí se muestran todos los grupos a los que pertenece el buzón de correo.

Figura 183: Menú de grupos

6. Haga clic en la cruz junto al nombre del grupo del que desee quitar el buzón de correo.

   El buzón de correo se quita del grupo. El grupo se ha retirado de la lista de grupos.

Se ha quitado un buzón de correo de un grupo.

Activar o desactivar un buzón de correo

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

Solo los usuarios con buzones de correo activados en Control Panel pueden iniciar sesión en él. Nuestros servicios se aplican y facturan tanto sobre buzones activados como sobre desactivados. Puede activar y desactivar buzones de correo en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo que desee activar o desactivar.

Figura 184: Abrir el menú

   Se abre un menú.

5. Haga clic en el botón **Activo** o **Inactivo**.

   Se despliega un menú desplegable.

6. Haga clic en **Activar** o **Desactivar**.

El buzón de correo se activa o desactiva. En función del estado de activación, el símbolo de activación se mostrará en blanco ("activado") o rojo ("desactivado").

Se ha activado o desactivado un buzón de correo.

Añadir una dirección alias

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** puede añadir direcciones alias a direcciones de correo principales. Las direcciones alias se asignan a buzones de correo principales. En el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63), los propietarios de buzones de correo principales pueden ver también los correos de las direcciones alias. Puede añadir varias direcciones alias a un solo buzón de correo principal. Las direcciones alias son gratuitas.

Nota:

No es posible asignar direcciones alias a buzones de correo de tipo LDAP (véase Tipos de buzón de correo en la página 235).

Atención:

Si los datos de los buzones de correo de un cliente no se sincronizan a través de un servicio de directorio, el cliente deberá añadir todas las direcciones alias del dominio manualmente a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240). De lo contrario, durante la creación automática de buzones de correo, las direcciones alias (véase Creación automática de buzones de correo en la página 236) no serían reconocidas como direcciones alias de buzones de correo principales existentes, sino como nuevos buzones de correo principales. Esto implicaría la creación de buzones de correo principales en Control Panel para las direcciones alias, con el consiguiente coste (véase Buzones de correo en la página 230).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del buzón de correo principal al cual desee añadir una dirección alias.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo al que desee añadir una dirección alias.

Figura 185: Abrir el menú

Se abre un menú.

5. Haga clic en **Alias**.

Se abre un menú.

6. En **Alias**, introduzca el alias deseado seguido del dominio, y haga clic en **Añadir**.

Figura 186: Introducir una dirección alias

La dirección alias se añade.

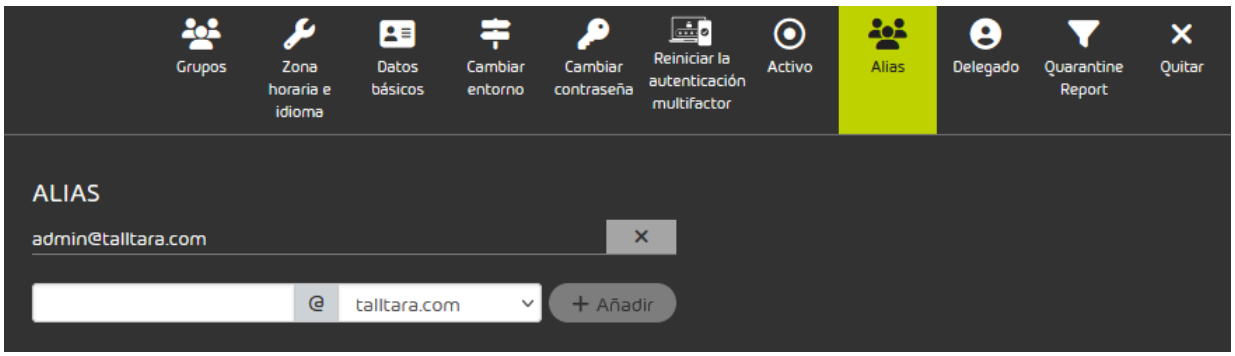


Figura 187: Dirección alias añadida

Se ha añadido una dirección alias a un buzón de correo principal.

Designar un delegado

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** puede designar un delegado para un buzón de correo principal. Los delegados tienen acceso a los correos para los cuales están registrados como tales en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63), y pueden efectuar allí acciones sobre los mismos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del buzón de correo al cual desee añadir un delegado.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú del buzón de correo deseado.

5. Haga clic en **Delegado**.

   Se despliega un menú desplegable.
6. Marque la casilla **Activar delegación de acceso**

   Aparece una lista de usuarios registrados.
7. Seleccione un delegado de la lista y haga clic en **Añadir**.

   El delegado se añade al buzón de correo. Por motivos de seguridad, el usuario a cuyo buzón de correo se ha asignado un delegado recibe una notificación al respecto por correo electrónico.

Se ha designado un delegado para un buzón de correo.

Importar destinatarios de buzones de reenvío desde un archivo CSV

En lugar de añadir destinatarios para buzones de reenvío manualmente, puede importarlos mediante una lista CSV en el módulo **Configuración de cliente** > **Buzones**. Esto puede realizarse tanto al principio, cuando aún no se han registrado datos, como posteriormente, a modo de complemento.

Nota:

No es posible asignar buzones de correo de reenvío a buzones de correo de tipo LDAP (véase Tipos de buzón de correo en la página 235). Por tanto, no es posible importar remitentes para buzones de reenvío para este tipo de buzones desde un archivo CSV.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Buzones**.

4. Haga clic en **Añadir**.

Se muestra un nuevo formulario.

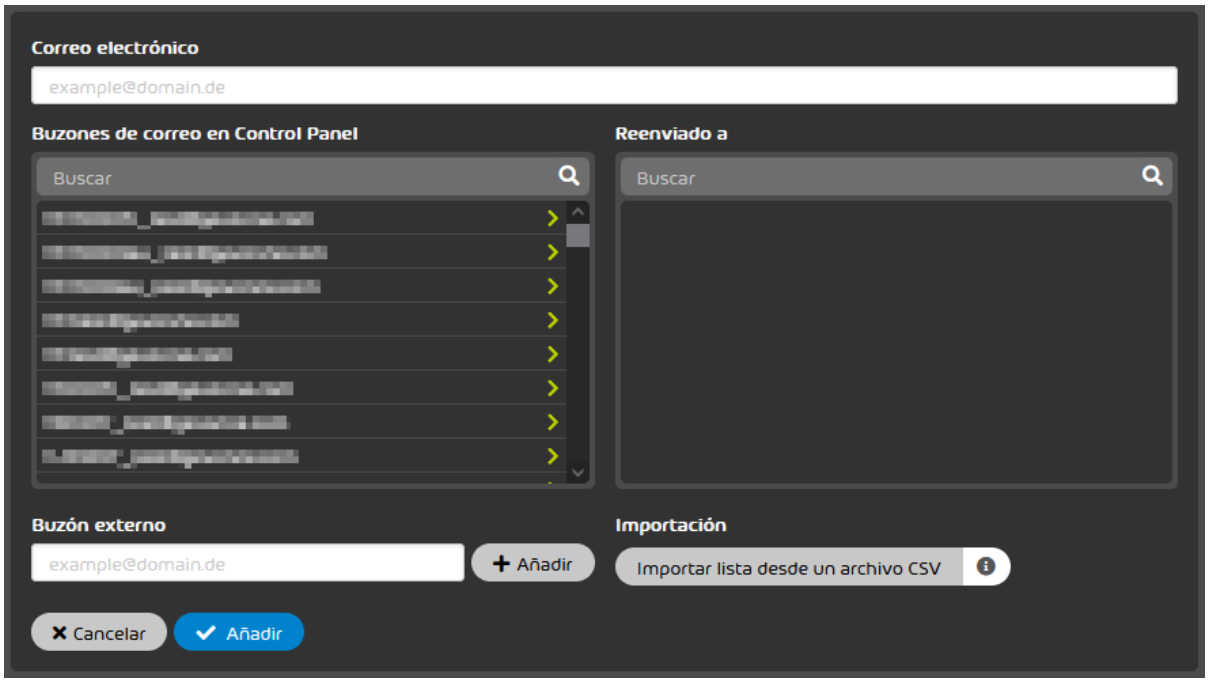


Figura 188: Importar destinatarios para un buzón de reenvío desde un archivo CSV

5. En **Correo electrónico**, introduzca la dirección de correo electrónico del buzón de reenvío.
6. Haga clic en **Importar lista desde un archivo CSV**.

Se abre una ventana de selección de archivos.

7. Seleccione el archivo CSV deseado.

> **Importante:**
>
> Para que un archivo CSV externo pueda importarse correctamente en Control Panel, éste deberá cumplir ciertas reglas de formato, estructura interna y sintaxis (véase Archivos CSV para importar destinatarios de buzones de reenvío en la página 267).

8. Haga clic en **Importar lista desde un archivo CSV**.

Los destinatarios se importan desde el archivo CSV y se muestran en el apartado **Reenviado a**.

> **Nota:**
>
> La importación de destinatarios para buzones de reenvío se rige por las siguientes reglas:
>
> - Las direcciones ya enumeradas en **Reenviado a** no se eliminan.
> - Solo se importan registros del archivo CSV que no estén aún incluidos en **Reenviado a**.
> - Los registros que aparecen duplicados en el archivo CSV solo se importan una vez.
> - Los registros con formato incorrecto son ignorados y no provocan la cancelación del proceso. Sin embargo, tras la importación, se informa al usuario sobre la presencia de registros inválidos mediante un mensaje de error.
> - Si el archivo CSV no contiene direcciones válidas que no estén ya en el apartado **Reenviado a**, se muestra un mensaje de error al respecto y no se importa ninguna dirección.

9. Haga clic en **Añadir**.

Se han importado destinatarios para buzones de reenvío desde un archivo CSV.

Archivos CSV para importar destinatarios de buzones de reenvío

Para que un archivo CSV externo con destinatarios de buzones de reenvío pueda importarse correctamente en Control Panel (véase Importar destinatarios de buzones de reenvío desde un archivo CSV en la página 265), deberá cumplir reglas especiales respecto a su extensión y su estructura interna.

Reglas estructurales de archivos CSV para la importación de destinatarios de buzones de reenvío

- La extensión del archivo a importar deberá ser siempre **.csv**. Otras extensiones, tales como .txt o .docx, no están permitidas y no se aceptan.
- El archivo CSV contiene una sola columna en la que se distribuyen verticalmente los diversos registros.
- La primera fila siempre se emplea para el nombre de la columna y puede nombrarse libremente.
- Las direcciones de los destinatarios deberán presentar una estructura correcta (conforme al patrón "partelocal@nombre-de-host.dominio-de-nivel-superior").

  > **Importante:**
  >
  > Las direcciones con estructura incorrecta se ignorarán durante la importación.

- Cada fila deberá contener una única dirección.
- Los registros dobles no afectan al procesamiento del archivo, pero deberán evitarse.

Configurar la zona horaria y el idioma de un buzón de correo

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** (véase Buzones de correo en la página 230) puede configurar una zona horaria, un idioma, un formato de fecha y un formato de hora distintos a los del dominio (véase el capítulo "Ajustar zona horaria e idioma por defecto" en el manual de Control Panel) para un buzón de correo individual. Los ajustes se aplican a la visualización en Control Panel y a los correos automáticos de Control Panel. Los datos de este módulo se sincronizan con los datos del usuario en la sección **Zona horaria e idioma** de **Configuración de usuario** (véase Cambiar la zona horaria y el idioma en la página 37).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del buzón de correo cuya configuración desee modificar.

3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo cuya configuración desee modificar.

Figura 189: Abrir el menú

Se abre un menú.

Figura 190: Menú

5. Haga clic en **Zona horaria e idioma**.

Se muestra un formulario.

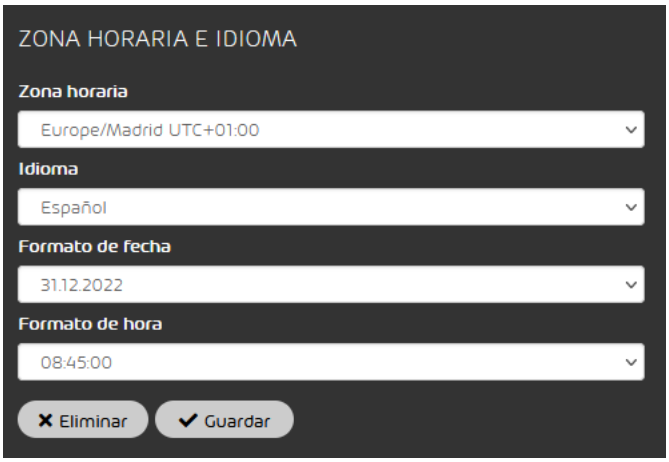


Figura 191: Zona horaria e idioma

6. Seleccione una zona horaria en el menú desplegable **Zona horaria**.

> **Nota:**
>
> La zona horaria determina el formato de número en Control Panel y en los correos automáticos de Control Panel.

7. Seleccione un idioma en el menú desplegable **Idioma**.
8. Seleccione un formato de fecha en el menú desplegable **Formato de fecha**.

> **Nota:**
>
> El formato de fecha determina el orden en el que se muestran los datos que estén disponibles para una fecha. Si no hay informaciones disponibles para todos los datos, no se muestran los datos que faltan.

9. Seleccione un formato de hora en el menú desplegable **Formato de hora**.

> **Nota:**
>
> El formato de hora determina el orden en el que se muestran los datos que estén disponibles para una hora. Si no hay informaciones disponibles para todos los datos, no se muestran los datos que faltan.

10. Haga clic en **Guardar**.

Los cambios se guardan.

> **Nota:**
>
> Los cambios no se aplicarán hasta que el usuario para el que se han realizado los cambios actualice la página o vuelva a iniciar sesión en Control Panel.

Se han configurado la zona horaria, el idioma, el formato de fecha y el formato de hora de un buzón de correo.

Editar los datos básicos de un buzón de correo

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

Los datos básicos son datos relativos al propietario de un buzón de correo. En el módulo **Configuración de cliente** > **Buzones** puede añadir datos básicos a buzones de correo.

Nota:

No es posible editar los datos básicos de buzones de correo de tipo LDAP (véase Tipos de buzón de correo en la página 235) en Control Panel. Si hay definidos datos básicos para un buzón de correo en un servicio de directorio sincronizado mediante LDAP, dichos datos se mostrarán en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el cliente en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo cuyos datos desee editar.

   Se abre un menú.

Figura 192: Menú

5. Haga clic en **Datos básicos**.

Se muestra un formulario.

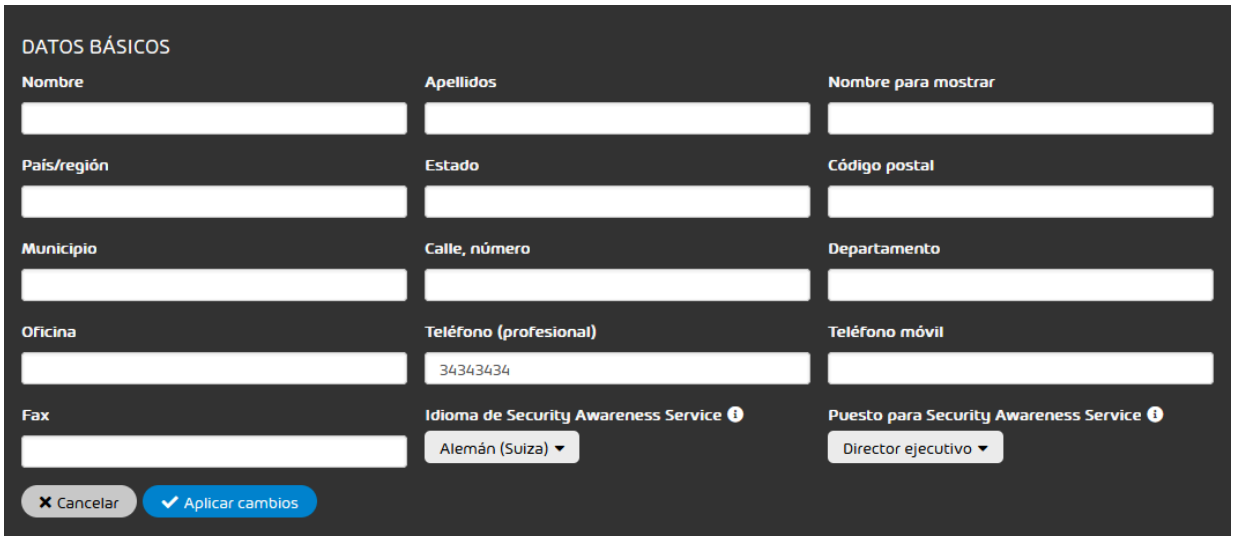


Figura 193: Datos básicos

6.

Nota:

Todos los campos son opcionales.

Nota:

En los campos **Teléfono (profesional)**, **Teléfono móvil** y **Fax**, los números de teléfono o fax deben introducirse en el siguiente formato:

- Prefijo de país: 00 o + y prefijo de país de dos dígitos. Opcionalmente también es posible escribir el prefijo de país entre paréntesis. He aquí algunos ejemplos de prefijos de país correctos: **(0034)**, **(+34)**, **0049**, **+49**.
- Espacio, punto o guion para separar el prefijo de país del prefijo provincial (opcional).
- Prefijo provincial o de telefonía móvil de cinco dígitos como máximo.
- Espacio, punto o guion para separar el prefijo provincial o de telefonía móvil del número de teléfono (opcional).
- Número de teléfono de cualquier longitud.

He aquí algunos ejemplos de números de teléfono o fax correctos:

- **(0034) 7432 1354913**
- **+49.157.1354913**
- **0049 157-1354913**

Introduzca en el formulario los datos del usuario al que pertenezca el buzón de correo. Los campos tienen los siguientes significados:

- **Nombre**: Nombre del usuario
- **Apellidos**: Apellidos del usuario
- **Nombre para mostrar**: Nombre de usuario mostrado en Control Panel
- **País/región**: País o región en que tiene su domicilio la organización del usuario
- **Estado**: Estado federado o cantón en el que tiene su domicilio la organización del usuario
- **Código postal**: Código postal de la organización del usuario

- **Municipio**: Municipio en que tiene su domicilio la organización del usuario
- **Calle, número**: Calle y número en que tiene su domicilio la organización del usuario
- **Departamento**: Departamento al que pertenece el usuario
- **Oficina**: Oficina en que trabaja el usuario
- **Teléfono (profesional)**: Número de teléfono profesional del usuario
- **Teléfono móvil**: Número de teléfono móvil del usuario
- **Fax**: Número de fax del usuario

7. Haga clic en **Aplicar cambios**.

   Los cambios se guardan.

Los datos básicos de un buzón de correo se han editado.

Cambiar la contraseña de emergencia

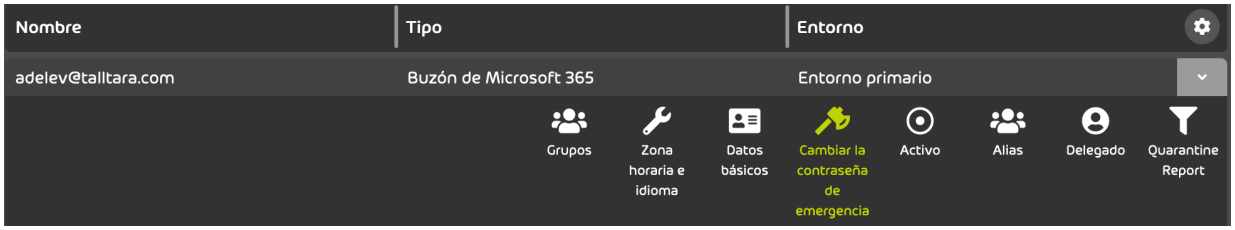
Sus buzones de correo se sincronizan mediante LDAP obligado a sus usuarios definir una contraseña de emergencia (véase Activar la contraseña de emergencia).

En el módulo **Configuración de cliente** > **Buzones** puede cambiar la contraseña de emergencia de un buzón de correo.

> **Nota:**
>
> Las contraseñas de emergencia solo pueden modificarse para buzones de correo de tipo LDAP (véase Tipos de buzón de correo en la página 235).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Buzones**.

4. Haga clic en la flecha de menú junto al buzón de correo cuya contraseña de emergencia desee cambiar.



5. Haga clic en **Cambiar la contraseña de emergencia**.

Se muestra un campo de introducción de datos.

6. Introduzca la nueva contraseña de emergencia en el campo de introducción de datos.

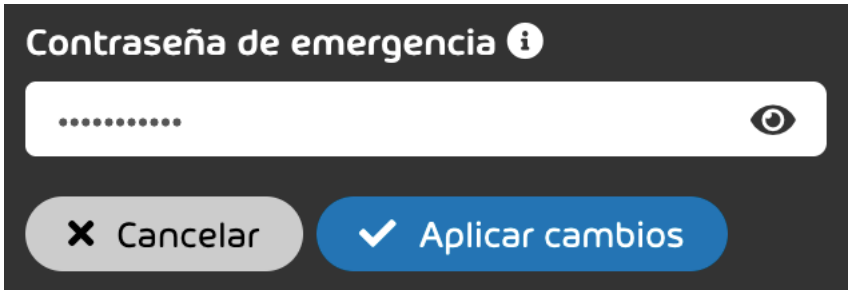


Figura 194: Cambiar la contraseña de emergencia

7. Haga clic en **Aplicar cambios**.

La contraseña de emergencia se guarda.

Se ha cambiado la contraseña de emergencia de un buzón de correo.

Cambiar de entorno

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).
Ha definido el servidor de destino al cual dirigir el tráfico de correo entrante del buzón de correo como entorno primario (véase Configurar el entorno primario en la página 484) o secundario (véase Crear un entorno secundario en la página 123).

El entorno de un buzón de correo determina el servidor de destino al cual debe dirigirse el tráfico de correo entrante del buzón. Los buzones de correo tienen asignados por defecto el entorno primario (véase Configuración del entorno primario en la página 483). Si desea dirigir el tráfico de correo entrante de determinados buzones de correo a otro servidor de destino, puede asignarles un entorno secundario en lugar del primario (véase Entornos secundarios en la página 120). Puede cambiar los entornos de los buzones de correo en el módulo **Configuración de cliente** > **Buzones**. No es posible asignar entornos a buzones de reenvío (véase Tipos de buzón de correo en la página 235) y buzones de correo sincronizados en Control Panel, ya que los buzones de reenvío se administran sin entorno en Control Panel y a los buzones de correo sincronizados se les asigna como entorno su sistema original.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del buzón de correo cuyo entorno desee cambiar.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo cuyo entorno desee cambiar.

Figura 195: Abrir el menú

Se abre un menú.

5. Haga clic en **Cambiar entorno**.

   Se muestra un formulario.

6. En el menú desplegable de **Entorno**, seleccione el entorno al que dirigir el tráfico de correo entrante del buzón.

Figura 196: Seleccionar un entorno

7. Haga clic en **Aplicar cambios**.

Se ha cambiado el entorno del buzón de correo.

Cambiar la contraseña

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** puede cambiar la contraseña de un buzón de correo creado manualmente (véase Tipos de buzón de correo en la página 235).

Nota:

Las contraseñas de los buzones de correo de tipo LDAP no pueden cambiarse en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Buzones**.

4. Haga clic en la flecha de menú junto al buzón de correo cuya contraseña desee cambiar.

Figura 197: Abrir el menú

Se abre un menú.

5. Haga clic en **Cambiar contraseña**.

Se abre un menú.

6.
> **Importante:**
>
> La nueva contraseña debe cumplir las reglas definidas en el módulo **Autenticación** (véase Autenticación en la página 319).

> **Importante:**
>
> Por razones de seguridad, la nueva contraseña no debe ser idéntica a la anterior.

Introduzca la nueva contraseña en el campo **Contraseña nueva**.

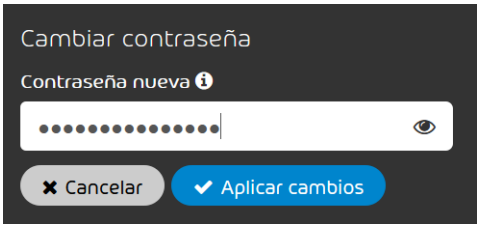


Figura 198: Introducir contraseña

7. Haga clic en **Aplicar cambios**.

   La contraseña se guarda. Se muestra un mensaje de confirmación. Por motivos de seguridad, el usuario recibe una notificación acerca del cambio de contraseña por correo electrónico.

Se ha cambiado la contraseña de un buzón de correo creado manualmente.

Reiniciar la autenticación multifactor

Ha habilitado la autenticación multifactor para los usuarios de un dominio (véase Habilitar la autenticación multifactor en la página 323). Un usuario del dominio ha configurado la autenticación multifactor para su cuenta de Control Panel (véase "Configurar la autenticación multifactor" en el manual de Control Panel).

Si un usuario tiene problemas con la autenticación multifactor (véase "Solución de problemas: Problemas con la autenticación multifactor" en el manual de Control Panel), puede reiniciar la autenticación multifactor para el usuario. De este modo, la autenticación multifactor se desactivará para el usuario y su configuración de la autenticación multifactor se eliminará.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del usuario para el cual desee reiniciar la autenticación multifactor.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo para el cual desee reiniciar la autenticación multifactor.

   Se abre un menú.

Figura 199: Menú

5. Haga clic en **Reiniciar la autenticación multifactor**.

Se abre una vista avanzada.

6. Haga clic en **Reiniciar la autenticación multifactor**.

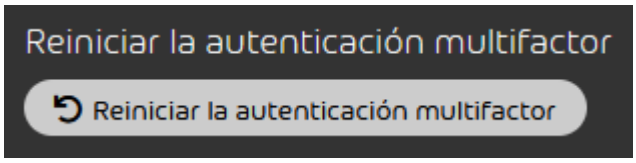


Figura 200: Reiniciar la autenticación multifactor

Aparece una ventana de confirmación.

7. Haga clic en **Confirmar**.

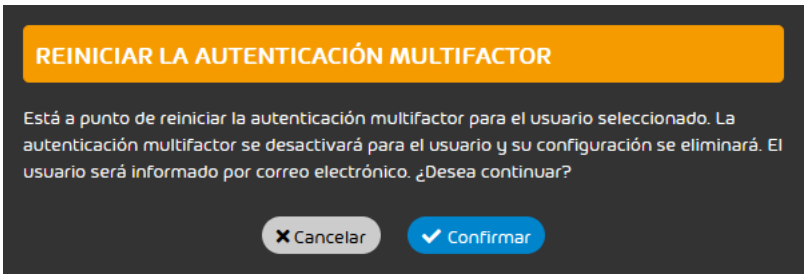


Figura 201: Confirmar

La autenticación multifactor se desactiva para el usuario y su configuración de la autenticación multifactor se elimina. El usuario es informado por correo electrónico de que se ha desactivado la autenticación multifactor para su cuenta. A partir de ahora, el usuario puede iniciar sesión en Control Panel sin utilizar la autenticación multifactor.

La autenticación multifactor se ha reiniciado para un usuario.

El usuario puede reconfigurar la autenticación multifactor para su cuenta (véase "Configurar la autenticación multifactor" en el manual de Control Panel).

Quitar un buzón de correo

Ha añadido un buzón de correo a Control Panel (véase Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** puede quitar buzones de correo creados manualmente (véase Tipos de buzón de correo en la página 235) de Control Panel.

Todos los ajustes relativos a un buzón de correo se eliminan junto a éste. Las consecuencias de la eliminación son las siguientes:

- La conexión a Control Panel se interrumpe y los futuros correos del buzón ya no se procesan mediante nuestros servicios.
- Los propietarios de buzones de correo eliminados no pueden iniciar sesión en Control Panel con sus datos de acceso.
- Los buzones de correo eliminados se eliminan de los grupos (véase Grupos en la página 288) a los que pertenezcan.
- Las asignaciones de roles (véase Roles en la página 53) a usuarios de buzones de correo eliminados también se eliminan.
- Las direcciones alias (véase Añadir una dirección alias en la página 261) de buzones de correo eliminados también se eliminan.
- Los buzones de correo eliminados se eliminan de las listas de reenvíos de buzones de reenvío (véase Añadir un buzón de reenvío en la página 255).
- Los buzones de correo eliminados se eliminan de las listas de delegados (véase Designar un delegado en la página 263) de otros buzones de correo. Las relaciones de delegación entre buzones de correo eliminados y otros buzones de correo también se eliminan.

Los datos relativos a correos dirigidos a buzones de correo eliminados o enviados por éstos se conservan en Control Panel, donde se encuentran accesibles a administradores y usuarios a los cuales se les hayan asignado dichos buzones de correo.

Nota:

La eliminación de un buzón de correo de Control Panel solo afecta a los datos y ajustes de éste en Control Panel. El buzón de correo en sí continúa existiendo.

Importante:

Los buzones de correo de tipo LDAP no pueden quitarse manualmente de Control Panel.

Nota:

Aparte de eliminar buzones de correo individualmente, los administradores pueden también eliminar varios buzones al mismo tiempo (véase Eliminar varios buzones de correo en la página 283).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del que desee eliminar un buzón de correo.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú del buzón de correo deseado.

Figura 202: Abrir el menú

Se abre un menú.

5. Haga clic en **Quitar**.

   Aparece una ventana de confirmación.

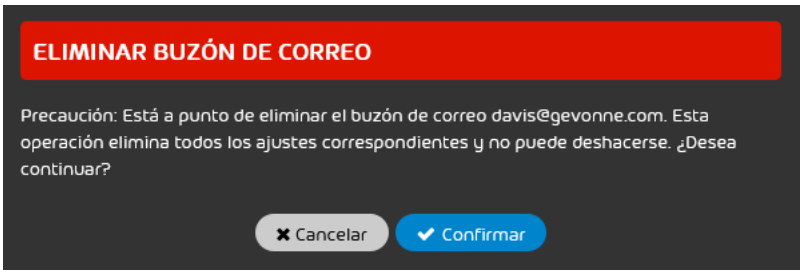


Figura 203: Quitar un buzón de correo

6. Haga clic en **Confirmar**.

   El buzón de correo se quita de Control Panel. Se muestra un mensaje de confirmación.

Se ha eliminado de Control Panel un buzón de correo creado manualmente.

Eliminar varios buzones de correo

Ha añadido un buzón de correo a Control Panel (véanse Añadir un buzón de correo en la página 237 y Importar buzones de correo desde un archivo CSV en la página 240).

En el módulo **Configuración de cliente** > **Buzones** puede eliminar varios buzones de correo creados manualmente (véase Tipos de buzón de correo en la página 235) de Control Panel al mismo tiempo.

Todos los ajustes relativos a un buzón de correo se eliminan junto a éste. Las consecuencias de la eliminación son las siguientes:

- La conexión a Control Panel se interrumpe y los futuros correos del buzón ya no se procesan mediante nuestros servicios.

- Los propietarios de buzones de correo eliminados no pueden iniciar sesión en Control Panel con sus datos de acceso.
- Los buzones de correo eliminados se eliminan de los grupos (véase Grupos en la página 288) a los que pertenezcan.
- Las asignaciones de roles (véase Roles en la página 53) a usuarios de buzones de correo eliminados también se eliminan.
- Las direcciones alias (véase Añadir una dirección alias en la página 261) de buzones de correo eliminados también se eliminan.
- Los buzones de correo eliminados se eliminan de las listas de reenvíos de buzones de reenvío (véase Añadir un buzón de reenvío en la página 255).
- Los buzones de correo eliminados se eliminan de las listas de delegados (véase Designar un delegado en la página 263) de otros buzones de correo. Las relaciones de delegación entre buzones de correo eliminados y otros buzones de correo también se eliminan.

Los datos relativos a correos dirigidos a buzones de correo eliminados o enviados por éstos se conservan en Control Panel, donde se encuentran accesibles a administradores y usuarios a los cuales se les hayan asignado dichos buzones de correo.

Nota:

La eliminación de un buzón de correo de Control Panel solo afecta a los datos y ajustes de éste en Control Panel. El buzón de correo en sí continúa existiendo.

Importante:

Los buzones de correo de tipo LDAP no pueden quitarse manualmente de Control Panel.

Nota:

En lugar de eliminar varios buzones de correo al mismo tiempo, los administradores pueden también eliminar buzones de correo individualmente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al cual desee eliminar buzones de correo.

3. Vaya a **Configuración de cliente** > **Buzones**.
4. En el módulo, haga clic en .

   Aparece una columna con casillas en la lista de dominios.
5. Marque las casillas de los buzones de correo que desee eliminar.

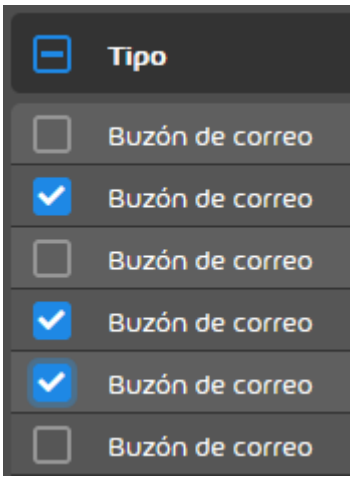


Figura 204: Seleccionar buzones de correo

El botón **Quitar** se habilita.

6. Haga clic en **Quitar**.

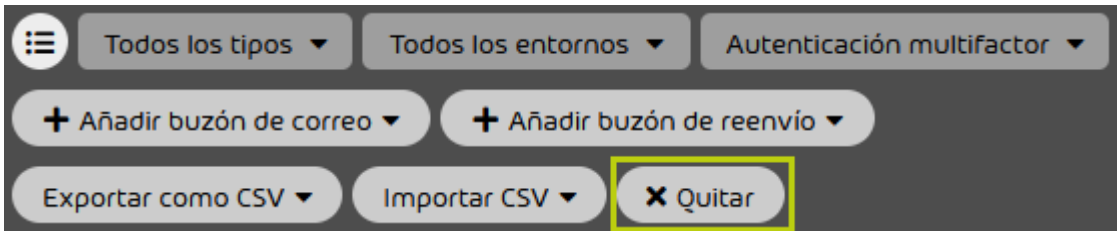


Figura 205: Eliminar buzones de correo

Se muestra una ventana de confirmación.

7. Haga clic en **Confirmar**.

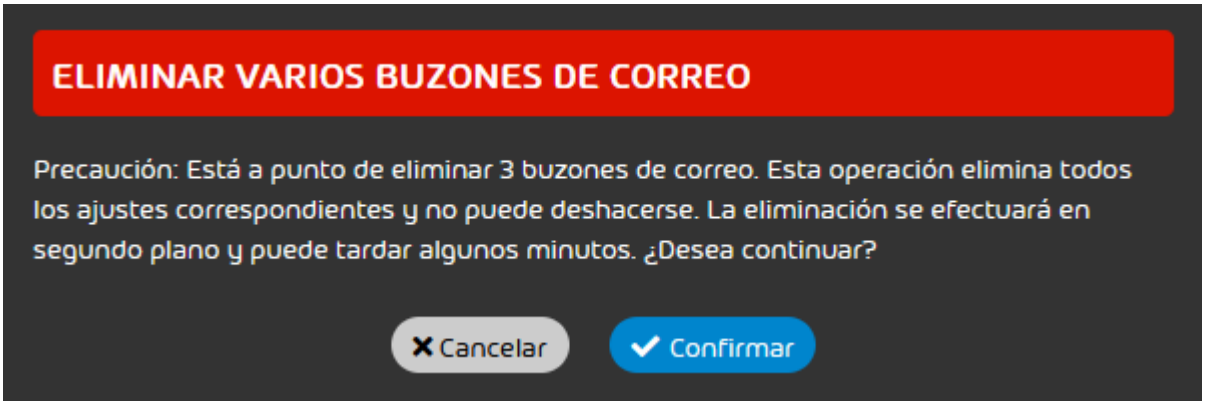


Figura 206: Confirmar la eliminación

Los buzones de correo se eliminan de Control Panel. La eliminación se efectúa en segundo plano y puede tardar unos minutos.

Se han eliminado al mismo tiempo de Control Panel varios buzones de correo creados manualmente.

Desactivar **Simulacro de suplantación de identidad**

Puede desactivar el simulacro de suplantación de identidad (envío de correos del simulacro de phishing en nombre de ususarios de su organización) para determinados buzones de correo en el módulo **Configuración de cliente** > **Buzones**. Esto puede ser necesario si empleados quitan su organización, pero el buzón de correo debe seguir existiendo para recibir correos. Pero no podrá volver a activar el simulacro de suplantación de identidad.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee desactivar la suplantación de identidad para un buzón de correo.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Haga clic en la flecha de menú junto al buzón de correo que desee añadir a un grupo.

   Se abre un menú.

Figura 207: Acciones para buzones de correo

5. Haga clic en **Simulacro de suplantación de identidad**.

   Aparece una ventana de confirmación.

6. **Nota:**

   Si desactiva el simulacro de suplantación de identidad, no podrá volver a activarlo. Solo el usuario del buzón de correo podrá activarlo (véase Activar o desactivar Simulacro de suplantación de identidad como usuario en la página 41).

   Haga clic en **Confirmar**.

   El icono **Simulacro de suplantación de identidad** se pone gris y el simulacro de suplantación de identidad se desactiva para el buzón de correo.

Se ha desactivado el simulacro de suplantación de identidad para un buzón de correo.

Grupos

Control Panel permite realizar grupos de buzones de correo. Algunos servicios de Control Panel solo pueden aplicarse a grupos. Otros servicios permiten realizar ajustes por grupos. Por tanto, los grupos simplifican la configuración de los servicios en Control Panel.

En el módulo **Configuración de cliente** > **Grupos**, los administradores a nivel de cliente pueden crear grupos y añadir miembros individualmente (véase Crear un grupo en la página 290), así como administrar los grupos disponibles. Es posible importar listas de miembros de grupos desde un archivo CSV (véase Importar miembros de un grupo desde un archivo CSV en la página 292). Estos archivos CSV deben cumplir determinados requisitos (véase Archivos CSV para la importación de miembros de grupos en la página 296). También es posible exportar listas de miembros de grupos en formato CSV (véase Exportar grupos en formato CSV en la página 303).

Nota:

La pertenencia de buzones de correo de Microsoft 365 (véase el capítulo "Tipos de buzón de correo" del manual de 365 Total Protection) a grupos se administra exclusivamente en Microsoft 365. Por tanto, los buzones de Microsoft 365 no pueden añadirse a grupos de Control Panel. Sin embargo, es posible visualizar grupos de Microsoft 365 en Control Panel creando en éste grupos con los mismos nombres. Para más información sobre la sincronización de grupos de Microsoft 365, véase el capítulo "Sincronizar grupos de Microsoft 365 en Control Panel" del manual de 365 Total Protection.

En el menú de cada grupo, los administradores a nivel de cliente disponen de las siguientes opciones de administración.

Tabla 18: Administrar grupos

SÍMBOLO	TEXTO	DESCRIPCIÓN
	Detalles	Datos detallados del grupo
	Administrar miembros	Adición/eliminación de miembros (véase Administrar miembros en la página 297)
	Renombrar	Cambio de nombre del grupo (véase Cambiar el nombre de un grupo en la página 299)
	Personalizar descripción	Personalización de la descripción del grupo (véase Personalizar la descripción de un grupo en la página 301)
	Eliminar	Eliminación del grupo (véase Eliminar un grupo en la página 305)

Crear un grupo

En el módulo **Configuración de cliente** > **Grupos** puede crear un grupo nuevo a partir de buzones de correo ya registrados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee crear un grupo.
3. Vaya a **Configuración de cliente** > **Grupos**.
4. Haga clic en **Añadir**.

   Se despliega un menú desplegable.

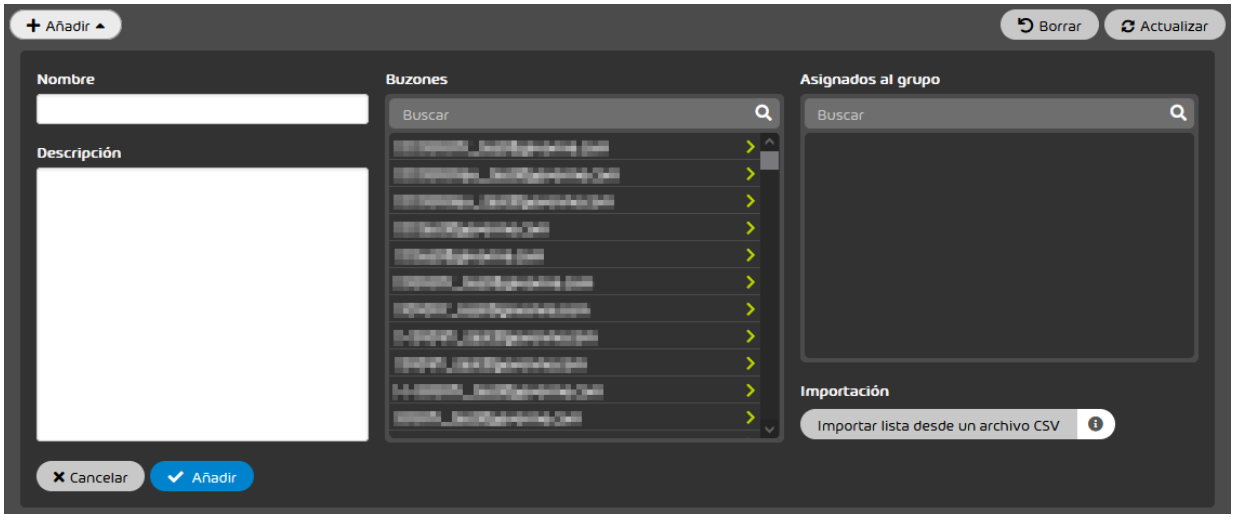


Figura 208: Añadir un nuevo grupo

5. Defina un nombre para el grupo en **Nombre**.
6. Opcional: Describa el grupo en el campo **Descripción**.

7. Añada buzones de correo al nuevo grupo. Tiene dos opciones:

   - En **Buzones**, seleccione al menos un buzón de correo que añadir al grupo. Para añadir un buzón de correo al grupo, haga clic en el buzón de correo.

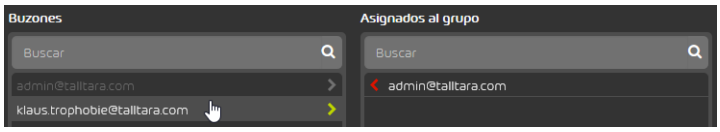


Figura 209: Añadir un buzón de correo individual

   - Importe una lista de miembros previa desde un archivo CSV (véase Importar miembros de un grupo desde un archivo CSV en la página 292). Solo se pueden importar miembros a un único grupo por importación.

   Los buzones de correo seleccionados o importados se muestran en **Asignados al grupo**.

8. Haga clic en **Añadir**.

   El grupo se guardó.Los buzones de correo de **Asignados al grupo** se añaden al grupo.

Se ha creado un grupo.

A continuación puede administrar los miembros del grupo (véanse Administrar miembros en la página 297 y Importar miembros de un grupo desde un archivo CSV en la página 292), cambiar el nombre del grupo (véase Cambiar el nombre de un grupo en la página 299), personalizar la descripción del grupo (véase Personalizar la descripción de un grupo en la página 301), exportar el grupo en formato CSV (véase Exportar grupos en formato CSV en la página 303) o eliminar el grupo (véase Eliminar un grupo en la página 305).

Importar miembros de un grupo desde un archivo CSV

En lugar de asignar manualmente usuarios a un grupo, puede añadir usuarios mediante a una lista en formato CSV en el módulo **Configuración de cliente** > **Grupos**. Puede asignar usuarios de una lista CSV tanto a grupos recién creados como a grupos preexistentes.

Nota:

Solo se pueden importar miembros a un único grupo por importación.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al cual desee importar miembros de grupos.
3. Vaya a **Configuración de cliente** > **Grupos**.

4. Tiene dos opciones:

   - Crear un nuevo grupo e importar miembros desde un archivo CSV (véase Sección a)
   - Añadir miembros de un archivo CSV a un grupo existente (véase Sección b)

   a) Haga clic en **Añadir**.

   Se muestra un formulario.

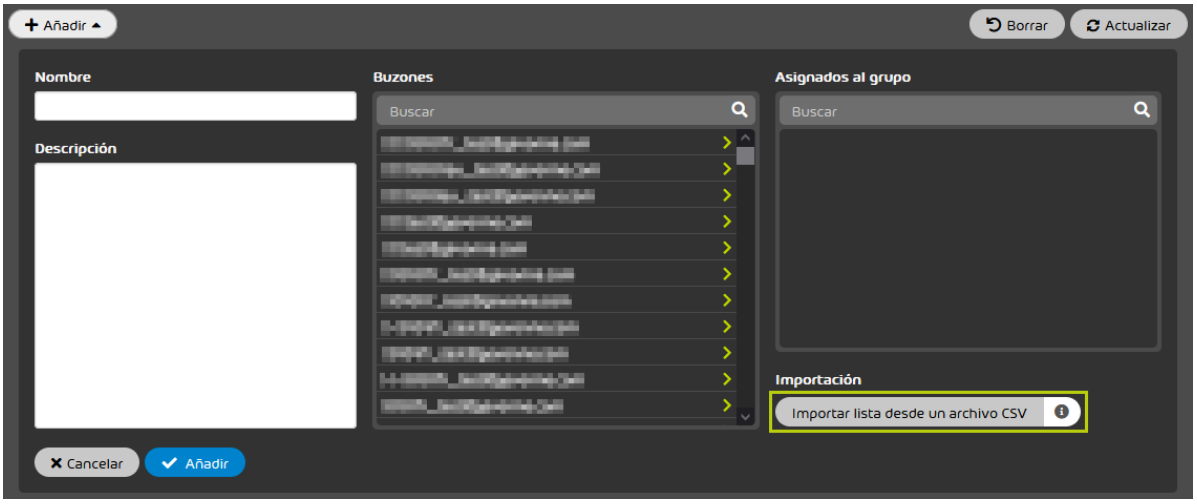


Figura 210: Importar miembros de grupo desde un archivo CSV a un nuevo grupo

   b) Seleccione un grupo en la zona inferior de la página y haga clic en **Administrar miembros**.

   Se muestra un formulario.

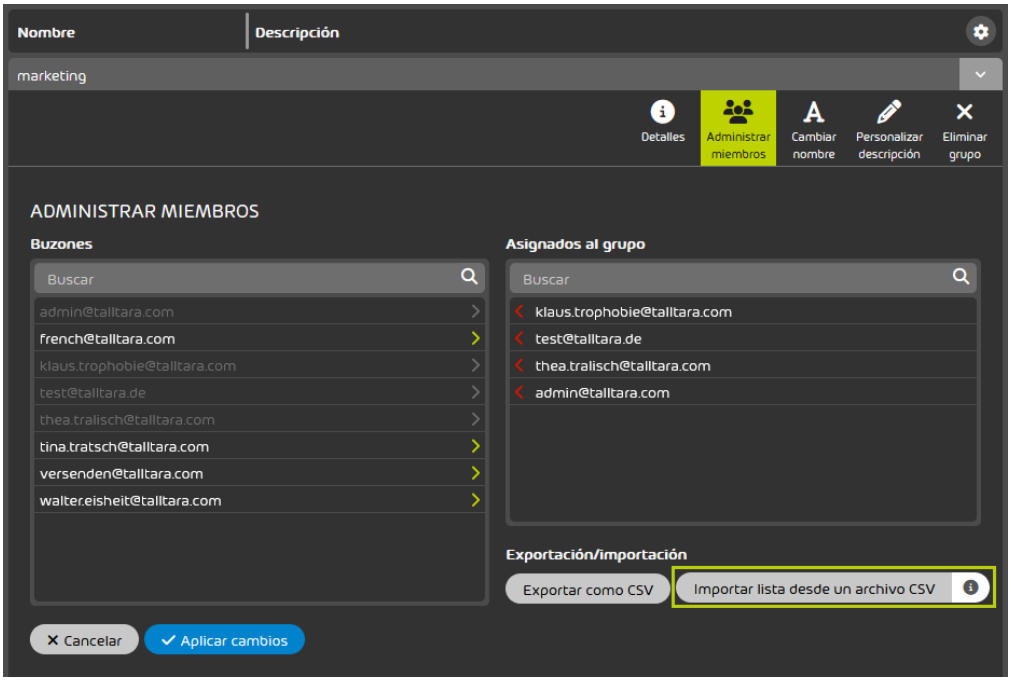


Figura 211: Importar miembros de grupo desde un archivo CSV a un grupo previo.

5. Haga clic en **Importar lista desde un archivo CSV**.

> **Nota:**
>
> Los miembros de grupo del archivo CSV solo se importan al grupo que esté seleccionado actualmente.

Se abre una ventana de selección de archivos.

6. Seleccione el archivo CSV deseado.

> **Importante:**
>
> Para que un archivo CSV externo con miembros de un grupo pueda importarse correctamente en Control Panel, éste deberá cumplir ciertas reglas de formato, estructura interna y sintaxis (véase Archivos CSV para la importación de miembros de grupos en la página 296).

En **Asignados al grupo** se muestran todos los miembros de grupo leídos del archivo CSV.

> **Nota:**
>
> La importación de miembros de grupo de archivos CSV se rige por las siguientes reglas:
>
> - Desde un archivo CSV es posible importar incluso miembros que ya estén asignados a otro grupo. Los miembros del grupo se muestran en **Asignados al grupo**.
> - Si se leen registros de varios archivos CSV, los registros repetidos entre archivos se detectan automáticamente. Los registros repetidos sólo se importan y muestran una vez en **Asignados al grupo**.
> - Los registros repetidos dentro de un solo archivo CSV se importan sólo una vez y se muestran en **Asignados al grupo**.
> - Los registros inválidos también se importan desde el archivo CSV y se muestran en **Asignados al grupo**. Al guardar el grupo, se comprueba si los registros de la lista son válidos. Si la lista contiene registros inválidos, se mostrará un mensaje de error. Elimine todos los registros inválidos (véase Archivos CSV para la importación de miembros de grupos en la página 296) y guarde el grupo.

7. Haga clic en **Añadir** o **Aplicar cambios** para guardar los cambios.

El grupo se guardó.

> **Importante:**
>
> Si la lista de **Asignados al grupo** contiene registros inválidos o miembros de otros grupos, se mostrará un mensaje de error. Elimine los registros inválidos de la lista y los miembros de otros grupos para guardar el grupo.

Se han importado miembros de un grupo desde un archivo CSV y se han añadido a un grupo.

Archivos CSV para la importación de miembros de grupos

Para que un archivo CSV externo con información sobre miembros de grupos pueda importarse correctamente en Control Panel (véase Importar miembros de un grupo desde un archivo CSV en la página 292), deberá cumplir reglas especiales respecto a su extensión y su estructura interna.

Reglas estructurales de archivos CSV para la importación de miembros de grupos

- La extensión del archivo a importar deberá ser siempre **.csv**. Otras extensiones, tales como .txt o .docx, no están permitidas y no se aceptan.
- El archivo CSV contiene una sola columna en la que se distribuyen verticalmente los diversos registros.
- La primera fila siempre se emplea para el nombre de la columna y puede nombrarse libremente.
- Los miembros de grupos se nombran mediante sus direcciones de correo electrónico. Las direcciones deberán presentar una estructura correcta (conforme al patrón "partelocal@nombredehost.dominio-de-nivel-superior").

> **Importante:**
>
> Las direcciones con estructura incorrecta se ignorarán durante la importación.

- Cada fila deberá contener una única dirección.
- Los registros dobles no afectan al procesamiento del archivo, pero deberán evitarse.

Administrar miembros

Ha creado un grupo (véase Crear un grupo en la página 290).

En el módulo **Configuración de cliente** > **Grupos** puede añadir buzones de correo creados manualmente (véase Tipos de buzón de correo en la página 235) a grupos o retirarlos de ellos independientemente de si los grupos se sincronizan o no.

Nota:

Los buzones de correo de tipo LDAP no pueden añadirse a grupos ni eliminarse de los mismos en Control Panel. Su pertenencia a grupos se administra exclusivamente en el servicio de directorio correspondiente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el grupo cuyos miembros desee administrar.
3. Vaya a **Configuración de clientes** > **Grupos** y haga clic en la fecha de menú del dominio deseado.

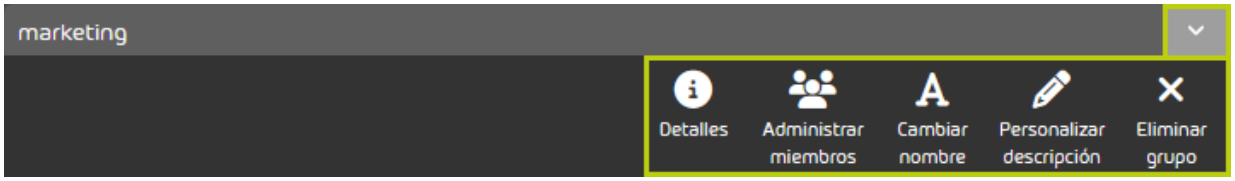


Figura 212: Abrir el menú de grupos

4. Haga clic en **Administrar miembros**.

Se abren dos ventanas. La de la izquierda muestra todos los buzones de correo registrados, y la de la derecha todos los buzones de correo asignados al grupo.

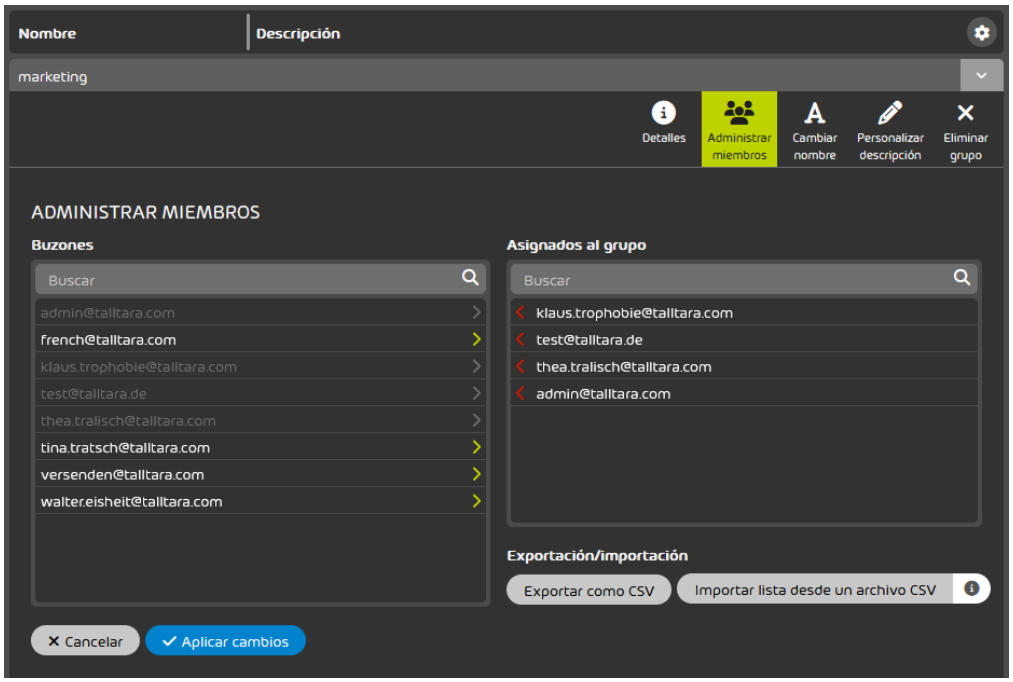


Figura 213: Administrar los miembros de un grupo

5. Administre los miembros de un grupo:

   - Si desea añadir más miembros al grupo, haga clic sobre los miembros deseados en la tabla **Buzones** (a la izquierda). Para ello puede importar listas de grupos previas desde un archivo CSV (véase Importar miembros de un grupo desde un archivo CSV en la página 292).

- Si desea eliminar miembros de un grupo, haga clic sobre los mismos en la tabla **Asignados al grupo** (a la derecha).

> **Nota:**
>
> Los buzones de correo de tipo LDAP se muestran en gris en las tablas **Buzones** y **Asignados al grupo** y no pueden desplazarse entre las mismas.

Los miembros se añaden al grupo o se eliminan del grupo.

6. Haga clic en **Aplicar cambios**.

Los cambios se guardan en Control Panel.

> **Nota:**
>
> Los cambios realizados en grupos sincronizados no se añaden al servicio de directorio durante la sincronización, pero se mantienen en Control Panel.

Se han administrado los miembros de un grupo.

Cambiar el nombre de un grupo

Ha creado un grupo (véase Crear un grupo en la página 290).

En **Configuración de cliente** > **Grupos** puede cambiar los nombres de los grupos (véase Grupos en la página 288).

Importante:

Los grupos sincronizados con un servicio de directorio dejan de sincronizarse después del cambio de nombre.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del grupo cuyo nombre desee cambiar.
3. Vaya a **Configuración de clientes** > **Grupos** y haga clic en la fecha de menú del dominio deseado.

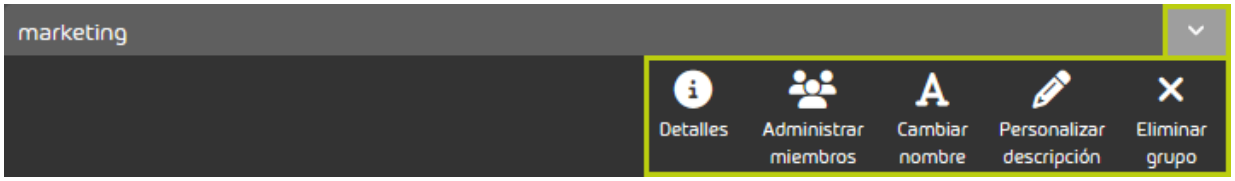
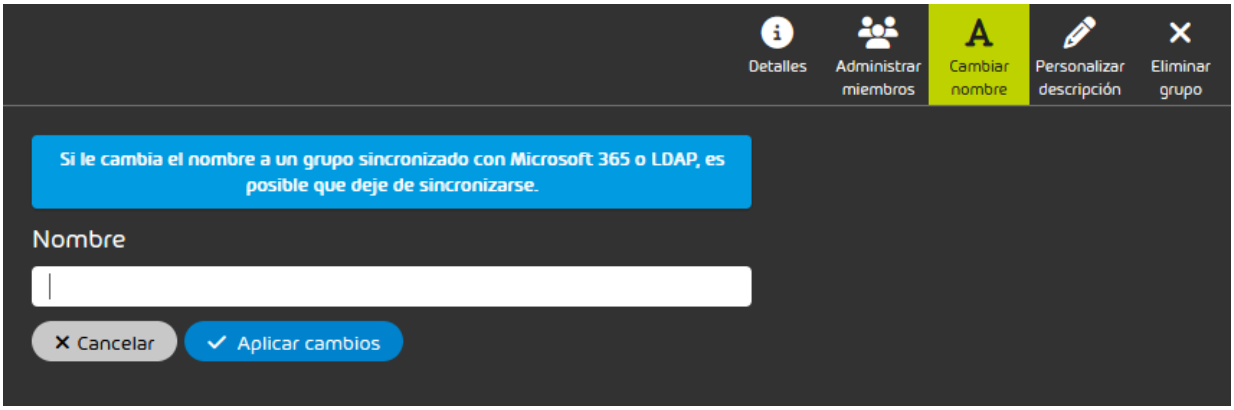


Figura 214: Abrir el menú de grupos

4. Haga clic en **Cambiar nombre**.

Se despliega un menú desplegable.



5. **Importante:**

   Si un grupo previamente no sincronizado recibe el nombre de un grupo de un servicio de directorio sincronizado mediante LDAP, el grupo comenzará a sincronizarse de inmediato. Al grupo de Control Panel se le asignarán los buzones de correo sincronizados que haya asignados al grupo del servicio de directorio. La pertenencia de los buzones de correo sincronizados a los grupos se sincroniza de modo continuo. Los buzones de correo no sincronizados que se hayan asignado manualmente al grupo en Control Panel siguen asignados a sus grupos y no se ven afectados por la sincronización.

   Introduzca el nuevo nombre del grupo en el campo de introducción de datos.
6. Haga clic en **Aplicar cambios**.

Se ha cambiado el nombre de un grupo.

Personalizar la descripción de un grupo

Ha creado un grupo (véase Crear un grupo en la página 290).

En el módulo **Configuración de cliente** > **Grupos** puede personalizar las descripciones de los grupos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del grupo cuya descripción desee personalizar.

3. Vaya a **Configuración de clientes** > **Grupos** y haga clic en la fecha de menú del dominio deseado.

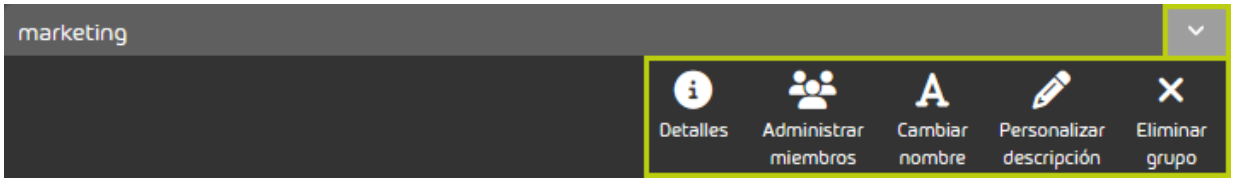
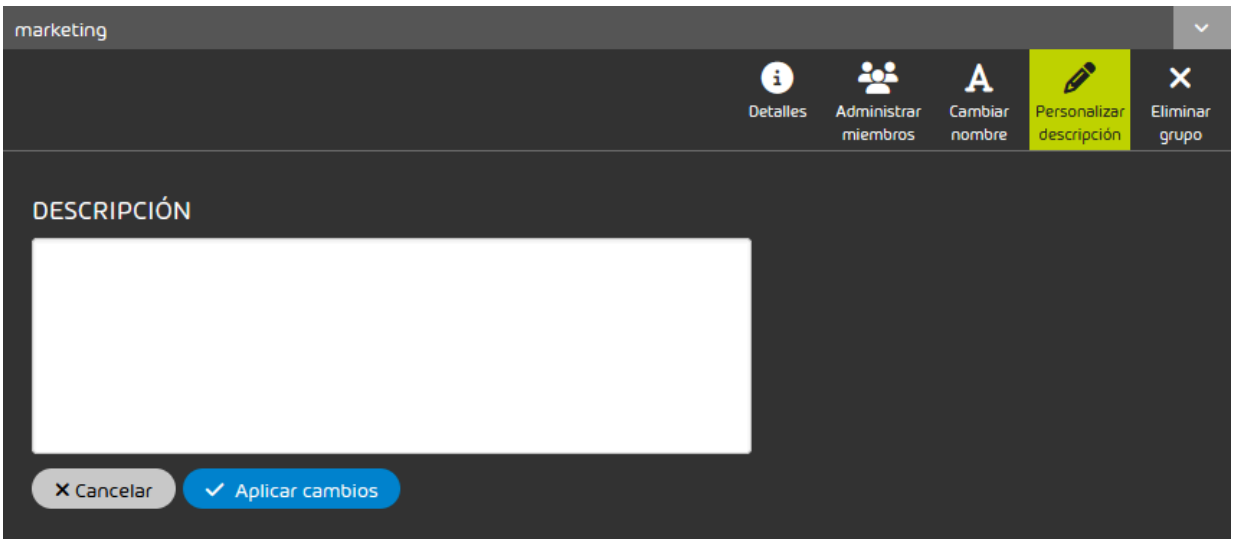


Figura 215: Abrir el menú de grupos

4. Haga clic en **Personalizar descripción**.

Se despliega un menú desplegable.



5. Introduzca la descripción deseada para el grupo y haga clic en **Aplicar cambios**.

Se ha personalizado la descripción de un grupo.

Exportar grupos en formato CSV

Ha creado un grupo (véase Crear un grupo en la página 290).

En el módulo **Configuración de cliente** > **Grupos** puede exportar miembros de un grupo en formato CSV.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Grupos**.
4. Haga clic en **Exportar como CSV**.

   Se abre una vista avanzada.

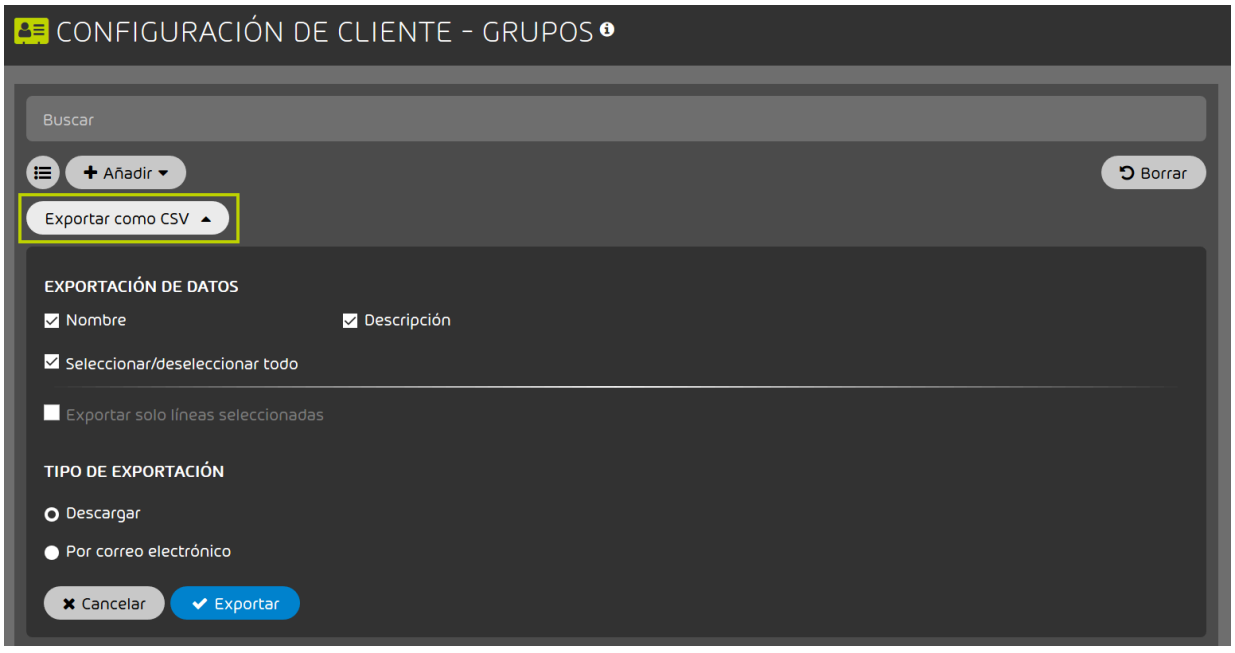


Figura 216: Seleccionar datos para la exportación

5. En la sección **Exportación de datos**, marque las casillas correspondientes a los datos que desee exportar.
   - **Nombre**: Se exportan los nombres de los grupos.
   - **Descripción**: Se exportan las descripciones de los grupos.
   - **Seleccionar/deseleccionar todo**: Todas las casillas descritas se marcan o desmarcan.
6. Opcional: Si solo desea exportar datos de grupos seleccionados, proceda del siguiente modo:
   a) En el módulo, haga clic en .

   Una columna con casillas aparece en la tabla.

   b) Marque las casillas de las filas cuyos datos desee exportar.

Figura 217: Seleccionar filas

   La casilla **Exportar solo líneas seleccionadas** se habilita en la vista avanzada.

   c) Marque la casilla habilitada **Exportar solo líneas seleccionadas**.

Figura 218: Exportar las filas seleccionadas

7. Opcional: En **Exportación de datos**, seleccione si desea exportar ambas columnas (**Nombre** y **Descripción**).

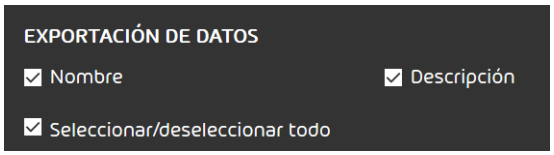


Figura 219: Seleccionar columnas

8. En **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o correo electrónico.
   - **Descargar**: El archivo CSV se facilita para su descarga.
   - **Por correo electrónico**: El archivo CSV se envía por correo.

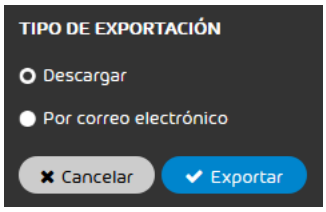


Figura 220: Seleccionar el tipo de exportación

9. Haga clic en **Exportar**.

Los datos de un grupo se han exportado en formato CSV.

Eliminar un grupo

Ha creado un grupo (véase Crear un grupo en la página 290).

En el módulo **Configuración de cliente** > **Grupos** puede eliminar grupos (véase Grupos en la página 288).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee eliminar un grupo.

3. Vaya a **Configuración de clientes** > **Grupos** y haga clic en la fecha de menú del dominio deseado.

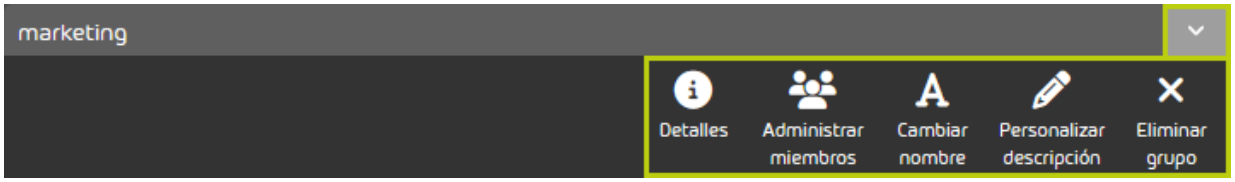
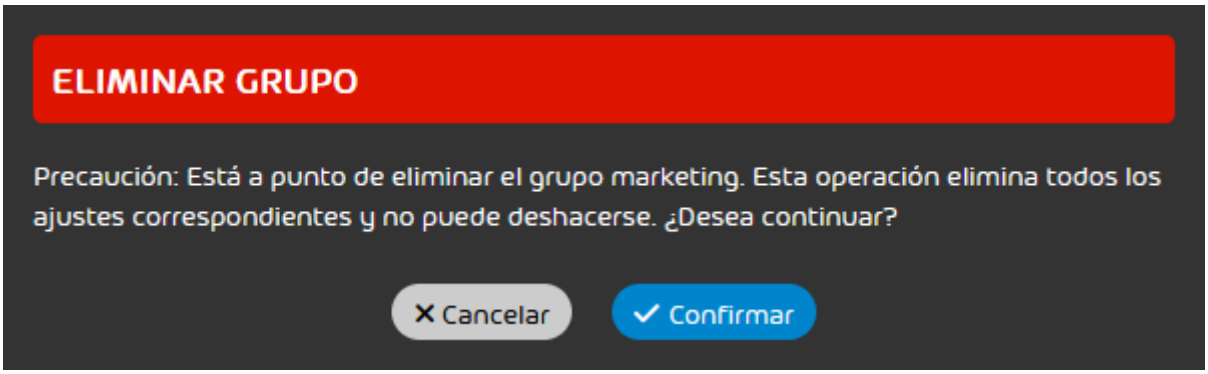


Figura 221: Abrir el menú de grupos

4. Haga clic en **Confirmar**.

> **PRECAUCIÓN:**
>
> Al eliminar un grupo se eliminarán también definitivamente todos los ajustes y miembros del mismo.

Se muestra un mensaje de advertencia.



5. Confirme el mensaje de advertencia haciendo clic en **Confirmar**.

Se ha eliminado un grupo.

Dominios

En el módulo **Configuración de cliente** > **Dominios** se muestran y administran el dominio principal y los dominios alias de un cliente.

Nota:

Los dominios alias pueden emplearse, por ejemplo, cuando se poseen varios dominios de nivel superior para un mismo dominio. Por ejemplo, el administrador del dominio principal **dominiodecliente.es** puede registrar adicionalmente los dominios de nivel superior **.de** y **.com**. En tal caso, **dominiodecliente.de** y **dominiodecliente.com** serían los dominios alias del dominio principal.

Los dominios alias no suponen coste adicional.

En este módulo, los administradores a nivel de cliente pueden crear nuevos dominios alias (véase Añadir dominios alias en la página 307) y eliminar dominios alias previos (véase Eliminar dominios alias en la página 314). El dominio principal no puede eliminarse. Además, los administradores pueden exportar en formato CSV los dominios mostrados (véase Exportar dominios en formato CSV en la página 311) e importar dominios alias nuevos desde archivos CSV (véase Importar dominios alias desde un archivo CSV en la página 309). Estos archivos CSV deben cumplir determinados requisitos (véase Archivos CSV para la importación de dominios alias en la página 310).

Por motivos de seguridad, comprobamos si un cliente está autorizado a administrar los dominios registrados en Control Panel (véase Verificación de dominios en la página 316).

Añadir dominios alias

En el módulo **Configuración de cliente** > **Dominios**, como administrador a nivel de cliente, puede añadir dominios alias al dominio principal de un cliente. Con el procedimiento aquí descrito puede añadir dominios alias individualmente. También existe la opción de importar una lista de dominios alias desde un archivo CSV (véase Importar dominios alias desde un archivo CSV en la página 309).

Nota:

Los dominios alias pueden emplearse, por ejemplo, cuando se poseen varios dominios de nivel superior para un mismo dominio. Por ejemplo, el administrador del dominio principal **dominiodecliente.es** puede registrar adicionalmente los dominios de nivel superior **.de** y **.com**. En tal caso, **dominiodecliente.de** y **dominiodecliente.com** serían los dominios alias del dominio principal.

Los dominios alias no suponen coste adicional.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente a cuyo dominio principal desee añadir un dominio alias.
3. Vaya a **Configuración de cliente** > **Dominios**.
4. Haga clic en **Añadir dominio**.

   Se muestran ajustes adicionales.
5. **Importante:**

   El dominio alias debe ser un dominio válido.

   Introduzca el dominio alias en el campo **Dominio**.

6. Haga clic en **Añadir**.

   El dominio alias se añade a la lista de dominios. Al principio, el dominio alias se muestra con el estado **No verificado** en la columna **Verificado**. Al cabo de algunos minutos, se comprueba si es posible verificar el dominio alias (véase Verificación de dominios en la página 316).

Se ha añadido un dominio alias al dominio principal de un cliente.

A continuación puede exportar los dominios del cliente en formato CSV (véase Exportar dominios en formato CSV en la página 311) o eliminar el dominio alias (véase Eliminar dominios alias en la página 314).

Importar dominios alias desde un archivo CSV

Además de añadir dominios alias a un dominio principal uno por uno (véase Añadir dominios alias en la página 307), puede importar dominios alias de una lista en formato CSV en el módulo **Configuración de cliente** > **Dominios**. Es posible importar dominios alias con una lista CSV tanto al principio, antes de que se hayan añadido al sistema datos de este tipo, como en cualquier momento posterior.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente a cuyo dominio principal desee añadir dominios alias.
3. Vaya a **Configuración de cliente** > **Dominios**.
4. Haga clic en **Importar lista desde un archivo CSV**.

   Se abre una ventana de selección de archivos.

5. Seleccione el archivo CSV deseado.

> **Importante:**
>
> Para que un archivo CSV externo con dominios alias pueda importarse correctamente en Control Panel, éste deberá cumplir ciertas reglas de formato, estructura interna y sintaxis (véase Archivos CSV para la importación de dominios alias en la página 310).

Si el archivo CSV contiene dominios alias que aún no se encuentren disponibles en Control Panel, éstos se añadirán a la lista de dominios.

Se han importado dominios alias desde un archivo CSV y se han añadido al dominio principal del cliente en Control Panel.

A continuación puede exportar los dominios del cliente en formato CSV (véase Exportar dominios en formato CSV en la página 311) o eliminar dominios alias (véase Eliminar dominios alias en la página 314).

Archivos CSV para la importación de dominios alias

Para que un archivo CSV externo con dominios alias pueda importarse correctamente en Control Panel (véase Importar dominios alias desde un archivo CSV en la página 309), deberá cumplir reglas especiales respecto a su extensión y su estructura interna.

Reglas estructurales de archivos CSV para la importación de dominios alias

- La extensión del archivo a importar deberá ser siempre **.csv**. Otras extensiones, tales como .txt o .docx, no están permitidas y no se aceptan.
- El archivo CSV contiene una sola columna en la que se distribuyen verticalmente los diversos registros.
- La primera fila siempre se emplea para el nombre de la columna y puede nombrarse libremente.

- Los nombres de los dominios deben estar en un formato correcto.

> **Importante:**
>
> Si un archivo contiene un nombre de dominio en formato incorrecto, la importación se interrumpirá inmediatamente. En tal caso, los registros correctos que contenga el archivo tampoco se importarán.

- Cada fila deberá contener un único nombre de dominio.
- No deberá haber registros duplicados.

> **Importante:**
>
> Si un archivo contiene registros duplicados, la importación se interrumpirá inmediatamente. En tal caso, los registros correctos que contenga el archivo tampoco se importarán.

Exportar dominios en formato CSV

En el módulo **Configuración de cliente** > **Dominios** puede exportar los dominios de un cliente en formato CSV. El archivo CSV exportado contiene dos columnas. La primera columna contiene los nombres de los dominios. La segunda columna contiene los tipos de los dominios. Se hace distinción entre el dominio principal y los dominios alias. Puede exportar todos los dominios del cliente o una selección de los mismos.

> **Nota:**
>
> Los archivos CSV exportados no pueden emplearse para importar dominios alias (véase Importar dominios alias desde un archivo CSV en la página 309 y Archivos CSV para la importación de dominios alias en la página 310).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente cuyos dominios desee exportar.
3. Vaya a **Configuración de cliente** > **Dominios**.

4. Haga clic en **Exportar como CSV**.

Se muestran los ajustes para la exportación en formato CSV.

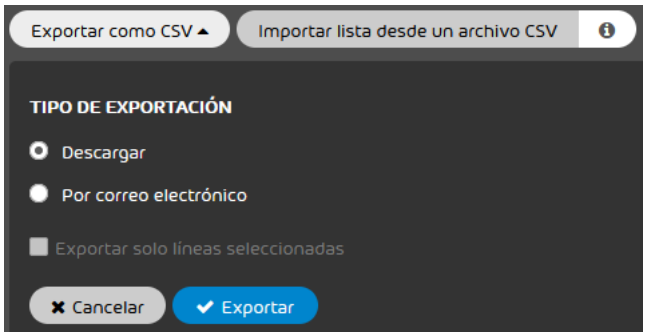


Figura 222: Ajustes para la exportación en formato CSV

5. Opcional: Si solo desea exportar una selección de dominios, proceda del siguiente modo:

a) En el módulo, haga clic en .

Aparece una columna con casillas en la lista de dominios.

b) Marque las casillas correspondientes a las filas que desee exportar.

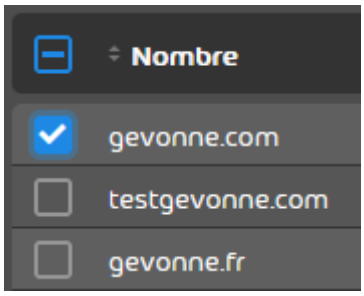


Figura 223: Seleccionar filas

En los ajustes para la exportación en formato CSV se habilita la casilla **Exportar solo líneas seleccionadas**.

c) Marque la casilla **Exportar solo líneas seleccionadas**.

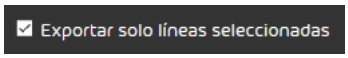


Figura 224: Exportar las filas seleccionadas

6. En **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o enviarlo por correo electrónico.
   - **Descargar**: El archivo CSV se facilita para su descarga.
   - **Por correo electrónico**: El archivo CSV se envía por correo electrónico.

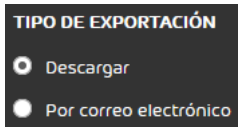


Figura 225: Seleccionar el tipo de exportación

Si se elige la opción **Por correo electrónico**, se muestra un campo de introducción de datos.

7. Si elige la opción **Por correo electrónico**, introduzca la dirección de correo electrónico a la que enviar el archivo CSV en el campo de introducción de datos.
8. Haga clic en **Exportar**.

Los dominios se exportan en forma de archivo CSV. El archivo CSV se presenta para su descarga o se envía por correo electrónico.

Todos o algunos dominios de un cliente se han exportado en formato CSV.

Eliminar dominios alias

Ha añadido dominios alias al dominio principal del cliente (véanse Añadir dominios alias en la página 307 y Importar dominios alias desde un archivo CSV en la página 309).

Puede eliminar dominios alias de un cliente de Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el cliente para el cual desee eliminar un dominio alias.
3. Vaya a **Configuración de cliente** > **Dominios**.

4. Haga clic en la flecha de menú junto al dominio alias que desee eliminar.

Se abre un menú.

5. **PRECAUCIÓN:**

   Una vez eliminado el dominio alias, todas las direcciones de correo electrónico y todos los ajustes del mismo se eliminarán definitivamente.

   Si una dirección de correo electrónico del dominio eliminado es la dirección principal de un buzón de correo que tenga asignada una dirección de correo electrónico de otro dominio como dirección alias, la dirección alias se convertirá en la nueva dirección principal del buzón de correo. Si el buzón de correo tiene asignadas varias direcciones alias, la dirección alias creada primero se convertirá en la dirección principal y las demás direcciones alias se mantendrán. En el futuro, el usuario del buzón de correo deberá utilizar la nueva dirección principal como nombre de usuario en Control Panel.

   Haga clic en **Eliminar dominio**.

Figura 226: Eliminar un dominio

Se muestra un mensaje de advertencia.

6. Haga clic en **Confirmar**.

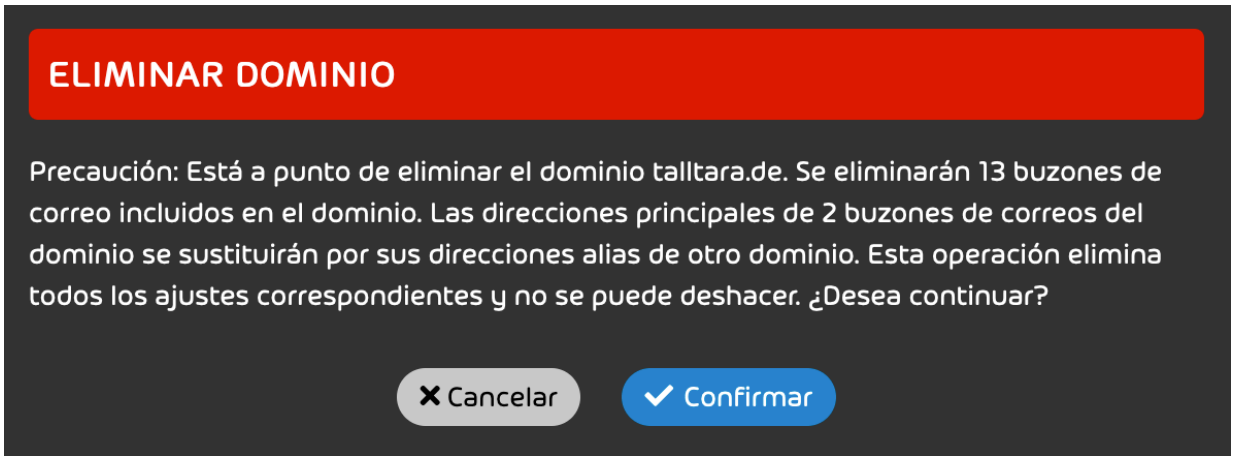


Figura 227: Confirmar la eliminación

El dominio alias, sus buzones de correo y los ajustes del dominio alias se eliminan de Control Panel. El dominio alias se elimina de la lista de dominios.

Un dominio alias se ha eliminado de Control Panel.

Verificación de dominios

Por motivos de seguridad, comprobamos si un cliente está autorizado a administrar los dominios registrados en Control Panel. Por tanto, comprobamos los dominios registrados a nombre de un cliente en el módulo **Configuración de cliente** > **Dominios** (véase Dominios en la página 307).

Nota:

Los administradores a nivel de cliente pueden acceder a dicho módulo seleccionando el dominio principal del cliente en la selección de ámbitos (véase Selección de ámbitos en la página 58).

Una vez superada la prueba, el dominio se verifica. El estado de verificación se muestra mediante un icono en la columna **Verificado** del módulo **Configuración de cliente** > **Dominios**. Solo es posible confirmar un mismo dominio para un único cliente en Control Panel.

Tabla 19: Verificación de dominios

SÍMBOLO	EXPLICACIÓN
	El dominio está verificado.
	El dominio no está verificado.

Comprobamos los dominios por primera vez al cabo de algunos minutos de haberse añadido a Control Panel. En el proceso determinamos si los registros MX de los dominios apuntan hacia nosotros (véase "Modificación de los registros MX"Configuración inicial de los servicios en el manual Configuración inicial de los servicios). Para los dominios sin verificar, la comprobación se repite una vez al día. Sin embargo, los administradores a nivel de cliente pueden iniciar manualmente la comprobación de dominios no verificados en todo momento (véase Verificar dominios en la página 318).

Nota:

Si se producen problemas durante la verificación de un dominio, el cliente puede ponerse en contacto con el soporte técnico o con su persona de contacto.

La verificación de los dominios tiene consecuencias para el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63). En este módulo solo se muestran correos de buzones de dominios verificados. El domino del buzón de correo se indica en el campo **Dominio del propietario** de los detalles de cada correo (véase Información avanzada de correos en la página 84). Una vez verificado un dominio, todos los correos de buzones de dicho dominio enviados a nuestra infraestructura se muestran en el módulo **Email Live Tracking**.

Nota:

Los correos antiguos con el campo **Dominio del propietario** vacío también se muestran en el módulo **Email Live Tracking**.

También se muestran en dicho módulo los correos clasificados como **Rechazado**. De este modo se evita la pérdida de correos que hayan sido enviados a nuestra infraestructura antes de haberse añadido el dominio a Control Panel y que, por tanto, hayan sido rechazados.

Verificar dominios

Los dominios sin verificar en el módulo **Configuración de cliente** > **Dominios** se comprueban automáticamente una vez al día para ver si es posible verificarlos (véase Verificación de dominios en la página 316). Adicionalmente, usted puede iniciar manualmente la comprobación de dominios no verificados en todo momento.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio principal del cliente para el cual desee comprobar dominios.
3. Vaya a **Configuración de cliente** > **Dominios**.
4. Haga clic en la flecha de menú junto al dominio sin verificar cuya comprobación desee iniciar.

Figura 228: Abrir el menú

Se abre un menú.

5. Haga clic en **Iniciar verificación**.

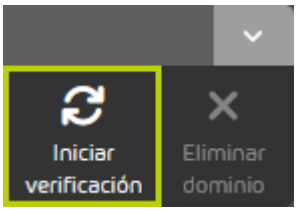


Figura 229: iniciar comprobación

Comprobamos si los registros MX del dominio. Si el dominio pasa la prueba, su estado en la columna **Verificado** pasa a **Verificado**.

Se ha iniciado la comprobación de un dominio no verificado.

Autenticación

En el módulo **Configuración de cliente** > **Autenticación**, los administradores pueden definir ajustes para el inicio de sesión en Control Panel.

Los administradores a nivel de cliente y partner pueden definir reglas para contraseñas para las cuentas de usuarios de Control Panel (véase Definir la longitud de contraseñas en la página 321). Si lo desean, los administradores pueden restablecer las reglas para contraseñas por defecto más tarde (véase Restablecer la longitud de contraseñas en la página 322).

Nota:

Las reglas para contraseñas solo se aplican a las contraseñas administradas en Control Panel (véase Tipos de buzón de correo en la página 235).

En el caso de los buzones LDAP, los administradores a nivel de cliente pueden establecer que se utilicen los datos de acceso de los usuarios del servicio del directorio para iniciar sesión en Control Panel (véase Configurar el acceso a Control Panel mediante LDAP en la página 142) o que las contraseñas de los usuarios se administren en Control Panel en su lugar.

Los administradores a nivel de cliente pueden habilitar la autenticación multifactor para los usuarios de un cliente (véase Habilitar la autenticación multifactor en la página 323). De este modo, los usuarios obtendrán el permiso de configurar la autenticación multifactor para su cuenta (véase el capítulo "Configurar la autenticación multifactor" en el manual de Control Panel). La autenticación multifactor aumenta la seguridad al iniciar sesión en Control Panel ya que se requiere una contraseña de uso único de una aplicación de autenticación además de la contraseña de Control Panel. También es posible forzar la autenticación multifactor para los administradores (véase Forzar la autenticación multifactor para los administradores en la página 325). Los administradores pueden volver a desactivar la autenticación multifactor para los usuarios de un cliente más tarde (véase Desactivar la autenticación multifactor en la página 327).

Nota:

Solo los usuarios cuyas contraseñas se administren en Control Panel o en un servicio de directorio mediante LDAP pueden configurar la autenticación multifactor en Control Panel.

Por razones de seguridad, las sesiones de usuarios inactivos se cierran por defecto en Control Panel automáticamente al cabo de 24 horas. Los administradores a nivel de cliente pueden ajustar un tiempo de cierre de sesión automático más breve o desactivar el cierre de sesión automático para los usuarios de un cliente (véase Configurar el cierre de sesión automático en la página 329). Si lo desean, los administradores a nivel de cliente pueden restaurar los ajustes por defecto (véase Restaurar la configuración de cierre de sesión automático por defecto en la página 331).

Por defecto, el acceso a Control Panel puede realizarse desde todas las direcciones IPv4. Sin embargo, para aumentar la seguridad, los administradores a nivel de partner y cliente pueden

establecer que sus usuarios solo puedan acceder a Control Panel desde direcciones y rangos IPv4 específicos. Los administradores pueden limitar el acceso a direcciones y rangos IPv4 específicos añadiendo las direcciones y los rangos IPv4 al módulo **Configuración de cliente** > **Autenticación** (véase Definir direcciones IP en la página 332). Los administradores también pueden volver a eliminar las direcciones y los rangos IPv4 del módulo (véase Eliminar una dirección IP en la página 333). Si el módulo no contiene ninguna dirección y ningún rango IPv4, el acceso puede realizarse desde todas las direcciones IPv4. De lo contrario, el inicio de sesión se limita a las direcciones y los rangos IPv4 introducidos.

Definir la longitud de contraseñas

También puede consultar los requisitos mínimos para contraseñas nuevas impuestos por Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio dentro del cual desee definir reglas para contraseñas.
3. Vaya a **Configuración de cliente** > **Autenticación**.

> **Importante:**
>
> Las reglas para contraseñas de los partners se transmiten a sus clientes. Los clientes subordinados pueden definir reglas más estrictas, pero no más laxas. De tal modo pueden, por ejemplo, aumentar la longitud de las contraseñas, pero no reducirla.

4. Introduzca la longitud mínima de contraseña en el campo **Longitud de contraseña**.

> **Nota:**
>
> La longitud mínima de contraseña debe ascender como mínimo a 8 caracteres.

> **Nota:**
>
> En el módulo se muestran otros requisitos mínimos para contraseñas nuevas establecidos por Control Panel y que no pueden modificarse. Estos establecen que las contraseñas nuevas deben contener al menos una letra mayúscula, una letra minúscula, una cifra y un carácter especial.

5. Haga clic en **Guardar** para aplicar la configuración.

La longitud mínima de contraseña se actualiza en Control Panel.

> **Nota:**
>
> La nueva longitud mínima de contraseña es de obligado cumplimiento para las contraseñas nuevas y no afecta en modo alguno a las contraseñas ya en uso.

Se ha definido la longitud mínima de contraseña para un dominio.

A continuación puede eliminar reglas para contraseñas (véase Restablecer la longitud de contraseñas en la página 322).

Restablecer la longitud de contraseñas

Ha definido una longitud de contraseña mínima para un dominio (véase Definir la longitud de contraseñas en la página 321).

En el módulo **Configuración de cliente** > **Autenticación** puede restablecer la longitud mínima de contraseña predeterminada para un dominio. A modo de configuración por defecto se emplea la definida por administradores de nivel superior.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee restablecer la longitud mínima de contraseña predeterminada.
3. Vaya a **Configuración de cliente** > **Autenticación**.
4. Haga clic en **Configuración por defecto** para restablecer la longitud mínima de contraseña predeterminada.
5. Haga clic en **Guardar** para aplicar la configuración.

Se ha restablecido la longitud mínima de contraseña predeterminada para un dominio.

Habilitar la autenticación multifactor

Puede habilitar la autenticación multifactor para los usuarios de un dominio. De este modo, los usuarios del dominio obtendrán el permiso de configurar la autenticación multifactor para su cuenta de Control Panel (véase el capítulo "Configurar la autenticación multifactor" en el manual de Control Panel).

Nota:

Solo los usuarios cuyas contraseñas se administren en Control Panel o en un servicio de directorio mediante LDAP pueden configurar la autenticación multifactor en Control Panel.

La autenticación multifactor aumenta la seguridad al iniciar sesión en Control Panel ya que se requiere una contraseña de uso único de una aplicación de autenticación además de la contraseña de Control Panel. Recomendamos especialmente que los administradores configuren la autenticación multifactor para su cuenta.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.

2. En la selección de ámbitos, seleccione el dominio para el cual desee habilitar la autenticación multifactor.
3. Vaya a **Configuración de cliente** > **Autenticación**.
4. Accione el interruptor **Autenticación multifactor** de **Habilitar la autenticación multifactor para sus usuarios**.

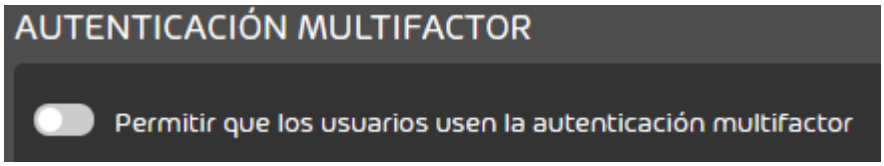


Figura 230: Habilitar la autenticación multifactor

El interruptor se pone verde y se abre una ventana de confirmación.

5. Haga clic en **Confirmar**.

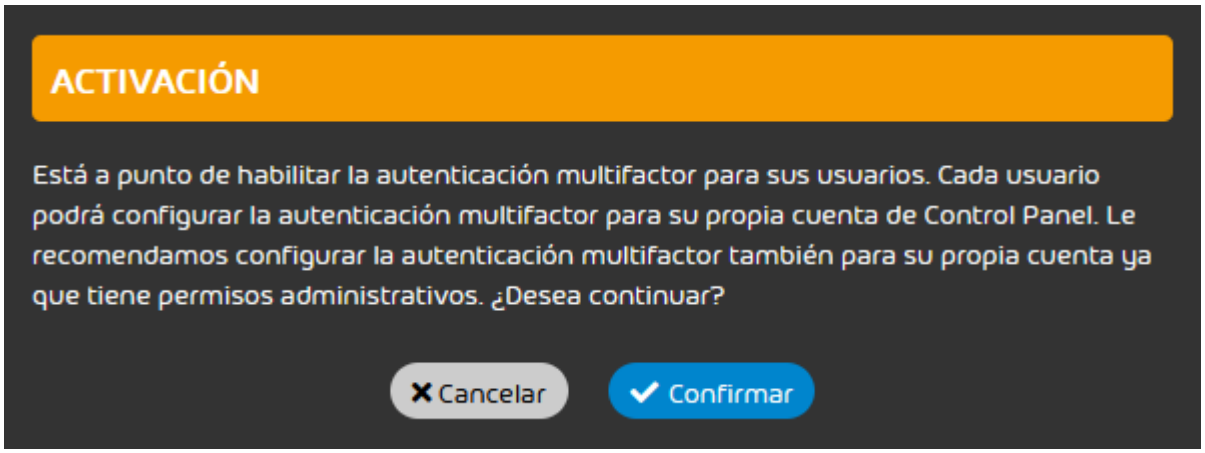


Figura 231: Confirmar

La autenticación multifactor se habilita para los usuarios del dominio.

La autenticación multifactor se ha habilitado para los usuarios de un dominio.

A continuación, los usuarios del dominio pueden configurar la autenticación multifactor para su cuenta de Control Panel (véase el capítulo "Configurar la autenticación multifactor" en el manual de Control Panel). Si un usuario tiene problemas con la autenticación multifactor, usted puede reiniciar la autenticación multifactor para el usuario (véase Reiniciar la autenticación multifactor en la página 279).

Forzar la autenticación multifactor para los administradores

Ha habilitado la autenticación multifactor (véase Habilitar la autenticación multifactor en la página 323).

Puede forzar la autenticación multifactor para los administradores de un cliente. De este modo, se les obligará a todos los administradores del cliente a configurar la autenticación multifactor para su cuenta de Control Panel (véase el capítulo «Configurar la autenticación multifactor» en el manual de Control Panel).

Nota:

Solo los usuarios cuyas contraseñas se administren en Control Panel o en un servicio de directorio mediante LDAP pueden configurar la autenticación multifactor en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyos administradores desee forzar la autenticación multifactor.
3. Vaya a **Configuración de cliente** > **Autenticación**.

4. Accione el interruptor **Autenticación multifactor** de **Forzar la autenticación multifactor para administradores**.

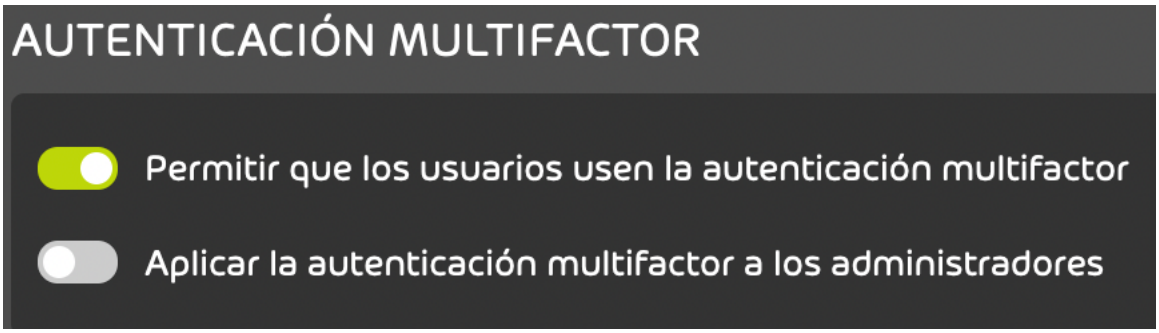


Figura 232: Forzar la autenticación multifactor para los administradores

El interruptor se pone verde. Aparece una ventana de confirmación.

5. Haga clic en **Confirmar**.

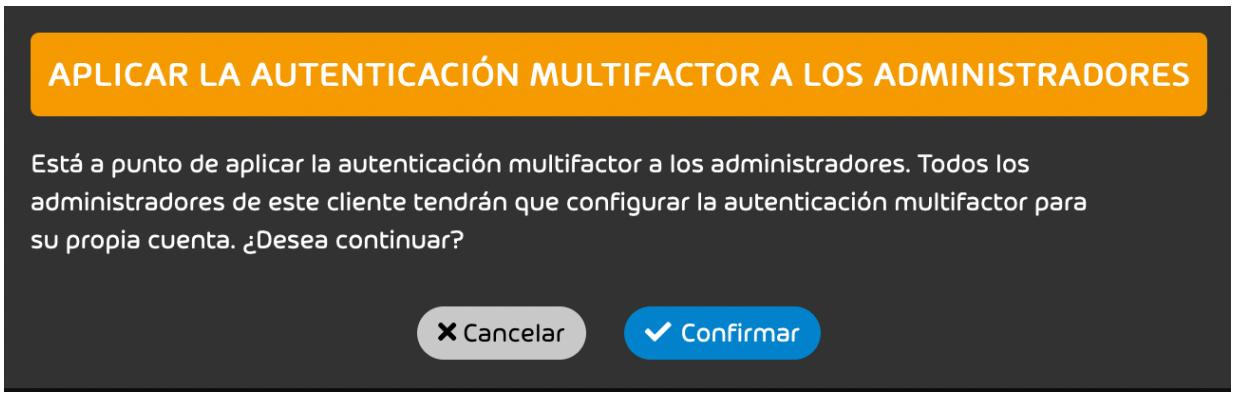


Figura 233: Confirmar

La autenticación multifactor se fuerza para todos los administradores del cliente.

La autenticación multifactor se ha forzado para todos los administradores de un cliente.

Cuando los administradores del cliente vuelvan a iniciar sesión en Control Panel, deberán configurar la autenticación multifactor para su cuenta de Control Panel (véase Configurar la autenticación multifactor a partir del paso 7 en la página 30el capítulo «Configurar la autenticación multifactor» a partir del paso 7 en la página 30 en el manual de Control Panel).

Desactivar la autenticación multifactor

Ha habilitado la autenticación multifactor para los usuarios de un dominio (véase Habilitar la autenticación multifactor en la página 323).

Puede desactivar la autenticación multifactor para los usuarios de un dominio. Entonces, los usuarios ya no tendrán permiso para configurar la autenticación multifactor para su cuenta de Control Panel. Para los usuarios que ya tenían configurada la autenticación multifactor, se elimina la configuración.

Nota:

Solo los usuarios cuyas contraseñas se administren en Control Panel o en un servicio de directorio mediante LDAP pueden configurar la autenticación multifactor en Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyos usuarios desee desactivar la autenticación multifactor.
3. Vaya a **Configuración de cliente** > **Autenticación**.
4. Accione el interruptor **Autenticación multifactor** de **Habilitar la autenticación multifactor para sus usuarios**.

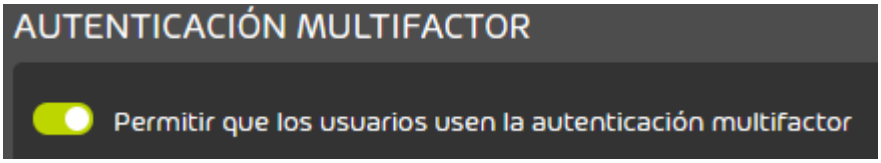


Figura 234: Desactivar la autenticación multifactor

El interruptor se pone gris y se abre una ventana de confirmación.

5. Haga clic en **Confirmar**.

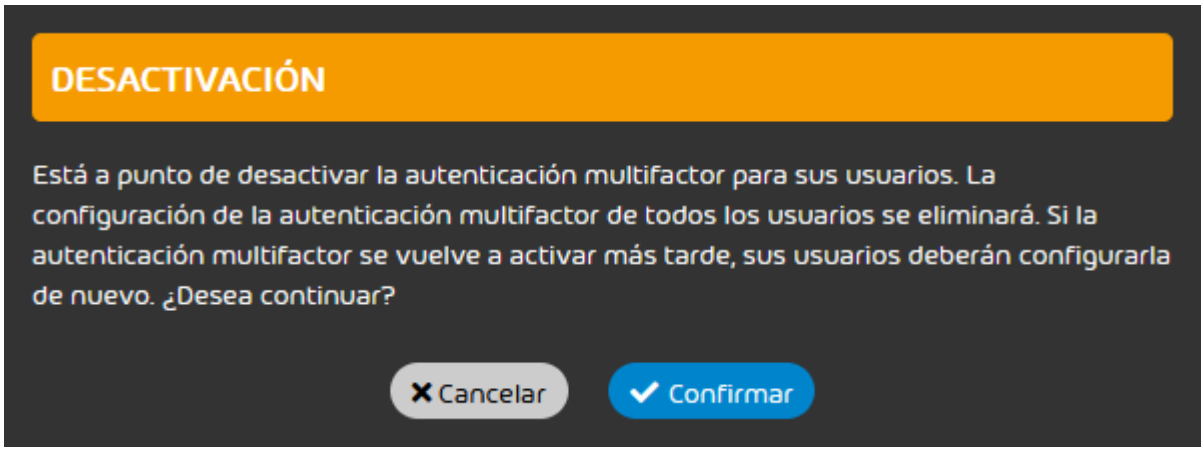


Figura 235: Confirmar

La autenticación multifactor se desactiva para los usuarios del dominio. Para los usuarios que ya tenían configurada la autenticación multifactor, se elimina la configuración. A partir de ahora, los usuarios solo deben introducir su contraseña de Control Panel al iniciar sesión en Control Panel.

Nota:

Si la autenticación multifactor se vuelve a habilitar para el dominio más tarde (véase Habilitar la autenticación multifactor en la página 323), los usuarios pueden reconfigurar la autenticación multifactor (véase el capítulo "Configurar la autenticación multifactor" en el manual de Control Panel).

La autenticación multifactor se ha desactivado para los usuarios de un dominio.

Configurar el cierre de sesión automático

Por razones de seguridad, las sesiones de usuarios inactivos en Control Panel se cierran automáticamente.

> **Nota:**
>
> Por defecto, las sesiones de usuarios inactivos en Control Panel se cierran automáticamente al cabo de 24 horas.

En el módulo **Configuración de cliente** > **Autenticación** (véase Autenticación en la página 319) puede ajustar un tiempo de cierre de sesión automático más breve o desactivar el cierre de sesión automático para los usuarios de un cliente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee modificar la configuración del cierre de sesión automático.
3. Vaya a **Configuración de cliente** > **Autenticación**.
4. Si desea configurar un tiempo de cierre de sesión automático más breve, ajuste el tiempo deseado en los campos **horas** y **minutos** del apartado **Cierre de sesión automático**.

   > **Nota:**
   >
   > El tiempo hasta el cierre de sesión automático puede ascender, como máximo, a 24 horas.

Figura 236: Ajustar el tiempo

5. Si desea crear una nueva cuenta de administrador, desmarque la casilla **Tiempo hasta el cierre de sesión** de la sección **Cierre de sesión automático**.

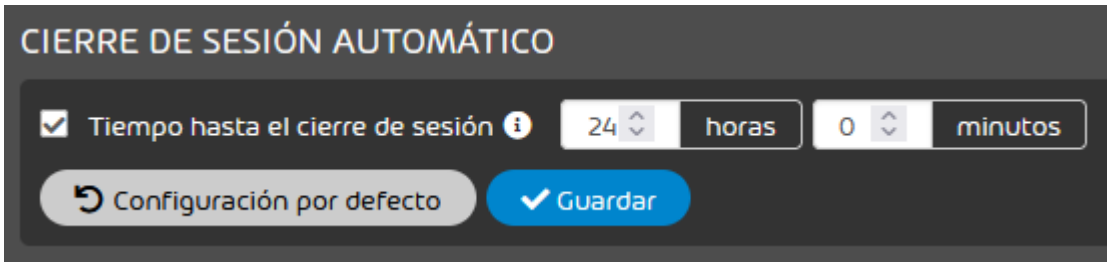


Figura 237: Desactivar el cierre de sesión automático

La casilla se desmarca y los ajustes de tiempo se deshabilitan.

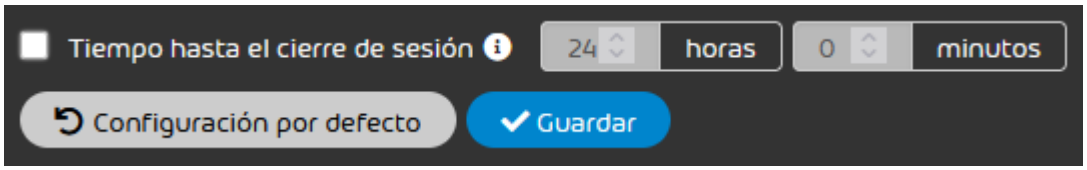


Figura 238: Sin cierre de sesión automático

6. Haga clic en **Guardar**.

Los ajustes se guardan. Se muestra un mensaje de éxito.

Se ha modificado la configuración del cierre de sesión automático de los usuarios de un cliente.

A continuación puede restaurar la configuración por defecto del cierre de sesión automático (véase Restaurar la configuración de cierre de sesión automático por defecto en la página 331).

Restaurar la configuración de cierre de sesión automático por defecto

Ha modificado la configuración del cierre de sesión automático de los usuarios de un cliente (véase Configurar el cierre de sesión automático en la página 329).

En el módulo **Configuración de cliente** > **Autenticación** (véase Autenticación en la página 319) puede restaurar la configuración por defecto del cierre de sesión automático de los usuarios de un cliente.

Nota:

Por defecto, las sesiones de usuarios inactivos en Control Panel se cierran automáticamente al cabo de 24 horas.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee restaurar la configuración por defecto del cierre de sesión automático.
3. Vaya a **Configuración de cliente** > **Autenticación**.

4. En la sección **Cierre de sesión automático**, haga clic en **Configuración por defecto**.

Figura 239: Restaurar los ajustes por defecto

Se restaura la configuración por defecto del cierre de sesión automático. Se muestra un mensaje de éxito.

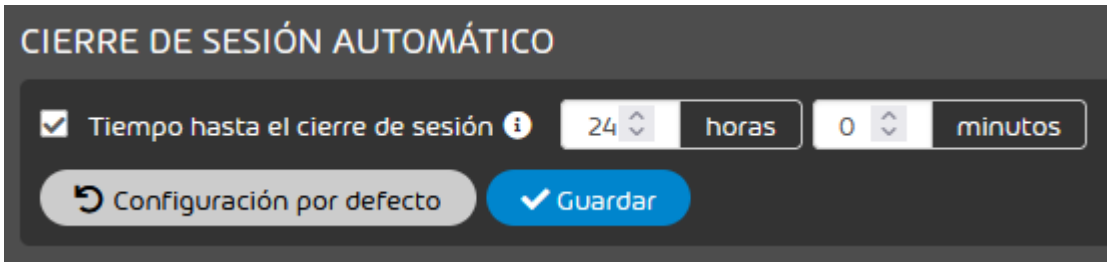


Figura 240: Configuración por defecto

Se ha restaurado la configuración por defecto del cierre de sesión automático para los usuarios de un cliente.

Definir direcciones IP

En el módulo **Configuración de cliente** > **Autenticación** puede establecer que solo sea posible acceder a Control Panel desde determinadas direcciones IP o rangos de direcciones IP para un dominio determinado.

Nota:

Si no hay registrada ninguna dirección IP, se podrá acceder a Control Panel desde cualquier dirección IP.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio deseado en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Autenticación**.
4. Haga clic en **Añadir restricción** bajo **Direcciones IP permitidas para acceder a Control Panel**.
5. Introduzca una dirección IPv4 válida o un rango de direcciones IPv4 válido y haga clic en **Añadir**.

Se ha añadido una dirección IP o rango de direcciones IP para el acceso a Control Panel para un dominio.

A continuación puede eliminar las direcciones IP registradas (véase Eliminar una dirección IP en la página 333).

Eliminar una dirección IP

Ha establecido que solo sea posible acceder a Control Panel desde determinadas direcciones IPv4 o rangos IPv4 para un dominio (véase Definir direcciones IP en la página 332).

En el módulo **Configuración de cliente** > **Autenticación** puede eliminar direcciones IP o rangos de direcciones IP definidas para un dominio para evitar el acceso a Control Panel desde los mismos. El acceso a Control Panel solo puede realizarse desde las direcciones IP o rangos de direcciones IP registrados.

Nota:

Si no hay registrada ninguna dirección IPv4, se podrá acceder a Control Panel desde cualquier dirección IPv4.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio deseado en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Autenticación**.
4. Haga clic en la flecha de menú de la fila correspondiente a la dirección IP o rango de direcciones IP que desee eliminar.
5. Haga clic en **Eliminar** para eliminar la dirección IP o el rango de direcciones IP.

Se ha eliminado una dirección IP o rango IP de la lista de direcciones IP permitidas para el acceso a Control Panel. Si aún quedan direcciones en la lista, ya no será posible acceder a Control Panel desde la dirección IP o el rango de direcciones IP eliminado. Si la lista está vacía, podrá accederse a Control Panel desde cualquier dirección IP.

Listas blancas y negras

Acerca de las listas blancas y negras

El módulo **Listas blancas y negras** contiene la lista blanca y la lista negra de un usuario o cliente. Cada usuario tiene su propia lista blanca y su propia lista negra que puede administrar por sí mismo. Los administradores a nivel de cliente pueden también acceder a las listas blancas y negras personales de cada uno de sus usuarios seleccionándolos en la selección de ámbitos. Adicionalmente, los administradores a nivel de cliente pueden administrar una lista blanca y una lista negra para todo su dominio. Además de registros aplicables a todos los usuarios del dominio, en la lista blanca y negra a nivel de dominio se muestran también los registros de usuarios individuales del dominio. Las listas blancas y negras se procesan en un orden determinado (véase Procesamiento de registros de listas blancas y negras en la página 379).

La lista negra permite a los usuarios y administradores a nivel de cliente hacer que el filtrado de spam clasifique como spam determinados correos entrantes de un usuario o todos los usuarios de un cliente. Los correos clasificados como **Spam** no se entregan directamente al destinatario, sino que se ponen en cuarentena. Si así lo desean, los destinatarios pueden hacerse entregar correos clasificados como **Spam** desde el módulo **Email Live Tracking** o desde los informes de cuarentena.

Nota:

En el módulo **Email Live Tracking** (véase el capítulo "Email Live Tracking" en el manual de Control Panel) también se muestran correos cuyos remitentes figuren en la lista negra.

Que los correos de los remitentes incluidos en la lista negra se muestren en los informes de cuarenta (véase el capítulo "Acerca de Quarantine Report" en el manual de Control Panel) depende de la configuración de los informes de cuarentena. Los usuarios pueden ver en su configuración de usuario si los correos de los remitentes incluidos en la lista negra se excluyen de sus informes de cuarentena (véase el capítulo "Configurar los informes de cuarentena" en el manual de Control Panel). Si el administrador lo permite, los usuarios pueden modificar este ajuste por sí mismos.

La lista blanca permite a los usuarios y administradores a nivel de cliente evitar que se apliquen el filtrado de spam y/u otros filtros a determinados correos entrantes de un usuario o de todos los usuarios de un dominio.

Importante:

La lista blanca a nivel de un usuario tan solo permite que los correos eviten el filtrado de spam. Si un remitente figura en la lista blanca, aquéllos de sus correos que de lo contrario se clasificarían como **Spam** se entregan a sus destinatarios clasificados como **Limpio**. Aunque su remitente se encuentre en la lista blanca, no se entregarán correos clasificados como **Contenido**, **Threat**, **AdvThreat** o **Rechazado**.

Por el contrario, al crear registros de lista blanca a nivel de dominio, los administradores a nivel de cliente pueden seleccionar los filtros a evitar. Además del filtrado de spam, es posible seleccionar otros filtros (véase Crear un registro de lista blanca para un dominio en la página 344). A nivel de dominio, los administradores a nivel de cliente pueden crear registros de lista blanca tanto para un dominio entero como para usuarios individuales de un cliente.

Los usuarios y administradores a nivel de cliente pueden crear registros de lista negra y blanca directamente en el módulo **Listas blancas y negras** (véanse Crear un registro de lista negra para un usuario en la página 337 y Crear un registro de lista blanca para un usuario en la página 340 para la creación de registros para un usuario y Crear un registro de lista negra para un dominio en la página 342 y Crear un registro de lista blanca para un dominio en la página 344 para la creación de registros para todos los usuarios de un dominio). Además, los usuarios y administradores a nivel de cliente pueden importar registros de lista blanca y negra desde un archivo CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351). Los archivos CSV deben presentar determinada estructura.Los archivos CSV para importar registros de lista blanca y negra a nivel de usuario o registros de lista negra a nivel de dominio tienen requisitos de formato distintos (véase Archivos CSV para la importación de registros de listas blancas y negras en la página 356) a los aplicables a archivos CSV para importar registros de lista blanca a nivel de dominio (véase Archivos CSV para importar registros de lista blanca para un dominio en la página 356).

Nota:

La importación de archivos CSV a nivel de dominio permite a los administradores a nivel de cliente importar registros de lista blanca para usuarios individuales además de registros de lista blanca para un dominio (véase Archivos CSV para importar registros de lista blanca para un dominio en la página 356). A este nivel, también se pueden importar registros de lista blanca para usuarios individuales que permiten evitar filtros distintos al filtrado de spam (véase Archivos CSV para importar registros de lista blanca para un dominio en la página 356).

Para simplificar la administración de registros de listas blancas y negras, los usuarios y administradores a nivel de cliente pueden exportar registros de lista negra o blanca en formato CSV (véase Exportar registros de lista blanca o negra en formato CSV. en la página 373). También es posible buscar registros de listas blancas y negras en Control Panel (véase Buscar registros de listas blancas o negras en la página 378). Los registros que ya no sean necesarios pueden eliminarse (véase Eliminar un registro de lista blanca o negra en la página 375).

Crear un registro de lista negra para un usuario

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede añadir direcciones de correo electrónico, dominios o direcciones IPv4 a su lista negra o a la lista negra de un usuario de su dominio. El filtrado de spam clasifica como spam los correos entrantes del usuario procedentes de estas direcciones de correo, dominios y direcciones IP.

Nota:

Los administradores a nivel de cliente pueden además crear registros de lista negra para todos los usuarios de su dominio (véase Crear un registro de lista negra para un dominio en la página 342).

Nota:

Además de crear registros de lista negra uno por uno, los usuarios y administradores a nivel de cliente pueden importar una lista de registros de lista negra en formato CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Si en lugar de crear un registro para su propia lista negra desea hacerlo para la de un usuario de su dominio, seleccione al usuario en la selección de ámbitos.

   Nota:

   Si no hay ningún ámbito seleccionado en la selección de ámbitos, estará seleccionado el ámbito del usuario que ha iniciado sesión en Control Panel.
3. Vaya a **Listas blancas y negras**.
4. Seleccione la pestaña **Lista negra**.
5. Haga clic en **Añadir elemento**.

Se abre una vista avanzada.

Figura 241: Vista avanzada

6. Introduzca en el campo de la izquierda la dirección de correo, el dominio o la dirección IPv4 cuyos correos no deban clasificarse como spam mediante el filtrado de spam.

> **Nota:**
>
> Los dominios deben respetar el siguiente formato: **nombrededominio.tld**.

7. Opcional: Introduzca una descripción del registro de lista negra en el campo **Descripción**.

> **Nota:**
>
> La descripción tiene una longitud máxima de 100 caracteres.

8. Haga clic en **Añadir**.

> **Importante:**
>
> Si el registro ya existe en la lista contraria, se eliminará de la misma y se añadirá a la lista actual.

El registro se crea y se añade a la tabla de registros de lista negra del usuario.

> **Nota:**
>
> El registro de lista negra también se mostrará en la lista negra del dominio del usuario.

Se ha creado un registro de lista negra para un usuario.

A continuación puede exportar los registros de lista negra en formato CSV (véase Exportar registros de lista blanca o negra en formato CSV. en la página 373). Si deja de necesitar algún registro de lista negra, puede eliminarlo (véase Eliminar un registro de lista blanca o negra en la página 375).

Crear un registro de lista blanca para un usuario

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede añadir direcciones de correo electrónico, dominios o direcciones IPv4 a su lista blanca o a la lista blanca de un usuario de su dominio. Los correos entrantes del usuario procedentes de estas direcciones de correo, dominios y direcciones IPv4 evitan el filtrado de spam.

Nota:

Los administradores a nivel de cliente pueden además crear registros de lista blanca para todos los usuarios de su dominio (véase Crear un registro de lista negra para un dominio en la página 342).

Importante:

La lista blanca a nivel de un usuario tan solo permite que los correos eviten el filtrado de spam. Si un remitente figura en la lista blanca, aquéllos de sus correos que de lo contrario se clasificarían como **Spam** se entregan a sus destinatarios clasificados como **Limpio**. Aunque su remitente se encuentre en la lista blanca, no se entregarán correos clasificados como **Contenido**, **Threat**, **AdvThreat** o **Rechazado**.

Por el contrario, al crear registros de lista blanca a nivel de dominio, los administradores a nivel de cliente pueden seleccionar los filtros a evitar. Además del filtrado de spam, es posible seleccionar otros filtros (véase Crear un registro de lista blanca para un dominio en la página 344). A nivel de dominio, los administradores a nivel de cliente pueden crear registros de lista blanca tanto para un dominio entero como para usuarios individuales de un cliente.

Nota:

Además de crear registros de lista blanca uno por uno, los usuarios y administradores a nivel de cliente pueden importar listas de registros de lista blanca en formato CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Si en lugar de crear un registro para su propia lista blanca desea hacerlo para la de un usuario de su dominio, seleccione al usuario en la selección de ámbitos.

> **Nota:**
>
> Si no hay ningún ámbito seleccionado en la selección de ámbitos, estará seleccionado el ámbito del usuario que ha iniciado sesión en Control Panel.

3. Vaya a **Listas blancas y negras**.
4. Seleccione la pestaña **Lista blanca**.
5. Haga clic en **Añadir elemento**.

Se abre una vista avanzada.

Figura 242: Vista avanzada

6. En el campo de la izquierda, introduzca la dirección de correo, el dominio o la dirección IPv4 cuyos correos no deban marcarse como spam mediante el filtrado de spam.

> **Nota:**
>
> Los dominios deben respetar el siguiente formato: **nombrededominio.tld**.

7. Opcional: Introduzca una descripción del registro de lista blanca en el campo **Descripción**.

> **Nota:**
>
> La descripción tiene una longitud máxima de 100 caracteres.

8. Haga clic en **Añadir**.

> **Importante:**
>
> Si el registro ya existe en la lista contraria, se eliminará de la misma y se añadirá a la lista actual.

El registro se crea y se añade a la tabla de registros de lista blanca del usuario.

> **Nota:**
>
> El registro de lista blanca también se mostrará en la lista blanca del dominio del usuario.

A continuación puede exportar los registros de lista blanca en formato CSV (véase Exportar registros de lista blanca o negra en formato CSV. en la página 373). Si deja de necesitar algún registro de lista blanca, puede eliminarlo (véase Eliminar un registro de lista blanca o negra en la página 375).

Crear un registro de lista negra para un dominio

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede añadir direcciones de correo electrónico, dominios o direcciones IPv4 a la lista negra de su dominio. El filtrado de spam clasifica como spam los correos entrantes de los usuarios de su dominio procedentes de estas direcciones de correo, dominios y direcciones IP.

Nota:

Además de crear registros de lista negra uno por uno, los administradores a nivel de cliente pueden importar listas de registros de lista negra en formato CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee crear un registro de lista negra.
3. Vaya a **Listas blancas y negras**.
4. Seleccione la pestaña **Lista negra**.
5. Haga clic en **Añadir elemento**.

   Se abre una vista avanzada.

Figura 243: Vista avanzada

6. Introduzca en el campo de la izquierda la dirección de correo, el dominio o la dirección IPv4 cuyos correos no deban clasificarse como spam mediante el filtrado de spam.

Nota:

Los dominios deben respetar el siguiente formato: **nombrededominio.tld**.

7. Opcional: Introduzca una descripción del registro de lista negra en el campo **Descripción**.

> **Nota:**
>
> La descripción tiene una longitud máxima de 100 caracteres.

8. Haga clic en **Añadir**.

> **Importante:**
>
> Si el registro ya existe en la lista contraria, se eliminará de la misma y se añadirá a la lista actual.

El registro se crea y se añade a la tabla de registros de lista negra del dominio.

Se ha creado un registro de lista negra para un dominio.

A continuación puede exportar los registros de lista negra en formato CSV (véase Exportar registros de lista blanca o negra en formato CSV. en la página 373). Si deja de necesitar algún registro de lista negra, puede eliminarlo (véase Eliminar un registro de lista blanca o negra en la página 375).

Crear un registro de lista blanca para un dominio

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede crear registros de lista blanca a nivel de un dominio. Puede crear tanto registros de lista blanca para su dominio que se apliquen a todos los usuarios del cliente como registros para usuarios individuales del cliente. Un registro de lista blanca permite a determinados correos entrantes evitar los filtros que se desee. A diferencia de los registros de lista blanca creados a nivel de usuario (véase Crear un registro de lista blanca para un usuario en la página 340), en los registros de lista blanca a nivel de dominio es posible seleccionar los filtros a evitar mediante los mismos.

Nota:

Además de crear registros de lista blanca individuales, los administradores a nivel de cliente pueden importar listas de registros de lista blanca en formato CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee crear un registro de lista blanca.
3. Vaya a **Listas blancas y negras**.
4. Seleccione la pestaña **Lista blanca**.
5. Haga clic en **Añadir elemento**.

   Se abre una vista avanzada.

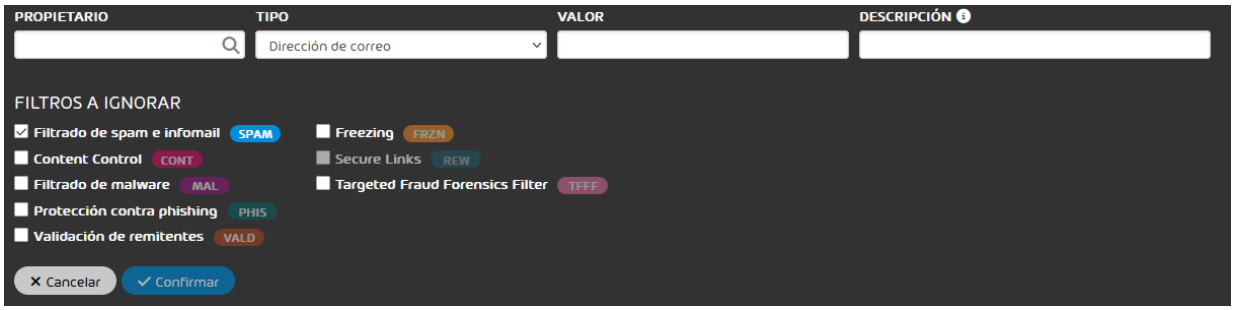


Figura 244: Vista avanzada

6. **Importante:**

   En el caso de Targeted Fraud Forensics Filter, el propietario no se tiene en cuenta. Los registros de lista blanca empleados para eludir este filtro se aplican a todos los usuarios del cliente.

   Opcional: Si el registro de lista blanca debe aplicarse solo a un usuario determinado del cliente, introduzca la dirección de correo electrónico del usuario en el campo **Propietario**.

Para activar la función de sugerencias automáticas, introduzca al menos tres caracteres seguidos.

> **Nota:**
>
> Si el campo permanece vacío, el registro de lista blanca se aplica al dominio del cliente. En este caso, el registro de lista blanca se aplica a todos los usuarios del cliente.

7. En el menú desplegable **Tipo**, seleccione la información del correo a la que se refiere el registro de lista blanca. Tiene las siguientes opciones:

   - **Dirección de correo**: El registro de lista blanca se aplica a correos enviados desde una dirección de correo concreta.
   - **Dominio**: El registro de lista blanca se aplica a correos enviados desde direcciones de correo de un dominio concreto.
   - **Dirección o rango IP**: El registro de lista blanca se aplica a correos enviados desde una dirección IPv4 concreta o un rango IPv4 concreto.
   - **Dominio de página web (solo para Secure Links)**: Los registros de lista blanca de este tipo solo evitan el motor Secure Links de Advanced Threat Protection (véase el capítulo "Descripción de los motores de ATP" del manual de Control Panel). Este registro de lista blanca impide que el motor Secure Links reescriba enlaces de un determinado sitio web en correos entrantes. El efecto del registro de lista blanca puede ampliarse también a los subdominios del dominio indicado.

Si se elige la opción **Dominio de página web (solo para Secure Links)**, debajo del campo **Valor** se mostrará la casilla de verificación **Incluir subdominios**. Además, al elegir esta opción, se marca la casilla de verificación **Secure Links** de la sección **Filtros a ignorar**, y el resto de casillas de la sección quedan desactivadas. Si se elige una opción distinta, la casilla marcada será **Filtrado de spam e infomail**.

8. Introduzca en el campo **Valor** el valor que deben presentar a los correos a los que se aplicará el registro de lista blanca. Introduzca uno de los siguientes valores en función de lo que haya elegido en el paso 7 en la página 346:

   - **Dirección de correo**: Dirección de correo electrónico del remitente
   - **Dominio**: Dominio del remitente
   - **Dirección o rango IP**: Dirección IPv4 o rango IPv4 desde el que se envió el correo
   - **Dominio de página web (solo para Secure Links)**: Dominio del sitio web al que un enlace del correo hace referencia

   El botón **Confirmar** se habilita.

9. Opcional: Si en el paso 7 en la página 346 ha seleccionado la opción **Dominio de página web (solo para Secure Links)** y el registro de lista blanca también debe aplicarse a enlaces de un subdominio del dominio indicado en el paso 8 en la página 347, marque la casilla **Incluir subdominios**.

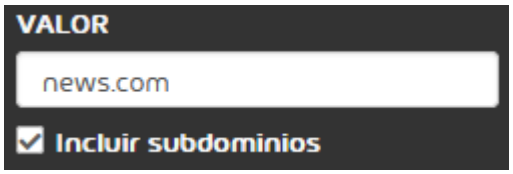


Figura 245: Incluir subdominios

10. Opcional: Introduzca una descripción del registro de lista blanca en el campo **Descripción**.

> **Nota:**
>
> La descripción tiene una longitud máxima de 100 caracteres.

11. En la sección **Filtros a ignorar**, marque las casillas de los filtros a evitar mediante el registro de lista blanca. Tiene las siguientes opciones:

    - **Filtrado de spam e infomail**: Se evitan los filtros de spam e infomail de Spam and Malware Protection. El registro de lista blanca impide que el filtrado de spam clasifique los correos como spam y el filtrado de infomail los clasifique como infomail.

      > **Nota:**
      >
      > Este filtro aparece marcado por defecto en todos los registros de lista blanca salvo en los del tipo **Dominio de página web (solo para Secure Links)**, pues se trata del filtro evitado por los registros de lista blanca creados a nivel de usuario (véase Crear un registro de lista blanca para un usuario en la página 340).

    - **Content Control**: Se evita el filtro Content Control (véase el capítulo "Acerca de Content Control" del manual de Control Panel) de Spam and Malware Protection. El registro de lista blanca impide que los correos se clasifiquen como **Contenido**.
    - **Filtrado de malware**: Se evita el filtrado de malware de Spam and Malware Protection. El registro de lista blanca impide que los correos con malware se clasifiquen como **Threat**.
    - **Protección contra phishing**: Se evita la protección frente a phishing de Spam and Malware Protection. El registro de lista blanca impide que los correos de phishing se clasifiquen como **Threat**.
    - **Validación de remitentes**: Se evita la validación de usuarios de Spam and Malware Protection. El registro de lista blanca impide que nuestro servidor de correo rechace correos que no hayan aprobado la validación de destinatarios.
    - **Freezing**: Se evita el motor Freezing (véase el capítulo "Descripción de los motores de ATP" del manual de Control Panel) de Advanced Threat Protection.
    - **Secure Links**: Se evita el motor Secure Links (véase el capítulo "Descripción de los motores de ATP" del manual de Control Panel) de Advanced Threat Protection.

> **Nota:**
>
> El motor Secure Links solo puede evitarse para los registros de lista blanca de tipo **Dominio de página web (solo para Secure Links)** (véase el paso 7 en la página 346). En los correos entrantes del propietario, el motor Secure Links no se aplicará a los enlaces del dominio indicado (véase el paso 8 en la página 347).

- **Targeted Fraud Forensics Filter**: El motor Targeted Fraud Forensics Filter (véase el capítulo "Descripción de los motores de ATP" del manual de Control Panel) de Advanced Threat Protection no comprueba si determinados correos de una dirección de correo externa dan la impresión de haberse enviado en nombre de determinado usuario de Control Panel. Sin embargo, el Targeted Fraud Forensics Filter sigue comprobando si

dichos correos dan la impresión de haberse enviado en nombre de otros usuarios de Control Panel.

Nota:

En el siguiente ejemplo puede ser útil evitar el motor Targeted Fraud Forensics Filter para determinado usuario. Un usuario del cliente se comunica frecuentemente con otros empleados de la empresa mediante una dirección de correo electrónico distinta a la registrada para el mismo en Control Panel (por ejemplo, mediante su dirección de correo particular). Para que estos correos no se clasifiquen como **AdvThreat**, el administrador del cliente puede añadir un registro de lista blanca para esta dirección de correo alternativa y dejar el motor Targeted Fraud Forensics Filter sin efecto para el usuario correspondiente en Control Panel.

Nota:

Los filtros forman parte de determinados servicios. Si uno de dichos servicios no se encuentra activado para el cliente, no es posible activar tampoco el filtro correspondiente. En tal caso se mostrará un triángulo de advertencia amarillo detrás del nombre del filtro. Si se trata de evitar dicho filtro, no ocurrirá nada. Sin embargo, es posible elegirlo.

12. Si ha elegido la opción **Targeted Fraud Forensics Filter**, introduzca en el campo **Usuario de Control Panel asociado** la dirección de correo electrónico del usuario para el que dejar de aplicar el motor Targeted Fraud Forensics Filter.

13. Haga clic en **Confirmar**.

> **Importante:**
>
> Si el registro ya existe en la lista contraria, se eliminará de la misma y se añadirá a la lista actual.

El registro de lista blanca se guarda y se añade a la tabla de registros de lista blanca.

Se ha creado un registro de lista blanca a nivel de un dominio.

A continuación puede exportar los registros de lista blanca en formato CSV (véase Exportar registros de lista blanca o negra en formato CSV. en la página 373). Si deja de necesitar algún registro de lista blanca, puede eliminarlo (véase Eliminar un registro de lista blanca o negra en la página 375).

Importar registros de listas blancas y negras en formato CSV

En lugar de crear registros de lista blanca o negra para un usuario (véanse Crear un registro de lista negra para un usuario en la página 337 y Crear un registro de lista blanca para un usuario en la página 340) o un dominio (véanse Crear un registro de lista negra para un dominio en la página 342 y Crear un registro de lista blanca para un dominio en la página 344) uno por uno, en el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede usted importar múltiples registros de lista blanca o negra desde un archivo CSV.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.

2. Si desea importar registros en la lista blanca o negra de un dominio o de un usuario del dominio, seleccione dicho dominio o usuario en la selección de ámbitos.

> **Nota:**
>
> Si no hay ningún ámbito seleccionado en la selección de ámbitos, estará seleccionado el ámbito del usuario que ha iniciado sesión en Control Panel.

3. Vaya a **Listas blancas y negras**.
4. Si desea importar registros de lista negra, seleccione la pestaña **Lista negra**. Si desea importar registros de lista blanca, seleccione la pestaña **Lista blanca**.
5. Haga clic en **Importar CSV**.

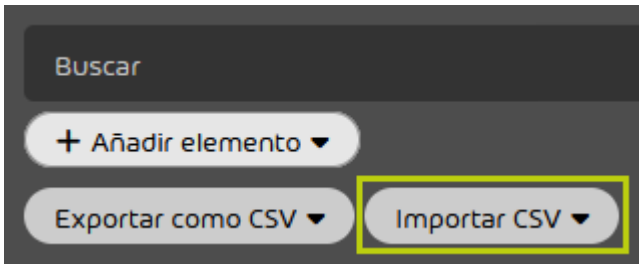


Figura 246: Importar un archivo CSV

Se abre una vista avanzada.

6. Haga clic en **Cargar archivo**.

Figura 247: Cargar el archivo

7.

Importante:

El archivo CSV debe cumplir determinados requisitos de formato. Los requisitos de formato de los archivos para importar registros de lista negra y blanca para un usuario, así como para importar registros de lista negra para un dominio (véase Archivos CSV para la importación de registros de listas blancas y negras en la página 356) son distintos a los requisitos de formato de los archivos para importar registros de lista blanca a nivel de dominio (véase Archivos CSV para importar registros de lista blanca para un dominio en la página 356).

Seleccione el archivo CSV de su sistema de archivos y haga clic en **Abrir**.

Se determina cuántos registros válidos pueden importarse desde el archivo CSV.

Nota:

Si no es posible importar un registro, se muestra una advertencia acerca del mismo.

Figura 248: Registros a añadir para un usuario

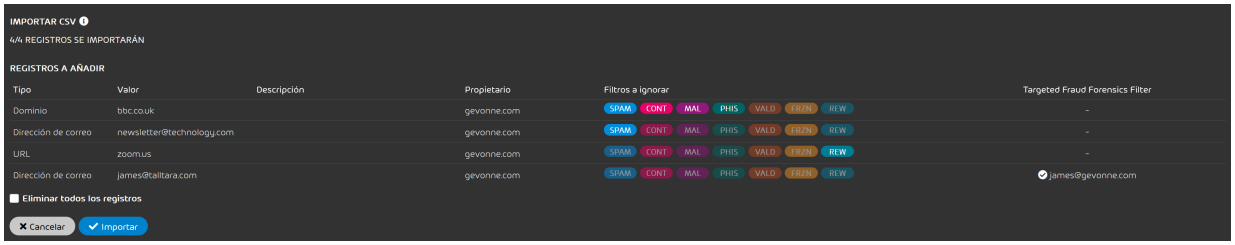


Figura 249: Registros a añadir a la lista blanca de un dominio

8. Opcional: Si desea eliminar todos los registros de lista negra o blanca previos de Control Panel, haga clic en **Eliminar todos los registros**.

Una vez realizado el paso 9 en la página 355, se eliminarán todos los registros que contenga la lista blanca o negra y se importarán en la misma los registros que contenga el archivo CSV.

9. Haga clic en **Importar**.

Los registros del archivo CSV se importan en la lista blanca o negra. Los registros inválidos o que ya estén en el sistema no se importan.

Figura 250: Registros importados para un usuario

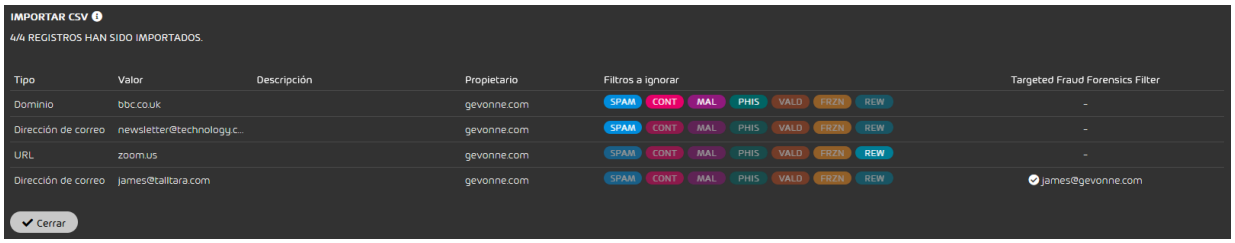


Figura 251: Registros importados en la lista blanca de un dominio

Se han importado registros de una lista blanca o negra desde un archivo CSV.

A continuación puede exportar los registros de lista blanca o negra en formato CSV (véase Exportar registros de lista blanca o negra en formato CSV. en la página 373). Si deja de necesitar algún registro, puede eliminarlo (véase Eliminar un registro de lista blanca o negra en la página 375).

Archivos CSV para la importación de registros de listas blancas y negras

Los archivos CSV para la importación de registros de listas blancas y negras (véase Acerca de las listas blancas y negras en la página 335) deben respetar determinada estructura. El archivo de importación debe cumplir los siguientes requisitos:

- La extensión del archivo a importar es .csv. No se aceptan otras extensiones, tales como .txt o .docx.
- La primera fila contiene el nombre de columna **value**.
- Las líneas posteriores contienen dominios, direcciones de correo electrónico o direcciones IPv4.
- Si una fila contiene varios registros, éstos están separados por punto y coma.

Archivos CSV para importar registros de lista blanca para un dominio

Los archivos CSV para la importación de registros de lista blanca a nivel de dominio (véase Acerca de las listas blancas y negras en la página 335) deben respetar determinada estructura. El archivo de importación debe cumplir los siguientes requisitos.

Reglas sobre la extensión

- La extensión del archivo a importar es .csv. No se aceptan otras extensiones, tales como .txt o .docx.

Reglas sobre columnas y filas

- El archivo CSV contiene 14 columnas.
- Las columnas están separadas entre sí mediante puntos y comas.
- La primera fila contiene los nombres de las columnas (véase la tabla Tabla 20: Columnas en la página 357).
- A partir de la segunda fila, cada fila contiene un registro de lista blanca.
- A partir de la segunda fila, cada columna contiene un valor (véase la tabla Tabla 20: Columnas en la página 357).
- Las filas no terminan en signo de puntuación.

Tabla 20: Columnas

NÚMERO	NOMBRE DE COLUMNA	VALOR
1	value	Esta columna puede contener una dirección de correo electrónico, un dominio, una URL, una dirección IPv4 o un rango IPv4. Se corresponde con el valor introducido en el campo **Valor** al crear registros de lista blanca manualmente (véase Crear un registro de lista blanca para un dominio en la página 344). El tipo de valor a introducir en esta columna depende del tipo de registro de lista blanca, es decir, del valor de la columna 4**entry_type**. Para más información acerca de los valores permitidos, véase el paso 8 en la página 347 del capítulo Crear un registro de lista blanca para un dominio en la página 344.

NÚMERO	NOMBRE DE COLUMNA	VALOR
2	description	Esta columna contiene una descripción de un registro de lista blanca. Se corresponde con el valor introducido en el campo **Descripción** al crear registros de lista blanca manualmente (véase Crear un registro de lista blanca para un dominio en la página 344). La descripción tiene una longitud máxima de 100 caracteres. La descripción es opcional. Por tanto, esta columna puede estar vacía.

NÚMERO	NOMBRE DE COLUMNA	VALOR
3	owner	Esta columna indica al propietario del registro de lista blanca. Si el registro de lista blanca debe aplicarse a todos los usuarios de un cliente, el valor introducido en esta columna será el dominio principal del cliente. Sin embargo, también es posible indicar al usuario de un cliente como propietario. Si el registro de lista blanca debe aplicarse a un único usuario del cliente, el valor introducido en esta columna será la dirección de correo electrónico del usuario. **Importante:** En el caso de Targeted Fraud Forensics Filter, el propietario no se tiene en cuenta. Los registros de lista blanca empleados para eludir este filtro se aplican a todos los usuarios del cliente.

NÚMERO	NOMBRE DE COLUMNA	VALOR
4	entry_type	Esta columna indica el tipo de registro de lista blanca. Se corresponde con el valor introducido en el campo **Tipo** al crear registros de lista blanca manualmente (véase Crear un registro de lista blanca para un dominio en la página 344). Están disponibles los siguientes valores: • **EMAIL**: Este valor se corresponde con la opción **Dirección de correo**. • **DOMAIN**: Este valor se corresponde con la opción **Dominio**. • **IP**: Este valor se corresponde con la opción **Dirección o rango IP**. • **URL**: Este valor se corresponde con la opción **Dominio de página web (solo para Secure Links)**. Para más información acerca de las opciones, véase el paso 7 en la página 346 del capítulo Crear un registro de lista blanca para un dominio en la página 344. **Importante:** Si esta columna contiene el valor **URL**,

NÚMERO	NOMBRE DE COLUMNA	VALOR
5	spam_protection	El valor de esta columna indica si el registro de lista blanca evita el filtrado de spam (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará el filtrado de spam. El valor **1** indica que se evitará el filtrado de spam. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
6	content_filter	El valor de esta columna indica si el registro de lista blanca evita Content Control (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que se no se evitará Content Control. El valor **1** indica que se evitará Content Control. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
7	malware_protection	El valor de esta columna indica si el registro de lista blanca evita el filtrado de malware (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará el filtrado de malware. El valor **1** indica que se evitará el filtrado de malware. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
8	phishing_protection	El valor de esta columna indica si el registro de lista blanca evita la protección frente a phishing (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará la protección frente a phishing. El valor **1** indica que se evitará la protección frente a phishing. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
9	sender_validation	El valor de esta columna indica si el registro de lista blanca evita la validación de destinatarios (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará la validación de destinatarios. El valor **1** indica que se evitará la validación de destinatarios. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
10	email_freezing	El valor de esta columna indica si el registro de lista blanca evita el motor Freezing de Advanced Threat Protection (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará el motor Freezing. El valor **1** indica que se evitará el motor Freezing. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
11	atp_url_rewriting	El valor de esta columna indica si el registro de lista blanca evita el motor Secure Links de Advanced Threat Protection (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará el motor Secure Links. El valor **1** indica que se evitará el motor Secure Links. **Importante:** Si la columna entry_type contiene el valor **URL**, esta columna deberá contener el valor **1**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
12	atp_tfff	El valor de esta columna indica si el registro de lista blanca evita el motor Targeted Fraud Forensics Filter de Advanced Threat Protection (véase el paso 11 en la página 348 del capítulo Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará el motor Targeted Fraud Forensics Filter. El valor **1** indica que se evitará el motor Targeted Fraud Forensics Filter. **Importante:** Si la columna 4**entry_type** contiene el valor **URL**, este filtro no se podrá evitar, y esta columna deberá contener el valor **0**.

NÚMERO	NOMBRE DE COLUMNA	VALOR
13	atp_tfff_related_user	**Importante:** Esta columna solo puede contener un valor si es preciso evitar el motor Targeted Fraud Forensics Filter, es decir, si la columna 12**atp_tfff** contiene el valor **1**. De lo contrario, esta columna deberá estar vacía. El valor de esta columna es la dirección de correo del usuario de Control Panel para el que debe evitarse el motor Targeted Fraud Forensics Filter. Se corresponde con el valor introducido en el campo **Usuario de Control Panel asociado** al crear registros de lista blanca manualmente (véase Crear un registro de lista blanca para un dominio en la página 344).

NÚMERO	NOMBRE DE COLUMNA	VALOR
14	atp_url_rewriting_include_subdomains	**Importante:** Esta columna solo deberá contener el valor **1** si el registro de lista blanca se refiere a una URL para Secure Links, es decir, si la columna **entry_type** contiene el valor **URL**. El valor de esta columna indica si es preciso evitar el motor Secure Links también para URLs de un subdominio del dominio indicado en la columna 1**value**. Esta columna se corresponde con el campo **Incluir subdominios** al crear registros de lista blanca manualmente (véase Crear un registro de lista blanca para un dominio en la página 344). La columna puede contener los valores **0** o **1**. El valor **0** indica que no se evitará el motor Secure Links para URLs de subdominios. El valor **1** indica que se evitará el motor Secure Links para URLs de subdominios.

Regla sobre registros repetidos

- Los registros repetidos no afectan al procesamiento del archivo CSV.

Editar un registro de lista blanca para un dominio

Ha creado registros de lista blanca para un dominio (véase Crear un registro de lista blanca para un dominio en la página 344) o los ha importado desde un archivo CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede editar registros de lista blanca para su dominio. Esto le permite, por ejemplo, modificar los filtros a evitar mediante un registros de lista blanca.

Nota:

A nivel de dominio, los administradores a nivel de cliente también pueden editar registros de lista blanca de usuarios de su dominio. Los registros de lista blanca creados a nivel de usuario (véase Crear un registro de lista blanca para un usuario en la página 340) solo evitan el filtrado de spam. Sin embargo, a nivel de dominio, los administradores a nivel de cliente pueden modificar los registros de lista blanca de usuarios de tal modo que puedan evitar otros filtros. Independientemente de los filtros evitados, los registros continuarán mostrándose a nivel de usuario, y los usuarios podrán eliminarlos (véase Eliminar un registro de lista blanca o negra en la página 375).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee editar un registro de lista blanca.
3. Vaya a **Listas blancas y negras**.
4. Seleccione la pestaña **Lista blanca**.

5. Haga clic en la flecha de menú junto al registro de lista blanca que desee editar.

Figura 252: Abrir el menú

Se abre un menú.

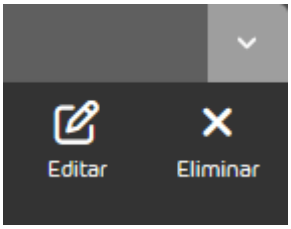


Figura 253: Menú

6. Haga clic en **Editar**.

Se abre un formulario con la configuración de un registro de lista blanca.

Figura 254: Configuración del registro de lista blanca

7. Ajuste la configuración como desee (véase Crear un registro de lista blanca para un dominio en la página 344).

8. Haga clic en **Confirmar**.

   Los cambios se guardan.

Se ha editado un registro de lista blanca

Exportar registros de lista blanca o negra en formato CSV.

Ha creado registros de lista blanca o negra (véanse Crear un registro de lista negra para un usuario en la página 337 y Crear un registro de lista blanca para un usuario en la página 340 para la creación de registros de lista negra y lista blanca para un usuario y Crear un registro de lista negra para un dominio en la página 342 y Crear un registro de lista blanca para un dominio en la página 344 para la creación de los mismos para un dominio) o los ha importado desde un archivo CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) puede exportar todos los registros de una lista blanca o negra en formato CSV.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Si, en lugar de sus propios registros, desea exportar los registros de la lista blanca o negra de su dominio o de un usuario del mismo, seleccione dicho dominio o usuario en la selección de ámbitos.

   Nota:

   Si no hay ningún ámbito seleccionado en la selección de ámbitos, estará seleccionado el ámbito del usuario que ha iniciado sesión en Control Panel.
3. Vaya a **Listas blancas y negras**.
4. Si desea exportar los registros de la lista negra, seleccione la pestaña **Lista negra**. Si desea exportar los registros de la lista blanca, seleccione la pestaña **Lista blanca**.

5. Haga clic en **Exportar como CSV**.

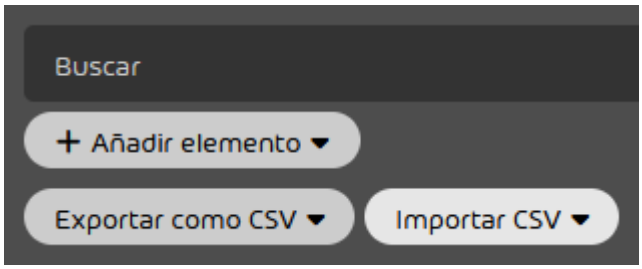


Figura 255: Exportar registros en formato CSV

Se muestran los ajustes para la exportación en formato CSV.

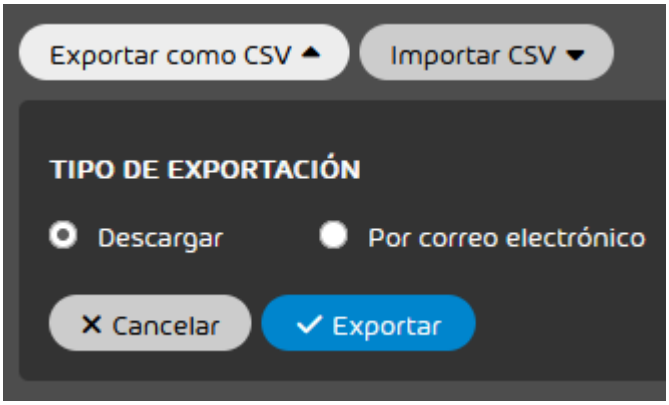


Figura 256: Ajustes para la exportación en formato CSV

6. En **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o enviarlo por correo electrónico.
   - **Descargar**: El archivo CSV se facilita para su descarga.
   - **Por correo electrónico**: El archivo CSV se envía por correo electrónico.

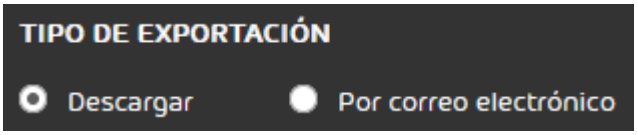


Figura 257: Seleccionar el tipo de exportación

Si se elige la opción **Por correo electrónico**, se muestra un campo de introducción de datos.

7. Opcional: Si elige la opción **Por correo electrónico**, introduzca la dirección de correo electrónico a la que enviar el archivo CSV en el campo de introducción de datos.
8. Haga clic en **Exportar**.

Ha exportado los registros de la lista blanca o negra en formato CSV. El archivo CSV se presenta para su descarga o se envía por correo electrónico.

Los registros de lista blanca o negra se han exportado en formato CSV.

Eliminar un registro de lista blanca o negra

Ha creado registros de lista blanca o negra (véanse Crear un registro de lista negra para un usuario en la página 337 y Crear un registro de lista blanca para un usuario en la página 340 para la creación de registros de lista negra y lista blanca para un usuario y Crear un registro de lista negra para un dominio en la página 342 y Crear un registro de lista blanca para un dominio en la página 344 para la creación de los mismos para un dominio) o los

ha importado desde un archivo CSV (véase Importar registros de listas blancas y negras en formato CSV en la página 351).

Si deja de necesitar algún registro en una lista blanca o negra, puede eliminarlo en el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Si desea eliminar un registro de la lista blanca o negra de su dominio o de un usuario del dominio, seleccione el dominio o el usuario en la selección de ámbitos.

   Nota:

   Si no hay ningún ámbito seleccionado en la selección de ámbitos, estará seleccionado el ámbito del usuario que ha iniciado sesión en Control Panel.
3. Vaya a **Listas blancas y negras**.
4. Si desea eliminar un registro de lista negra, seleccione la pestaña **Lista negra**. Si desea eliminar un registro de lista blanca, seleccione la pestaña **Lista blanca**.
5. Si desea eliminar un registro de lista blanca o negra de un usuario o un registro de lista negra de un dominio, haga clic en la cruz junto al registro correspondiente. Si desea eliminar un

registro de lista blanca de un dominio, haga clic en la flecha de menú junto al registro de lista blanca.

Figura 258: Eliminar un registro de lista blanca o negra de un usuario o un registro de lista negra de un dominio

Figura 259: Abrir el menú del registro de lista blanca de un dominio

Si se ha seleccionado un registro de lista negra o blanca de un usuario o un registro de lista negra de un dominio, se elimina el registro correspondiente. Si se ha seleccionado un registro de lista blanca, se abre un menú.

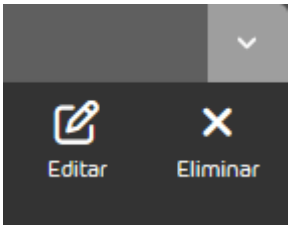


Figura 260: Menú del registro de lista blanca de un dominio

6. Si desea eliminar un registro de lista blanca de un dominio, haga clic en **Eliminar**.

El registro de lista blanca se elimina.

Se ha eliminado un registro de lista blanca o negra.

Buscar registros de listas blancas o negras

En el módulo **Listas blancas y negras** (véase Acerca de las listas blancas y negras en la página 335) es posible buscar registros de listas blancas y negras. Dentro del módulo **Listas blancas y negras**, la búsqueda funciona de un modo similar a la búsqueda en el módulo **Email Live Tracking** (véase "Buscar correos" en el manual de Control Panel).

La barra de búsqueda permite introducir términos de búsqueda. Es posible buscar expresiones tanto en todos los campos al mismo tiempo como en los campos **Valor**, **Descripción** y **Propietario** individualmente. Los registros se filtran de modo dinámico.

Aparte esto, los administradores a nivel de cliente pueden buscar registros de lista blanca para dominios por los filtros eludidos (véase Crear un registro de lista blanca para un dominio en la página 344). Para ello, en la parte superior de la pestaña **Lista blanca** existen botones de colores con los nombres de los filtros eludidos. Por defecto, todos los botones están desactivados y se muestran registros de lista blanca para todos los filtros. Para que solo se muestren los registros de lista blanca con los que se eludan uno o varios filtros concretos, los administradores a nivel de cliente pueden hacer clic en los botones de dichos filtros y, de este modo, modificar la vista.

Figura 261: Botones de filtros eludidos en registros de lista blanca

Ejemplo: Buscar registros en listas blancas o negras

El término **domain** se busca en la lista negra del usuario **klaus.trophobie@talltara.com**. Solo se muestran resultados que comiencen por **domain**.

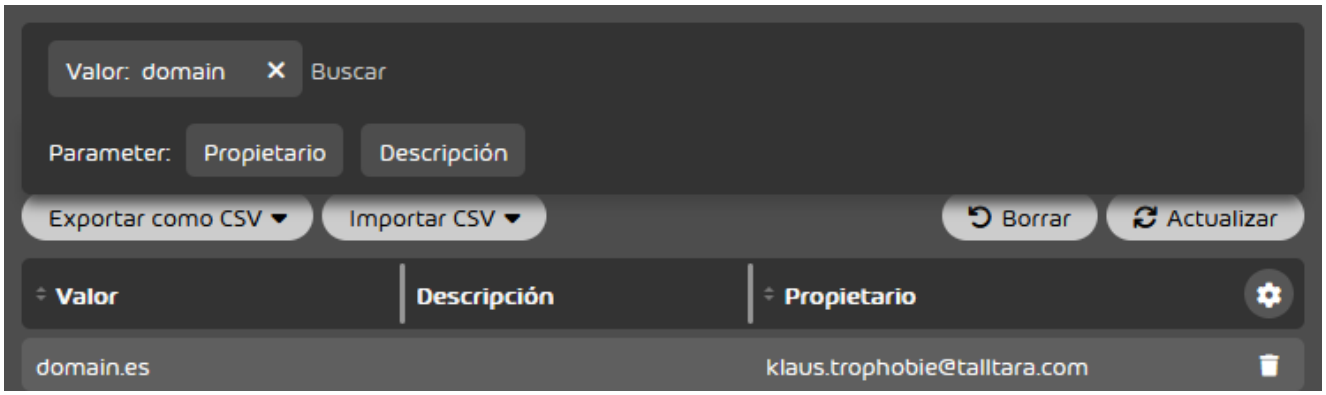


Figura 262: Buscar registros de lista blanca o negra

Procesamiento de registros de listas blancas y negras

Los registros de listas blancas y negras (véase Acerca de las listas blancas y negras en la página 335) se procesan del siguiente modo, desde la prioridad más alta hasta la prioridad más baja:

- Lista blanca de usuario
- Lista negra de usuario
- Lista blanca de dominio y grupo
- Lista negra de dominio y grupo

Nota:

Ya no es posible crear registros de listas blancas o negras a nivel de partner o para grupos. Sin embargo, es posible que tales listas aún existan para clientes antiguos.

Si se encuentra un registro adecuado en una de las listas, el procesamiento se detiene y el resto de listas no se tienen en cuenta.

Ejemplo: Secuencia de procesamiento de registros de listas blancas y negras

Un administrador añade al remitente **example@example.com** a la lista negra del dominio. Por el contrario, un usuario de ese dominio añade al mismo remitente a su lista blanca. Ese usuario recibirá todos los correos del remitente **example@example.com**. Al resto de usuarios, que no tienen al remitente en sus listas blancas, no se les entregarán.

Configuración de seguridad

Configuración de seguridad

- Advanced Threat Protection
- Quarantine Report
- Spam and Malware Protection
- Content Control
- Compliance Filter
- Signature and Disclaimer
- Continuity Service

Advanced Threat Protection (ATP)

Estructura y funcionamiento de ATP

Advanced Threat Protection (ATP) protege a las empresas frente a ataques selectivos e individuales.

Advanced Threat Protection (ATP) protege a las empresas frente a ataques selectivos e individuales. Unos innovadores motores de análisis forense se encargan de impedir los ataques al momento. Al mismo tiempo, esta solución proporciona datos detallados sobre ataques contra empresas.

ATP se compone de los siguientes motores de análisis (véase Descripción de los motores de ATP en la página 384):

- Motor de sandbox
- Secure Links
- URL Scanning
- Congelación
- Targeted Fraud Forensics

Los correos electrónicos captados por ATP se clasifican como **AdvThreat** y se ponen en cuarentena, y pueden ser entregados manualmente (véase el capítulo "Roles" del manual de Control Panel), por regla general, por usuarios con derechos administrativos.

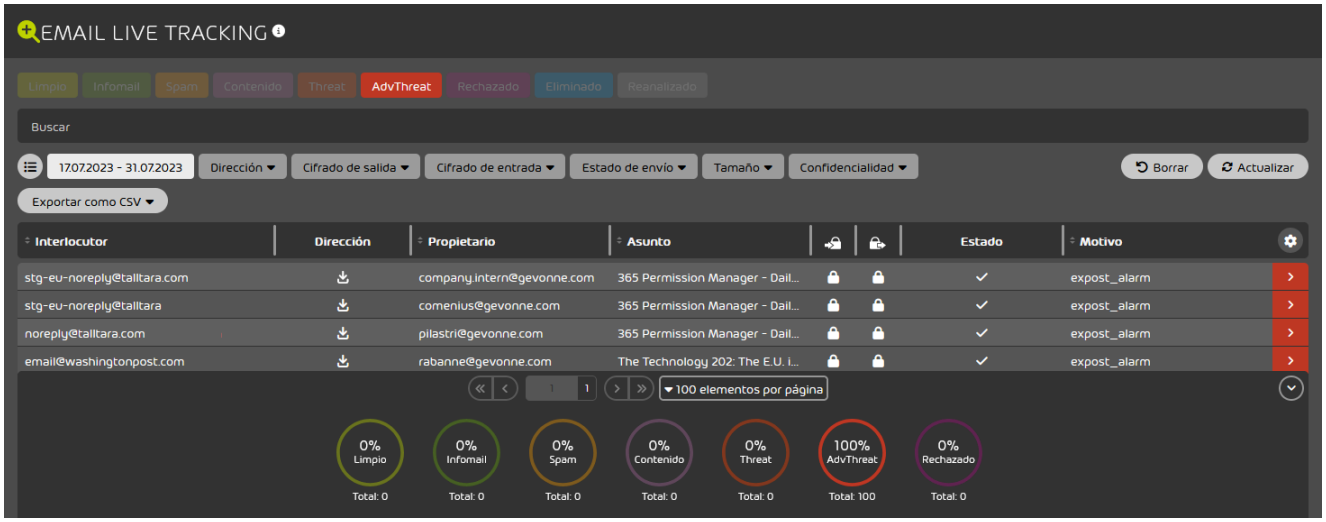


Figura 263: Categoría AdvThreat

ATP informa a los responsables de seguridad de las empresas sobre eventos relevantes para la seguridad en dos momentos:

- Inmediatamente tras la recepción de los correos que provoquen una respuesta de Real-Time Alert (véase Notificaciones en tiempo real en la página 388).
- Inmediatamente tras la detección de nuevas amenazas en correos ya entregados, mediante la función Ex Post Alert (véase Ex Post Alert en la página 388).

El siguiente diagrama muestra el papel de ATP en el procesamiento de correos mediante nuestra infraestructura.

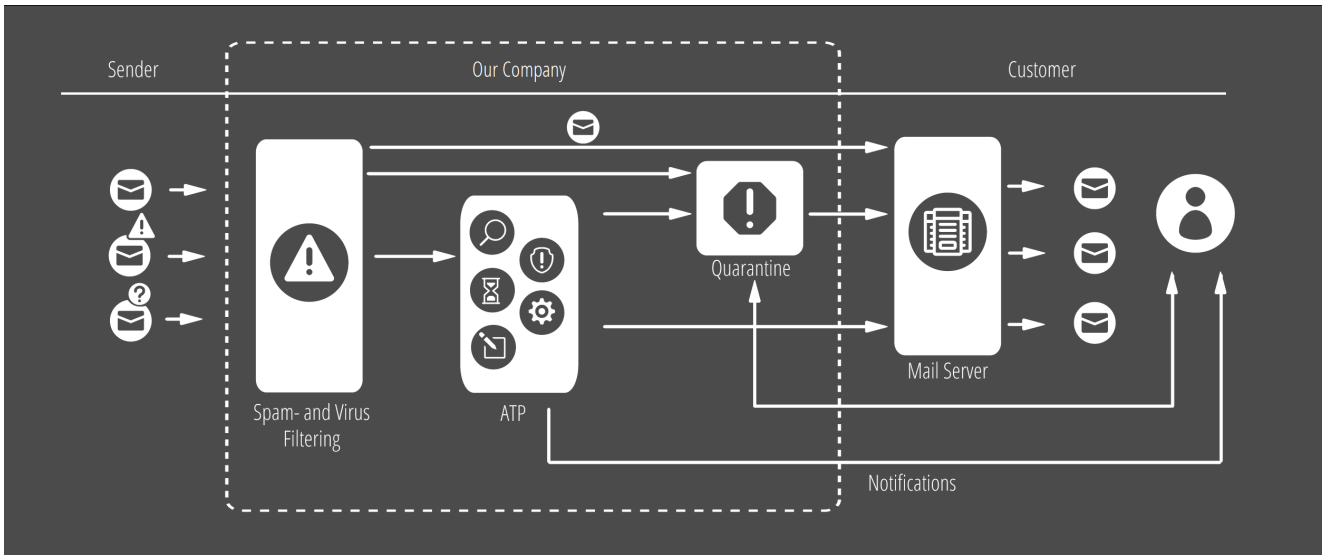


Figura 264: Funcionamiento de ATP

Además del análisis automático de los correos, tanto a su llegada como posteriormente en el contexto de la función Ex Post Alert, ATP ofrece la posibilidad de efectuar análisis manuales de correos con archivos adjuntos ejecutables. Con los denominados escaneos ATP (véase Escaneo ATP en la página 402), el usuario, además de aumentar su seguridad, obtiene información detallada sobre los correos en cuestión en forma de informes ATP (véase Informe ATP en la página 82).

Para que un cliente pueda emplear Advanced Threat Protection, un administrador debe activar el servicio (véase Activar ATP en la página 389). A continuación es posible administrar los destinatarios de notificaciones en tiempo real de Real-Time Alert y Ex Post Alert (véanse Añadir destinatarios de notificaciones en la página 391 y Eliminar destinatarios de notificaciones en la página 393). Los motores Secure Links y Targeted Fraud Forensics Filter deben activarse individualmente (véanse Activar Secure Links en la página 396 y Activar Targeted Fraud Forensics Filter en la página 397, respectivamente). Además, los administradores pueden decidir a qué grupos de usuarios se aplicará el motor Targeted Fraud Forensics Filter (véanse Añadir un grupo a la lista de grupos de TFFF en la página 399 y Retirar un grupo de la lista de grupos de TFFF en la página 401).

Descripción de los motores de ATP

Advanced Threat Protection emplea diversos motores para detectar y rechazar ataques.

Tabla 21: Motores de ATP

MOTORES DE ATP	MODO DE FUNCIONAMIENTO Y VENTAJAS
Motor de sandbox	Los archivos adjuntos se ejecutan en numerosos entornos para analizar su comportamiento. Si resulta tratarse de malware, se lo notificamos. Protege frente a ransomware y ataques combinados.

MOTORES DE ATP	MODO DE FUNCIONAMIENTO Y VENTAJAS
Secure Links	Secure Links impide que los enlaces incluidos en correos electrónicos lleven a los usuarios a páginas web maliciosas. Si Secure Links está activado para un cliente, los enlaces incluidos en los correos entrantes de los usuarios se reescriben al recibirse éstos en nuestra infraestructura. Esta reescritura permite que Secure Links compruebe las páginas web con posterioridad. Cuando un usuario hace clic en un enlace reescrito de un correo, Secure Links analiza la página web correspondiente utilizando nuestras bases de datos de inteligencia de dominios y direcciones URL. Estas bases de datos contienen miles de millones de registros de phishing y malware y se amplían continuamente. Durante las pruebas, se muestran consejos de seguridad al usuario en el navegador. Si la página web supera la primera prueba, Secure Links la analiza en cuanto a otros indicios de peligrosidad. Esto incluye enlaces insertados a malware o formularios de phishing. Solo en caso de que la página web supere ambas pruebas se derivará al usuario a la misma. De lo contrario, el navegador del usuario mostrará una página con uno de los siguientes mensajes: • **La página web está bloqueada**: Debido a un comportamiento sospechoso en la página web solicitada, se ha denegado el acceso a la misma. • **Advertencia**: La página web solicitada podría no ser fiable, porque no ha sido posible efectuar un análisis completo.

Nota:

MOTORES DE ATP	MODO DE FUNCIONAMIENTO Y VENTAJAS
URL Scanning	Los documentos adjuntos a un correo (p. ej., archivos PDF o de Microsoft) pueden contener enlaces. Sin embargo, no es posible sustituir los enlaces sin dañar la integridad del documento. El motor URL Scanning deja el documento intacto y se limita a comprobar el destino de los enlaces.
QR Code Analyzer	Las imágenes adjuntas a un correo (p. ej., en formato PNG, JPEG, GIF and BMP) pueden contener códigos QR. QR Code Analyzer comprueba el destino del código QR y bloquea el correo si éste conduce a una página web peligrosa.
Congelación	Los correos que no es posible clasificar con claridad, pero que resultan sospechosos, se retienen mediante congelación durante un breve periodo de tiempo. A continuación se efectúa un nuevo análisis con firmas actualizadas. Protege frente a ransomware, ataques combinados y suplantación de identidad.

MOTORES DE ATP	MODO DE FUNCIONAMIENTO Y VENTAJAS
Targeted Fraud Forensics Filter	Targeted Fraud Forensics Filter detecta ataques personalizados sin malware o enlaces. Incluye los siguientes mecanismos de detección: • Intention Recognition System: Alerta en caso de patrones de contenido que indiquen malas intenciones. • Fraud Attempt Analysis: Comprueba la autenticidad y la integridad de los metadatos y contenidos de los correos. • Identity Spoofing Recognition: Detección y bloqueo de identidades falsas de remitentes. • Spy-Out Detection: Protección antiespionaje de ataques para la obtención de información sensible. • Feign Facts Identification: Análisis de mensajes en cuanto a falsas apariencias. • Targeted Attack Detection: Detección de ataques selectivos contra personas concretas. Este motor debe activarse por separado (véase Activar Targeted Fraud Forensics Filter en la página 397). Targeted Fraud Forensics Filter se aplica a grupos de usuarios seleccionados que se administran mediante una lista de grupos (véanse Añadir un grupo a la lista de grupos de TFFF en la página 399 y Retirar un grupo de la lista de grupos de TFFF en la página 401).

Notificaciones en tiempo real

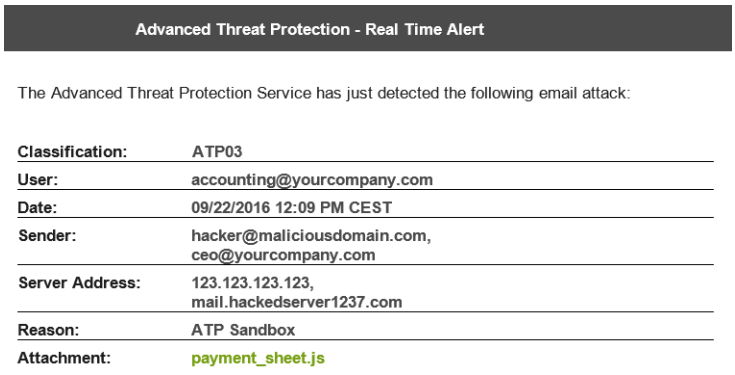
Real-Time Alert es una función de notificación de Advanced Threat Protection que informa acerca de las razones por las que se ha detenido un correo.

Tan pronto Advanced Threat Protection detecta un ataque, se envía una notificación a la empresa del cliente informándola sobre una posible amenaza. Las notificaciones incluyen información sobre el tipo y el objetivo del ataque, el remitente y el motivo por el que se ha detenido el correo.

Se envían notificaciones en los siguientes casos:

- El motor de sandbox ha detectado código malicioso (véase Motor de sandbox).
- Secure Links ha bloqueado una página web o una descarga (véase Secure Links).
- URL Scanning ha detectado un URL malicioso (véase URL Scanning).
- Targeted Fraud Forensics Filter ha filtrado correos (véase Targeted Fraud Forensics Filter).

Los destinatarios de las notificaciones pueden añadirse (véase Añadir destinatarios de notificaciones en la página 391) o eliminarse (véase Eliminar destinatarios de notificaciones en la página 393) mediante **Configuración de seguridad** > **Advanced Threat Protection**.



Advanced Threat Protection - Real Time Alert

The Advanced Threat Protection Service has just detected the following email attack:

Classification:	**ATP03**
User:	**accounting@yourcompany.com**
Date:	**09/22/2016 12:09 PM CEST**
Sender:	**hacker@maliciousdomain.com, ceo@yourcompany.com**
Server Address:	**123.123.123.123, mail.hackedserver1237.com**
Reason:	**ATP Sandbox**
Attachment:	**payment_sheet.js**

Figura 265: Notificación a tiempo real

Ex Post Alert

Mediante Ex Post Alert, los equipos de seguridad informática de las empresas reciben notificaciones cuando correos ya entregados se clasifican como dañinos a posteriori.

Los destinatarios de Ex Post Alert reciben una evaluación detallada del ataque de modo que puedan tomar inmediatamente medidas tales como comprobar sus sistemas o concienciar a sus empleados.

Los destinatarios de las notificaciones pueden añadirse (véase Añadir destinatarios de notificaciones en la página 391) o eliminarse (véase Eliminar destinatarios de notificaciones en la página 393) mediante **Configuración de seguridad** > **Advanced Threat Protection**.

Nota:

Ex Post Alert se activa para todos los buzones de correo de un cliente al activarse Advanced Threat Protection.

Configuración básica

Activar ATP

Ha activado Spam and Malware Protection.

Puede activar Advanced Threat Protection para proteger a su empresa en tiempo real frente a ciberataques selectivos e individualizados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Advanced Threat Protection.
3. Vaya a **Configuración de seguridad** > **Advanced Threat Protection**.
4. Accione el interruptor **Activar Advanced Threat Protection**.

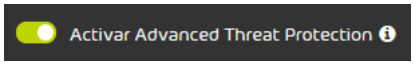


Figura 266: Activar Advanced Threat Protection

Se muestra una ventana de confirmación.

5. **Atención:**

   Una vez activado Advanced Threat Protection, comenzará un periodo de prueba gratuito de 30 días. Al finalizar el periodo de prueba, el servicio se volverá de pago.

   Haga clic en **Confirmar**.

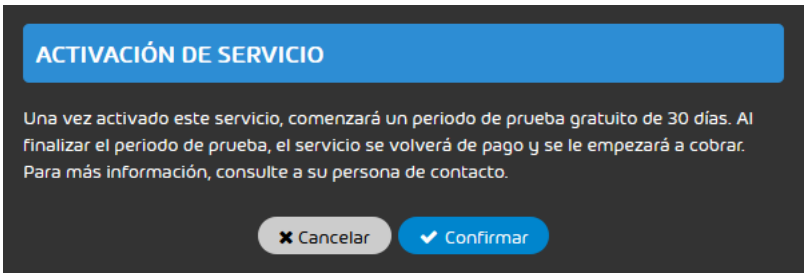


Figura 267: Confirmar

Advanced Threat Protection se ha activado para el dominio.

Importante:

Con su activación, se activan también todos los motores ATP (véase Descripción de los motores de ATP en la página 384) salvo Secure Links y Targeted Fraud Forensics Filter para el dominio. Secure Links y Targeted Fraud Forensics Filter deben activarse por separado.

A continuación puede administrar los destinatarios de notificaciones de Advanced Threat Protection (véanse Añadir destinatarios de notificaciones en la página 391 y Eliminar destinatarios de notificaciones en la página 393). También puede activar los motores Secure Links y Targeted Fraud Forensics Filter (véase Activar Secure Links en la página 396 y Activar Targeted Fraud Forensics Filter en la página 397).

Añadir destinatarios de notificaciones

Ha activado Advanced Threat Protection (véase Activar ATP en la página 389).

En el módulo **Configuración de seguridad** > **Advanced Threat Protection** puede añadir las direcciones de correo de los usuarios que han de recibir notificaciones de Real-Time Alert (véase Notificaciones en tiempo real en la página 388) y Ex Post Alert (véase Ex Post Alert en la página 388).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar añadir destinatarios de notificaciones.
3. Vaya a **Configuración de seguridad** > **Advanced Threat Protection**.
4. Haga clic en **Añadir destinatario**.

> **Nota:**
>
> Es recomendable registrar a los responsables de seguridad de su empresa como destinatarios.

Figura 268: Añadir un destinatario

Se abre una vista avanzada.

5. Introduzca la dirección de correo electrónico deseada en el campo de introducción de datos.

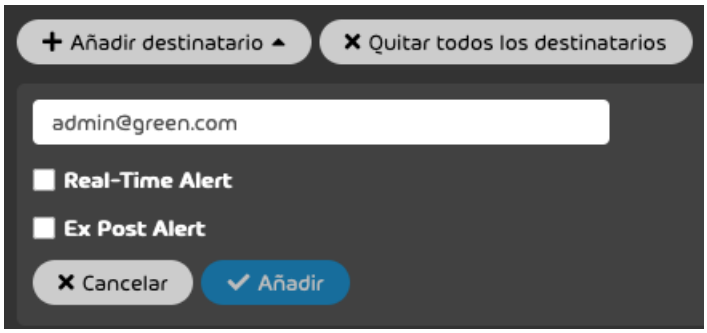


Figura 269: Introducir una dirección de correo electrónico

6. Marque las casillas de los tipos de notificaciones que el destinatario ha de recibir. Tiene las siguientes opciones.

   - **Real-Time Alert** (véase Notificaciones en tiempo real en la página 388)
   - **Ex Post Alert** (véase Ex Post Alert en la página 388)

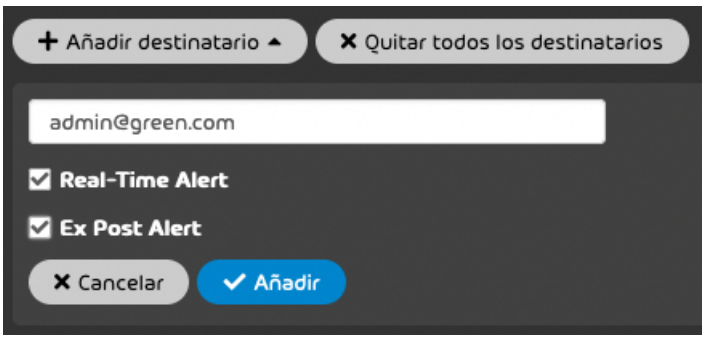


Figura 270: Seleccionar tipos de notificaciones

7. Haga clic en **Añadir**.

La dirección de correo se añade a la lista **Destinatarios de notificaciones**. Las marcas en las columnas **Ex Post Alert** y **Real-Time Alert** indican que el destinatario recibe notificaciones de este tipo.

Figura 271: Destinatario añadido

Se ha añadido una dirección de correo electrónico para la recepción de notificaciones de Real-Time Alert y/o Ex Post Alert.

Eliminar destinatarios de notificaciones

Ha activado Advanced Threat Protection (véase Activar ATP en la página 389) y añadido destinatarios de notificaciones (véase Añadir destinatarios de notificaciones en la página 391).

En el módulo **Configuración de seguridad** > **Advanced Threat Protection** puede eliminar direcciones de correo electrónico de la lista de destinatarios de notificaciones de Advanced Threat Protection (véase Estructura y funcionamiento de ATP en la página 381). Puede elegir entre eliminar direcciones de correo seleccionadas o eliminarlas todas a la vez.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el destinatario que desee eliminar de Advanced Threat Protection.
3. Vaya a **Configuración de seguridad** > **Advanced Threat Protection**.

4. Para eliminar un único destinatario, proceda del siguiente modo:

   a) Seleccione en la lista **Destinatarios de notificaciones** la dirección de correo que desee eliminar.

Figura 272: Seleccionar una dirección de correo

   b) Haga clic en la cruz de la fila de la dirección de correo que desee eliminar.

La dirección de correo se elimina de la lista.

5. Para eliminar todos los destinatarios al mismo tiempo, proceda del siguiente modo:

a) Haga clic en **Quitar todos los destinatarios**.

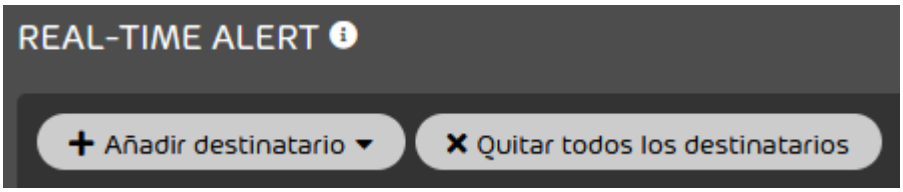


Figura 273: Eliminar todos los destinatarios

Aparece una ventana de confirmación.

b) Haga clic en **Confirmar**.

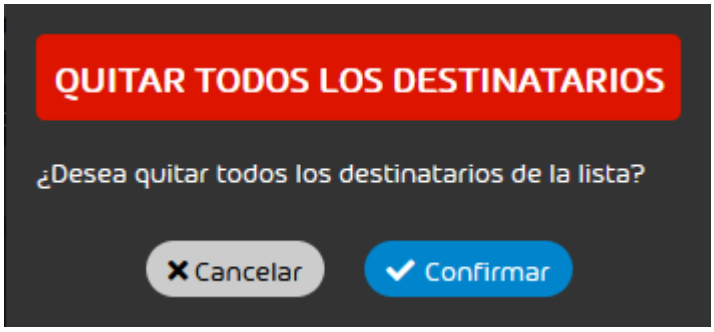


Figura 274: Confirmar

Todas las direcciones de correo se eliminan de la lista.

Se han eliminado algunas o todas las direcciones de correo de la lista de destinatarios de notificaciones de Advanced Threat Protection.

Activar Secure Links

Ha activado Advanced Threat Protection (véase Activar ATP en la página 389).

En el módulo **Configuración de seguridad** > **Advanced Threat Protection** puede activar el motor de ATP Secure Links (véase Descripción de los motores de ATP en la página 384). Secure Links se activa por defecto para todos los usuarios de sus dominios principal y alias.

Nota:

Si Secure Links no debe aplicarse a algunos usuarios del dominio, es preciso comunicar las excepciones al soporte técnico.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar Secure Links.
3. En Control Panel, vaya a **Configuración de seguridad** > **Advanced Threat Protection**.
4. Accione el interruptor **SECURE LINKS** de **Activar Secure Links**.

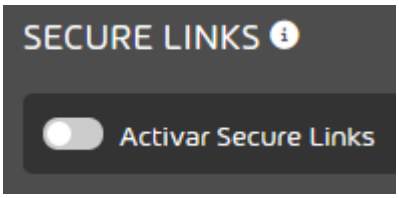


Figura 275: Activar Secure Links

El interruptor se pone verde y se abre una ventana de confirmación.

Nota:

Secure Links se activa por defecto para todos los buzones de correo de sus dominios principal y alias. Si no desea activar Secure Links para todos los dominios, póngase en contacto con el soporte técnico e indíquele qué dominios desea excluir de la activación antes de hacerlo.

5. Haga clic en **Confirmar**.

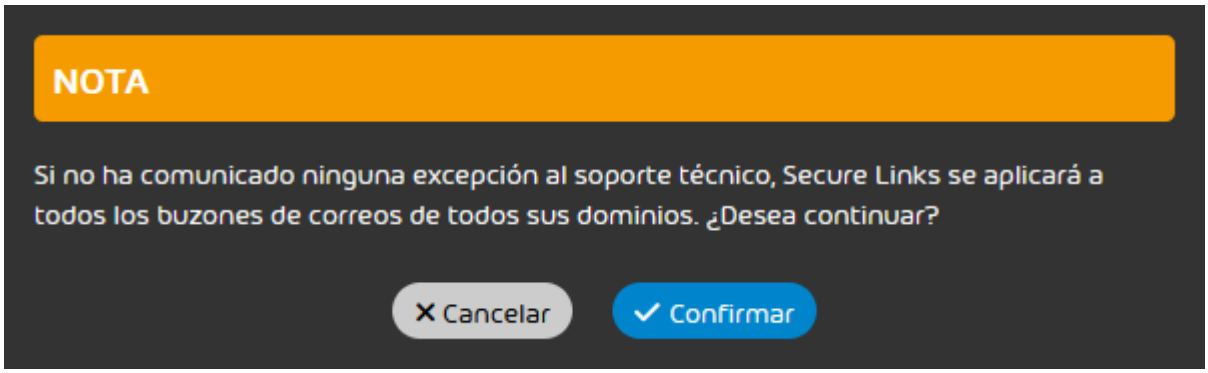


Figura 276: Confirmar

Secure Links se ha activado para todos los buzones de correo de sus dominios principal y alias no definidos como excepciones.

Activar Targeted Fraud Forensics Filter

Ha activado Advanced Threat Protection (véase Activar ATP en la página 389) y creado grupos de usuarios (véase el capítulo "Grupos" del manual de Control Panel). Ha activado la comprobación SPF (véase el capítulo "Activar la comprobación SPF" del manual de Control Panel).

En el módulo **Configuración de seguridad** > **Advanced Threat Protection** puede activar el motor de ATP Targeted Fraud Forensics Filter (véase Descripción de los motores de ATP en la página 384) para los grupos de usuarios seleccionados.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar Targeted Fraud Forensics Filter.
3. En Control Panel, vaya a **Configuración de seguridad** > **Advanced Threat Protection**.

4. Accione el interruptor **TARGETED FRAUD FORENSICS FILTER** de **Activar Targeted Fraud Forensics Filter**.

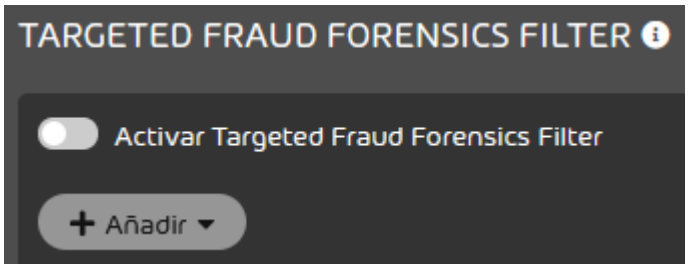


Figura 277: Activar Targeted Fraud Forensics Filter

El interruptor se pone verde. Targeted Fraud Forensics Filter se activa, pero aún no se aplica a ningún grupo de usuarios. El botón **Añadir** se habilita y se muestra un mensaje.

5. Haga clic en **Confirmar**.

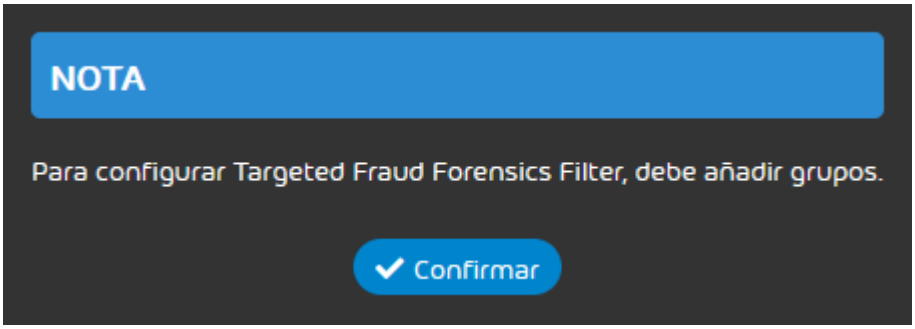


Figura 278: Confirmar

6. Añada los grupos de usuarios deseados a la lista de grupos (véase Añadir un grupo a la lista de grupos de TFFF en la página 399).

Targeted Fraud Forensics Filter se aplica a todos los grupos de usuarios añadidos.

El motor de ATP Targeted Fraud Forensics Filter se ha activado.

A continuación, puede añadir grupos a Targeted Fraud Forensics Filter (véase Añadir un grupo a la lista de grupos de TFFF en la página 399) o eliminarlos de allí (véase Retirar un grupo de la lista de grupos de TFFF en la página 401).

Añadir un grupo a la lista de grupos de TFFF

Ha activado Targeted Fraud Forensics Filter (véase Activar Targeted Fraud Forensics Filter en la página 397) y ha creado grupos de usuarios o los ha sincronizado con LDAP (véase el capítulo "Grupos" del manual de Control Panel).

Targeted Fraud Forensics Filter no se aplica a dominios, sino a grupos de usuarios. Para aplicar Targeted Fraud Forensics Filter a un grupo, debe incluirlo en la lista de grupos del Targeted Fraud Forensics Filter.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el grupo que desee añadir a Targeted Fraud Forensics Filter.
3. En Control Panel, vaya a **Configuración de seguridad** > **Advanced Threat Protection**.

4. En el apartado **TARGETED FRAUD FORENSICS FILTER**, haga clic en **Añadir**.

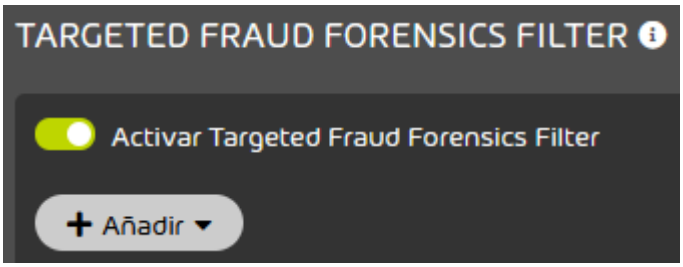


Figura 279: Añadir grupos

Se abre una vista avanzada.

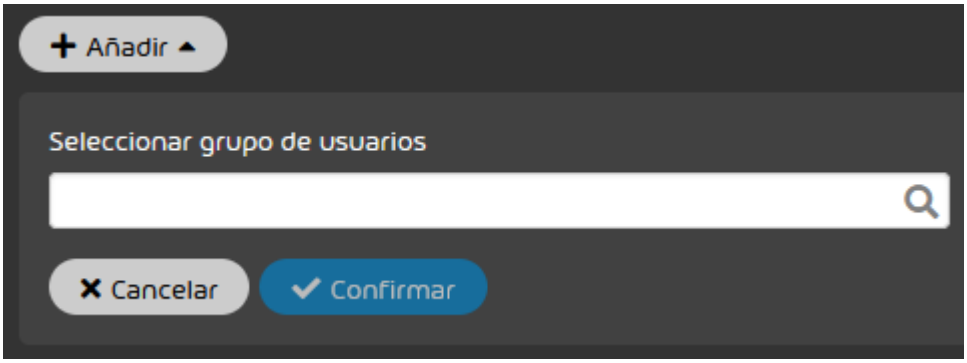


Figura 280: Vista avanzada

5. Introduzca el nombre del grupo deseado en el campo de búsqueda.

Se despliega un menú desplegable con los resultados de la búsqueda.

6. Seleccione el grupo de usuarios.

7. Haga clic en **Confirmar**.

Figura 281: Confirmar

El grupo se ha añadido a la lista de grupos. Targeted Fraud Forensics Filter se aplica inmediatamente a todos los buzones de correo de este grupo.

Se ha añadido un grupo a la lista de grupos de Targeted Fraud Forensics Filter.

A continuación puede eliminar el grupo de la lista de grupos de Targeted Fraud Forensics Filter (véase Retirar un grupo de la lista de grupos de TFFF en la página 401).

Retirar un grupo de la lista de grupos de TFFF

Ha activado Targeted Fraud Forensics Filter (véase Activar ATP en la página 389) y ha añadido grupos de usuarios a la lista de grupos (véase Añadir un grupo a la lista de grupos de TFFF en la página 399).

Targeted Fraud Forensics Filter se aplica a grupos de usuarios. Para dejar de aplicar Targeted Fraud Forensics Filter a un grupo, debe retirarlo de la lista de grupos del Targeted Fraud Forensics Filter.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio al que pertenezca el grupo que desee eliminar de Targeted Fraud Forensics Filter.
3. Vaya a **Configuración de seguridad** > **Advanced Threat Protection**.

4. Seleccione el grupo deseado en la lista de usuarios de la sección **TARGETED FRAUD FORENSICS FILTER**.

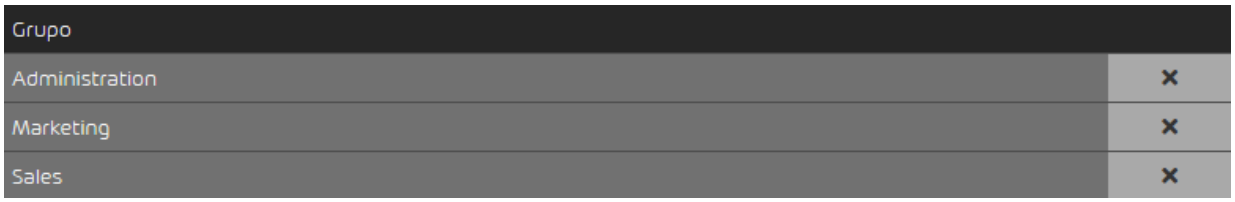


Figura 282: Seleccionar un grupo

5. Haga clic en la cruz junto al grupo que desee eliminar.

El grupo se ha retirado de la lista de grupos. Targeted Fraud Forensics Filter ya no se aplicará a los buzones de correo de este grupo.

Se ha eliminado un grupo de la lista de grupos de Targeted Fraud Forensics Filter.

Escaneo ATP

Con el escaneo ATP, los administradores puede analizar adicionalmente correos. El escaneo ATP se efectúa manualmente (véase Iniciar el escaneo ATP en la página 80) y comprueba correos con archivos adjuntos ejecutables en cuanto a contenido malicioso. En el proceso, el motor de sandbox analiza el correo seleccionado y elabora un informe detallado al respecto, el informe ATP (véase Informe ATP en la página 82).

El escaneo ATP también está disponible para clientes que no hayan contratado ATP. Sin embargo, el número de análisis mensuales está limitado para este tipo de clientes.

Como los correos de clientes de ATP ya se analizan automáticamente mediante el motor de sandbox (véase Descripción de los motores de ATP en la página 384), el escaneo ATP es para ellos, principalmente, una medida de seguridad adicional (p. ej., antes de la entrega manual de correos clasificados como **AdvThreat**). Además, con el informe ATP, los clientes de ATP obtienen información adicional.

Iniciar el escaneo ATP

Ha activado Advanced Threat Protection (véase Activar ATP en la página 389).

Con el escaneo ATP (véase el capítulo "Escaneo ATP" del manual de Control Panel) puede comprobar manualmente correos con archivos adjuntos ejecutables en cuanto a contenidos perjudiciales en el módulo **Email Live Tracking** (véase el capítulo "Email Live Tracking" del manual de Control Panel).

Nota:

El escaneo ATP solo está disponible para correos con archivos adjuntos ejecutables (p. ej., archivos .exe).

Atención:

Si no ha contratado Advanced Threat Protection (siehe das Kapitel "Estructura y funcionamiento de ATP" im Control-Panel-Handbuch), podrá realizar dos escaneos ATP gratuitos al mes. Solo podrá efectuar más escaneos ATP después de contratar el servicio de pago de ATP.

1. Inicie sesión en Control Panel con sus datos de acceso.
2. Si, en lugar de sus propios correos, desea ver los correos de los usuarios de un dominio, seleccione el dominio en la selección de ámbitos.
3. Vaya al módulo **Email Live Tracking**.

4. Haga clic en la flecha a la derecha de la fila del correo deseado.

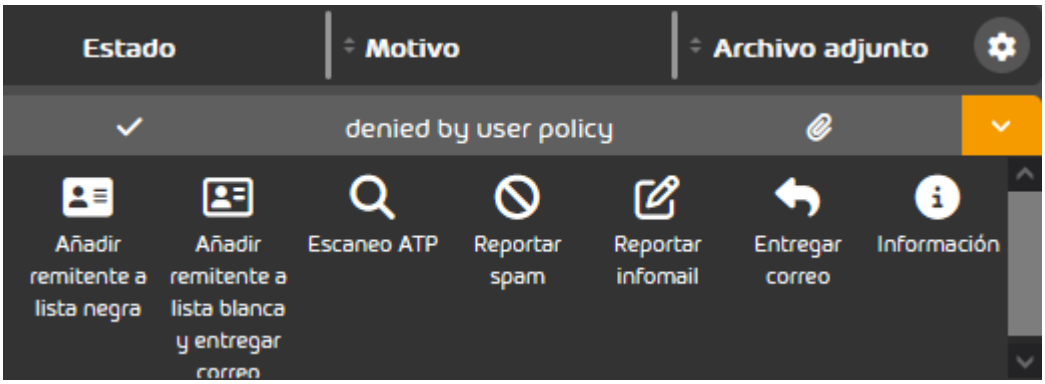


Figura 283: Análisis ATP en Email Live Tracking

La vista de opciones avanzadas se abre.

5. Haga clic en **Escaneo ATP** para iniciar el escaneo.

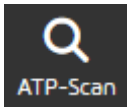


Figura 284: Iniciar el escaneo ATP

Se ha iniciado el escaneo ATP para el correo.

Tan pronto como finalice el escaneo ATP, podrá consultar el informe ATP en la vista de opciones avanzadas del correo (véase Informe ATP en la página 82) desde **Escaneo ATP**.

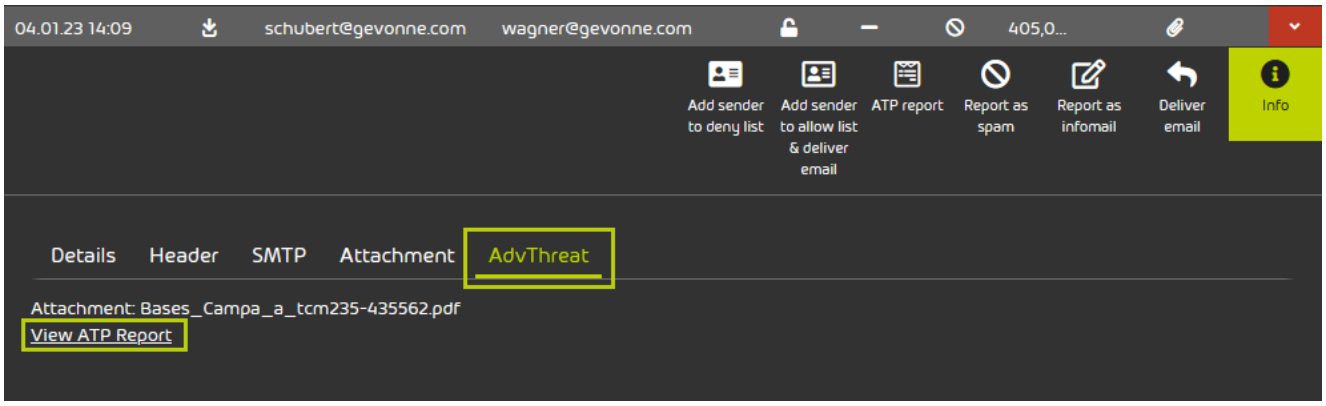


Figura 285: Consultar el informe ATP

Informe ATP

El informe ATP es un informe detallado que se genera tras analizarse un correo con el escaneo ATP (véase el capítulo "Escaneo ATP" del manual de Control Panel y Iniciar el escaneo ATP en la página 80). El informe ATP informa acerca del correo analizado. Los informes ATP están disponibles para los correos analizados en el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63). El informe ATP de un correo puede consultarse desde el punto de menú **Informe ATP** o **Información** de la pestaña **AdvThreat**.

El informe ATP se divide en cuatro ventanas principales:

Summary

Aquí se muestra un resumen del archivo analizado. También se asigna al archivo una puntuación (**Score**) de 0 a 10. 0 significa que el archivo no comporta ningún riesgo, mientras que 10 es el nivel de riesgo más alto.

En la sección **Signatures** (firmas), el archivo se asigna a una de las siguientes categorías en función de su comportamiento:

- Información (verde)
- Atención (amarillo)
- Advertencia (rojo)

Si hace clic en una firma, se le mostrará información avanzada sobre el proceso.

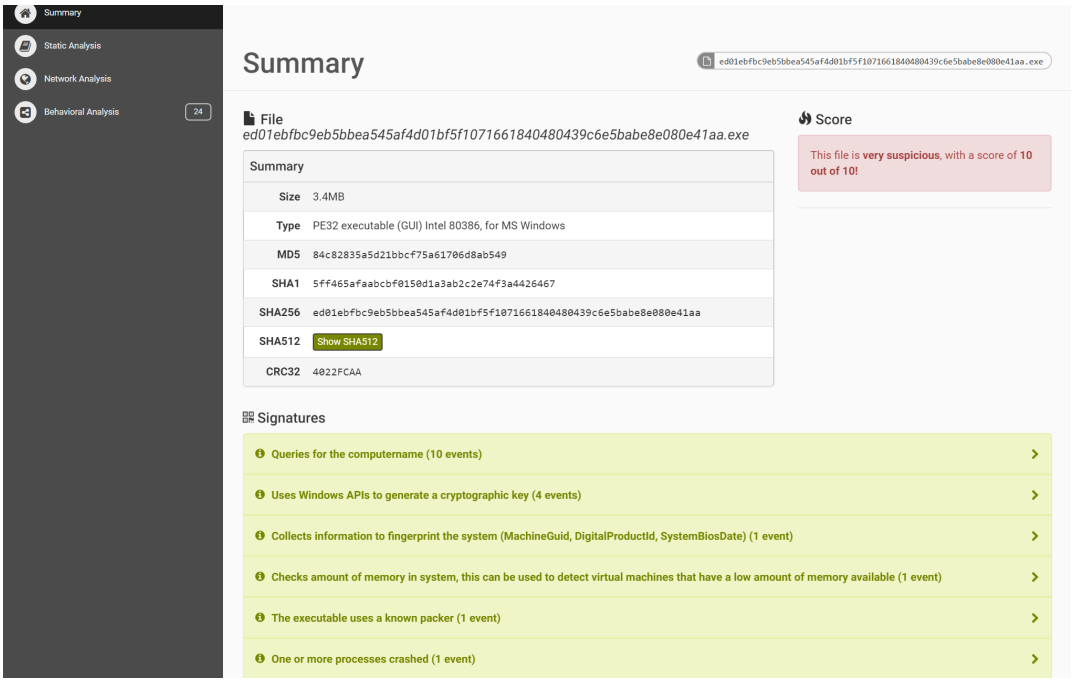


Figura 286: Resumen del informe ATP

Static Analysis

El análisis estadístico se divide, a su vez, en tres subcategorías:

- Static Analysis – Análisis estadístico del archivo. Depende del formato del archivo.
- Strings – Reproducción de las cadenas de caracteres del archivo.
- Antivirus – Análisis del archivo mediante diversos antivirus.

Network Analysis

En este análisis de red se analiza todo el tráfico de la red y se enumera por protocolos (p. ej., HTTP, TCP, UDP).

Behavioral Analysis

En el análisis de comportamiento se analiza el archivo en tiempo de ejecución.

Se muestran todas las llamadas a APIs y recursos del sistema registrados durante un análisis dinámico en sandbox.

Los resultados se dividen en dos secciones:

- Process Tree – Aquí se muestran los procesos en sucesión jerárquica.
- Process Contents – Si selecciona un proceso del "Process Tree", se le mostrarán aquí las llamadas a APIs ejecutadas en orden cronológico.

Email Authentication

Acerca de Email Authentication

Email Authentication ofrece a los administradores a nivel de cliente diversas opciones de autenticación de remitentes de correo electrónico (véase Métodos de autenticación de remitentes en la página 409). Están disponibles los siguientes métodos:

- Validación SPF (Sender Policy Framework) (véase Comprobación SPF en la página 410)
- Validación y firma DKIM (DomainKeys Identified Mail) (véase Validación DKIM y firma DKIM en la página 422)
- Validación DMARC (Domain-based Message Authentication, Reporting and Conformance (véase Validación DMARC en la página 427)

Email Authentication solo puede emplearse si Spam and Malware Protection se encuentra activado (véase "Activar Spam and Malware Protection" en el manual de Control Panel). Antes de activar los métodos de autenticación de remitentes, los administradores a nivel de cliente deben comprobar la configuración de DNS de sus propios dominios (véase Comprobar la configuración de DNS de dominios propios en la página 407).

Comprobar la configuración de DNS de dominios propios

Ha activado Spam and Malware Protection (véase "Activar Spam and Malware Protection" en el manual de Control Panel).

Nota:

Solo puede comprobar la configuración de DNS de los dominios para los cuales haya activado Spam and Malware Protection.

Antes de configurar un procedimiento de autenticación de remitentes, es preciso comprobar que la configuración de DNS de sus dominios sea correcta. En el proceso se comprueba el estado de la configuración SPF, DKIM y DMARC de sus dominios.

Importante:

Solo puede activar la comprobación SPF (véase Comprobación SPF en la página 410), la validación DKIM (véase Validación DKIM y firma DKIM en la página 422) y la validación DMARC (véase Validación DMARC en la página 427) para aquellos de sus dominios para los cuales se hayan realizado correctamente los ajustes correspondientes en la configuración de DNS.

Nota:

Para saber cómo definir un registro SPF, véase Definir un registro SPF en la página 413.

Para saber cómo definir un registro CNAME, véase Definir un registro CNAME en la página 422.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.

4. Haga clic en **Actualizar configuración de DNS** para comprobar el estado de la configuración de DNS de sus dominios.

Figura 287: Actualizar la configuración de DNS

Recibirá un resumen en forma de tabla del estado de la configuración de DNS de sus dominios. Hay tres resultados posibles:

	La configuración del dominio es correcta.
	No se han definido registros para el dominio.
	La configuración del dominio es incorrecta.

La configuración de DNS de sus dominios se ha comprobado.

A continuación puede activar métodos de autenticación de remitentes (véase Métodos de autenticación de remitentes en la página 409).

Métodos de autenticación de remitentes

Los administradores a nivel de cliente pueden activar diversos métodos de autenticación de remitentes de correos para sus dominios. Están disponibles los siguientes métodos:

- Comprobación SPF en la página 410
- Validación DKIM y firma DKIM en la página 422
- Validación DMARC en la página 427

Estos métodos aumentan la protección de infraestructuras de correo electrónico de empresas frente al spam y la suplantación de identidad. Los administradores a nivel de cliente pueden emplear un método individualmente o combinar métodos entre sí.

La máxima protección se obtiene combinando varios métodos. Por ejemplo, en servidores que solo emplean DKIM, es posible distribuir spam mediante un correo con firma DKIM válida. Siempre y cuando dicho correo no se modifique y, por tanto, su firma DKIM continúe siendo válida, éste podrá enviarse de modo masivo a distintas personas. Para evitarlo, es posible emplear adicionalmente SPF. SPF comprueba el origen del correo comprobando la dirección IPv4 y el nombre de dominio del servidor de correo. SPF rechaza los correos procedentes de servidores no autorizados. De este modo se impide la distribución de spam mediante correos con firma DKIM válida.

Los administradores a nivel de cliente también pueden definir excepciones a estos métodos para algunos de sus dominios (véase Añadir excepciones en la página 442).

Los correos cuya autenticación de remitentes ha finalizado con un error se rechazan o se marcan como spam. Para los correos cuya comprobación SPF, validación DKIM o validación DMARC ha fallado se indican motivos de clasificación especiales en Control Panel (véase Motivos de clasificación von Email Authentication en la página 444).

Comprobación SPF

SPF (Sender Policy Framework) es un método de autenticación de remitentes que comprueba si se ha falsificado la dirección del remitente. Durante una comprobación SPF, el servidor de entrada comprueba si un correo entrante procede de un servidor autorizado. Para ello, el servidor de entrada comprueba si la dirección IP del servidor de salida está inscrita en un registro SPF en la zona de DNS del dominio del remitente. En los registros SPF se inscriben las direcciones P de los servidores autorizados para el envío de correos de un dominio. Para más información sobre la lógica de las comprobaciones SPF, véase Lógica de la comprobación SPF en la página 411.

Los administradores a nivel de cliente pueden establecer la comprobación SPF para los correos entrantes de sus dominios. Para ello, los administradores deben primero definir registros SPF (véase Definir un registro SPF en la página 413) para todos aquellos de sus dominios a cuyos correos entrantes deseen realizar comprobaciones SPF. A continuación, los administradores deben activar la comprobación SPF (véase Activar la comprobación SPF en la página 414) y configurar las opciones avanzadas (véase Configurar opciones avanzadas de comprobación SPF en la página 417).

En el capítulo Solución de problemas en la página 420 se explica cómo subsanar errores ocurridos en comprobaciones SPF.

Lógica de la comprobación SPF

La lógica de las comprobaciones SPF se describe a continuación.

Al recibir un correo, el servidor de destino compara la dirección IP del servidor de origen con los datos del registro TXT del dominio de la dirección de correo del remitente. Si la dirección IP del servidor de origen no se encuentra en el registro TXT, se emite un error. En la comprobación del registro TXT se distingue, por gravedad, entre fallos graves y fallos leves.

Los administradores a nivel de cliente pueden decidir las medidas que se tomarán ante cada tipo de error (véase Activar la comprobación SPF en la página 414). Si no se producen errores, el correo se entrega como de costumbre.

Nota:

Las siguientes indicaciones se refieren al caso de que se comprueben tanto los datos del remitente del sobre (MAIL FROM) como los datos del remitente del encabezado (From). Si solo se comprueba uno de sus datos, solo se efectúa una comprobación, y el tipo de fallo de dicha comprobación es determinante.

Para comprobar el registro TXT se aplica la siguiente lógica:

1. En el primer paso, se comprueban al mismo tiempo los dominios indicados en el sobre (MAIL FROM) y en el encabezado (From). Si alguna de las comprobaciones termina en fallo, se actuará en función de su tipo en el siguiente paso. Si ambas comprobaciones terminan en fallo, en el siguiente paso se actuará en función del tipo de fallo más grave de los dos. Existen tres opciones:

   Tabla 22: Opción 1 - Ambas comprobaciones SPF terminan en fallo leve

   Si las comprobaciones SPF del sobre y el encabezado terminan en fallo leve, en el siguiente paso se actuará conforme a un fallo leve.

PARTE DEL CORREO ELECTRÓNICO	CONFIGURACIÓN	TIPO DE FALLO
Sobre (MAIL FROM)	~all	Fallo leve
Encabezado (From)	~all	Fallo leve

Tabla 23: Opción 2 - Ambas comprobaciones SPF terminan en fallo grave

Si las comprobaciones SPF del sobre y el encabezado terminan en fallo grave, en el siguiente paso se actuará conforme a un fallo grave.

PARTE DEL CORREO ELECTRÓNICO	CONFIGURACIÓN	TIPO DE FALLO
Sobre (MAIL FROM)	-all	Fallo grave
Encabezado (From)	-all	Fallo grave

Tabla 24: Opción 3 - Ambas comprobaciones SPF terminan en fallos diferentes

Si las comprobaciones SPF del sobre y el encabezado terminan en fallos diferentes, en el siguiente paso se actuará conforme a un fallo grave.

PARTE DEL CORREO ELECTRÓNICO	CONFIGURACIÓN	TIPO DE FALLO
Sobre (MAIL FROM)	-all	Fallo grave
Encabezado (From)	~all	Fallo leve

2. En el segundo paso se comprueban las medidas que haya definido usted para un fallo grave o leve y se aplican dichas medidas.

Nota:

En el contexto de la comprobación SPF, solo pueden emplearse los calificadores **-** y **~**. El calificador **-** representa el código de resultado fallo grave y el calificador **~** representa el código de resultado fallo leve. El calificador **?** no puede emplearse.

Definir un registro SPF

Puede definir un registro SPF en la zona de DNS de su dominio para autorizar a nuestros servidores a enviar correos en nombre de su dominio. Spam and Malware Protection (véase "Spam and Malware Protection" en el manual de Control Panel) puede detectar a tiempo intentos de fraude como la suplantación de identidad en base al registro SPF. Los destinatarios externos a su organización pueden emplear el registro SPF para realizar comprobaciones SPF de correos de su dominio. Además, usted necesita un registro SPF para que Email Authentication pueda realizar comprobaciones SPF de correos entrantes (véase "Comprobación SPF" en el manual de Control Panel).

Importante:

Inscriba en el registro SPF todos los servidores autorizados a enviar correos de su dominio.

Nota:

Nuestro registro SPF no es necesario para clientes que hayan configurado su entorno primario con la opción **IP/Nombre de host** pero sin indicar direcciones de servidores de retransmisión para correos salientes. Para más información sobre cómo configurar el entorno primario, véase .

Debe añadir el registro SPF a la zona de DNS de su dominio por sí mismo. Para más información sobre cómo añadir correctamente el registro SPF a la zona de DNS, póngase en contacto con el soporte técnico.

Activar la comprobación SPF

Ha añadido un registro SPF válido a la zona de DNS de sus dominios (véase Definir un registro SPF en la página 413). Ha activado Spam and Malware Protection para su dominio (véase "Activar Spam and Malware Protection" en el manual de Control Panel).

> **Importante:**
>
> Las comprobaciones SPF solo se efectúan para dominios con registros SPF válidos.

> **Importante:**
>
> La comprobación SPF solo puede activarse si el cliente cumple alguna de las siguientes condiciones:
>
> - El cliente ha configurado su entorno primario con la opción **IP/Nombre de host** y ha introducido direcciones de servidores de retransmisión para correos salientes. El cliente ha introducido nuestro registro SPF junto a sus propios registros SPF en la zona de DNS (véase Definir un registro SPF en la página 413).
> - El cliente ha configurado su entorno primario con la opción **IP/Nombre de host** pero no ha introducido direcciones de servidores de retransmisión para correos salientes. El cliente ha introducido sus propios registros SPF en la zona de DNS.
>
> Para más información sobre cómo configurar el entorno primario, véase el capítulo "Configurar el entorno primario" en el manual de Control Panel.

Puede activar la comprobación SPF para comprobar si la dirección IP del servidor de origen de un correo entrante está incluida en los registros SPF del dominio del remitente y, por tanto, dicho servidor está autorizado a enviar correos de dicho dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.

4. En la sección **Autenticación de remitente**, marque la casilla **Activar comprobación SPF**.

Figura 288: Activar la comprobación SPF

Se muestra un mensaje de advertencia.

5. Haga clic en **Confirmar**.

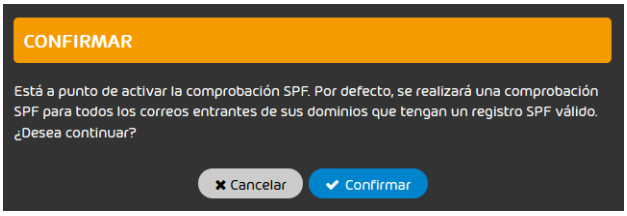


Figura 289: Confirmar

La comprobación SPF se activa para todos los dominios subordinados al dominio seleccionado para los cuales se hayan definido registros SPF correctos.

6. Elija en qué casos deberá realizarse una comprobación SPF.
   - Si desea comprobar todos los correos entrantes para cuyo dominio de remitente haya definido un registro SPF, seleccione **Para todos los correos entrantes**.

     Nota:

     Esta variante se recomienda en caso de que se haya observado un elevado volumen de falsificaciones de direcciones de diferentes dominios de salida. Si emplea esta variante es posible que aumente la tasa de falsos positivos si sus interlocutores no han definido correctamente sus registros TXT.
   - Si solo desea comprobar correos enviados por el dominio o un dominio alias del destinatario, seleccione **Solo para los correos dentro de uno de sus propios dominios**.

     Nota:

     De este modo solo se comprueban correos electrónicos internos. Esta variante se recomienda para impedir ataques selectivos mediante una dirección de correo electrónico falsificada del propio dominio del destinatario.

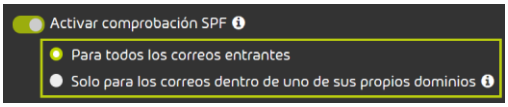


Figura 290: Elegir correos para la comprobación SPF

La comprobación SPF se activa.

Nota:

Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

La comprobación SPF se ha activado.

A continuación puede configurar las opciones avanzadas para la comprobación SPF (véase Configurar opciones avanzadas de comprobación SPF en la página 417).

Configurar opciones avanzadas de comprobación SPF

Ha activado la comprobación SPF (véase Activar la comprobación SPF en la página 414).

En el módulo **Configuración de seguridad** > **Email Authentication** puede configurar las acciones a realizar en función de los resultados de las comprobaciones SPF (véase Comprobación SPF en la página 410).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.
4. Haga clic en **Opciones avanzadas**.

Figura 291: Abrir las opciones avanzadas

Se muestra un mensaje de advertencia.

5. **Importante:**

   Si realiza modificaciones en las opciones avanzadas, puede ocurrir que se entreguen correos maliciosos.

   Para modificar las opciones avanzadas, haga clic en **Confirmar**.

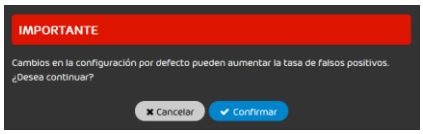


Figura 292: Confirmar

6. Opcional: En **Comportamiento después de un fallo grave de SPF**, elija qué hacer en caso de fallo grave en la comprobación SPF Tiene las siguientes opciones:

   - **Poner correo en cuarentena como spam**: El correo se marca como spam y se pone en cuarentena.
   - **Rechazar correo**: El correo se rechaza. El correo no se entrega al destinatario ni se pone en cuarentena.
   - **No realizar ninguna acción**: El fallo grave de SPF no provoca ninguna acción. A continuación, el correo pasa por otros filtros de nuestros servicios.

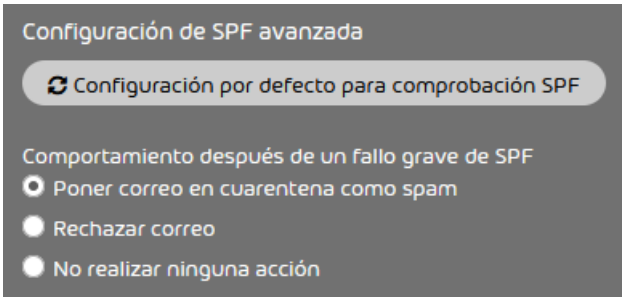


Figura 293: Seleccionar las acciones tras un fallo grave de SPF

7. Opcional: En **Comportamiento después de un fallo leve de SPF**, elija qué hacer en caso de fallo leve en la comprobación SPF. Tiene tres opciones:

   - **Poner correo en cuarentena como spam**: El correo se marca como spam y se pone en cuarentena.
   - **Rechazar correo**: El correo se rechaza. El correo no se entrega al destinatario ni se pone en cuarentena.
   - **No realizar ninguna acción**: El fallo leve de SPF no provoca ninguna acción. A continuación, el correo pasa por otros filtros de nuestros servicios.

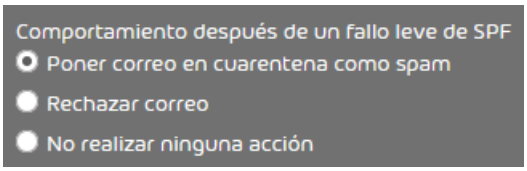


Figura 294: Seleccionar las acciones tras un fallo leve de SPF

8. Opcional: En **Análisis**, elija qué componentes de los correos deberán analizarse. Tiene las siguientes opciones:

   - **Solo analizar 'envelope from'**
   - **Solo analizar 'header from'**
   - **Analizar 'envelope from' y 'header from'**

> **Nota:**
>
> Si se comprueban los dos datos, aumenta la seguridad, pero también la tasa de falsos positivos.

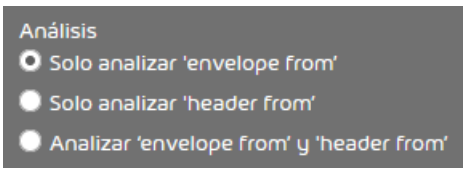


Figura 295: Configurar el análisis

9. Opcional: Para restaurar la configuración por defecto de SPF, haga clic en **Configuración por defecto para comprobación SPF**.

> **Nota:**
>
> Según la configuración por defecto, después de un fallo grave o leve, los correos se ponen en cuarentena como spam y solo se analiza el campo "MAIL FROM:" del sobre.

Los cambios se guardan.

> **Nota:**
>
> Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

Se han configurado las opciones avanzadas de la comprobación SPF.

Solución de problemas

Los siguientes errores ocurridos durante comprobaciones SPF pueden solucionarse:

- Errores debidos a comprobaciones SPF al enviar correos (véase Solución de problemas: Problemas al enviar correos cuando el registro SPF está definido en la página 420)
- Errores debidos a comprobaciones SPF al recibir correos (véase Solución de problemas: Problemas provocados por comprobaciones SPF al recibir correos en la página 421)

Solución de problemas: Problemas al enviar correos cuando el registro SPF está definido

Condición:

Se cumple una de las siguientes condiciones:

- Las comprobaciones SPF solo se realizarán cuando coincidan el dominio del remitente y dominio del destinatario. Correos internos entrantes se declaran incorrectamente inválidos.

- Su interlocutor le informa de que los correos de su dominio se declaran inválidos en las comprobaciones SPF.

Causa: Errores en registro TXT propio

Las direcciones IP inscritas en el registro TXT de su servidor de correo. correo son incorrectas o están incompletas.

Solución: Corregir el registro TXT

Añada las direcciones IPv4 de sus servidores de correo de correo al registro TXT o corrija las direcciones IPv4 incorrectas.

Solución de problemas: Problemas provocados por comprobaciones SPF al recibir correos

Condición:

Las comprobaciones SPF se realizan para todos los correos procedentes de dominios para los que se hayan definido registros TXT. Los correos entrantes de determinados dominios se declaran erróneamente inválidos.

Causa: Errores en registro TXT del interlocutor

Solución: Informar al interlocutor

Informe al interlocutor sobre la posibilidad de que haya errores en su configuración de SPF.

Solución: Añadir direcciones IP a la lista blanca

1. Abra Control Panel.
2. Seleccione el dominio afectado en la selección de ámbitos.
3. Vaya a **Listas blancas y negras**.
4. Seleccione la pestaña **Lista blanca**.
5. Introduzca la dirección IPv4 del interlocutor en el campo **Añadir elemento**.
6. Haga clic en **Añadir** para confirmar los datos introducidos.

Validación DKIM y firma DKIM

DKIM (DomainKeys Identified Mail) es un método de autenticación de correos electrónicos que comprueba si éstos han sido manipulados durante su transmisión. El proceso de firma DKIM añade una firma DKIM al encabezado de los correos salientes. Tan pronto como un servidor recibe un correo electrónico con firma DKIM y efectúa una validación DKIM, el servidor del destinatario consulta la clave pública almacenada en un registro TXT en la zona de DNS del dominio del remitente. Esta clave le permite comprobar si la firma DKIM es correcta. La validación DKIM revela si el correo se ha modificado durante el envío.

Los remitentes de correos entrantes pueden autenticarse con validaciones DKIM. Para ello, los administradores a nivel de cliente deben activar en primer lugar la validación DKIM (véase Activar la validación DKIM en la página 423) y, a continuación, configurar las opciones avanzadas (véase Configurar opciones avanzadas de validación DKIM en la página 424).

Los administradores a nivel de cliente pueden permitir a los destinatarios de correos salientes de sus dominios efectuar validaciones DKIM. Para ello es preciso añadir a la zona de DNS de sus dominios registros CNAME que apunten a nuestros registros DKIM (véase Definir un registro CNAME en la página 422). A continuación, los administradores deben activar las firmas DKIM para los correos salientes de sus dominios (véase Activar la firma DKIM en la página 426). De este modo podremos firmar con DKIM los correos salientes que se envíen a través de nuestra infraestructura.

Definir un registro CNAME

Si desea emplear DKIM, deberá añadir un registro CNAME a la zona de DNS de su dominio (véase Validación DKIM y firma DKIM en la página 422). Estos registros apuntan a nuestros registros DKIM. Los destinatarios de correos de su dominio consultan dichos registros para obtener la clave pública de cifrado de nuestra firma DKIM y otros datos necesarios para efectuar la validación DKIM.

1. Póngase en contacto con el soporte técnico para obtener los registros CNAME.
2. Añada los registros CNAME a la zona de DNS de su dominio.

Se ha añadido un registro CNAME a la zona de DNS de su dominio.

A continuación puede activar la validación DKIM (véase Activar la validación DKIM en la página 423).

Activar la validación DKIM

Ha activado Spam and Malware Protection para su dominio (véase "Activar Spam and Malware Protection" en el manual de Control Panel).

Puede activar la validación DKIM (véase Validación DKIM y firma DKIM en la página 422) para comprobar las firmas DKIM de los correos entrantes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.
4. **Importante:**

   La validación DKIM solo puede activarse para aquéllos de sus dominios que tengan una configuración de DKIM válida.

   Marque la casilla **Activar validación DKIM para correos entrantes** en **Autenticación de remitente**.

Figura 296: Activar la validación DKIM

La validación DKIM se activa para correos entrantes.

Nota:

Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

La validación DKIM de correos entrantes se ha activado para su dominio.

A continuación puede configurar las opciones avanzadas para la validación DKIM (véase Configurar opciones avanzadas de validación DKIM en la página 424).

Configurar opciones avanzadas de validación DKIM

Ha activado la validación mediante DKIM (véase Activar la validación DKIM en la página 423).

En el módulo **Configuración de seguridad** > **Email Authentication** puede configurar las acciones a realizar en función de los resultados de las validaciones DKIM (véase Validación DKIM y firma DKIM en la página 422).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.
4. Haga clic en **Opciones avanzadas**.

Figura 297: Abrir las opciones avanzadas

Se muestra un mensaje de advertencia.

5. **Importante:**

   Si realiza modificaciones en las opciones avanzadas, puede ocurrir que se entreguen correos maliciosos.

   Para modificar las opciones avanzadas, haga clic en **Confirmar**.

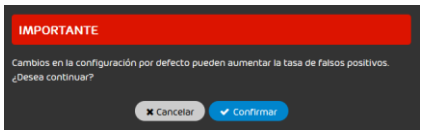


Figura 298: Confirmar

6. Opcional: En **Configuración de DKIM avanzada**, elija qué hacer en caso de fallo en la validación DKIM Tiene las siguientes opciones:

   - **Poner correo en cuarentena como spam**: El correo se marca como spam y se pone en cuarentena.
   - **Rechazar correo**: El correo se rechaza. El correo no se entrega al destinatario ni se pone en cuarentena.

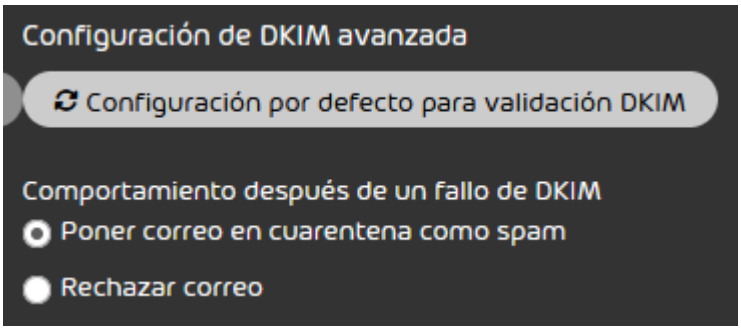


Figura 299: Seleccionar "Opciones avanzadas"

7. Opcional: Para restaurar la configuración por defecto de DKIM, haga clic en **Configuración por defecto para validación DKIM**.

> **Nota:**
>
> Según la configuración por defecto, los correos afectados por un fallo en la validación DKIM se ponen en cuarentena marcados como spam.

Los cambios se guardan.

> **Nota:**
>
> Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

Se han configurado las opciones avanzadas de la validación DKIM.

Activar la firma DKIM

Ha añadido un registro CNAME válido a la zona de DNS de su dominio (véase Definir un registro CNAME en la página 422). Ha activado Spam and Malware Protection para su dominio (véase "Activar Spam and Malware Protection" en el manual de Control Panel).

En el módulo **Configuración de seguridad** > **Email Authentication** puede activar la firma DKIM para correos salientes de sus dominios de modo que los destinatarios de los correos puedan realizar validaciones DKIM.

1. Inicie sesión en Control Panel con datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.

4. **Importante:**

   La validación DKIM solo puede activarse para aquéllos de sus dominios para los cuales haya registros DKIM válidos.

   Marque la casilla **Activar firma DKIM para correos salientes** en **Autenticación de remitente**.

Figura 300: Activar la firma DKIM

La firma DKIM se activa para correos salientes.

Nota:

Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

La firma DKIM de correos salientes se ha activado para su dominio.

Validación DMARC

DMARC (Domain-based Message Authentication, Reporting and Conformance) determina cómo tratar los correos electrónicos entrantes en función de los resultados de la comprobación SPF y la validación DKIM, así como de otras comparaciones de direcciones y dominios.

Una validación DMARC comprueba si un correo entrante concuerda con lo que el destinatario sabe sobre el remitente. Si la zona de DNS del dominio del remitente contiene un registro DMARC, la validación DMARC se efectuará después de la comprobación SPF y la validación DKIM. A partir de los resultados de la comprobación SPF y de la validación DKIM, así como de los resultados de comparar las direcciones indicadas en los campos "MAIL FROM" y "From" del encabezado del correo

(comparación SPF) por una parte y los dominios indicados en el campo "From" del encabezado y la firma DKIM (comparación DKIM) por la otra, la validación DMARC decide cómo tratar el correo. Para más información sobre la matriz de decisiones de DMARC, véase Matriz de decisiones de DMARC en la página 432.

Los administradores a nivel de cliente pueden establecer la validación DMARC para los correos entrantes de sus dominios. Para hacerlo, los administradores deben añadir en primer lugar un registro DMARC a la zona de DNS de sus dominios (véanse Añadir un registro DMARC en la página 428 y Etiquetas de los registros DMARC en la página 429), activar la validación DMARC (véase Activar la validación DMARC en la página 437) y, por último, configurar las opciones avanzadas (véase Configurar opciones avanzadas de validación DMARC en la página 438).

Añadir un registro DMARC

Los registros DMARC son imprescindibles para poder realizar validaciones DMARC (véase Validación DMARC en la página 427) de los correos de un dominio. Puede añadir un registro DMARC para su dominio.

1. Cree un registro TXT con el nombre indicado a continuación en la zona de DNS de su dominio. Sustituya **<dominio.tld>** por su propio dominio.
   _dmarc.<dominio.tld>

2. En el registro TXT, defina la configuración de DMARC conforme al esquema indicado a continuación. Sustituya **<nombredeusuario@dominio.tld>** por una dirección de correo electrónico.
   v=DMARC1;p=quarantine;pct=100;rua=mailto:<nombredeusuario@dominio.tld>

   > **Importante:**
   >
   > El capítulo Etiquetas de los registros DMARC en la página 429 contiene una relación con explicaciones de las etiquetas que pueden emplearse en registros DMARC.

   > **Nota:**
   >
   > Los datos del registro DMARC se aplican a los correos enviados a destinatarios de fuera del dominio. La configuración para correos enviado a destinatarios de dentro del dominio pueda ajustarse en el módulo **Email Authentication**.

Se ha añadido un registro DMARC a la zona de DNS del dominio.

Etiquetas de los registros DMARC

Los registros DMARC están compuestos de etiquetas. Las etiquetas de un registro DMARC contienen especificaciones para las validaciones DMARC de correos enviados desde el dominio a destinatarios de fuera del dominio.

La siguiente tabla contiene una relación de etiquetas que pueden emplearse en registros DMARC junto con explicaciones. Salvo las etiquetas **v** y **p**, todas son opcionales.

> **Importante:**
>
> Las etiquetas **v** y **p** son obligatorias.

ETIQUETA	EXPLICACIÓN	VALORES POSIBLES
v	Esta etiqueta determina la versión empleada del protocolo DMARC.	**v=DMARC1** **Nota:** El único valor posible para esta etiqueta es **v=DMARC1**.
p	Esta etiqueta determina el modo en que deben tratarse los correos del dominio en caso de fallo de la validación DMARC.	**p=quarantine**: El correo se pone en cuarentena. **p=reject**: El correo se rechaza. **p=none**: No se realiza ninguna acción para el correo. **Nota:** Recomendamos **p=quarantine**.
pct	Esta etiqueta determina el porcentaje de correos para los cuales han de realizarse validaciones DMARC. Los valores permitidos para esta etiqueta son números del 1 al 100.	**pct=100** **Nota:** Recomendamos el valor **pct=100**, para que se realicen validaciones DMARC para todos los correos del dominio.

ETIQUETA	EXPLICACIÓN	VALORES POSIBLES
rua	Esta etiqueta determina la dirección de correo a la que enviar diariamente informes globales sobre validaciones DMARC fallidas.	**rua=mailto:<nombredeusuario@dominio.** En lugar de **<nombredeusuario@dominio.com>** se indica la dirección de correo electrónico a la que enviar los informes globales.
ruf	Esta etiqueta determina la dirección de correo electrónico a la que enviar informes forenses sobre correos individuales para los que haya fallado la validación DMARC.	**ruf=mailto:<nombredeusuario@dominio.** En lugar de **<nombredeusuario@dominio.com>** se indica la dirección de correo electrónico a la que enviar los informes forenses.
sp	Esta etiqueta determina el modo en que deben tratarse los correos de un subdominio del dominio en caso de fallo de la validación DMARC.	**sp=quarantine**: El correo se pone en cuarentena. **sp=reject**: El correo se rechaza. **sp=none**: No se realiza ninguna acción para el correo.
adkim	Esta etiqueta determina el modo de concordancia de firmas DKIM (véase Validación DKIM y firma DKIM en la página 422). El modo de concordancia determina la exactitud con la que el correo debe coincidir con la firma DKIM para ser aceptado.	**adkim=r**: El modo de concordancia es relajado. Basta con una coincidencia parcial. **adkim=s**: El modo de concordancia es estricto. Se requiere una coincidencia completa.

ETIQUETA	EXPLICACIÓN	VALORES POSIBLES
aspf	Esta etiqueta determina el modo de concordancia de los dominios del encabezado y el sobre de un correo (véase Comprobación SPF en la página 410). El modo de concordancia determina la exactitud con la que deben coincidir ambos dominios entre sí para que el correo sea aceptado.	**aspf=r**: El modo de concordancia es relajado. Basta con una coincidencia parcial. **aspf=s**: El modo de concordancia es estricto. Se requiere una coincidencia completa.

Matriz de decisiones de DMARC

La matriz de decisiones de DMARC indica qué hacer con los correos en caso de resultados positivos o negativos en comprobaciones SPF y validaciones DKIM.

Tabla 25: Matriz de decisiones de DMARC

COMPROBACIÓN SPF	VALIDACIÓN DKIM	COMPARACIÓN SPF	COMPARACIÓN DKIM	RESULTADO DMARC	CONSECUENCIAS
Superada	Superada	Superada	Superada	Superada	Entrega
Superada	Superada	Superada	No superada	Superada	Entrega
Superada	Superada	No superada	Superada	Superada	Entrega

COMPROBACIÓN SPF	VALIDACIÓN DKIM	COMPARACIÓN SPF	COMPARACIÓN DKIM	RESULTADO DMARC	CONSECUENCIAS
Superada	Superada	No superada	No superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente
Superada	No superada	Superada	Superada	Superada	Entrega
Superada	No superada	Superada	No superada	Superada	Entrega
Superada	No superada	No superada	Superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente

COMPROBACIÓN SPF	VALIDACIÓN DKIM	COMPARACIÓN SPF	COMPARACIÓN DKIM	RESULTADO DMARC	CONSECUENCIAS
Superada	No superada	No superada	No superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente
No superada	Superada	Superada	Superada	Superada	Entrega
No superada	Superada	Superada	No superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente
No superada	Superada	No superada	Superada	Superada	Entrega

COMPROBACIÓN SPF	VALIDACIÓN DKIM	COMPARACIÓN SPF	COMPARACIÓN DKIM	RESULTADO DMARC	CONSECUENCIAS
No superada	Superada	No superada	No superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente
No superada	No superada	Superada	Superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente
No superada	No superada	Superada	No superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente

COMPROBACIÓN SPF	VALIDACIÓN DKIM	COMPARACIÓN SPF	COMPARACIÓN DKIM	RESULTADO DMARC	CONSECUENCIAS
No superada	No superada	No superada	Superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente
No superada	No superada	No superada	No superada	No superada	Poner en cuarentena como spam, rechazar o tratar conforme a la directiva DMARC del remitente

La validación DMARC solo se supera si se superan al mismo tiempo la comprobación SPF (véase Comprobación SPF en la página 410) o la validación DKIM (véase Validación DKIM y firma DKIM en la página 422) y comparación correspondiente (SPF o DKIM). Si el resultado de la validación DMARC es positivo, el correo se entrega. De lo contrario, en función de los ajustes del módulo **Email Authentication** (véase Configurar opciones avanzadas de validación DMARC en la página 438), el correo se pone en cuarentena como spam, se rechaza o se trata conforme a la directiva DMARC del dominio del remitente (si la hay).

Activar la validación DMARC

Ha añadido registros SPF, DKIM y DMARC válidos para al menos uno de sus dominios (véanse Definir un registro SPF en la página 413, Definir un registro CNAME en la página 422 y Añadir un registro DMARC en la página 428). Ha activado Spam and Malware Protection para su dominio (véase "Activar Spam and Malware Protection" en el manual de Control Panel).

Puede activar la validación DMARC para determinar el tratamiento de correos entrantes en función de los resultados de comprobaciones SPF (véase Comprobación SPF en la página 410) y validaciones DKIM (véase Validación DKIM y firma DKIM en la página 422).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.
4. **Importante:**

   La validación DMARC solo puede activarse para dominios suyos para los cuales haya registros SPF, DKIM y DMARC válidos.

   Marque la casilla **Activar validación DMARC para correos entrantes** en **Autenticación de remitente**.

Figura 301: Activar la validación DMARC

La validación DKIM se activa para correos entrantes.

Nota:

Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

La validación DMARC de correos entrantes se ha activado.

A continuación puede configurar las opciones avanzadas para la validación DMARC (véase Configurar opciones avanzadas de validación DMARC en la página 438).

Configurar opciones avanzadas de validación DMARC

Ha activado la validación DMARC (véase Activar la validación DMARC en la página 437).

En el módulo **Configuración de seguridad** > **Email Authentication** puede configurar las acciones a realizar en función de los resultados de las validaciones DKIM (véase Validación DMARC en la página 427).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.
4. Haga clic en **Opciones avanzadas**.

Figura 302: Abrir las opciones avanzadas

Se muestra un mensaje de advertencia.

5.

Importante:

Si realiza modificaciones en las opciones avanzadas, puede ocurrir que se entreguen correos maliciosos.

Para modificar las opciones avanzadas, haga clic en **Confirmar**.

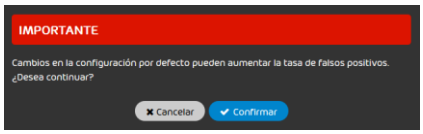


Figura 303: Confirmar

6. Opcional: En **Configuración de DMARC avanzada**, elija qué hacer en caso de fallo en la validación DMARC. Tiene las siguientes opciones:

   - **Poner correo en cuarentena como spam**: El correo se marca como spam y se pone en cuarentena.
   - **Rechazar correo**: El correo se rechaza. El correo no se entrega al destinatario ni se pone en cuarentena.
   - **Aplicar norma del dominio del remitente**: Tras un fallo de DMARC se aplican las acciones determinadas por la directiva DMARC del dominio del remitente. Ésta es la configuración por defecto.

   > **Nota:**
   >
   > Si elige esta opción, confiará en las directivas DMARC de terceros.

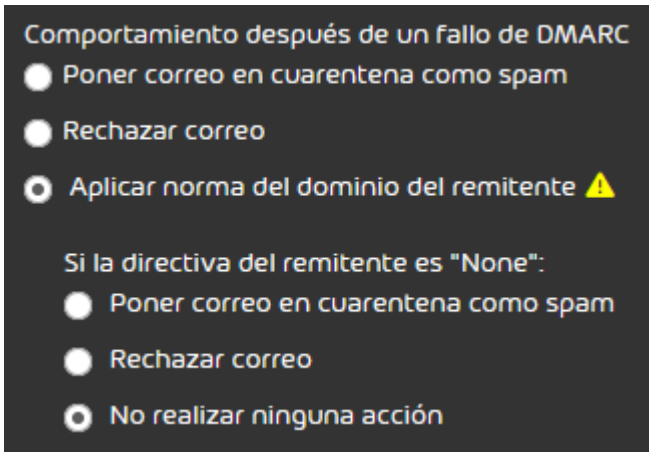


Figura 304: Seleccionar acciones tras un fallo de DMARC

Si elige la opción **Aplicar norma del dominio del remitente**, se mostrarán opciones adicionales.

7. Si ha elegido la opción **Aplicar norma del dominio del remitente**, determine en **Si la directiva del remitente es "None":** las acciones a realizar en caso de que la directiva de DMARC del dominio del remitente esté ajustada a "None". Tiene las siguientes opciones:

   - **Poner correo en cuarentena como spam**: El correo se marca como spam y se pone en cuarentena.
   - **Rechazar correo**: El correo se rechaza. El correo no se entrega al destinatario ni se pone en cuarentena.
   - **No realizar ninguna acción**: El fallo de DMARC no provoca ninguna acción. A continuación, el correo pasa por otros filtros de nuestros servicios.

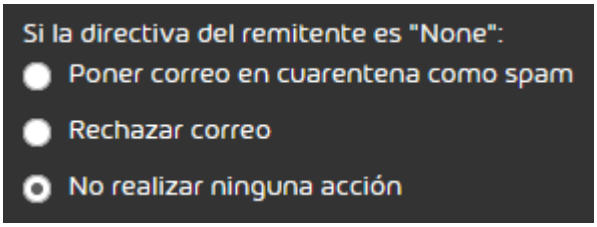


Figura 305: Acciones en caso de directiva de remitente ajustada a "None"

8. Opcional: Para restaurar la configuración por defecto de DMARC, haga clic en **Configuración por defecto para validación DMARC**.

> **Nota:**
>
> Conforme a la configuración por defecto, los correos se tratan conforme a la directiva DMARC del remitente en caso de fallo de DMARC. Por defecto, si la directiva DMARC del remitente contiene el valor **None** (véase Añadir un registro DMARC en la página 428), no se realiza ninguna acción.

Los cambios se guardan.

> **Nota:**
>
> Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

Se han configurado las opciones avanzadas de la validación DMARC.

Añadir excepciones

Ha activado métodos de autenticación de remitentes en el módulo **Email Authentication** (véase Métodos de autenticación de remitentes en la página 409).

Si ha activado la comprobación SPF (véase Comprobación SPF en la página 410), la validación DKIM (véase Validación DKIM y firma DKIM en la página 422) y/o la validación DMARC (véase Validación DMARC en la página 427) y desea desactivarlas para alguno de sus dominios, defina una excepción.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Email Authentication**.

4. En **Excepciones**, haga clic en **Añadir excepción**.

Figura 306: agregar excepción

Se abre una vista avanzada.

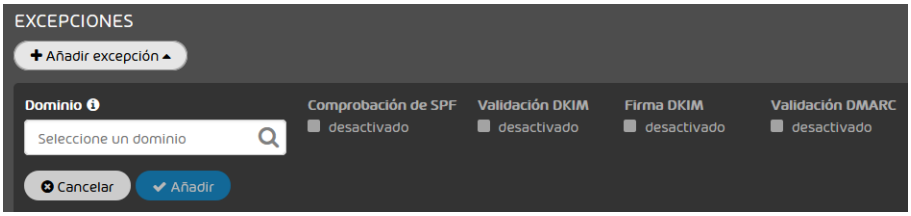


Figura 307: Vista avanzada

5. En **Dominio**, seleccione el dominio para el cual desee definir la excepción.

> **Nota:**
>
> Solo puede seleccionar dominios para los cuales haya activado Spam and Malware Protection.

6. Marque la casilla bajo la comprobación que desee desactivar para el dominio.

> **Nota:**
>
> Solo puede desactivar la comprobación SPF, la validación DKIM o la validación DMARC para dominios que tengan los ajustes correspondientes correctamente definidos en la configuración de DNS. Las comprobaciones no se aplican a ningún otro dominio.

7. Haga clic en **Añadir**.

La excepción se añade y aparece en la tabla de abajo.

> **Nota:**
>
> Debido al almacenamiento en caché de DNS, el cambio puede tardar hasta 72 horas en hacerse efectivo.

Se ha añadido una excepción a Email Authentication.

Motivos de clasificación von Email Authentication

Para los correos cuya autenticación de remitentes con Email Authentication ha finalizado con un error se indican motivos de clasificación especiales en Control Panel. Para más información sobre los motivos de clasificación véase el capítulo "Motivos de clasificación" del manual de Control Panel.

SPF

En función de su configuración (véase Configurar opciones avanzadas de comprobación SPF en la página 417), los correos para los cuales se haya detectado que no fueron enviados por un servidor registrado en la zona DNS mediante una comprobación SPF se ponen en cuarentena como spam, se rechazan o se entregan.

En Control Panel, estos correos se muestran con los motivos de clasificación **Envelope SPF Failure** y **Message Header SPF Failure** en el módulo **Email Live Tracking** independientemente de la acción que se les haya aplicado.

DKIM

En función de su configuración (véase Configurar opciones avanzadas de validación DMARC en la página 438), los correos cuya validación DKIM haya fallado se ponen en cuarentena o rechazan.

Para estos correos se indica el motivo de clasificación **DKIM Failure** en el módulo **Email Live Tracking** de Control Panel.

DMARC

En función de su configuración (véase Configurar opciones avanzadas de validación DMARC en la página 438), los correos para los cuales se haya detectado que no cumplen los requisitos establecidos para SPF y/o DKIM durante la validación DMARC se ponen en cuarentena como spam o se rechazan.

Para estos correos se indica el motivo de clasificación **DMARC Failure** en el módulo **Email Live Tracking** de Control Panel.

Quarantine Report

Acerca de Quarantine Report

Quarantine Report es una función de Spam and Malware Protection (véase el capítulo "Spam and Malware Protection" del manual de Control Panel) que permite a los administradores a nivel de cliente configurar informes de cuarentena para los usuarios de sus dominios.

Quarantine Report genera informes denominados informes de cuarentena, bien individualmente para un solo usuario o bien para todo un dominio, y los entrega por correo electrónico a sus destinatarios. Los administradores a nivel de cliente pueden seleccionar un diseño para los informes de cuarentena (véase Diseños para informes de cuarentena en la página 447). Dependiendo de su diseño, los informes de cuarentena permiten realizar diversas acciones para correos electrónicos (véase Acciones para correos en informes de cuarentena en la página 451).

En los informes de cuarentena se enumeran todos los correos clasificados como **Spam** y **Infomail** (véase el capítulo "Categorías de correo electrónico" en el manual de Control Panel), así como correos que se hayan puesto en cuarentena en lugar de entregarse a los usuarios. Si el destinatario de los informes de cuarentena posee los permisos necesarios, puede hacerse entregar dichos correos posteriormente si lo desea (véase Acciones para correos en informes de cuarentena en la página 451).

Nota:

En el módulo **Spam and Malware Protection** es posible configurar qué correos pueden hacerse entregar los usuarios (véase el capítulo "Permitir o prohibir acciones de usuarios" en el manual de Control Panel).

Nota:

La cantidad de correos mostrados está limitada. Los informes de cuarentena pueden mostrar un máximo de 1000 correos.

Los informes de cuarentena se generan por buzón de correos principal. Si un usuario posee buzones de correo alias, recibirá un único informe de cuarentena en el que se incluirán los correos enviados tanto al buzón de correo principal como a los buzones de correos alias. Cuando el usuario se haga entregar un correo desde un informe de cuarentena (véase Entregar un correo de un informe de cuarentena en la página 473), se indicará el buzón de correos al que estaba dirigido el correo en cuestión. Los informes de cuarentena se generan también para buzones de reenvío (véase el capítulo "Tipos de buzón de correo" del manual de Control Panel). En tal caso, todos los destinatarios de los reenvíos reciben una copia del informe de cuarentena.

Nota:

Los informes de cuarentena reenviados por buzones de correo de reenvío a sus destinatarios finales no permiten realizar todas las acciones para correos descritas en el capítulo Acciones para correos en informes de cuarentena en la página 451.

Los administradores a nivel de cliente pueden activar el módulo **Quarantine Report** para un dominio (véase Activar Quarantine Report para un dominio en la página 455) y configurarlo (véase Configurar Quarantine Report para un dominio en la página 456). Además, dichos administradores pueden configurar el módulo **Quarantine Report** individualmente para un buzón de correo (véase Configurar Quarantine Report para un buzón de correo en la página 463). Si lo desean, los administradores pueden volver a desactivar el módulo **Quarantine Report** para un dominio (véase Desactivar Quarantine Report para un dominio en la página 472).

Diseños para informes de cuarentena

En el módulo **Quarantine Report** (véase Acerca de Quarantine Report en la página 445), los administradores a nivel de cliente pueden seleccionar un diseño para los informes de cuarentena de sus dominios (véase Configurar Quarantine Report para un dominio en la página 456). El diseño determina las acciones para correos que los destinatarios pueden ejecutar desde sus informes de cuarentena (véase Acciones para correos en informes de cuarentena en la página 451).

Nota:

Al pie de los informes de cuarentena se muestran los datos de soporte técnico del módulo **Personalización** (véase el capítulo "Añadir datos de soporte técnico a Control Panel" en el manual de Control Panel).

Están disponibles los siguientes diseños:

- **Diseño estándar**. Este diseño es nuestro diseño por defecto.

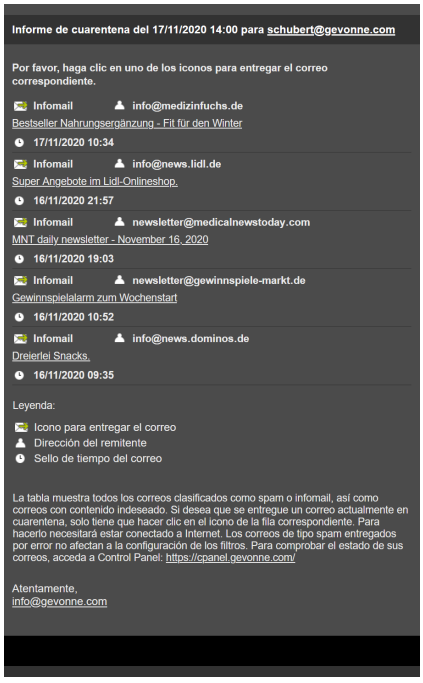


Figura 308: Diseño estándar

- **Diseño estándar con vista previa de los correos electrónicos**: Este diseño es nuestro diseño por defecto con botones adicionales para la entrega y previsualización de correos (véase Vista previa de correos en la página 99).

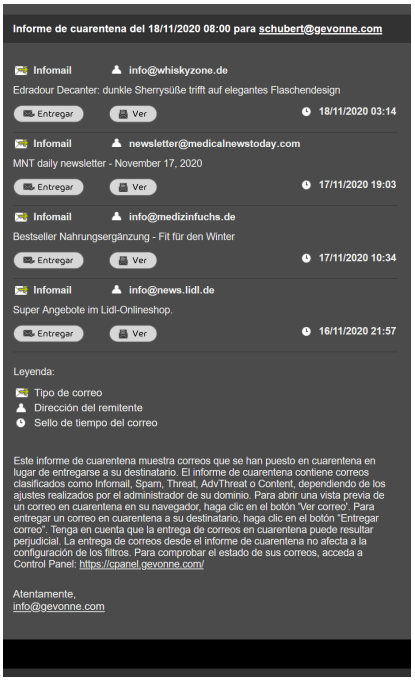


Figura 309: Diseño estándar con vista previa de los correos electrónicos

- **Inbox Manager con vista previa de los correos electrónicos y opción de exclusión**: Este diseño es nuestro diseño por defecto con botones adicionales para la entrega y previsualización de correos, así como para excluir los correos de un remitente de futuros informes de cuarentena. En los informes de cuarentena con este diseño, no se muestran correos de remitentes que se encuentren en la lista negra del usuario o del dominio. Para excluir los correos de un remitente de futuros informes de cuarentena, el destinatario del informe de cuarentena puede añadir el remitente de un correo en cuarentena a su propia lista negra (véase el capítulo "Acerca de las

listas blancas y negras" en el manual de Control Panel) utilizando el botón **No mostrar nunca el remitente**.

> **Importante:**
>
> Este diseño solo se muestra y puede elegirse activando previamente la opción **Excluir de los informes de cuarentena remitentes en la lista negra.** en la configuración de informes de cuarentena. Para más información sobre la configuración de los informes de cuarentena, véase Configurar Quarantine Report para un dominio en la página 456.

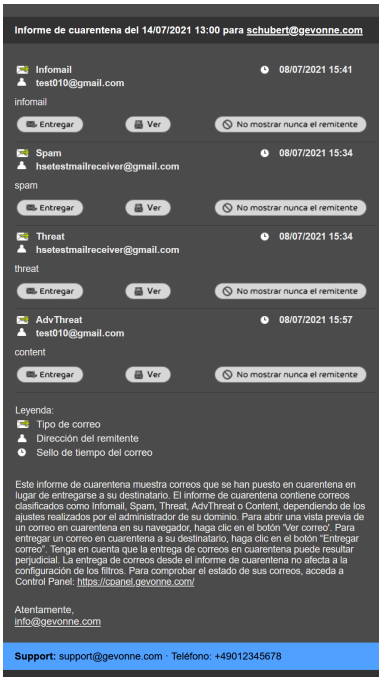


Figura 310: Inbox Manager con vista previa de los correos electrónicos y opción de exclusión

- **Diseño para ordenador de escritorio**: Este diseño es óptimo para los ordenadores de escritorio, pues aprovecha el ancho del monitor. Los informes de cuarentena incluyen botones para entregar correos y botones para añadir remitentes a la lista blanca.

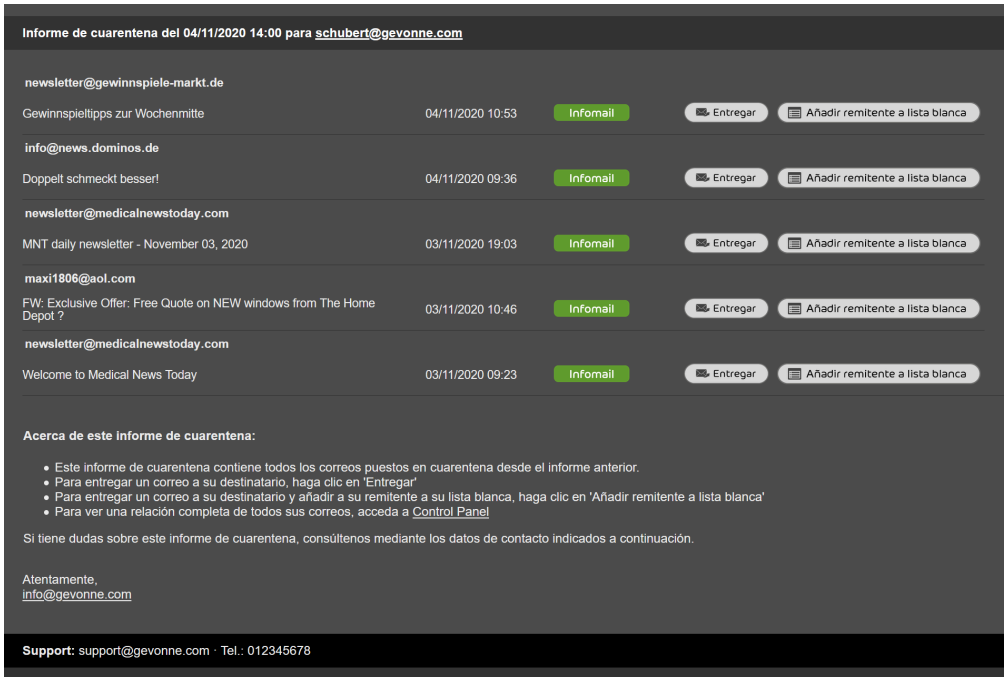


Figura 311: Diseño para ordenador de escritorio

- **Diseño para ordenador de escritorio con vista previa de los correos electrónicos**: Este diseño es nuestro diseño para ordenadores de escritorio con botones adicionales para la vista previa de correos (véase Vista previa de correos en la página 99).

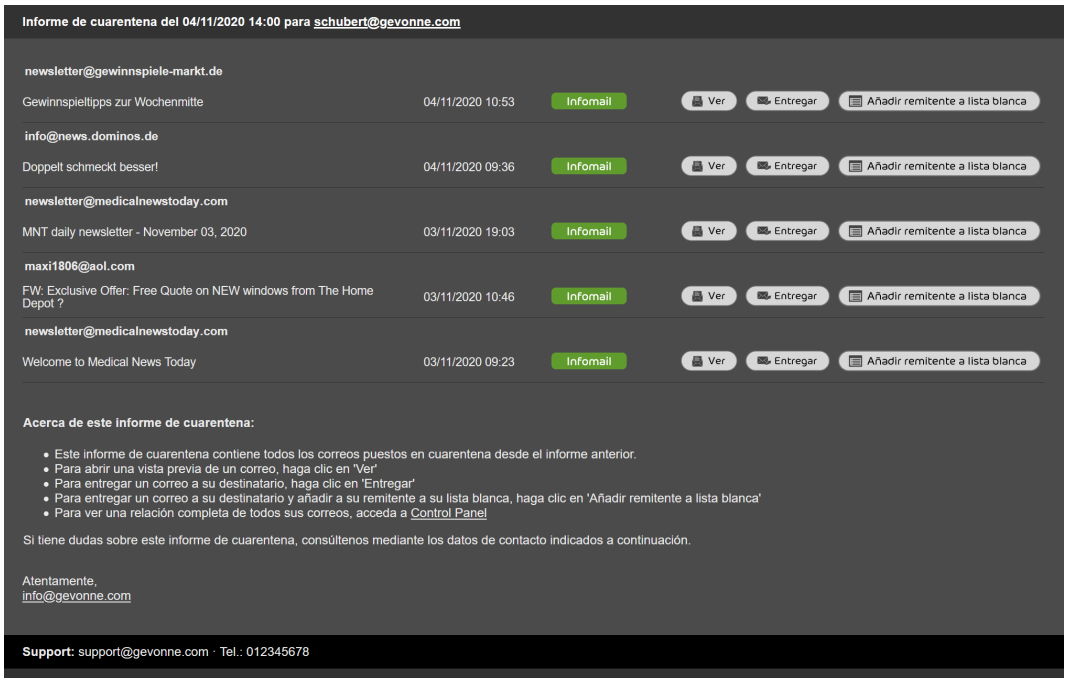


Figura 312: Diseño para ordenador de escritorio con vista previa de los correos electrónicos

Acciones para correos en informes de cuarentena

Los informes de cuarentena contienen botones que permiten ejecutar alguas acciones para correos del módulo **Email Live Tracking**. Las acciones disponibles dependen del diseño de los informes de cuarentena (véase Diseños para informes de cuarentena en la página 447). En la siguiente tabla se explican las acciones y se indican los diseños en los que se encuentran disponibles dichas acciones.

Tabla 26: Acciones para correos en informes de cuarentena

ACCIÓN	DISEÑO	EXPLICACIÓN
Entregar	Diseño estándar Diseño estándar con vista previa de los correos electrónicos Inbox Manager con vista previa de los correos electrónicos y opción de exclusión Diseño para ordenador de escritorio Diseño para ordenador de escritorio con vista previa de los correos electrónicos	Los correos seleccionados se entregan al destinatario. **Nota:** En el caso de informes de cuarentena para buzones de reenvío, los correos se entregan a todos los destinatarios del reenvío. Para más información, véase el capítulo "Acciones para correos" del manual de Control Panel.

ACCIÓN	DISEÑO	EXPLICACIÓN
Añadir remitente a lista blanca	**Diseño para ordenador de escritorio** **Diseño para ordenador de escritorio con vista previa de los correos electrónicos**	Los remitentes de los correos seleccionados se añaden a la lista blanca del usuario y los correos se entregan. Los correos enviados por estos remitentes que se reciban a partir de ahora se entregarán automáticamente. **Nota:** Esta acción no puede ejecutarse en informes de cuarentena para buzones de reenvío. Si un usuario intenta ejecutar dicha acción, se mostrará un mensaje de error.

ACCIÓN	DISEÑO	EXPLICACIÓN
Ver	**Diseño estándar con vista previa de los correos electrónicos** **Inbox Manager con vista previa de los correos electrónicos y opción de exclusión** **Diseño para ordenador de escritorio con vista previa de los correos electrónicos**	Mediante un enlace cifrado, se accede a un servicio online en una nueva ventana en la que el contenido del correo seleccionado se muestra de modo seguro. Las imágenes, enlaces y otros contenidos activos del correo se desactivan o sustituyen mediante sustitutivos seguros. Cuando sea preciso y posible, se modificarán ligeramente el diseño y la codificación para poder mostrar el contenido del correo. Para más información, véase el capítulo "Vista previa de correos" del manual de Control Panel.

ACCIÓN	DISEÑO	EXPLICACIÓN
No mostrar nunca el remitente	**Inbox Manager con vista previa de los correos electrónicos y opción de exclusión**	El remitente del correo seleccionado se añade (véase el capítulo "Acciones para correos" en el manual de Control Panel) a la lista negra (véase el capítulo "Acerca de las listas blancas y negras" en el manual de Control Panel) del destinatario. Los correos de este remitente dejarán de mostrarse en los futuros informes de cuarentena del usuario. **Nota:** Esta acción no puede ejecutarse en informes de cuarentena para buzones de reenvío. Si un usuario intenta ejecutar dicha acción, se mostrará un mensaje de error.

Activar Quarantine Report para un dominio

Ha activado Spam and Malware Protection (véase el capítulo "Activar Spam and Malware Protection" del manual de Control Panel).

Puede activar el módulo **Quarantine Report** (véase Acerca de Quarantine Report en la página 445) para un dominio para que los usuarios del mismo reciban informes de cuarentena.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar el módulo **Quarantine Report**.
3. Vaya a **Configuración de seguridad** > **Quarantine Report**.
4. **Importante:**

   Si desea personalizar el informe de cuarentena, introduzca todos los datos necesarios en el módulo **Personalización** antes de activar el módulo **Quarantine Report**. El informe de cuarentena se personaliza automáticamente en base a los datos de dicho módulo. Si no introduce ningún dato en dicho módulo, el informe de cuarentena no se personalizará.

   Accione el interruptor **Activar Quarantine Report**.

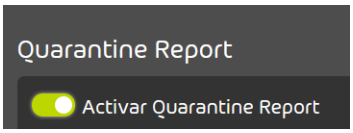


Figura 313: Activar Quarantine Report

El interruptor se pone verde.

El módulo **Quarantine Report** se ha desactivado para un dominio.

A continuación puede configurar el módulo **Quarantine Report** para el dominio (véase Configurar Quarantine Report para un dominio en la página 456).

Configurar Quarantine Report para un dominio

Ha activado el módulo **Quarantine Report** para el dominio (véase Activar Quarantine Report para un dominio en la página 455).

Puede configurar los informes de cuarentena para un dominio en el módulo **Quarantine Report** (véase Acerca de Quarantine Report en la página 445).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Vaya a **Configuración de seguridad** > **Quarantine Report**.
3. **Importante:**

   Por defecto, todos los usuarios del dominio reciben informes de cuarentena individuales en sus propias direcciones de correo electrónico. Alternativamente, es posible generar un informe de cuarentena para todo un dominio. Si se genera un informe de cuarentena para todo un dominio, los usuarios no recibirán informes de cuarentena.

   Opcional: Para generar un informe de cuarentena para todo un dominio, accione el interruptor **Generar un informe de cuarentena para todo el dominio**.

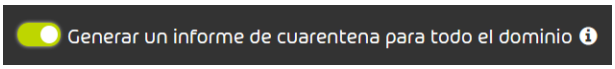
   

   Figura 314: Generar un informe de cuarentena para un dominio completo

   Se muestra el campo **Dirección del destinatario del informe de cuarentena**.
4. **Importante:**

   La dirección de correo electrónico del campo **Dirección del destinatario del informe de cuarentena** no debe estar definida como dirección del destinatario del informe de cuarentena de otro cliente.

   Opcional: En el campo **Dirección del destinatario del informe de cuarentena**, introduzca la dirección de correo electrónico a la que enviar el informe de cuarentena.

5. En **Opciones de diseño para los informes de cuarentena**, seleccione un diseño para sus informes de cuarentena (véase Diseños para informes de cuarentena en la página 447).

   - **Diseño estándar**
   - **Diseño estándar con vista previa de los correos electrónicos**
   - **Inbox Manager con vista previa de los correos electrónicos y opción de exclusión**

     Importante:

     Este diseño solo se muestra y puede elegirse activando previamente la opción **Excluir de los informes de cuarentena remitentes en la lista negra.** en la configuración de informes de cuarentena.

   - **Diseño para ordenador de escritorio**
   - **Diseño para ordenador de escritorio con vista previa de los correos electrónicos**

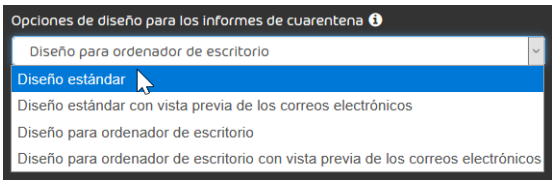


Figura 315: Seleccionar un diseño

Nota:

Los diseños con vista previa de correos no están disponibles para informes de cuarentena generados para dominios enteros.

Nota:

Para más información sobre la vista previa de correos, véase el capítulo "Vista previa de correos" en el manual de Control Panel.

6. Opcional: Si desea eliminar enlaces a Control Panel de los informes de cuarentena, accione el interruptor **Incluir enlace a Control Panel en informes de cuarentena**.

> **Nota:**
>
> Por defecto, los informes de cuarentena contienen enlaces a Control Panel.

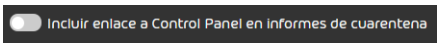


Figura 316: Eliminar enlace a Control Panel

El interruptor se pone gris.

7. Marque las casillas de los tipos de correos a mostrar en los informes de cuarentena. Puede elegir entre los siguientes tipos de correo.

- **Infomail**
- **Spam**
- **Threat y AdvThreat**
- **Contenido**

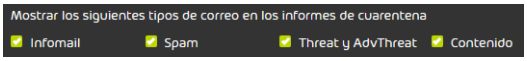
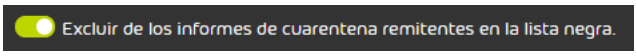


Figura 317: Seleccionar tipos de correo

8. Si desea excluir de los informes de cuarentena correos de remitentes que se encuentren en la lista negra del destinatario correspondiente o del dominio, accione el interruptor **Excluir de los informes de cuarentena remitentes en la lista negra.**



Importante:

Si se genera un informe de cuarentena para todo el dominio (véase más arriba), solo se retirarán de él los correos procedentes de remitentes que se encuentren en la lista negra del dominio. Las listas negras de los remitentes no se tendrán en cuenta.

Figura 318: Excluir de los informes de cuarentena remitentes en la lista negra..

El interruptor se activa. El diseño **Inbox Manager con vista previa de los correos electrónicos y opción de exclusión** se habilita en el menú desplegable **Opciones de diseño para los informes de cuarentena**.

9. En **Horas de entrega**, seleccione las horas a las que entregar los informes de cuarentena. Puede marcar los días y horas deseados o hacer clic en los siguientes botones:

   - **Cada hora**: Se seleccionan todas las horas.
   - **Cada día**: Se seleccionan todos los días.
   - **En días laborables**: Se seleccionan los días de lunes a viernes.
   - **Desactivar**: No se selecciona ningún día ni ninguna hora. Los informes de cuarentena están desactivados por defecto para todos los usuarios del dominio.

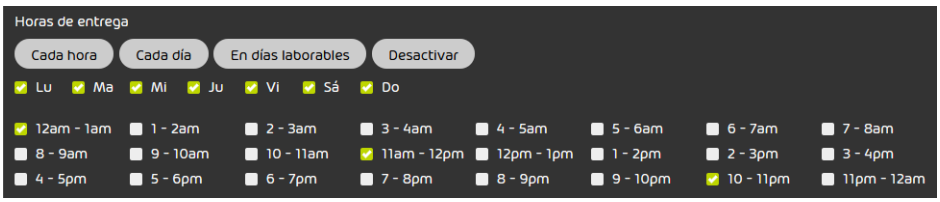


Figura 319: Seleccionar horas

Nota:

Solo se enviará un informe de cuarentena a las horas de entrega seleccionadas si nuevos correos se han puesto en cuarentena desde el último informe de cuarentena.

10. **Importante:**

    Por defecto, los usuarios del dominio reciben los informes de cuarentena a las horas de entrega definidas para el dominio. Si se han seleccionado horas de entrega para el dominio, por regla general, los usuarios no pueden modificar las horas de entrega de sus propios informes de cuarentena.

    Si no se han seleccionado horas de entrega para el dominio, los usuarios pueden modificar las horas de entrega de sus propios informes de cuarentena. En tal caso, no es posible retirar dicho permiso.

    Opcional: Para permitir a los usuarios que modifiquen las horas de entrega de sus informes de cuarentena, accione el interruptor **Permitir a los usuarios definir las horas de entrega de sus informes de cuarentena**.

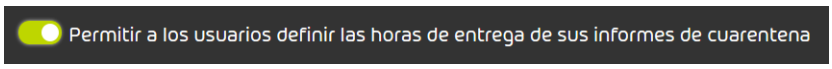


Figura 320: Permitir a los usuarios modificar las horas de entrega

El interruptor se pone verde.

11. Cree un texto personalizado en cada idioma en que se vayan a entregar los informes de cuarentena (véase Crear un texto personalizado para informes de cuarentena en la página 466).
12. Para aplicar los cambios, haga clic en **Guardar**.

El módulo **Quarantine Report** se ha configurado para un dominio.

A continuación puede configurar los informes de cuarentena de un modo distinto para un buzón de correo del dominio (véase Configurar Quarantine Report para un buzón de correo en la página 463).

Configurar Quarantine Report para un buzón de correo

Ha activado el módulo **Quarantine Report** para el dominio (véase Activar Quarantine Report para un dominio en la página 455). Ha configurado el módulo **Quarantine Report** para el dominio (véase Configurar Quarantine Report para un dominio en la página 456).

En el módulo **Configuración de cliente** > **Buzones** puede configurar los informes de cuarentena para un buzón de correo de modo distinto al del resto de buzones de correo del dominio (véase Configurar Quarantine Report para un dominio en la página 456).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio del buzón de correo para el cual desee configurar el módulo **Quarantine Report**.
3. Vaya a **Configuración de cliente** > **Buzones**.
4. Seleccione el buzón deseado de la lista y haga clic en la flecha junto al mismo.

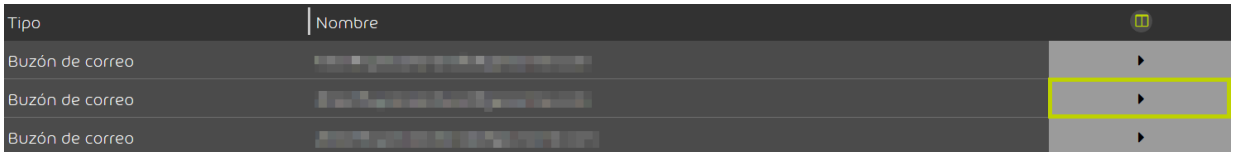


Figura 321: Mostrar configuración avanzada

Se abre un menú.

5. En el menú, haga clic en **Quarantine Report**.

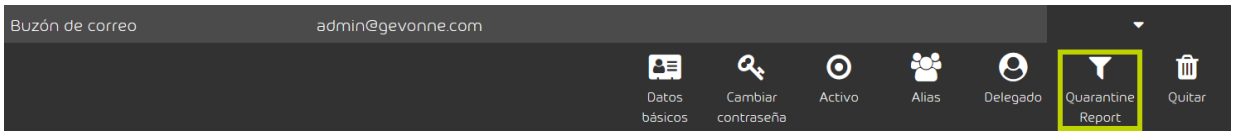


Figura 322: Menú

Se muestra la configuración del módulo **Quarantine Report** para el buzón de correo. Si aún no ha configurado el módulo **Quarantine Report** para el buzón de correo, se mostrará la configuración propia del dominio.

6. Para configurar el módulo **Quarantine Report** para el buzón de correo, accione el interruptor **Definir horas de entrega propias**.

Figura 323: Definir horas de entrega individuales

El interruptor se pone verde. Puede desactivar el módulo **Quarantine Report** o cambiar las horas de entrega de informes de cuarentena para este buzón de correo.

7. Si desea excluir de los informes de cuarentena correos de remitentes que se encuentren en la lista negra del destinatario correspondiente o del dominio, accione el interruptor **Excluir de los informes de cuarentena remitentes en la lista negra.**.

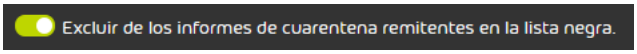


Figura 324: Excluir de los informes de cuarentena remitentes en la lista negra.

El interruptor se pone verde.

8. Si desea desactivar el módulo **Quarantine Report** para el buzón de correo, active el botón **Desactivar**.

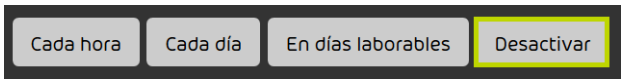


Figura 325: Desactivar Quarantine Report

Todos los días y horas de entrega están desactivados para el buzón de correo. No se entregan informes de cuarentena al buzón de correo. No es necesario hacer más ajustes.

9. Si módulo **Quarantine Report** se mantiene activado para el buzón de correos, seleccione los días en los que entregar los informes de cuarentena. Seleccione al menos un día.
   - Para hacer entregar los informes de cuarentena cada día, marque el botón **Cada día**.
   - Para hacer entregar los informes de cuarentena de lunes a viernes, marque el botón **En días laborables**.
   - Marque las casillas de los días deseados.

Figura 326: Seleccionar días

10. Elija las horas a las que entregar los informes de cuarentena. Seleccione al menos una hora.
    - Para hacer entregar los informes de cuarentena cada hora, active el botón **Cada hora**.
    - Marque las casillas de las horas deseadas.

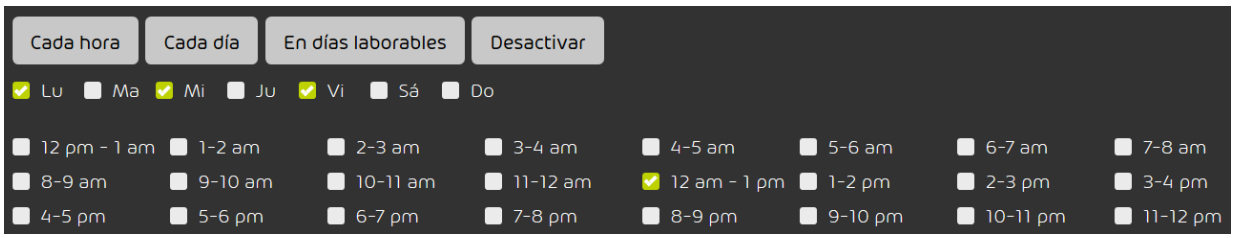


Figura 327: Seleccionar horas

> **Nota:**
>
> Solo se enviará un informe de cuarentena a las horas de entrega seleccionadas si nuevos correos se han puesto en cuarentena desde el último informe de cuarentena.

El módulo **Quarantine Report** se ha configurado para un buzón de correo.

Crear un texto personalizado para informes de cuarentena

Ha activado el módulo **Quarantine Report** (véase Activar Quarantine Report para un dominio en la página 455).

En el módulo **Quarantine Report** (véase Acerca de Quarantine Report en la página 445) puede usted personalizar los informes de cuarentena de su dominio con un texto personalizado en cada uno de los idiomas disponibles en Control Panel. En los informes de cuarentena, este texto aparecerá debajo de la lista de correos.

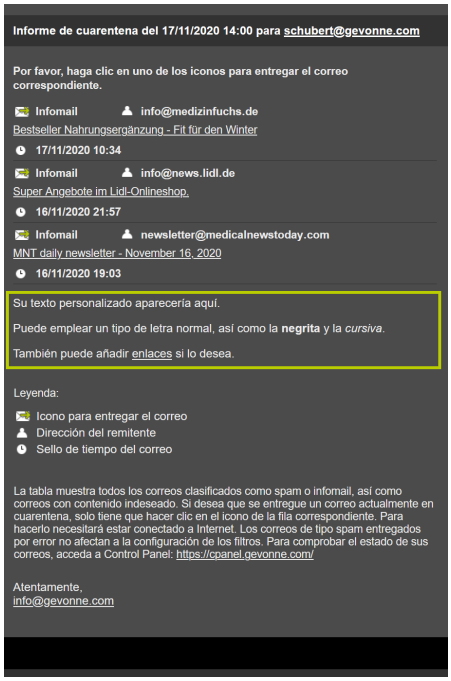


Figura 328: Ejemplo de texto personalizado

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Vaya a **Configuración de seguridad** > **Quarantine Report**.

3. Accione el interruptor **Utilizar texto personalizado en los informes de cuarentena**.

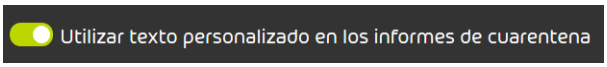


Figura 329: Emplear un texto personalizado

El interruptor se pone verde. El área de creación de textos personalizados se activa.

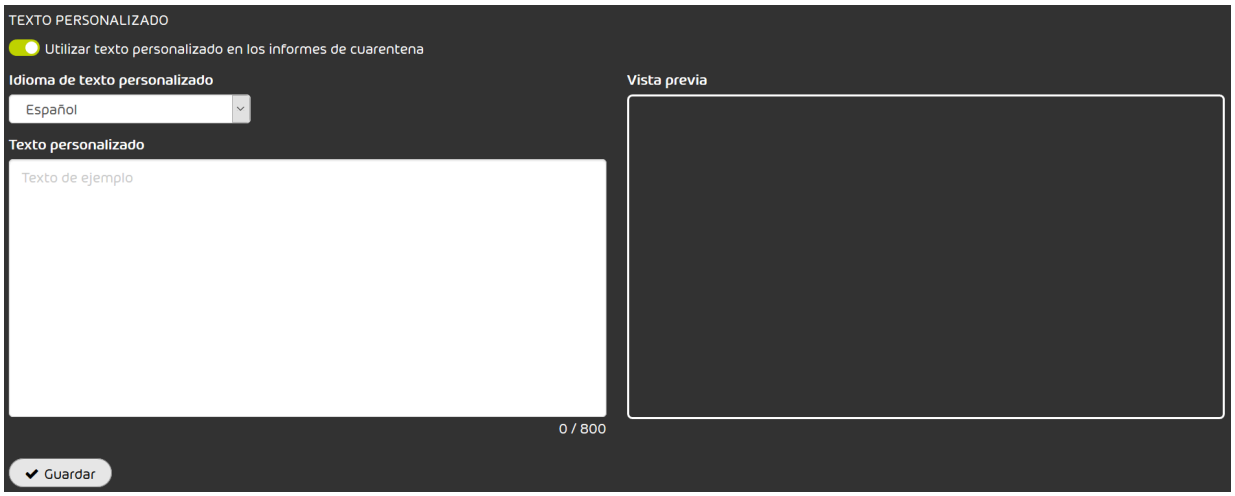


Figura 330: Editor de textos

4.

Importante:

Cada usuario recibe sus informes de cuarentena en el idioma que tenga ajustado para Control Panel en **Configuración de usuario** (véase Cambiar la zona horaria y el idioma en la página 37). Este idioma puede diferir del idioma por defecto del dominio en el módulo **Dashboard de servicios** (véase Ajustar zona horaria e idioma por defecto en la página 153).

Es posible redactar un texto personalizado para cada uno de los idiomas disponibles. Los textos individuales se añaden a los informes de cuarentena de su mismo idioma. Si no se ha creado ningún texto individual para alguno de los idiomas, los informes de cuarentena de dicho idioma se enviarán sin texto individual.

Seleccione el idioma del texto personalizado en **Idioma de texto personalizado**.

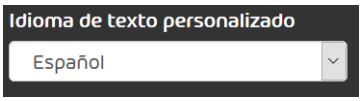


Figura 331: Idioma de texto personalizado

Nota:

Si selecciona otro idioma durante la redacción de un texto, el texto que haya introducido hasta el momento se conservará mientras permanezca en la página. Tan pronto como desactive el interruptor **Utilizar texto personalizado en los informes de cuarentena** y guarde los cambios, todos los textos personalizados en todos los idiomas se perderán al mismo tiempo.

5. Cree un texto personalizado en el idioma seleccionado.

> **Nota:**
>
> Hay un límite de longitud de 800 caracteres. Puede consultar la longitud actual en un contador situado debajo del campo de introducción de datos.

Figura 332: Cantidad de caracteres

6. Opcional: Formatee su texto a su gusto. Para hacerlo puede emplear algunas opciones de formato del lenguaje de marcado Markdown.

Nota:

Están disponibles las siguientes opciones de formato:

- Asterisco simple para cursiva: ***Cursiva***
- Doble asterisco para negrita: ****Negrita****.
- Los saltos de línea se representan mediante una línea en blanco. Sin esta línea en blanco, el texto aparecería en una sola línea dentro del informe de cuarentena. Ejemplo:

  Esto es un párrafo. Esto es otro párrafo.

- Una lista con viñetas se puede añadir empezando cada elemento de la lista como una línea independiente por un guión y un espacio en blanco. Una línea en blanco entre dos elementos de la lista es opcional y aumenta el espaciado entre los elementos de la lista. Sin embargo, es necesario separar el primer elemento de la lista por una línea en blanco del texto anterior. El último elemento de la lista también debe separarse por una línea en blanco del siguiente texto. Ejemplo:

  - Primer elemento de la lista

  - Segundo elemento de la lista

  - Tercer elemento de la lista

- Los enlaces pueden añadirse rodeando entre corchetes el texto mostrado, y la URL entre paréntesis. Ejemplo:

  Haga clic [aquí](https://una.url.tld).

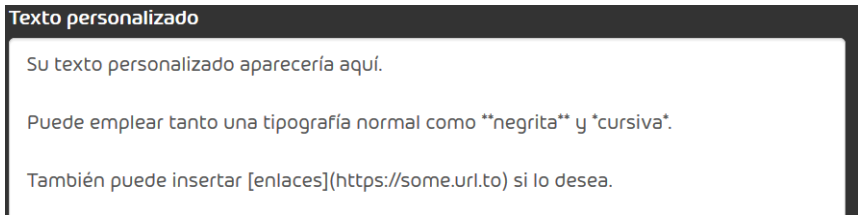


Figura 333: Texto de muestra en el campo de introducción de datos

7. Una vez haya escrito todos los textos en cada uno de los idiomas deseados, guárdelos con **Guardar**.

   Sus textos personalizados se guardan y se emplearán en la siguiente entrega de informes de cuarentena. La vista preliminar muestra el resultado en el idioma seleccionado después de hacer clic en **Guardar**.

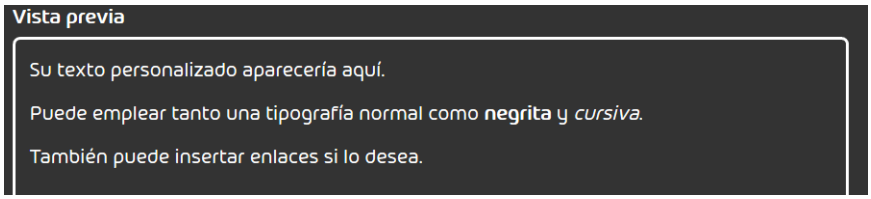


Figura 334: Ejemplo de texto en el campo de previsualización

Se han creado textos individuales para informes de cuarentena.

Desactivar Quarantine Report para un dominio

Ha activado el módulo **Quarantine Report** para el dominio (véase Activar Quarantine Report para un dominio en la página 455).

Si no es necesario generar más informes de cuarentena para un dominio, puede desactivar el módulo **Quarantine Report** (véase Acerca de Quarantine Report en la página 445) para el dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.

2. Seleccione un dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Quarantine Report**.
4. Accione el interruptor **Activar Quarantine Report**.

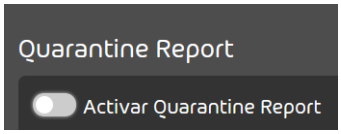


Figura 335: Desactivar Quarantine Report

El interruptor se pone gris.

El módulo **Quarantine Report** se ha desactivado para un dominio.

Entregar un correo de un informe de cuarentena

Ha activado el módulo **Quarantine Report** para el dominio (véase Activar Quarantine Report para un dominio en la página 455).

Puede entregar correos incluidos en informes de cuarentena (véase Acerca de Quarantine Report en la página 445).

1. Abra el informe de cuarentena en su cliente de correo electrónico.
2. Seleccione un el correo del informe de cuarentena que desee entregar.

3. Haga clic en **Entregar**.

El correo se entrega al destinatario. Se muestra una confirmación de entrega en el navegador.

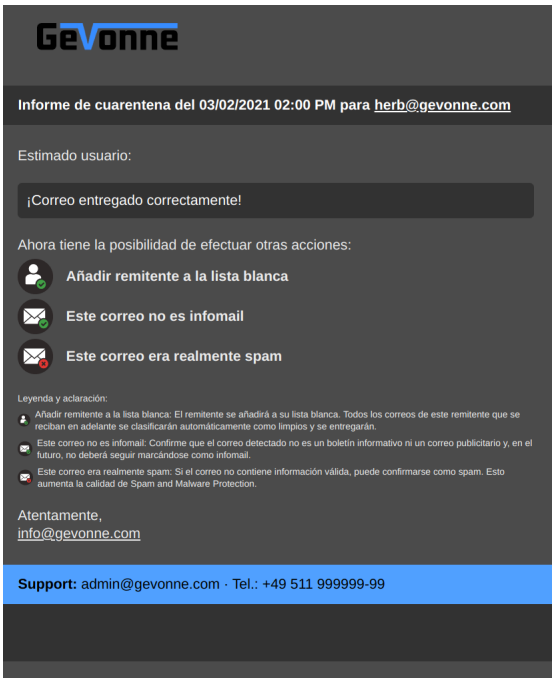


Figura 336: Confirmación de entrega

Nota:

Los informes de cuarentena se generan por buzón de correos principal. Si un buzón principal tiene asignados buzones de correo alias, los correos dirigidos a éstos se mostrarán en un único informe de cuarentena junto con los correos dirigidos al buzón de correo principal. Al entregar un correo de un informe de cuarentena, en la parte superior de la confirmación de entrega se indica el buzón de correo al que estaba dirigido el correo.

4. Haga clic en una de las opciones avanzadas:

   - **Añadir remitente a lista blanca**. El remitente se añade a la lista blanca del usuario.
   - **Este correo no es infomail**. El correo se clasifica como **Válido**.
   - **Este correo era realmente spam**. El correo se clasifica como **Spam** si estaba clasificado previamente como infomail.

   Se ejecuta la acción seleccionada. En lugar de la confirmación de entrega anterior, se muestra una confirmación al respecto en el navegador.

Figura 337: Ventana de confirmación

5. Cierre la confirmación de entrega.

Se ha entregado un correo desde un informe de cuarentena.

Ver vista previa de correos

Puede ver vistas previas de los correos incluidos en informes de cuarentena (véase Acerca de Quarantine Report en la página 445) de los cuales sea propietario. Para más información sobre la vista previa de correos, véase el capítulo "Vista previa de correos" en el manual de Control Panel.

1. Abra el informe de cuarentena en su cliente de correo electrónico.
2. Seleccione el correo del que quiera ver una vista previa.
3. Haga clic en **Ver**.

   Se muestra una vista previa simplificada del correo en el navegador.

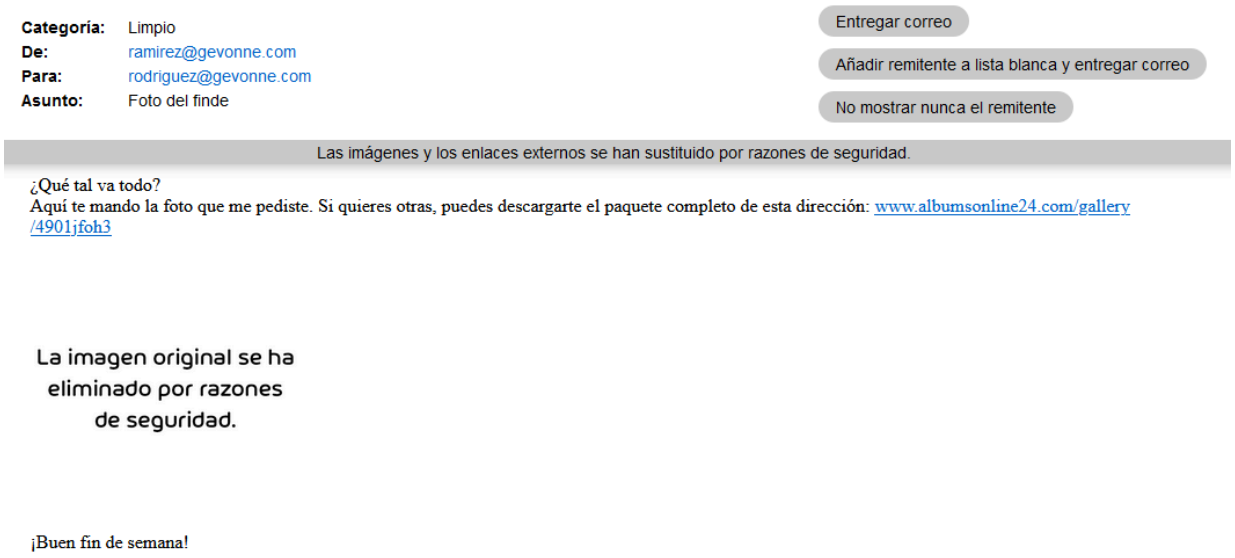


Figura 338: Vista previa de correos

4. Cierre la vista previa del correo.

Se ha mostrado la vista previa de un correo de un informe de cuarentena.

Spam and Malware Protection

Spam and Malware Protection

Spam and Malware Protection es un servicio que evita que el correo no deseado y los correos con virus lleguen al buzón de correo del destinatario. También permite detectar y elegir entre entregar, poner en cuarentena o marcar como tales los correos de tipo infomail, como boletines de noticias.

Spam and Malware Protection protege frente a amenazas, spam e infomail con las siguientes funciones:

- Análisis de virus en los correos con actualización automática de las firmas de virus y sistema de alerta temprana para virus nuevos y aún desconocidos.
- Link Tracking: Los correos entrantes y salientes se analizan automáticamente en cuanto a URLs maliciosas.
- Detección de correos de suplantación de identidad: Con diversos mecanismos, tales como el Link Tracking o la detección de órdenes de script maliciosas, los intentos de suplantación de identidad se previenen.
- Filtrado de salida: Los correos salientes se analizan en cuanto a spam y virus para evitar que el cliente envíe o retransmita software malicioso y spam involuntariamente.
- Gestión de devoluciones: Spam and Malware Protection rechaza los mensajes de devolución que se reciben como respuesta a spam enviado con direcciones de remitente falsificadas.

En **Configuración de seguridad** > **Spam and Malware Protection** pueden realizarse los siguientes ajustes relacionados con Spam and Malware Protection:

- Activar Spam and Malware Protection (véase Activar Spam and Malware Protection en la página 480)
- Configurar el entorno primario (véase Configuración del entorno primario en la página 483)
- Configurar el tratamiento de spam e infomail (véase Configuración del filtro de correo en la página 489)
- Permitir o prohibir acciones de usuarios (véase Permitir o prohibir acciones de usuarios en la página 496)

Spam and Malware Protection permite al administrador decidir por sí mismo cómo tratar el spam y el infomail (véase Configuración del filtro de correo en la página 489). En caso de falsos positivos, y dependiendo de la configuración del administrador, los usuarios pueden hacerse entregar correos clasificados como spam e infomail mediante **Email Live Tracking** (véase Acciones para correos en la página 95).

Además, Spam and Malware Protection incluye los servicios **Content Control** (véase Acerca de Content Control en la página 500) y **Compliance Filter** (véase Acerca de Compliance Filter en la página 516), para que el cliente los active si lo desea. El orden de las reglas (véase Orden de las reglas de todos los servicios en la página 478) muestra el orden de los filtros de todos los servicios.

Si el cliente no desea continuar utilizando Spam and Malware Protection, puede solicitar su desactivación al soporte técnico (véase Desactivar Spam and Malware Protection en la página 498).

Orden de las reglas de todos los servicios

Las reglas de Spam and Malware Protection (véase "Spam and Malware Protection" en el manual de Control Panel) tienen determinada prioridad de procesamiento. En cuanto aplica una regla de alta prioridad, las reglas de menor prioridad dejan de procesarse. Esto puede provocar que un correo acabe bloqueado aunque la dirección de su remitente esté registrada en una lista blanca si la dirección IPv4 del servidor de origen se encuentra en la lista negra RBL.

Reglas en orden descendente de prioridad:

Correos entrantes

1. Lista RBL (bloquear)
2. Detección de spam masivo (bloquear)
3. Compliance Filter
4. Email Authentication (bloquear)
5. Pruebas para detectar contenido malicioso (poner en cuarentena)

6. Email Authentication (poner en cuarentena)
7. Content Control, si está activado (poner en cuarentena)
8. Uso de lista blanca de usuario (entregar)
9. Uso de lista negra de usuario (poner en cuarentena)
10. Uso de lista blanca de administrador (entregar)

> **Nota:**
>
> Las listas blancas de administrador son un caso particular entre las reglas. Pues los administradores pueden seleccionar los filtros a evitar para los registros de listas blancas a nivel de dominio (véase «Crear un registro de lista negra para un dominio» en el manual de Control Panel). Al ser procesados, los correos afectados omitirán los filtros seleccionados. Esto también incluye los filtros que preceden el uso de lista blanca de administrador en la lista. La posición en la cual se encuentra el uso de lista blanca de administrador dentro de la lista se refiere a la configuración por defecto de registros de listas blancas a nivel de dominio. Por defecto, los registros solo evitan el filtrado de spam.

11. Uso de lista negra de administrador (poner en cuarentena)
12. Uso de lista blanca general (entregar)
13. Reglas generales de spam (poner en cuarentena)
14. Filtro de infomail (poner en cuarentena)

Nota:

Compliance Filter (véase Acerca de Compliance Filter en la página 516) se aplica antes que Content Control (véase Acerca de Content Control en la página 500). Por tanto, los administradores pueden emplear reglas de Compliance Filter que clasifiquen correos como **Limpio** para crear excepciones para Content Control.

Sin embargo, no es posible crear excepciones para Content Control mediante listas blancas o negras de usuario así como listas negras de administrador, ya que éstas se aplican después de Content Control. Solo listas blancas de administrador permiten evitar Content Control.

Correos salientes

1. Lista RBL
2. Compliance Filter
3. Pruebas para detectar contenido malicioso
4. Content Control, si está activado

Activar Spam and Malware Protection

En el módulo **Configuración de seguridad** > **Spam and Malware Protection** puede desactivar Spam and Malware Protection (véase Spam and Malware Protection en la página 477) para un dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar Spam and Malware Protection.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.

4. Seleccione en **Dominio** el dominio para el cual desee activar Spam and Malware Protection.

Figura 339: Seleccionar un dominio

> **Nota:**
>
> Spam and Malware Protection solo puede configurarse para dominios alias si ya está activado para el dominio principal correspondiente. Por defecto, los dominios alias heredan la configuración del dominio principal.

5. Accione el interruptor **Configuración del entorno primario** de **Activar Spam and Malware Protection**.

Figura 340: Activar Spam and Malware Protection

Se muestra una ventana de confirmación.

6. **Atención:**

   Una vez activado Spam and Malware Protection, comenzará un periodo de prueba gratuito de 30 días. Al finalizar el periodo de prueba, el servicio se volverá de pago.

   Importante:

   Los administradores no pueden desactivar Spam and Malware Protection por sí mismos. Solo el soporte técnico puede desactivar Spam and Malware Protection.

   Haga clic en **Confirmar**.

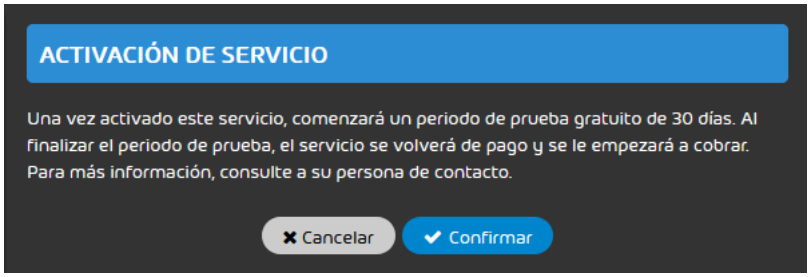


Figura 341: Confirmar

El interruptor se pone en verde y otros elementos de control de las secciones **Configuración del entorno primario** y **Configuración del filtro de correo** quedan habilitados.

7. Opcional: Si desea modificar la configuración de entorno de y la configuración del filtro de correo antes de activar Spam and Malware Protection, puede realizar ahora sus modificaciones (véanse Configurar el entorno primario en la página 484 y Configuración del filtro de correo en la página 489).
8. Haga clic en **Guardar**.

Spam and Malware Protection se ha activado para el dominio.

A continuación puede configurar su entorno primario (véase Configuración del entorno primario en la página 483) así como el filtro de correo (véase Configuración del filtro de correo en la página 489).

Configuración del entorno primario

En el módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477) se administra la configuración del entorno primario de un dominio.

Spam and Malware Protection requiere diversos ajustes relativos al entorno primario y a la recepción y el envío de correos electrónicos. En **Configuración del entorno primario**, los administradores a nivel de cliente pueden determinar el destino de los correos entrantes, definir direcciones IPv4 para servidores de retransmisión, activar la gestión de devoluciones y configurar la comprobación de usuarios.

Para mayor claridad, incluimos aquí una breve explicación sobre las opciones disponibles. Para saber más sobre la configuración, véase Configurar el entorno primario en la página 484.

- **Destino**: En el apartado **Destino** se indica el destino de los correos entrantes a procesar mediante Spam and Malware Protection. Las opciones disponibles son:
  - **IP/Nombre de host**: Se trata del caso más habitual. Aquí se hace establece una referencia a los servidores de correo del cliente, bien indicando las direcciones IPv4 o los nombres de host correspondientes. En caso de indicarse un nombre de host, al principio se resuelve el registro MX y, a continuación, el registro A.
- **Direcciones IP de servidores de retransmisión para correos salientes**: Si Spam and Malware Protection está activado, se filtran también los correos salientes. Por tanto, en **Direcciones IP de servidores de retransmisión para correos salientes** es posible indicar las direcciones IPv4 de los servidores de retransmisión desde los que se envían correos a nuestros servidores, de modo que Spam and Malware Protection pueda cotejarlas y decidir si un correo realmente procede del cliente.

  Aquí puede definir varias direcciones de servidores de retransmisión separadas entre sí por comas y en rangos de /24 como máximo. Hay un límite de longitud de 65.535 caracteres. También es posible indicar rangos CIDR. Al enviarse un correo a través de las direcciones IP registradas,

Spam and Malware Protection actúa. Si esta opción no se encuentra activada, Spam and Malware Protection filtrará todos los correos salientes procedentes de direcciones de correo del dominio.

> **Importante:**
>
> Las direcciones IP de servidores de retransmisión aquí indicadas también son necesarias para la firma y el cifrado de correos en el marco de Signature and Disclaimer. Si no se indican direcciones, no será posible tratar ningún correo con ninguno de estos dos servicios. Incluso si no se utilizan dichos servicios, recomendamos a los administradores a nivel de cliente indicar aquí las direcciones IP de los servidores de retransmisión.

- **Restringir el envío de correo electrónico a las direcciones IP de servidores de retransmisión**: Esta opción garantiza que los correos salientes de las direcciones de correo del dominio solo se envíen a través de nuestra infraestructura si se han enviado desde una de las direcciones de servidores de retransmisión indicadas.
- **Gestión de devoluciones (recomendado)**: La gestión de devoluciones es una función que, al recibirse mensajes de devolución, comprueba si los correos que los provocaron realmente fueron enviados a través del servidor de retransmisión del dominio o, si, por el contrario, se enviaron a través de una dirección falsificada como parte de un ataque de spam. En el segundo caso, los mensajes de devolución se rechazan.
- **Comprobación de usuarios**: Durante la comprobación de usuarios, Spam and Malware Protection comprueba que las direcciones de los destinatarios de mensajes entrantes realmente existan. Si la dirección del destinatario de un correo no existe, Spam and Malware Protection rechaza el correo. De este modo se evita que nuestros servidores de correo acepten correos a destinatarios inexistentes en los dominios de nuestros clientes que podrían estar utilizándose para realizar ataques DDOS contra nuestros clientes. La comprobación puede efectuarse en base a las listas de usuarios de Control Panel o bien directamente mediante solicitud SMTP a los servidores de correo del dominio de un cliente indicados en **Destino**.

Configurar el entorno primario

Ha activado Spam and Malware Protection.

Spam and Malware Protection (véase Spam and Malware Protection en la página 477) requiere configurar el entorno primario para la recepción y el envío de correos electrónicos. En Configuración del entorno primario en la página 483 encontrará más información sobre las funciones.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee configurar el entorno primario.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.
4. En **Dominio**, seleccione el dominio para el cual desee configurar el entorno primario.
5. Opcional: Si ha seleccionado un dominio alias que hasta ahora heredaba su configuración del dominio principal, accione el interruptor **Heredar de dominio principal**.

   El interruptor se pone gris. Los ajustes del módulo se habilitan.
6. Defina el servidor de destino de los correos entrantes en **Destino**. Existen las siguiente opciones:

   - Si dispone de su propio servidor de correo, marque la casilla **IP/Nombre de host** e introduzca la dirección IPv4 o el nombre de host del servidor de destino en el campo. Indique al menos una dirección IPv4 o un nombre de host. Opcionalmente puede indicar también el número de puerto y la prioridad. Al hacerlo, respete el formato **IPv4/Nombre de host:Puerto#Prioridad** y emplee el punto y coma para separar los registros entre sí.
   -
   -

   Nota:

   Este servidor de destino se denomina entorno primario en Control Panel. El tráfico entrante de los buzones de correo se dirige por defecto al entorno primario. Para dirigir el tráfico entrante de un buzón de correo determinado a otro servidor de destino, es posible asignarle un entorno secundario (véase "Entornos secundarios" en el manual de Control Panel) en lugar del primario (véase Cambiar de entorno en la página 276).

7. **Nota:**

   Este paso es opcional pero altamente recomendable. Las direcciones IP indicadas en **Direcciones IP de servidores de retransmisión para correos salientes** también son necesarias para la firma de correos en el marco de Signature and Disclaimer. Si no se indican direcciones, no será posible tratar ningún correo con ninguno de estos dos servicios.

   Opcional: Si desea indicar manualmente las direcciones IP de sus servidores de correo de retransmisión, accione el interruptor **Direcciones IP de servidores de retransmisión para correos salientes**.

   Se muestra un campo para introducir direcciones IPv4.

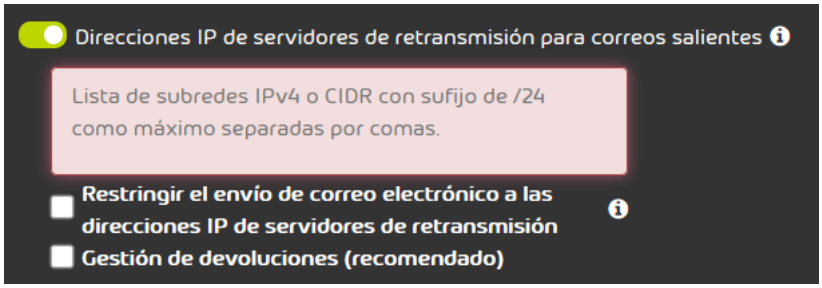


Figura 342: Definir direcciones IP de servicores de retransmisión para el correo saliente.

8. Opcional: Introduzca las direcciones IPv4 de sus servidores de retransmisión en el campo bajo el interruptor **Direcciones IP de servidores de retransmisión para correos salientes**. Si el interruptor está activado, este campo no deberá estar vacío.

   Nota:

   Aquí puede definir varias direcciones IPv4 de servidores de retransmisión separadas entre sí por comas y en rangos de /24 como máximo. Este campo no debe contener más de 65.535 caracteres.

9. Opcional: Para garantizar que los correos salientes del dominio solo se envíen desde las direcciones IP de servidores de retransmisión indicadas, marque la casilla **Restringir el envío de correo electrónico a las direcciones IP de servidores de retransmisión**.

   Nota:

   Esta opción está activada por defecto. Esta opción garantiza que los correos salientes de las direcciones de correo del dominio solo se envíen a través de nuestra infraestructura si se han enviado desde una de las direcciones IPv4 servidores de retransmisión indicadas.

10. Opcional: Si desea activar la gestión de devoluciones para evitar mensajes de devolución incorrectos, marque la casilla **Gestión de devoluciones (recomendado)**.

11. **Nota:**

    Este paso es solo para clientes que hayan seleccionado **IP/Nombre de host** como destino para su entorno primario.

    Opcional: Configure la comprobación de usuarios en la sección **Comprobación de usuarios**. Tiene las siguientes opciones:

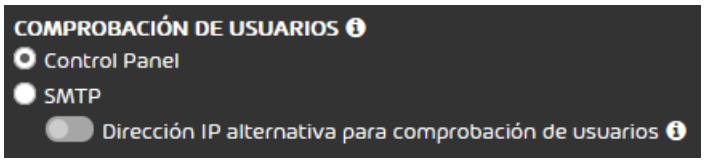


Figura 343: Configurar la comprobación de usuarios

- **Control Panel**: Si marca esta casilla, Spam and Malware Protection comprobará si la dirección del destinatario está registrada en la lista de usuarios de Control Panel. Esta

opción evita la creación automática de buzones de correo en Control Panel (véase Buzones de correo en la página 230).

> **Nota:**
>
> Si se selecciona esta opción, todos los buzones de correo deseados y sus direcciones alias deben incluirse en Control Panel. Los buzones de correo pueden añadirse a Control Panel bien manualmente o bien mediante sincronización con un servicio de directorio mediante LDAP.

- **SMTP**. Si marca esta casilla, Spam and Malware Protection comprobará la dirección del destinatario mediante "rellamada" SMTP. Para ello, Spam and Malware Protection pregunta al servidor de destino de la dirección del destinatario si ésta es válida. Por defecto, el servidor de destino se determina a partir de la parte de dominio de la dirección. Si desea emplear un servidor de destino distinto para la comprobación de usuarios con SMTP, accione el interruptor **Dirección IP alternativa para comprobación de usuarios** e introduzca la dirección IPv4 en el campo de introducción. Puede introducir una subred IPv4 o CIDR.

> **Nota:**
>
> Si la comprobación de usuarios causa problemas, póngase en contacto con el soporte técnico.

12. Haga clic en **Guardar**.

Si se elige la opción **SMTP** para la comprobación de usuarios, se muestra un mensaje de advertencia. De lo contrario, los ajustes se guardan.

13. Si ha seleccionado la opción **SMTP** para la comprobación de usuarios, haga clic en **Confirmar**.

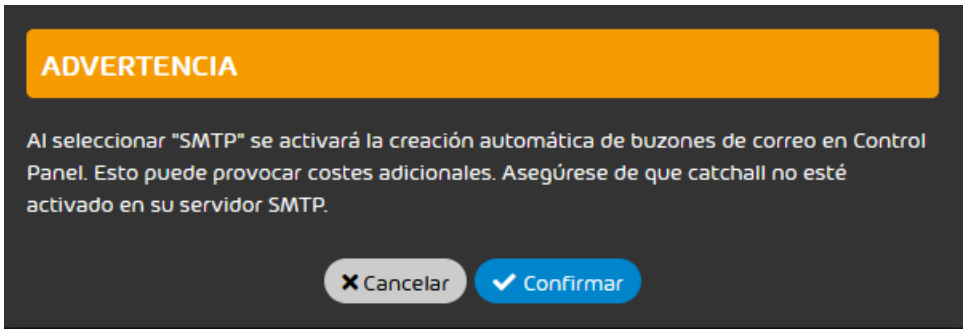


Figura 344: Confirmar

Los ajustes se guardan.

El entorno primario de Spam and Malware Protection se ha configurado.

A continuación puede editar la configuración del filtro de correo (véase Configuración del filtro de correo en la página 489) o permitir o prohibir acciones de usuarios (véase Permitir o prohibir acciones de usuarios en la página 496).

Configuración del filtro de correo

En el apartado **Configuración del filtro de correo** del módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477) los administradores a nivel de cliente pueden realizar diversos ajustes relativos al filtro de correo.

En **Configuración de seguridad** > **Spam and Malware Protection** > **Configuración del filtro de correo**, los administradores a nivel de cliente tienen las siguientes opciones:

- Configurar el tratamiento de Spam (véase Configurar el tratamiento de spam en la página 490).
- Activar el filtro de infomail (véase Activar el filtro de infomail en la página 492).

- Configurar el filtro de infomail (véase Configurar el filtro de infomail en la página 493).
- Configurar el tratamiento de infomail (véase Configurar el tratamiento de infomail en la página 494).

Configurar el tratamiento de spam

Ha activado **Spam and Malware Protection** (véase Activar Spam and Malware Protection en la página 480).

En el apartado **Tratamiento de spam** del módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477) puede decidir qué sucede con el spam captado por el filtro de correo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee configurar el tratamiento de spam.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.
4. En **Dominio**, seleccione el dominio para el cual desee configurar el tratamiento de spam.
5. Opcional: Si ha seleccionado un dominio alias que hasta ahora heredaba su configuración del dominio principal, accione el interruptor **Heredar de dominio principal**.

   El interruptor se pone gris. Los ajustes del módulo se habilitan.

6. Seleccione la opción de tratamiento de spam deseada en **Configuración del filtro de correo** > **Tratamiento de spam**. Tiene dos opciones:

   - Si desea almacenar el spam en cuarentena, seleccione la casilla **Poner en cuarentena**. El módulo **Email Live Tracking** ofrece diversas opciones para los correos en cuarentena.
   - Si desea etiquetar los correos de tipo spam con una frase personalizada, marque la casilla **Etiquetar**. A continuación se muestra el campo de introducción de datos **Frase para etiquetar**. Introduzca en él la frase con la que desee etiquetar los correos no deseados.

Figura 345: Etiquetar como spam

> **Nota:**
>
> Los correos clasificados como **Spam** solo se muestran en los informes de cuarentena (véase el capítulo «Acerca de Quarantine Report» en el manual de Control Panel) si se han puesto en cuarentena y si la categoría de correo electrónico se ha seleccionado para que se muestre en los informes de cuarentena (véase el capítulo «Configurar Quarantine Report para un dominio» en el manual de Control Panel).

7. Haga clic en **Guardar**.

El tratamiento de spam se ha configurado.

A continuación puede activar el filtro de infomail (véase Activar el filtro de infomail en la página 492) o permitir o prohibir acciones de usuarios (véase Permitir o prohibir acciones de usuarios en la página 496).

Activar el filtro de infomail

Ha activado **Spam and Malware Protection**(véase Activar Spam and Malware Protection en la página 480).

En la sección **Configuración del filtro de infomail** del módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477) puede activar el filtro de infomail para un dominio principal y realizar otros ajustes. Los ajustes también se aplicarán a los dominios alias del dominio principal.

El filtro de infomail detecta infomail y efectúa diversas acciones en función de la configuración. El filtro de infomail forma parte del ámbito de funciones del filtro de correo de **Spam and Malware Protection**. Para poder utilizar el filtro de infomail, es necesario activarlo antes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar el filtro de infomail.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.
4. Seleccione en **Dominio** el dominio principal para el cual desee activar el filtro de infomail.
5. Accione el interruptor **Activar filtro de infomail**.

   El interruptor se pone en verde y aparece un formulario con opciones adicionales.
6. Haga clic en **Guardar**.

El filtro de infomail se ha activado para un dominio principal y sus dominios alias.

A continuación puede configurar el filtro de infomail (véase Configurar el filtro de infomail en la página 493).

Configurar el filtro de infomail

Ha activado **Spam and Malware Protection** y el filtro de infomail (véanse Activar Spam and Malware Protection en la página 480 y Activar el filtro de infomail en la página 492).

En la sección **Configuración del filtro de infomail** del módulo **Spam and Malware Protection** (véase "Spam and Malware Protection" en el manual de Control Panel) puede configurar el filtro de infomail para regular su ámbito de aplicación para un cliente. La configuración se aplicará tanto al dominio principal como también a los dominios alias del cliente.

Puede activar o desactivar el filtro de infomail por defecto para todos los usuarios del cliente. También puede establecer si los usuarios pueden activar y desactivar el filtro de infomail para su propio buzón de correo (véase "Configurar los informes de cuarentena" en el manual de Control Panel). De este modo, los usuarios pueden decidir por sí mismos si desean utilizar el filtro de infomail.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee configurar el filtro de infomail.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.
4. Seleccione en **Dominio** el dominio principal para el cual desee configurar el filtro de infomail.
5. Si desea activar el filtro de infomail por defecto para todos los usuarios del cliente, marque la casilla **Activar filtro de infomail para todos los usuarios** de **Configuración del filtro de correo** > **Configuración del filtro de infomail**.
6. Si desea permitir que los usuarios del cliente activen y desactiven por sí mismos el filtro de infomail, marque la casilla **Permitir a los usuarios activar y desactivar el filtro de infomail**. Si la casilla está marcada, los usuarios podrán activar y desactivar el filtro de infomail en **Configuración de usuario** > **Filtros e Informes** (véase "Configurar los informes de cuarentena" en el manual de Control Panel). Combinando las dos casillas se obtienen las siguientes opciones:
   - **Activar filtro de infomail para todos los usuarios** activado, **Permitir a los usuarios activar y desactivar el filtro de infomail** desactivado: El filtro de infomail está activado para todos los usuarios. Los usuarios no pueden desactivar el filtro de infomail.

- **Activar filtro de infomail para todos los usuarios** activado, **Permitir a los usuarios activar y desactivar el filtro de infomail** desactivado: El filtro de infomail está activado por defecto para todos los usuarios. Los usuarios pueden desactivar el filtro de infomail.
- **Activar filtro de infomail para todos los usuarios** desactivado, **Permitir a los usuarios activar y desactivar el filtro de infomail** activado: El filtro de infomail está desactivado por defecto para todos los usuarios. Los usuarios pueden activar el filtro de infomail.
- **Activar filtro de infomail para todos los usuarios** desactivado, **Permitir a los usuarios activar y desactivar el filtro de infomail** desactivado: El filtro de infomail está desactivado para todos los usuarios. Los usuarios no pueden activar el filtro de infomail. Tan pronto como guarde los cambios, el interruptor **Activar filtro de infomail** se pondrá en gris, y las demás opciones se ocultarán.

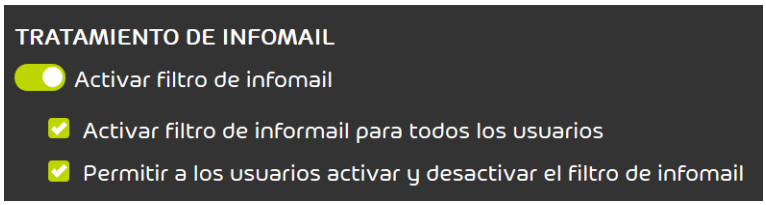


Figura 346: Configurar el filtro de infomail

7. Haga clic en **Guardar**.

Se ha configurado el filtro de infomail.

A continuación puede configurar el tratamiento de infomail (véase Configurar el tratamiento de infomail en la página 494) o permitir o prohibir acciones de usuarios (véase Permitir o prohibir acciones de usuarios en la página 496).

Configurar el tratamiento de infomail

Ha activado **Spam and Malware Protection** y el filtro de infomail (véase Activar Spam and Malware Protection en la página 480 y Activar el filtro de infomail en la página 492).

En el apartado **Configuración del filtro de infomail** del módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477) puede decidir qué sucede con el infomail captado por el filtro de correo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee configurar el tratamiento de infomail.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.
4. En **Dominio**, seleccione el dominio para el cual desee configurar el tratamiento de infomail.
5. Opcional: Si ha seleccionado un dominio alias que hasta ahora heredaba su configuración del dominio principal, accione el interruptor **Heredar de dominio principal**.
6. Seleccione la opción de tratamiento de infomail deseada en **Configuración del filtro de correo** > **Configuración del filtro de infomail**. Tiene dos opciones:
   - Si desea almacenar el infomail en cuarentena, seleccione la casilla **Poner en cuarentena**. El módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) ofrece diversas acciones (véase Acciones para correos en la página 95) para los correos en cuarentena.

- Si desea etiquetar los correos de tipo infomail con una frase personalizada, marque la casilla **Etiquetar**. A continuación se muestra el campo de introducción de datos **Frase para etiquetar**. Introduzca en él la frase con la que desee marcar el infomail.

Figura 347: Etiquetar infomail

> **Nota:**
>
> Independientemente de estos ajustes, todos los correos clasificados como **Infomail** se incluyen en los informes de cuarentena. Esto solo aplica si ha activado el filtro de infomail y ha seleccionado la categoría **Infomail** para su visualización en informes de cuarentena (véase Configurar Quarantine Report para un dominio en la página 456).

7. Haga clic en **Guardar**.

El tratamiento de infomail se ha configurado.

A continuación puede permitir o prohibir acciones de usuarios (véase Permitir o prohibir acciones de usuarios en la página 496).

Permitir o prohibir acciones de usuarios

En el apartado **Permisos de usuario** del módulo **Spam and Malware Protection** (véase Spam and Malware Protection en la página 477) puede permitir o prohibir a los usuarios de su dominio ejecutar acciones sobre correos interceptados por Spam and Malware Protection.

En el módulo **Email Live Tracking** (véase Email Live Tracking en la página 63) y los informes de cuarentena (véase Acerca de Quarantine Report en la página 445) los usuarios disponen de acciones para hacerse entregar correos propios interceptados por Spam and Malware Protection. Puede permitir o prohibir cada una de estas acciones. Independientemente de esos ajustes, los administradores a nivel de cliente pueden efectuar la entrega de todos los correos desde el módulo **Email Live Tracking**.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione un dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Spam and Malware Protection**.
4. Seleccione la pestaña **Permisos de usuario**.

   La pestaña **Permisos de usuario** se abre.

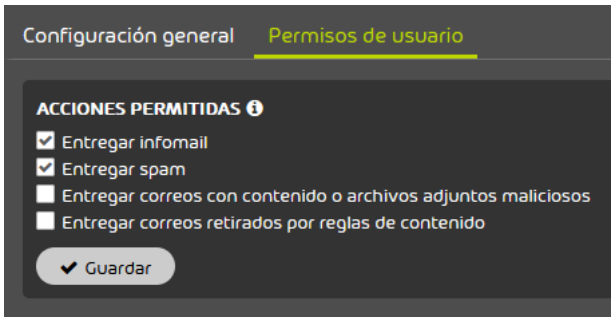


Figura 348: Permisos de usuario

5. En **Acciones permitidas**, marque las casillas de las acciones que desee permitir a los usuarios del dominio. Desmarque las casillas de las acciones que desee prohibir a los usuarios del dominio. Están disponibles las siguientes acciones:

   - **Entregar infomail**.
   - **Entregar spam**.
   - **Entregar correos con archivos adjuntos maliciosos**.
   - **Entregar correos retirados por reglas de contenido**.

   > **Nota:**
   >
   > Independientemente de estos ajustes, los usuarios no pueden hacerse entregar correos categorizados como **AdvThreat**. Solo los administradores y usuarios con el rol **Service Desk** pueden entregar correos de dicha categoría.

6. Haga clic en **Guardar**.

Se han permitido o prohibido acciones de usuarios sobre correos interceptados por Spam and Malware Protection.

A continuación puede activar el filtro de infomail (véase Activar el filtro de infomail en la página 492).

Desactivar Spam and Malware Protection

Ha activado Spam and Malware Protection (véase Spam and Malware Protection en la página 477) para un dominio principal. Ha vuelto a dirigir los registros MX en la zona de DNS de su dominio a su servidor de correo electrónico.

Si no desea seguir empleando Spam and Malware Protection, puede solicitar al soporte técnico que lo desactive. Los ajustes se guardarán por si desea volver a activar Spam and Malware Protection con posterioridad.

Aviso:

Si desactiva Spam and Malware Protection y no ha ajustado antes los registros MX en la zona de DNS de su dominio para que vuelvan a apuntar a su servidor de correo electrónico, los correos entrantes no se reenviarán al mismo y pueden perderse.

Antes de desactivar Spam and Malware Protection, asegúrese de que los registros MX de la zona de DNS de su dominio apunten a su servidor de correo electrónico.

PELIGRO:

Una vez desactivado Spam and Malware Protection, no podrá seguir utilizando los siguientes servicios aunque se muestren como activados en Control Panel:

- Advanced Threat Protection (véase Estructura y funcionamiento de ATP en la página 381)
- Compliance Filter (véase Acerca de Compliance Filter en la página 516)
- Content Control (véase Acerca de Content Control en la página 500)
- Continuity Service (véase Sobre Continuity Service en la página 636)
- Email Authentication (véase Acerca de Email Authentication en la página 407)
- Quarantine Report (véase Acerca de Quarantine Report en la página 445)

Importante:

Una vez desactivado Spam and Malware Protection para el dominio principal, ya no podrán modificarse sus configuraciones para los dominios alias. Por tanto, asegúrese de haber configurado Spam and Malware Protection correctamente para los dominios alias antes de desactivarlo para el dominio principal.

Comunique al soporte técnico o a su interlocutor que desea desactivar Spam and Malware Protection para el dominio principal o para un dominio alias.

El servicio técnico tramita la solicitud de desactivación.

Importante:

La desactivación de Spam and Malware Protection no supone la rescisión del contrato sobre dicho servicio. Para rescindir un contrato deberá ponerse en contacto con su interlocutor.

Spam and Malware Protection se ha deshabilitado.

Content Control

Acerca de Content Control

Content Control permite a administradores a nivel de cliente administrar el tratamiento de archivos adjuntos de correos entrantes y salientes.

Antes de poder utilizar Content Control, es preciso que un administrador a nivel de cliente lo active (véase Activar Content Control en la página 502). A continuación, los administradores a nivel de cliente pueden configurar Content Control (véase Configurar Content Control en la página 506).

Los administradores a nivel de cliente pueden determinar un tamaño máximo de correo. Los correos que superen dicho tamaño se filtrarán. A continuación, los administradores pueden decidir los tipos de archivos adjuntos que se han de filtrar. Es posible seleccionar los siguientes tipos de archivos adjuntos:

- Archivos adjuntos cifrados
- Archivos adjuntos ejecutables
- Archivos de Office con macros

Además, los administradores pueden prohibir tipos de archivo en función de su extensión. Los tipos de archivo prohibidos pueden definirse tanto para archivos adjuntos sueltos como para archivos dentro de archivos comprimidos. Además, es posible emplear categorías (véase Lista de categorías en la página 501) para prohibir varios tipos de archivo al mismo tiempo.

Los administradores a nivel de cliente pueden decidir entre poner los correos filtrados en cuarentena o entregarlos a sus destinatarios quitándoles primero los archivos adjuntos. En este segundo caso, se informa a los destinatarios de que los archivos adjuntos se han quitado.

Los ajustes pueden realizarse tanto para todos los buzones de correo de un dominio como para grupos de buzones de correo (véase "Grupos" en el manual de Control Panel). Para realizar ajustes para un grupo, éste debe añadirse antes a Content Control (véase Añadir un grupo a Content Control en la página 503). En Content Control, los grupos se ordenan por prioridad y se procesan en dicho orden. Si un buzón de correo pertenece a varios grupos, se le aplicará la configuración del grupo que tenga la mayor prioridad. Los administradores pueden modificar las prioridades de los grupos (véase Modificar prioridades de grupos en la página 511). Si se desea volver a aplicar la configuración general del dominio a los buzones de correo de un grupo, los administradores pueden eliminar dicho grupo de Content Control (véase Eliminar un grupo de Content Control en la página 513).

Lista de categorías

La siguiente tabla muestra las categorías por las que los administradores a nivel de cliente pueden filtrar archivos adjuntos de determinados tipos en Content Control (véase Acerca de Content Control en la página 500).

CATEGORÍA	TIPOS DE ARCHIVO RETIRADOS
.executable	.action .apk .app .bas .bat .bin .cab .chm .cmd .com .command .cpl .csh .dll .exe .gadget .hta .inf .ins .inx .ipa .isu .job .jar .js .jse .ksh .lnk .msc .msi .msp .mst .osx .paf .pcd .pif .prg .ps1 .reg .rgs .run .scr .sct .sh .shb .shs .u3p .vb .vba .vbe .vbs .vbscript. vbx .workflow .ws .wsc .wsf .wsh
.mediafile	.aif .flv .mp1 .mid .mp5 .mpa .wma .mp2 .mpe .swf .wmf .wav .mp4 .wmv .mpg .avi .mov .mp3 .mpv2 .mp2v .aiff .mpeg
.docmacro	Archivos de Microsoft Word con macros. Los archivos de Microsoft Word adjuntos se analizan

CATEGORÍA	TIPOS DE ARCHIVO RETIRADOS
	en cuanto a patrones de macros mediante un método heurístico. Este filtro no abarca todos los tipos de macro.
.xlsmacro	Archivos de Microsoft Excel con macros. Los archivos de Microsoft Excel adjuntos se analizan en cuanto a patrones de macros mediante un método heurístico. Este filtro no abarca todos los tipos de macro.
.pptmacro	Archivos de Microsoft PowerPoint con macros. Los archivos de Microsoft PowerPoint adjuntos se analizan en cuanto a patrones de macros mediante un método heurístico. Este filtro no abarca todos los tipos de macro.

Activar Content Control

Ha activado Spam and Malware Protection (véase "Activar Spam and Malware Protection" en el manual de Control Panel).

En el módulo **Configuración de seguridad** > **Content Control** puede activar Content Control (véase Acerca de Content Control en la página 500) para administrar el tratamiento de archivos adjuntos de correos entrantes y salientes para los usuarios de un dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Content Control**.

4. Accione el interruptor **Activar Content Control**.

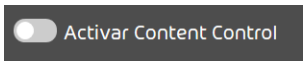


Figura 349: Activar Content Control

El interruptor se pone verde.

Content Control se ha activado para el dominio seleccionado. La configuración por defecto de Content Control se aplica a todos los usuarios del dominio.

A continuación puede realizar la configuración general de Content Control para el dominio (véase Configurar Content Control en la página 506). Si desea realizar ajustes para grupos, deberá añadir antes grupos a Content Control (véase Añadir un grupo a Content Control en la página 503). Si no desea seguir empleando Content Control, puede desactivarlo (véase Desactivar Content Control en la página 514).

Añadir un grupo a Content Control

Ha activado Content Control (véase Activar Content Control en la página 502). Ha creado un grupo dentro del dominio (véase "Crear un grupo" en el manual de Control Panel).

Los ajustes del módulo **Content Control** se aplican por defecto a todos los usuarios del dominio. Sin embargo, en el módulo **Configuración de seguridad** > **Content Control** puede añadir un grupo a Content Control para poder configurar Content Control para dichos grupos de un modo distinto al establecido para el resto de usuarios del dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee añadir un grupo a Content Control.
3. Vaya a **Configuración de seguridad** > **Content Control**.

4. Haga clic en el menú desplegable bajo **Grupos afectados**.

Figura 350: Seleccionar un grupo

El menú desplegable se abre. El menú desplegable contiene los grupos del dominio.

5. En el menú desplegable, seleccione el grupo que desee añadir a Content Control.

6. Haga clic en **Añadir**.

El grupo se añade a la lista de grupos de abajo. El grupo se añade al final de la lista.

> **Nota:**
>
> Los grupos están ordenados por prioridad. Las prioridades se indican en la columna **Prioridad**. Cuanto menor es el número, mayor es la prioridad de un grupo. Si un buzón de correos pertenece a varios grupos añadidos al módulo **Content Control**, se le aplicarán las reglas del grupo que tenga la prioridad más alta. Las prioridades de los grupos se pueden modificar (véase Modificar prioridades de grupos en la página 511).

Figura 351: Lista de grupos

Se ha añadido un grupo a Content Control.

A continuación puede configurar Content Control para el grupo (véase Configurar Content Control en la página 506), modificar la prioridad del grupo (véase Modificar prioridades de grupos en la página 511) o eliminar el grupo de Content Control (véase Eliminar un grupo de Content Control en la página 513).

Configurar Content Control

Ha activado Content Control (véase Activar Content Control en la página 502).

En el módulo **Configuración de seguridad** > **Content Control** puede configurar Content Control. Puede modificar los ajustes por defecto del dominio y los ajustes para los grupos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Content Control**.
4. En **Grupos afectados** elija si desea modificar la configuración por defecto o los ajustes de un grupo.

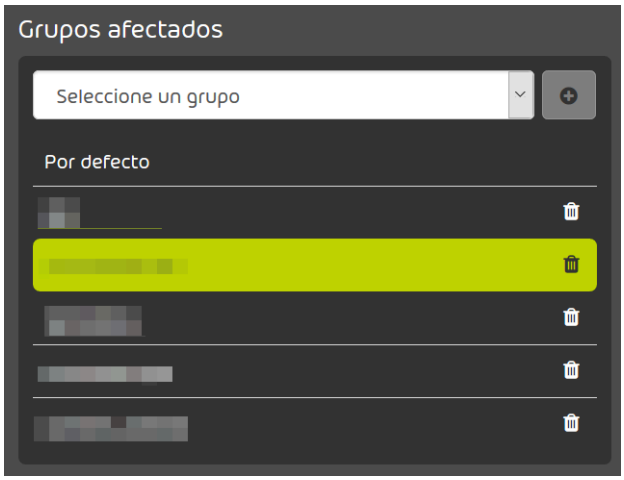


Figura 352: Seleccionar configuración por defecto o grupo

- Para modificar la configuración para todos los usuarios del dominio que no pertenecen a uno de los grupos enumerados, seleccione **Por defecto**.
- Para modificar la configuración para un grupo, seleccione el grupo.

Su selección se marca en verde.

5. Vaya a **Configuración** > **Para correos entrantes** para configurar Content Control para los correos entrantes.
6. En **Tamaño máx. de correo (MB)**, introduzca el tamaño máximo de correo en megabytes.

Figura 353: Indicar el tamaño máximo de correo

Nota:

El tamaño máximo de correo no deberá superar el límite de tamaño establecido por su servidor de correo electrónico. El tamaño máximo de correo se refiere a la carga útil del mismo. La carga útil se refiere al tamaño del correo y sus archivos adjuntos en el ordenador del destinatario. El tamaño real del correo, que incluye datos adicionales necesarios para la transmisión del mismo, puede ser aproximadamente un tercio mayor. Como el límite de tamaño establecido por su servidor de correo electrónico se refiere a dicho tamaño real, es preciso calcular el valor del campo **Tamaño máx. de correo (MB)** en función del tamaño máximo real. A modo orientativo se emplea un valor del 67% del tamaño máximo real.

Ejemplo: Si el límite de tamaño del servidor de destino es de 10 MB, deberá indicarse un tamaño máximo de correo de 6,7 MB en el campo.

Nota:

El campo **Tamaño máx. de correo (MB)** acepta valores de hasta 150 MB.

7. Haga clic en **Confirmar** para guardar los cambios.

8.

Nota:

Esta elección solo está disponible para correos entrantes. Los correos salientes con archivos adjuntos retirados se bloquean y el remitente recibe un mensaje de devolución.

En **Procedimiento en caso de archivos adjuntos retirados**, seleccione qué hacer con los correos que contengan archivos adjuntos retirados.

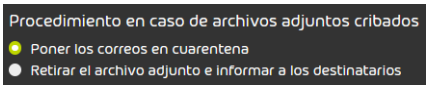


Figura 354: Seleccionar el tratamiento de archivos adjuntos retirados

- Para que los correos con archivos adjuntos retirados se pongan en cuarentena y no se entreguen a los destinatarios, seleccione **Poner los correos en cuarentena**.
- Para retirar los archivos adjuntos retirados de los correos y, en su lugar, entregar correos electrónicos con archivos adjuntos generados automáticamente en los que se hace referencia a los archivos adjuntos retirados, seleccione **Retirar el archivo adjunto e informar a los destinatarios**.

9. Seleccione qué archivos adjuntos se deben retirar. Para retirar archivos adjuntos, accione el interruptor correspondiente.

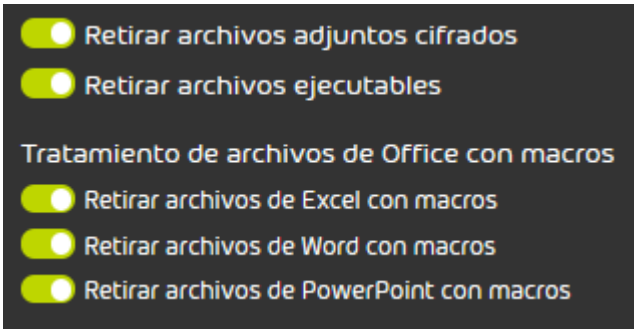


Figura 355: Retirar archivos adjuntos

- Seleccione **Retirar archivos adjuntos cifrados** para retirar archivos adjuntos cifrados con las siguientes extensiones de archivo:
  - .dot
  - .doc
  - .docx
  - .xls
  - .xlsx
  - .ppt
  - .pptx
  - .pdf
  - .zip
  - .rar
  - .7z
  - .gz
- Seleccione **Retirar archivos ejecutables** para retirar todos los archivos cifrados de los tipos incluidos en la categoría .executable (véase Lista de categorías en la página 501).
- Seleccione **Retirar archivos de Excel con macros** para retirar todos los archivos cifrados de los tipos incluidos en la categoría .xslmacro (véase Lista de categorías en la página 501).

- Seleccione **Retirar archivos de Word con macros** para retirar todos los archivos cifrados de los tipos incluidos en la categoría .docmacro(véase Lista de categorías en la página 501).
- Seleccione **Retirar archivos de PowerPoint con macros** para retirar todos los archivos cifrados de los tipos incluidos en la categoría .pptmacro (véase Lista de categorías en la página 501).

10.

Nota:

Puede emplear categorías para retirar grupos de tipos de archivos (véase Lista de categorías en la página 501).

Importante:

Content Control no solo comprueba las extensiones de los archivos, sino también sus tipos MIME. El tipo MIME puede no coincidir con la extensión del archivo.

Si se retiran archivos de tipo gzip, se retiran también todos los archivos con el tipo MIME application/gzip.

Figura 356: Ejemplo

Para retirar archivos adjuntos con otras extensiones de archivo, introduzca la extensión en el campo bajo el rótulo **Extensiones de archivo prohibidas (p. ej., ".jpg")** y haga clic en **Añadir**.

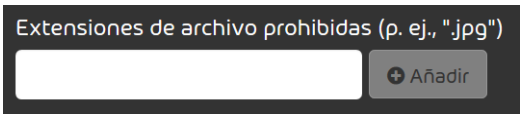


Figura 357: Retirar tipos de archivo

El tipo de archivo se añade a una lista mostrada abajo.

11. **Importante:**

    Content Control abre y escanea archivos comprimidos de tipo .rar, .zip y .7z. No se comprueban archivos comprimidos de otros tipos. En el caso de archivos comprimidos dentro de otros archivos comprimidos, Content Control los analiza hasta el cuarto nivel. Por nivel, Content Control analiza un máximo de 8 archivos comprimidos. Por correo electrónico, Content Control analiza un máximo de 1000 archivos en archivos comprimidos.

    Para retirar archivos de determinados tipos contenidos dentro de archivos comprimidos, proceda del siguiente modo.

    - Para adoptar los tipos de archivo de la lista de arriba, marque la casilla **Heredar extensiones de archivo prohibidas de arriba** bajo **Extensiones de archivo prohibidas en archivos comprimidos (p. ej., ".png")**.
    - Para retirar archivos con otras extensiones de archivo, introduzca la extensión en el campo bajo el rótulo **Extensiones de archivo prohibidas en archivos comprimidos (p. ej., ".png")** y haga clic en **Añadir**.

12. Vaya a **Configuración** > **Para correos salientes** para configurar Content Control para los correos salientes.
13. Configure Content Control para los correos salientes.
    - Para aplicar los ajustes para correos entrantes a los correos salientes, accione el interruptor **Utilizar la misma configuración que para los correos entrantes**.
    - Para ajustar Content Control para el correo saliente de un modo distinto que para el correo entrante, proceda del mismo modo que el descrito para los correos entrantes.

Content Control se ha configurado.

Modificar prioridades de grupos

Ha añadido varios grupos a Content Control (véase Añadir un grupo a Content Control en la página 503).

En el módulo **Configuración de seguridad** > **Content Control**, los grupos se ordenan por su prioridad. Las prioridades de los grupos se muestran en la columna **Prioridad** de la sección **Grupos afectados**. Cuanto menor es el número, mayor es la prioridad de un grupo. Si un buzón de correo pertenece a varios grupos añadidos al módulo **Configuración de seguridad** > **Content Control**, se le aplicarán las reglas del grupo que tenga la prioridad más alta. Puede modificar las prioridades de los grupos.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyos grupos desee modificar las prioridades en el módulo **Content Control**.
3. Vaya a **Configuración de seguridad** > **Content Control**.
4. En **Grupos afectados**, seleccione el grupo cuya prioridad desee cambiar.
5. Opcional: Cambie la prioridad del grupo desplazándolo a otra posición de la lista.
   a) Haga clic en los seis puntos junto al grupo y mantenga el botón izquierdo del ratón pulsado.

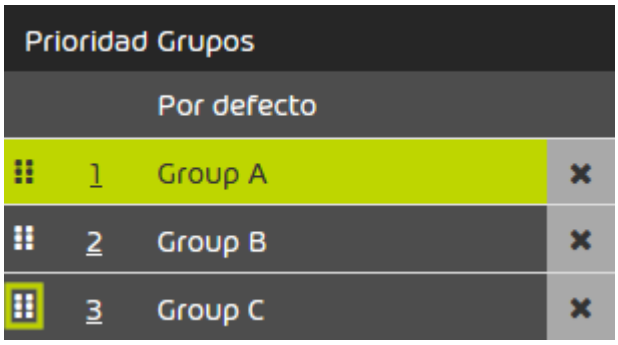


Figura 358: Desplazar un grupo

   b) Desplace el grupo hasta la posición correspondiente a la prioridad deseada.
   c) Suelte el botón izquierdo del ratón.

El grupo se deposita en la nueva posición. Las prioridades de todos los grupos que se hayan visto desplazados en la tabla se actualizan.

6. Sobrescriba la prioridad del grupo.

   a) Haga doble clic sobre la prioridad del grupo.

   El número se vuelve editable.

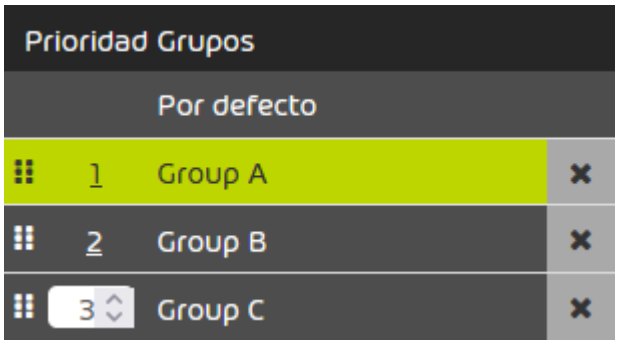


Figura 359: Campo de introducción de prioridad

   b) Introduzca el número correspondiente a la nueva prioridad en el campo o selecciónelo con las flechas.

   c) Confirme la nueva prioridad con la tecla Intro.

   La prioridad del grupo se guarda. El grupo se desplaza hasta la posición correspondiente a su nueva prioridad. Las prioridades de todos los grupos que se hayan visto desplazados en la tabla se actualizan.

Se han modificado las prioridades de los grupos.

Eliminar un grupo de Content Control

Ha añadido un grupo a Content Control (véase Añadir un grupo a Content Control en la página 503).

En el módulo **Configuración de seguridad** > **Content Control** puede eliminar un grupo de Content Control para volver a aplicar al mismo la configuración general de Content Control.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Content Control**.
4. Haga clic sobre la cruz junto al nombre del grupo.

Figura 360: Retirar un grupo

Se muestra un mensaje de advertencia.

5. Haga clic en **Confirmar**.

El grupo se elimina de Content Control.

Se ha eliminado un grupo de Content Control. Los ajustes por defecto de Content Control se aplican ahora a los miembros de dicho grupo.

Desactivar Content Control

Ha activado Content Control (véase Activar Content Control en la página 502).

En el módulo **Configuración de seguridad** > **Content Control** puede desactivar Content Control para un dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Content Control**.
4. Accione el interruptor **Activar Content Control**.

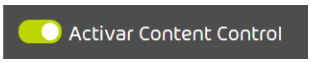


Figura 361: Desactivar Content Control

Se muestra un mensaje de advertencia.

5. Haga clic en **Confirmar** para eliminar definitivamente todos los ajustes de Content Control para el dominio.

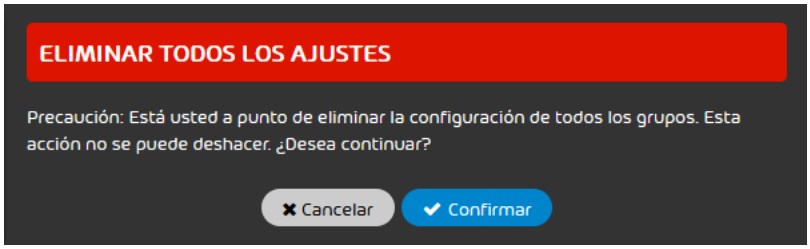


Figura 362: Confirmar

Content Control se ha desactivado para un dominio. Todos los ajustes de Content Control se han eliminado definitivamente para el dominio.

Compliance Filter

Acerca de Compliance Filter

Compliance Filter permite a los administradores a nivel de cliente definir reglas de filtrado propias para, por ejemplo, clasificar correos entrantes como **Limpio**, **Spam** o **Threat** (véase "Categorías de correo electrónico" en el manual de Control Panel). Además, le permite rechazar correos, desviarlos a través de otro servidor o reenviarlos a otros destinatarios. El lugar que ocupan las reglas de filtrado de Compliance Filter en la jerarquía de reglas de todos nuestros servicios se describe en Orden de las reglas de todos los servicios en la página 478.

PRECAUCIÓN:

Las reglas de filtrado incorrectas perjudican el tráfico de correo electrónico y pueden anular nuestros servicios.

Compliance Filter no es adecuado para reescribir direcciones.

Compliance Filter puede comprobar tanto correos entrantes como correos salientes. Después de activar Compliance Filter (véase Activar Compliance Filter en la página 519), los administradores a nivel de cliente pueden definir reglas de filtrado de los siguientes tipos:

- **Encabezado**
- **Cuerpo**
- **Avanzado**

En las condiciones de las reglas de filtrado es posible emplear expresiones regulares (véase Expresiones regulares en la página 570). Los administradores a nivel de cliente definen una acción para cada regla de filtrado. Esta acción se aplica automáticamente a los correos que satisfagan las especificaciones de la regla de filtrado. Para más información acerca de las reglas de filtrado, véase Reglas de filtrado en la página 520. En total pueden definirse hasta 1500 reglas de filtrado por cliente.

Además de reglas de filtrado para expresiones individuales, es posible crear reglas de filtrado complejas con ayuda de diccionarios, listas que pueden contener hasta 15000 expresiones literales

o hasta 1000 expresiones regulares (véase Diccionarios en la página 562). Los administradores a nivel de cliente pueden crear y mantener un máximo de 250 diccionarios por dominio principal. Los diccionarios reducen drásticamente el trabajo necesario para crear y mantener reglas de filtrado, especialmente contienen expresiones regulares.

Para poder activar y configurar Compliance Filter para un dominio, Spam and Malware Protection (véase "Spam and Malware Protection" en el manual de Control Panel) debe estar activado para el mismo.Al desactivar Spam and Malware Protection se desactiva también Compliance Filter, sin que sea posible configurarlo.

Los administradores a nivel de cliente pueden desactivar Compliance Filter si no desean continuar utilizándolo (véase Desactivar Compliance Filter en la página 584).

Orden de las reglas de todos los servicios

Las reglas de Spam and Malware Protection (véase "Spam and Malware Protection" en el manual de Control Panel) tienen determinada prioridad de procesamiento. En cuanto aplica una regla de alta prioridad, las reglas de menor prioridad dejan de procesarse. Esto puede provocar que un correo acabe bloqueado aunque la dirección de su remitente esté registrada en una lista blanca si la dirección IPv4 del servidor de origen se encuentra en la lista negra RBL.

Reglas en orden descendente de prioridad:

Correos entrantes

1. Lista RBL (bloquear)
2. Detección de spam masivo (bloquear)
3. Compliance Filter
4. Email Authentication (bloquear)
5. Pruebas para detectar contenido malicioso (poner en cuarentena)
6. Email Authentication (poner en cuarentena)
7. Content Control, si está activado (poner en cuarentena)

8. Uso de lista blanca de usuario (entregar)
9. Uso de lista negra de usuario (poner en cuarentena)
10. Uso de lista blanca de administrador (entregar)

> **Nota:**
>
> Las listas blancas de administrador son un caso particular entre las reglas. Pues los administradores pueden seleccionar los filtros a evitar para los registros de listas blancas a nivel de dominio (véase «Crear un registro de lista negra para un dominio» en el manual de Control Panel). Al ser procesados, los correos afectados omitirán los filtros seleccionados. Esto también incluye los filtros que preceden el uso de lista blanca de administrador en la lista. La posición en la cual se encuentra el uso de lista blanca de administrador dentro de la lista se refiere a la configuración por defecto de registros de listas blancas a nivel de dominio. Por defecto, los registros solo evitan el filtrado de spam.

11. Uso de lista negra de administrador (poner en cuarentena)
12. Uso de lista blanca general (entregar)
13. Reglas generales de spam (poner en cuarentena)
14. Filtro de infomail (poner en cuarentena)

> **Nota:**
>
> Compliance Filter (véase Acerca de Compliance Filter en la página 516) se aplica antes que Content Control (véase Acerca de Content Control en la página 500). Por tanto, los administradores pueden emplear reglas de Compliance Filter que clasifiquen correos como **Limpio** para crear excepciones para Content Control.
>
> Sin embargo, no es posible crear excepciones para Content Control mediante listas blancas o negras de usuario así como listas negras de administrador, ya que éstas se aplican después de Content Control. Solo listas blancas de administrador permiten evitar Content Control.

Correos salientes

1. Lista RBL
2. Compliance Filter
3. Pruebas para detectar contenido malicioso
4. Content Control, si está activado

Activar Compliance Filter

Ha activado Spam and Malware Protection para el dominio (véase "Activar Spam and Malware Protection" en el manual de Control Panel) para el que desee activar Compliance Filter.

En el módulo **Configuración de seguridad** > **Compliance Filter** puede activar Compliance Filter para poder crear sus propias reglas de filtrado de correos (véase Reglas de filtrado en la página 520).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Compliance Filter.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Accione el interruptor **Activar Compliance Filter**.

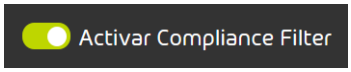


Figura 363: Activar Compliance Filter

Compliance Filter se activa.

Compliance Filter se ha activado. Una vez creadas reglas de filtrado, es posible emplear Compliance Filter.

A continuación puede crear reglas de filtrado (véase Reglas de filtrado en la página 520) y diccionarios (véase Diccionarios en la página 562) para Compliance Filter.

Reglas de filtrado

Compliance Filter comprueba los correos de un dominio. En el módulo **Compliance Filter**, los administradores a nivel de cliente pueden administrar reglas de filtrado para correos entrantes y salientes. Los administradores pueden crear reglas de filtrado para correos entrantes (véase Crear reglas de filtrado para correos entrantes en la página 521) y salientes (véase Crear reglas de filtrado para correos salientes en la página 528). Las reglas de filtrado creadas se muestran en dos tablas (véase Visualización de reglas de filtrado en la página 535).

Nota:

Es posible crear un máximo de 1500 reglas de filtrado por dominio principal.

Los administradores a nivel de cliente pueden seleccionar una acción (véase Acciones para reglas de filtrado en la página 537) para cada regla de filtrado. La acción se ejecuta tan pronto como la regla de filtrado se aplique a un correo.

Además, los administradores a nivel de cliente seleccionan un tipo (véase Tipos de reglas de filtrado en la página 540) para cada regla de filtrado. El tipo de regla de filtrado determina los correos a los que se aplicará la regla.

Una de las condiciones que se pueden emplear en reglas de filtrado es a quién se dirige el correo en cuestión. Si un correo se envía a varios destinatarios y hay una regla de filtrado que satisfagan algunos de estos destinatarios, la acción provocada por la regla solo afectará a la entrega del correo a los mismos. De este modo es posible ejecutar diferentes acciones para diferentes destinatarios de un mismo correo.

Los administradores a nivel de cliente pueden editar sus reglas de filtrado a posteriori (véase Editar reglas de filtrado en la página 547). Además, los administradores pueden cambiar la prioridad de las reglas de filtrado (véase Cambiar la prioridad de una regla de filtrado en la página 549). La prioridad determina el orden en el que se procesan las reglas de Compliance Filter. Para más

información acerca del orden de las reglas de filtrado de Compliance Filter, véase Orden de las reglas de filtrado en la página 551.

Si no se desea aplicar temporalmente alguna regla de filtrado, los administradores a nivel de cliente pueden desactivarla (véase Desactivar reglas de filtrado de Compliance Filter en la página 559). Las reglas de filtrado desactivadas pueden activarse de nuevo posteriormente (véase Activar reglas de filtrado en la página 558).

Si una regla de filtrado deja de ser necesaria, los administradores a nivel de cliente pueden eliminarla (véase Eliminar reglas de filtrado de Compliance Filter en la página 560).

Crear reglas de filtrado para correos entrantes

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede crear reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516) para correos entrantes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear la regla de filtrado.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.
5. En **Reglas para correos entrantes**, haga clic en **Añadir regla**.

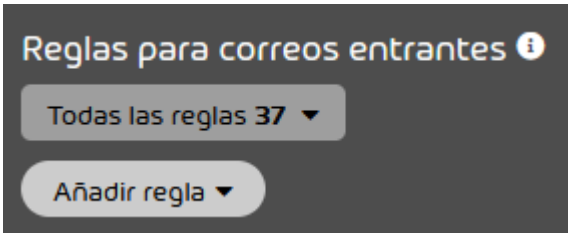


Figura 364: Añadir reglas

6. En **Acción**, elija qué hacer con los correos a los que se aplique la regla de filtrado. Puede elegir entre las siguientes acciones:

   - **Rechazar**
   - **Cambiar destinatario**
   - **Redirigir**
   - **Añadir BCC**
   - **Marcar como "Limpio"**
   - **Marcar como "Spam"**
   - **Marcar como "Threat"**

   Nota:

   En Acciones para reglas de filtrado en la página 537 encontrará una explicación de las acciones.

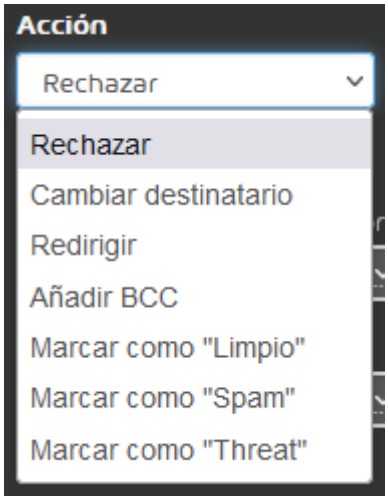


Figura 365: Seleccionar una acción

Si es necesario introducir datos adicionales para la acción seleccionada, aparecerá un campo adicional bajo el menú desplegable. Para más información acerca de los campos adicionales de las acciones, véase Acciones para reglas de filtrado en la página 537.

7. Seleccione en **Condiciones** el tipo de regla de filtrado. Tiene las siguientes opciones:

   - **Encabezado**: La regla de filtrado se aplica a todos los correos que contengan determinado término de búsqueda en su encabezado.
   - **Cuerpo**: La regla de filtrado se aplica a todos los correos que contengan determinado término de búsqueda en su cuerpo.
   - **Avanzado**: Puede determinar el remitente, el destinatario, la dirección IPv4 y el nombre de host de los correos. También puede definir términos de búsqueda para el asunto y los

archivos adjuntos de los correos, así como determinar un tamaño máximo de correo. La regla de filtrado atañe a todos los correos que presenten las características definidas.

Nota:

El tipo de regla de filtrado determina los correos a los que se aplicará la regla.

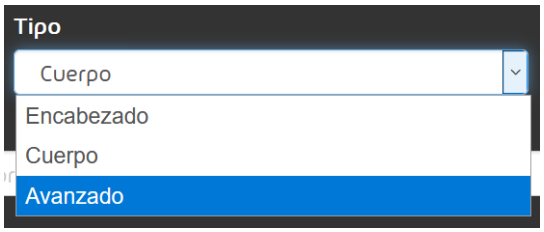


Figura 366: Seleccionar el tipo de regla de filtrado.

Bajo el menú desplegable se muestran campos para configurar la regla de filtrado. Los campos mostrados dependen del tipo de regla de filtrado seleccionado.

Nota:

En Tipos de reglas de filtrado en la página 540 encontrará una lista y explicaciones sobre los campos disponibles para cada tipo de regla de filtrado.

8. Si ha seleccionado el tipo **Avanzado**, siga los siguientes pasos:

   a) Seleccione en **Condiciones** la conjunción lógica aplicable entre las condiciones de la regla de filtrado. Tiene las siguientes opciones:

   - **Cumplir todas las condiciones**: Todas las condiciones seleccionadas deben cumplirse para que la regla de filtrado pueda aplicarse a un correo. Esta conjunción equivale a un AND lógico.
   - **Cumplir alguna condición**: Basta con que un correo cumpla una de la condiciones para que la regla de filtrado pueda aplicársele. Esta conjunción equivale a un OR lógico.

   b) Marque las casillas de las condiciones que desee emplear en la regla de filtrado.

   Los campos de las condiciones seleccionadas se habilitan.

   c) Si el campo de la condición seleccionada contiene un menú desplegable, elija el tipo de datos que desee introducir. Tiene las siguientes opciones:

   - **Expresión literal / regular**: El valor introducido se interpreta como una expresión literal o regular.
   - **Dentro de diccionario**: El valor introducido se interpreta como el nombre de un diccionario (véase Diccionarios en la página 562) vinculado a la condición. La condición se cumple si el valor del atributo correspondiente del correo coincide con alguno de los incluidos en el diccionario seleccionado.
   - **Fuera de diccionario**: El valor introducido se interpreta como el nombre de un diccionario (véase Diccionarios en la página 562) vinculado a la condición. La

condición se cumple si el valor del atributo correspondiente del correo no coincide con ninguno de los incluidos en el diccionario seleccionado.

d) Si ha elegido la condición **Remitente** o **Destinatario**, seleccione el campo del correo al que se refiere el valor introducido. Tiene las siguientes opciones:

- **Conforme al sobre**: El valor introducido debe coincidir con la dirección empleada como parámetro de **MAIL FROM:** (dirección del remitente) o **RCPT TO:** (dirección del destinatario) durante la transmisión del correo.
- **Conforme al encabezado**: El valor introducido debe coincidir con la dirección indicada en el campo **From** (dirección del remitente) o **To** (dirección del destinatario).
- **Conforme a ambos**: La dirección de remitente indicada debe, o bien haberse empleado como parámetro de **MAIL FROM:** o haberse indicado en el campo **From** del encabezado del correo. La dirección de destinatario indicada debe, o bien haberse empleado como parámetro de **RCPT TO:** o haberse indicado en el campo **To** del encabezado del correo.

9. En función del tipo de datos seleccionado, introduzca un término de búsqueda, un valor o el nombre de un diccionario en los campos de las condiciones.

> **Nota:**
>
> Los términos introducidos como expresiones literales o regulares se encontrarán incluso si están rodeados de texto.

> **Nota:**
>
> Para definir reglas más precisas y versátiles puede emplear expresiones regulares. Encontrará una descripción de la estructura y funcionalidad de las expresiones regulares en Expresiones regulares en la página 570 y Explicación de las expresiones regulares en la página 572. En Excepciones en las expresiones regulares en la página 580 encontrará una lista de caracteres prohibidos.
>
> Las expresiones regulares solo pueden emplearse en reglas de tipo **Avanzado**.

> **Nota:**
>
> En el campo **Mayor que**, introduzca el tamaño máximo de correo en megabytes.

10. Opcional: Introduzca una descripción de la regla de filtrado en **Descripción (opcional)**.

Figura 367: Describir reglas de filtrado

11. Haga clic en **Añadir**.

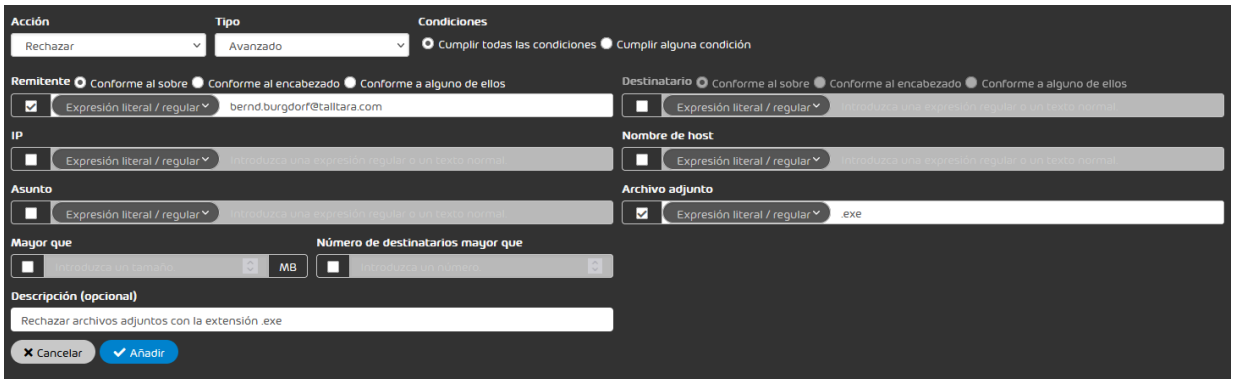


Figura 368: Añadir una regla de filtrado

La regla de filtrado se añade a la tabla bajo **Reglas para correos entrantes** (véase Visualización de reglas de filtrado en la página 535). La regla de filtrado obtiene la prioridad más baja de todas las presentes y se coloca al final de la tabla. La regla de filtrado se activa.

Se ha creado una regla de regla de filtrado para correos entrantes.

A continuación puede editar la regla filtrado (véase Editar reglas de filtrado en la página 547), modificar su prioridad (véase Cambiar la prioridad de una regla de filtrado en la página 549), desactivarla temporalmente (véase Desactivar reglas de filtrado de Compliance Filter en la página 559) o eliminarla (véase Eliminar reglas de filtrado de Compliance Filter en la página 560).

Crear reglas de filtrado para correos salientes

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede crear reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516) para correos salientes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear la regla de filtrado.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.
5. En **Reglas para correos salientes**, haga clic en **Añadir regla**.

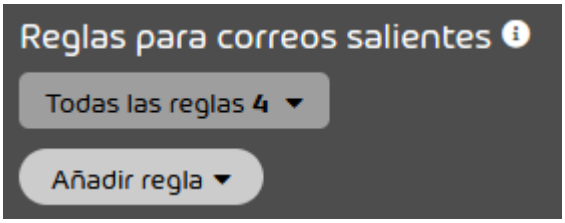


Figura 369: Añadir reglas

6. En **Acción**, elija qué hacer con los correos a los que se aplique la regla de filtrado. Puede elegir entre las siguientes acciones:

   - **Rechazar**
   - **Cambiar destinatario**
   - **Redirigir**
   - **Añadir BCC**
   - **Informar al remitente**

> **Nota:**
>
> En Acciones para reglas de filtrado en la página 537 encontrará una explicación de las acciones.

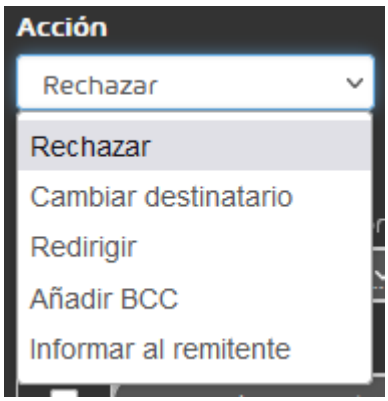


Figura 370: Seleccionar una acción

Si es necesario introducir datos adicionales para la acción seleccionada, aparecerá un campo adicional bajo el menú desplegable. Para más información acerca de los campos adicionales de las acciones, véase Acciones para reglas de filtrado en la página 537.

7. Seleccione el tipo de regla de filtrado en **Tipo**. Éste determina los correos a los que aplicar la regla de filtrado. Tiene las siguientes opciones:

   - **Encabezado**: La regla de filtrado se aplica a todos los correos que contengan determinado término de búsqueda en su encabezado.
   - **Cuerpo**: La regla de filtrado se aplica a todos los correos que contengan determinado término de búsqueda en su cuerpo.
   - **Avanzado**: Puede determinar el remitente, el destinatario, la dirección IPv4 y el nombre de host de los correos. También puede definir términos de búsqueda para el asunto y los archivos adjuntos de los correos, así como determinar un tamaño máximo de correo. La regla de filtrado atañe a todos los correos que presenten las características definidas.

Nota:

El tipo de regla de filtrado determina los correos a los que se aplicará la regla.

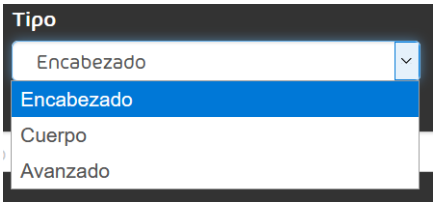


Figura 371: Seleccionar el tipo de regla de filtrado.

Bajo el menú desplegable se muestran campos para configurar la regla de filtrado. Los campos mostrados dependen del tipo de regla de filtrado seleccionado.

Nota:

En Tipos de reglas de filtrado en la página 540 encontrará una lista y explicaciones sobre los campos disponibles para cada tipo de regla de filtrado.

8. Si ha seleccionado el tipo **Avanzado**, siga los siguientes pasos:

   a) Seleccione en **Condiciones** la conjunción lógica aplicable entre las condiciones de la regla de filtrado. Tiene las siguientes opciones:

   - **Cumplir todas las condiciones**: Todas las condiciones seleccionadas deben cumplirse para que la regla de filtrado pueda aplicarse a un correo. Esta conjunción equivale a un AND lógico.
   - **Cumplir alguna condición**: Basta con que un correo cumpla una de la condiciones para que la regla de filtrado pueda aplicársele. Esta conjunción equivale a un OR lógico.

   b) Marque las casillas de las condiciones que desee emplear en la regla de filtrado.

   Los campos de las condiciones seleccionadas se habilitan.

   c) Si el campo de la condición seleccionada contiene un menú desplegable, elija el tipo de datos que desee introducir. Tiene las siguientes opciones:

   - **Expresión literal / regular**: El valor introducido se interpreta como una expresión literal o regular.
   - **Dentro de diccionario**: El valor introducido se interpreta como el nombre de un diccionario (véase Diccionarios en la página 562) vinculado a la condición. La condición se cumple si el valor del atributo correspondiente del correo coincide con alguno de los incluidos en el diccionario seleccionado.
   - **Fuera de diccionario**: El valor introducido se interpreta como el nombre de un diccionario (véase Diccionarios en la página 562) vinculado a la condición. La

condición se cumple si el valor del atributo correspondiente del correo no coincide con ninguno de los incluidos en el diccionario seleccionado.

d) Si ha elegido la condición **Remitente** o **Destinatario**, seleccione el campo del correo al que se refiere el valor introducido. Tiene las siguientes opciones:

- **Conforme al sobre**: El valor introducido debe coincidir con la dirección empleada como parámetro de **MAIL FROM:** (dirección del remitente) o **RCPT TO:** (dirección del destinatario) durante la transmisión del correo.
- **Conforme al encabezado**: El valor introducido debe coincidir con la dirección indicada en el campo **From** (dirección del remitente) o **To** (dirección del destinatario).
- **Conforme a ambos**: La dirección de remitente indicada debe, o bien haberse empleado como parámetro de **MAIL FROM:** o haberse indicado en el campo **From** del encabezado del correo. La dirección de destinatario indicada debe, o bien haberse empleado como parámetro de **RCPT TO:** o haberse indicado en el campo **To** del encabezado del correo.

9. En función del tipo de datos seleccionado, introduzca un término de búsqueda, un valor o el nombre de un diccionario en los campos de las condiciones.

> **Nota:**
>
> Los términos introducidos como expresiones literales o regulares se encontrarán incluso si están rodeados de texto.

> **Nota:**
>
> Para definir reglas más precisas y versátiles puede emplear expresiones regulares. Encontrará una descripción de la estructura y funcionalidad de las expresiones regulares en Expresiones regulares en la página 570 y Explicación de las expresiones regulares en la página 572. En Excepciones en las expresiones regulares en la página 580 encontrará una lista de caracteres prohibidos.
>
> Las expresiones regulares solo pueden emplearse en reglas de tipo **Avanzado**.

> **Nota:**
>
> En el campo **Mayor que**, introduzca el tamaño máximo de correo en megabytes.

10. Opcional: Introduzca una descripción de la regla de filtrado en **Descripción (opcional)**.

Figura 372: Describir reglas de filtrado

11. Haga clic en **Añadir**.

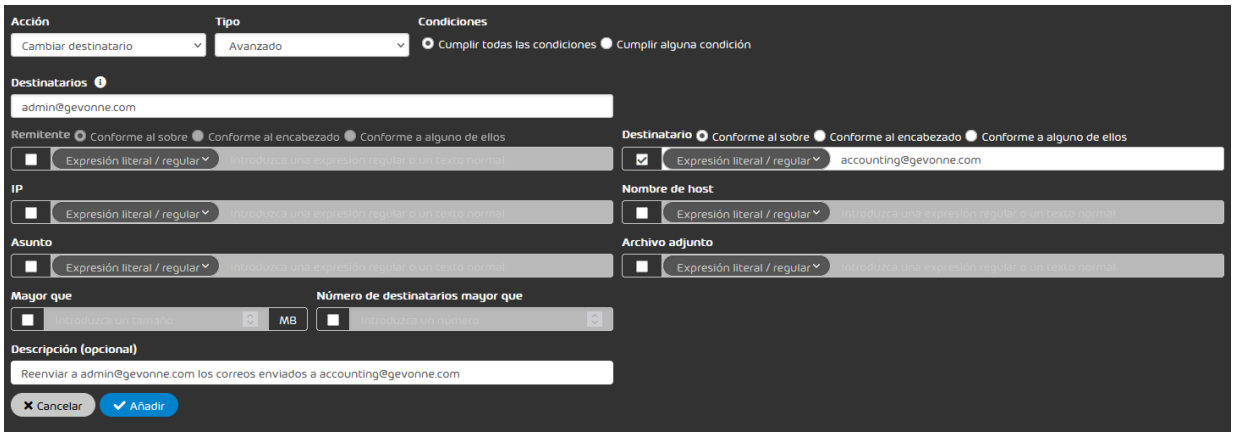


Figura 373: Añadir una regla de filtrado

La regla de filtrado se añade a la tabla bajo **Reglas para correos salientes** (véase Visualización de reglas de filtrado en la página 535). La regla de filtrado obtiene la prioridad más baja de todas las presentes y se coloca al final de la tabla. La regla de filtrado se activa.

Se ha creado una regla de regla de filtrado para correos salientes.

A continuación puede editar la regla filtrado (véase Editar reglas de filtrado en la página 547), modificar su prioridad (véase Cambiar la prioridad de una regla de filtrado en la página 549), desactivarla temporalmente (véase Desactivar reglas de filtrado de Compliance Filter en la página 559) o eliminarla (véase Eliminar reglas de filtrado de Compliance Filter en la página 560).

Visualización de reglas de filtrado

Tras su creación, las reglas de filtrado para correos entrantes y salientes se muestran en sus tablas correspondientes de las secciones **Reglas para correos entrantes** y **Reglas para correos salientes**.

Ambas tablas contienen las siguientes columnas:

- **Prioridad**: Prioridad de aplicación de la regla de filtrado. Cuanto menor sea el número en este campo, antes se aplicará la regla de filtrado. Las reglas de filtrado se muestran en la tabla por orden descendente de prioridad.
- **Activo**: Si esta casilla está marcada, significa que la regla de filtrado se encuentra activada.
- **Acción**: Aquí se indica la acción que ejecuta la regla de filtrado.
  - Acciones para correos entrantes: **Cambiar destinatario**, **Redirigir**, **Añadir BCC**, **Marcar como "Limpio"**, **Marcar como "Spam"**, **Marcar como "Threat"**.
  - Acciones para correos salientes: **Rechazar**, **Cambiar destinatario**, **Redirigir**, **Añadir BCC**, **Informar al remitente**.

  Nota:

  Las acciones disponibles se describen en el capítulo Acciones para reglas de filtrado en la página 537.
- **Tipo**: Aquí se indica el tipo de regla de filtrado.
- **Condiciones**: Aquí se indican las condiciones de filtrado en el idioma de sistema seleccionado. Si en un regla avanzada se hace referencia a un diccionario, se indica con la abreviatura **D**. La regla del siguiente ejemplo tiene en cuenta los remitentes del diccionario **forbiddensenders**: **Remitente: ?A=?D=forbiddensenders**. También es posible negar los registros de un

diccionario: La regla del siguiente ejemplo no tiene en cuenta los remitentes del diccionario **forbiddensenders**: **Remitente: ?A=?D!=forbiddensenders**.

> **Nota:**
>
> Además, en las condiciones de filtrado **Remitente** y **Destinatario** se indica el campo o campos al que se refiere el valor introducido (**Conforme al sobre**, **Conforme al encabezado** y **Conforme a ambos**, tal y como se describen en el capítulo Tipos de reglas de filtrado en la página 540). Dichos campos se indican con las abreviaturas **E** (de **Envelope**, "sobre" en inglés), **H** (de **Header**, "encabezado") y **A** (de **Any**, "cualquiera") independientemente del idioma.
>
> Por ejemplo, si en una regla se indica **Remitente:?E=mueller@gevonne.com**, quiere decir que debe aplicarse a correos con el remitente de sobre **mueller@gevonne.com**.

- **Descripción**: Descripción aportada por el autor de la regla de filtrado.
- **ID**: Identificador de la regla de filtrado asignado automáticamente por el sistema.

Acciones para reglas de filtrado

Cada regla de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516) tiene asignada una acción. Dicha acción se ejecuta tan pronto como una regla de filtro es aplicable a un correo.

Hay diversas disponibles para correos entrantes y salientes.

Las siguientes acciones solo están disponibles para correos entrantes:

- **Marcar como "Limpio"**
- **Marcar como "Spam"**
- **Marcar como "Threat"**

La acción **Informar al remitente** solo está disponible para correos salientes.

En la siguiente tabla se describen todas las acciones para las reglas de filtro del módulo **Compliance Filter**. Si se elige una acción que requiera datos adicionales en el módulo **Compliance Filter**, se muestra un campo adicional para la misma. Estos campos también están descritos en la tabla.

Tabla 27: Acciones para reglas de filtrado

ACCIÓN	DESCRIPCIÓN
Rechazar	**Atención:** El correo se rechaza. El servidor de correo de origen es informado sobre la interrupción de la conexión mediante un código de error y un texto (**554 5.6.9 customer rule based reject by Compliance-Filter**). Para más información, véase "Motivos de clasificación" en el manual de Control Panel. Corresponde al servidor de correo de origen informar al remitente.

ACCIÓN	DESCRIPCIÓN
Cambiar destinatario	En lugar de entregarse al destinatario original, el correo electrónico se entrega en una o varias direcciones de correo electrónico distintas. Si se elige esta acción, se muestra el campo **Enviar correo a:**. En este campo, los administradores a nivel de cliente deben introducir las direcciones de correo electrónico a las que reenviar el correo. Los administradores pueden introducir tantas direcciones de correo electrónico en el campo como deseen. Si se introducen varias direcciones de correo electrónico, deberán separarse con punto y coma.
Redirigir	El correo se desvía a través de otra dirección IPv4 o nombre de host. Si se elige esta acción, se muestra el campo **IP o nombre de host**. En este campo, los administradores a nivel de cliente deben introducir la dirección IPv4 o el nombre de host a través del cual desviar el correo. Los administradores solo pueden introducir una dirección IPv4 o un nombre de host.

ACCIÓN	DESCRIPCIÓN
Añadir BCC	Al correo se le añaden automáticamente uno o varios destinatarios en BCC. Si se elige esta acción, se muestra el campo **Enviar correo a:**. En este campo, los administradores a nivel de cliente deben introducir las direcciones de correo electrónico a las que enviar copias ocultas del correo electrónico. Los administradores pueden introducir tantas direcciones de correo electrónico en el campo como deseen. Si se introducen varias direcciones de correo electrónico, deberán separarse con punto y coma.
Informar al remitente	El remitente será informado por correo electrónico tan pronto como el correo saliente haya sido aceptado por el servidor de destino.
Marcar como "Limpio"	El correo entrante se clasifica como **Limpio**.
Marcar como "Spam"	El correo entrante se clasifica como **Spam**.
Marcar como "Threat"	El correo entrante se clasifica como **Threat**.

Tipos de reglas de filtrado

Durante la creación de reglas de filtrado en el módulo **Compliance Filter** (véase Acerca de Compliance Filter en la página 516), los administradores a nivel de cliente deben seleccionar el tipo de las mismas. El tipo de regla de filtrado permite a los administradores determinar las características de los correos a los que aplicar cada regla. En el módulo **Compliance Filter** aparecen campos relativos a diversas características para cada tipo de regla de filtrado.

Las siguientes tablas muestran todos los campos disponibles para cada tipo de regla de filtrado. Las tablas contienen descripciones de las características y ejemplos de posibles valores.

Nota:

Para definir reglas más precisas y versátiles es posible emplear expresiones regulares. La estructura y funcionalidad de las expresiones regulares se describen en Expresiones regulares en la página 570 y Explicación de las expresiones regulares en la página 572. El capítulo Excepciones en las expresiones regulares en la página 580 contiene una lista de caracteres prohibidos.

Nota:

Para simplificar la administración de las condiciones, los administradores a nivel de cliente pueden crear diccionarios con múltiples expresiones. Los diccionarios pueden vincularse a las condiciones de las reglas de filtrado introduciendo sus nombres en sus campos. Para más información sobre el funcionamiento, la creación y la administración de diccionarios, véase Diccionarios en la página 562.

Tabla 28: Tipo Encabezado

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Filtro: encabezado	El término de búsqueda introducido se busca en el encabezado del correo.	Factura

Tabla 29: Tipo Cuerpo

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Filtro: cuerpo	El término de búsqueda introducido se busca en el cuerpo descodificado del correo. **Nota:** Los archivos adjuntos no se examinan durante la búsqueda en el cuerpo del correo.	Orden de pago

Tabla 30: Tipo Avanzado

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Remitente	El término de búsqueda o las expresiones del diccionario asignado (véase Diccionarios en la página 562) se buscan en la dirección de remitente del correo. **Nota:** Los administradores a nivel de cliente pueden elegir entre las siguientes opciones en qué tipo de dirección de remitente buscar (véase Crear reglas de filtrado para correos entrantes): • **Conforme al sobre**: Dirección de remitente en el sobre (**MAIL FROM:**) • **Conforme al encabezado**: Dirección de remitente en el encabezado (**To:**) • **Conforme a ambos**: Ambas direcciones de remitente	**user@gevonne.com**

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Destinatario	El término de búsqueda o las expresiones del diccionario asignado se buscan en la dirección del destinatario. **Nota:** Los administradores a nivel de cliente pueden elegir entre las siguientes opciones en qué tipo de dirección de destinatario buscar (véase Crear reglas de filtrado para correos entrantes): • **Conforme al sobre**: Dirección de destinatario en el sobre (**RCPT TO:**) • **Conforme al encabezado**: Dirección de destinatario en el encabezado (**From:**) • **Conforme a ambos**: Ambas direcciones de destinatario **Nota:** Si se envía un correo a varios destinatarios y alguna regla de filtrado es aplicable	**user.extern@yahoo.com**

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
IP	El término de búsqueda o las expresiones del diccionario asignado se buscan en la dirección IPv4 pública del servidor de correo de origen. **Nota:** Introduzca como término de búsqueda la dirección IPv4 sin máscara de subred.	Bien: **0.0.0.0** Mal: **0.0.0.0/24**
Nombre de host	El término de búsqueda o las expresiones del diccionario asignado se buscan en el nombre de host (registro PTR) obtenido mediante resolución inversa de la dirección IPv4 del servidor de correo. Dependiendo de si la regla es para correos entrantes o salientes, se tratará del nombre de host del servidor de origen o destino.	**mailserver.domain.com**
Asunto	El término de búsqueda o las expresiones del diccionario asignado se buscan en el asunto del correo.	**Spam**

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Archivo adjunto	El término de búsqueda o las expresiones del diccionario asignado se buscan en los nombres y extensiones de los archivos adjuntos. **Nota:** Es posible buscar por la extensión o por una parte del nombre del archivo. Para buscar por extensión, ésta deberá introducirse como término de búsqueda. Para buscar por parte de nombre del archivo, ésta deberá introducirse como término de búsqueda. **Nota:** Para Compliance Filter no es posible emplear categorías de archivos adjuntos.	**.jpg** **express**

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Mayor que	Se comprueba si el correo supera el tamaño indicado. **Nota:** El tamaño máximo de correo se indica en megabytes.	**500**
Número de destinatarios mayor que	Se comprueba si la cantidad de destinatarios supera el valor indicado.	**10**

Editar reglas de filtrado

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 521 o Crear reglas de filtrado para correos salientes en la página 528).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede editar reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.

5. En la lista de reglas de filtrado para correos entrantes o salientes, haga clic en la flecha de menú junto a la regla de filtrado que desee editar.

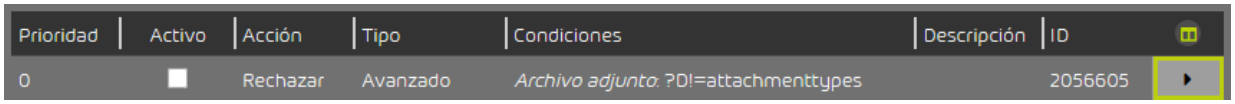


Figura 374: Abrir el menú

6. Haga clic en **Editar regla**.

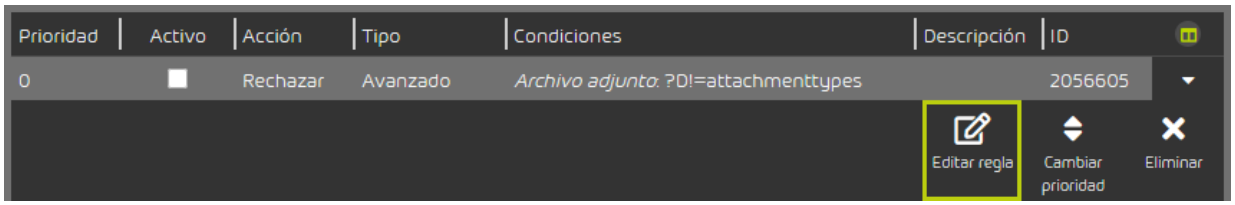


Figura 375: Editar reglas de filtrado

Se abre un menú con la configuración actual de la regla de filtrado.

7. Ajuste la configuración del modo deseado.

> **Nota:**
>
> Para más información, véase Crear reglas de filtrado para correos entrantes en la página 521 o Crear reglas de filtrado para correos salientes en la página 528.

8. Haga clic en **Aplicar cambios**.

Figura 376: Aplicar los cambios

Los cambios se aplican.

Se ha editado una regla de filtrado.

Cambiar la prioridad de una regla de filtrado

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 521 o Crear reglas de filtrado para correos salientes en la página 528).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede modificar el orden en que se procesan las reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516). Para modificar el orden de las reglas de filtrado, cambie su prioridad.

Importante:

El orden en que se procesan las reglas de filtrado de Compliance Filter depende tanto de la prioridad de las mismas como de su tipo (véase Orden de las reglas de filtrado en la página 551).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.
5. Haga clic en la lista de reglas de filtrado para correos entrantes o salientes en la flecha de menú junto a la regla de filtrado cuya prioridad desee cambiar.

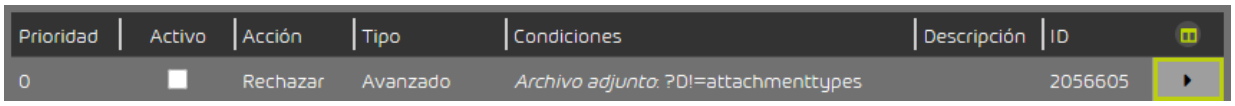


Figura 377: Abrir el menú

Se abre un menú.

6. Haga clic en **Cambiar prioridad**.

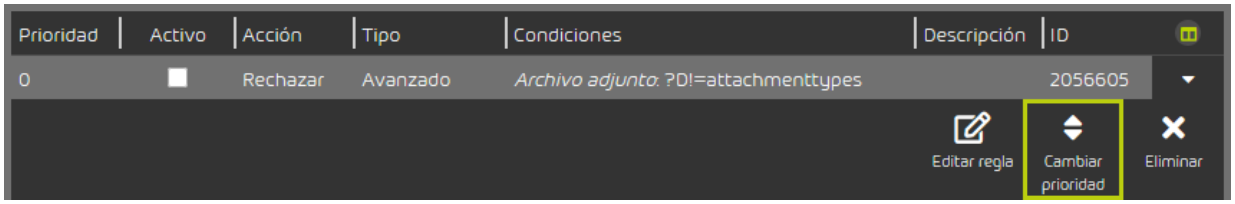


Figura 378: Cambiar la prioridad

Se abre un menú.

7. Introduzca la nueva prioridad de la regla de filtrado en **Prioridad**.

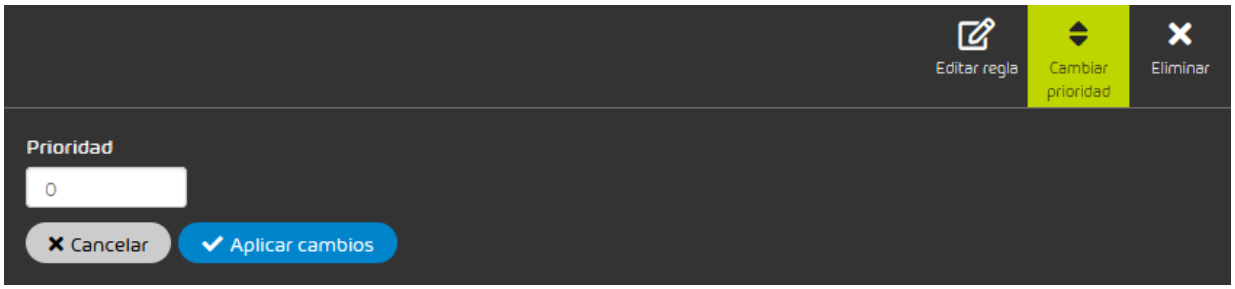


Figura 379: Indicar la prioridad

8. Haga clic en **Aplicar cambios**.

La nueva prioridad se asigna a la regla de filtrado. La regla de filtrado se mueve hasta la posición de la lista correspondiente a la nueva prioridad.

Se ha cambiado la prioridad de una regla de filtrado. De este modo, ha cambiado el orden en que se procesan las reglas de filtrado.

Orden de las reglas de filtrado

Importante:

Tenga en cuenta la posición en la que se encuentra Compliance Filter dentro de nuestra lista de servicios (véase Orden de las reglas de todos los servicios en la página 478). Tan pronto como una regla de un servicio se aplica a un correo, se detiene el procesamiento de reglas posteriores. Al correo en cuestión no se le aplica ninguna regla más.

Debido a este orden, es posible crear excepciones para Content Control con reglas de Compliance Filter que clasifiquen correos como **Limpio**.

Las reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516) se procesan conforme a su tipo (véase Tipos de reglas de filtrado en la página 540) en el siguiente orden:

1. **Cuerpo**
2. **Encabezado**
3. **Avanzado**

Figura 380: Orden de las reglas de filtrado por tipo

Las reglas de filtrado del mismo tipo se ordenan por prioridad y se procesan en dicho orden.

Nota:

Cuanto mayor sea su número, menor será la prioridad de una regla de filtrado.

Los administradores a nivel de cliente pueden modificar la prioridad de las reglas de filtrado (véase Cambiar la prioridad de una regla de filtrado en la página 549).

Los siguientes ejemplos ilustran el orden de procesamiento de las reglas.

Procesamiento sencillo de las reglas de filtrado.

Situación inicial:

Un administrador a nivel de cliente ha definido reglas de filtrado para Compliance Filter. No hay otras reglas aplicables al supuesto.

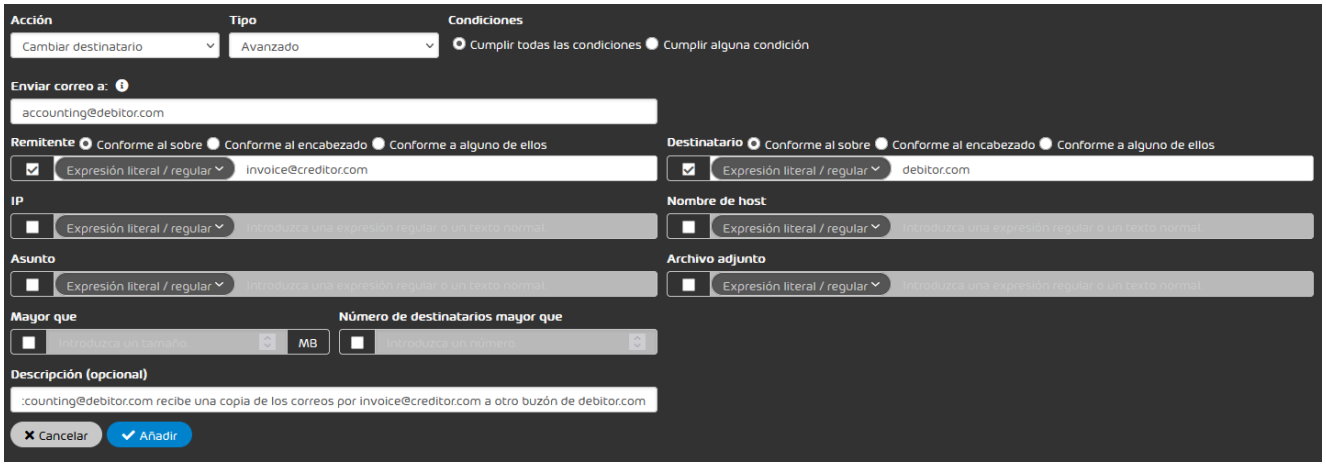


Figura 381: Regla de filtrado: Reenviar

Procedimiento:

1. Un correo de **invoice@creditor.com** se envía a un usuario cualquiera del dominio debitor.com.
2. Compliance Filter busca primero entre las reglas de filtrado de tipo **Cuerpo**, luego entre aquéllas de tipo **Encabezado** y, finalmente, encuentra una coincidencia entre las reglas de filtrado de tipo **Avanzado**.
3. La regla de filtrado se aplica. Compliance Filter no sigue buscando coincidencias con otras reglas de filtrado.

Conflicto entre varias reglas de filtrado del mismo tipo

Situación inicial:

Un administrador a nivel de cliente ha definido dos reglas de filtrado de Compliance Filter distintas de tipo **Avanzado** para el caso de que se envíe un correo saliente a **sales@creditor.com**. Ambas reglas de filtrado disponen que se añada un destinatario en copia oculta al correo. En una regla de filtrado se ha designado como destinatario en copia oculta la dirección **purchasing@creditor.com**, mientras que, en la otra, se ha designado **ceo@creditor.com**. La regla de filtrado con el destinatario **purchasing@creditor.com** tiene una prioridad superior a la de aquélla con el destinatario **ceo@creditor.com** y se encuentra por encima de ella en la lista de reglas de filtrado. No hay más reglas de filtrado aplicables al supuesto.

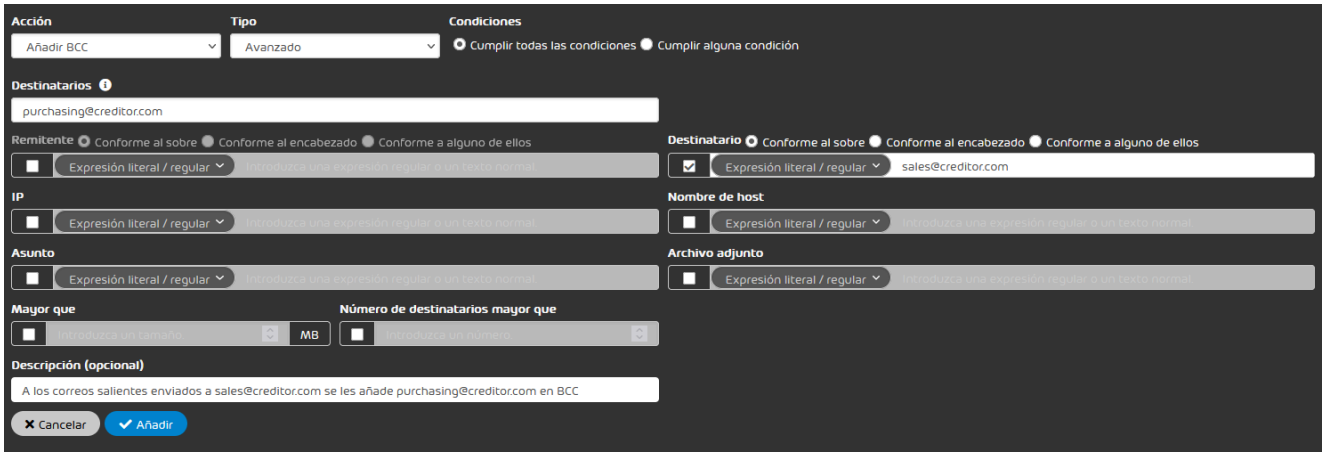


Figura 382: Regla de filtrado: añadir purchasing@creditor.com como destinatario de copia oculta

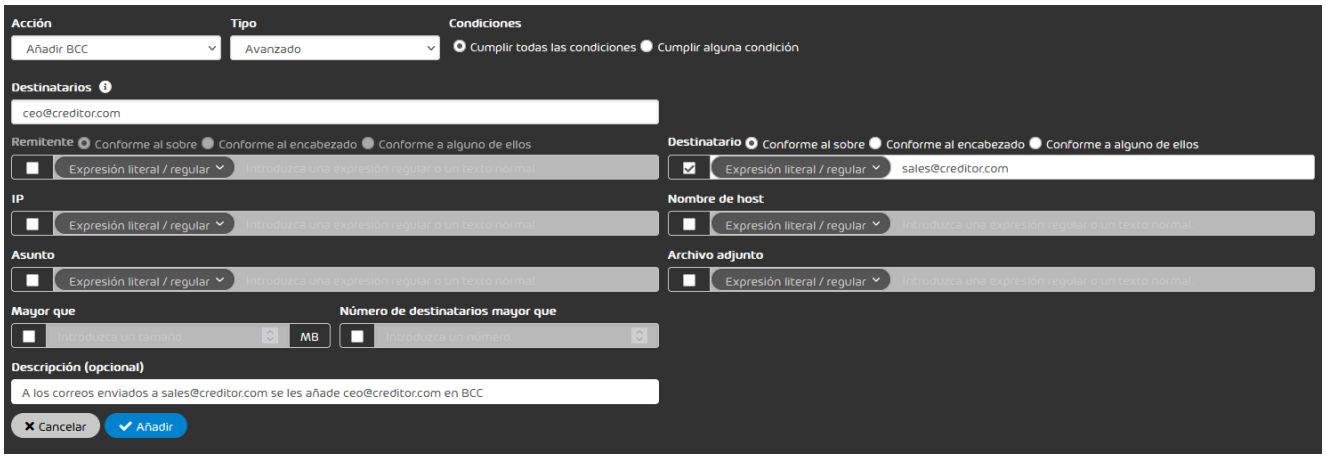
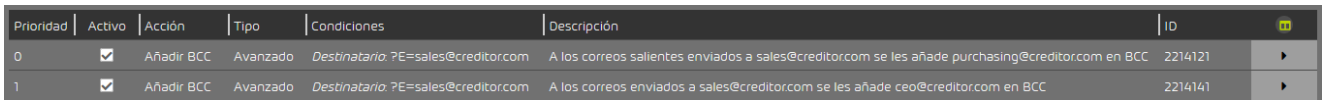


Figura 383: Regla de filtrado: añadir ceo@creditor.com como destinatario de copia oculta



Prioridad	Activo	Acción	Tipo	Condiciones	Descripción	ID
0	☑	Añadir BCC	Avanzado	*Destinatario* ?E=sales@creditor.com	A los correos salientes enviados a sales@creditor.com se les añade purchasing@creditor.com en BCC	2214121
1	☑	Añadir BCC	Avanzado	*Destinatario* ?E=sales@creditor.com	A los correos enviados a sales@creditor.com se les añade ceo@creditor.com en BCC	2214141

Figura 384: Orden de las reglas de filtrado

Procedimiento:

1. Un remitente cualquiera envía un correo a **sales@creditor.com**.
2. Compliance Filter busca primero entre las reglas de filtrado de tipo **Cuerpo**, luego entre aquéllas de tipo **Encabezado** y, finalmente, encuentra una coincidencia entre las reglas de filtrado de tipo **Avanzado**.
3. La regla de filtrado con la prioridad más alta (BCC a **purchasing@creditor.com**) se aplica. Compliance Filter no sigue buscando coincidencias con otras reglas de filtrado. La regla de filtrado con la prioridad más baja (BCC a **purchasing@creditor.com**) no se aplica.

Conflicto entre reglas de distintos tipos

Situación inicial:

Un administrador a nivel de cliente ha definido una regla de filtrado que clasifica correos entrantes con enlaces a Facebook como **Spam**. En otra regla de filtrado, el administrador ha definido una

excepción para el destinatario **marketing@debitor.com**. Con dicha excepción, el administrador ha determinado que los correos enviados directamente desde Facebook a **marketing@debitor.com** se clasifiquen como **Limpio**. La regla de filtrado con la excepción para **marketing@debitor.com** tiene una prioridad mayor que la regla de filtrado para correos con enlaces a Facebook y se encuentra por encima de la misma en la lista. No hay más reglas de filtrado aplicables al supuesto.

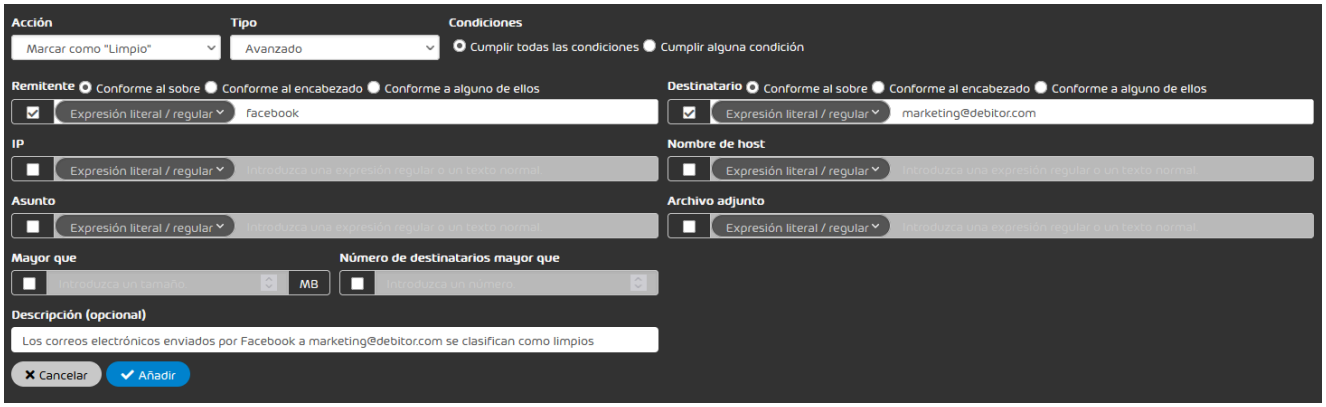


Figura 385: Regla de filtrado: Marcar como "limpio"

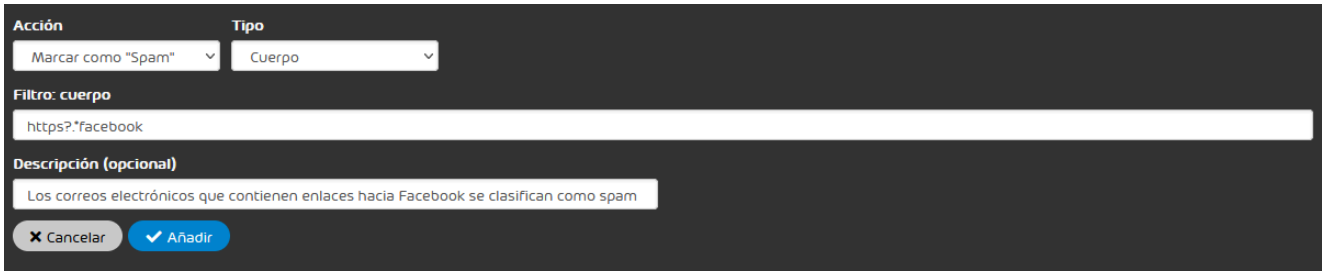


Figura 386: Regla de filtrado: Marcar como "spam"

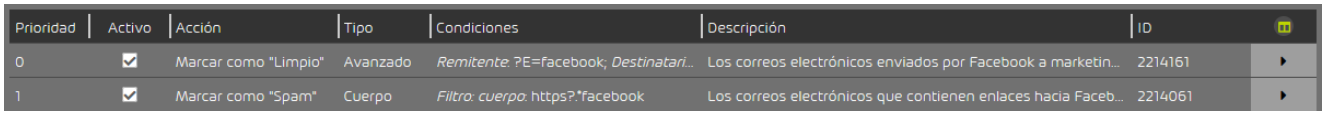


Figura 387: Orden de las reglas de filtrado

Procedimiento:

1. Facebook envía un correo con un enlace a **marketing@debitor.com**.

2. Compliance Filter busca en primer lugar entre las reglas de filtrado de tipo **Cuerpo** y encuentra una coincidencia en la regla de filtrado para correos que contienen enlaces de Facebook.

3. La regla de filtrado se aplica al correo, y éste se clasifica como **Spam**. Compliance Filter no sigue buscando coincidencias con otras reglas de filtrado. La regla de filtrado con la excepción para **marketing@debitor.com**, a pesar de tener una prioridad más alta, no se aplica, porque las reglas de filtrado de tipo **Cuerpo** tienen preferencia sobre reglas de otros tipos.

Conflicto entre Compliance Filter y nuestras reglas de filtrado.

Situación inicial:

Como cada vez estaba recibiendo más spam desde determinada dirección IPv4, un administrador a nivel de cliente definió una regla de filtrado para que los correos procedentes de dicha dirección se marcasen como spam. No hay más reglas de filtrado de Compliance Filter aplicables al supuesto. Además de las reglas de Compliance Filter, hay una regla de filtrado definida por nosotros aplicable al supuesto.

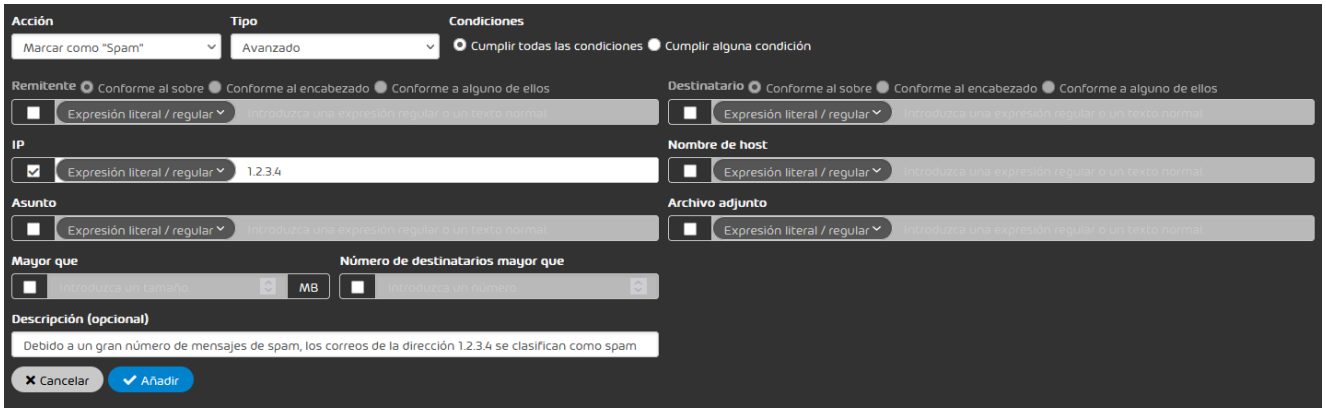


Figura 388: Regla de filtrado: Marcar correos de una dirección IPv4 como spam

Procedimiento:

1. Un remitente del dominio correspondiente a la dirección IPv4 envía un correo a un destinatario cualquiera.

2. Compliance Filter busca primero entre las reglas de filtrado de tipo **Cuerpo**, luego entre aquéllas de tipo **Encabezado** y, finalmente, encuentra una coincidencia entre las reglas de filtrado de tipo **Avanzado**.

3. La regla de filtrado se aplica al correo, y éste se clasifica como **Spam**. Compliance Filter no sigue buscando coincidencias con otras reglas de filtrado.

4. Ya hemos definido una regla de filtrado más precisa para este supuesto. La gran afluencia de spam se localizó en el remitente **info@**. Ninguna otra dirección de correo del dominio envía spam. Como nuestras reglas de filtrado no se siguen procesando, se aplica la regla que definió el administrador a nivel de cliente, y que tiene un rango de validez demasiado grande. Por tanto, algunos correos limpios podrían acabar marcándose como spam.

Activar reglas de filtrado

Ha desactivado una regla de filtrado de Compliance Filter (véase Desactivar reglas de filtrado de Compliance Filter en la página 559).

Si desea volver a aplicar una regla de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516) desactivada, puede volver a activarla en el módulo **Configuración de seguridad** > **Compliance Filter**.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.

5. Seleccione la regla de filtrado deseada de la lista de reglas para correos entrantes o salientes y marque la casilla de la columna **Activo**.

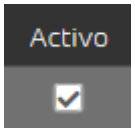


Figura 389: Activar reglas de filtrado

La regla de filtrado se activa. La regla de filtrado vuelve a aplicarse al tráfico de correo electrónico del dominio.

Se ha activado una regla de Compliance Filter.

Desactivar reglas de filtrado de Compliance Filter

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 521 o Crear reglas de filtrado para correos salientes en la página 528).

Si desea utilizar una regla de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516) temporalmente, puede desactivarla en el módulo **Configuración de seguridad** > **Compliance Filter**.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.

5. Seleccione la regla de filtrado deseada de la lista de reglas para correos entrantes o salientes y desmarque la casilla de la columna **Activo**.

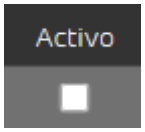


Figura 390: Desactivar reglas de filtrado

La regla de filtrado se desactiva. La regla de filtrado deja de aplicarse al tráfico de correo electrónico del dominio.

Se ha desactivado una regla de filtrado de Compliance Filter.

A continuación puede volver a activar la regla cuando desee volver a aplicarla (véase Activar reglas de filtrado en la página 558).

Eliminar reglas de filtrado de Compliance Filter

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 521 o Crear reglas de filtrado para correos salientes en la página 528).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede eliminar las reglas de filtrado de Compliance Filter que ya no necesite.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee eliminar una regla de filtrado.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Reglas**.

5. En la lista de reglas de filtrado para correos entrantes o salientes, haga clic en la flecha de menú junto a la regla de filtrado que desee eliminar.

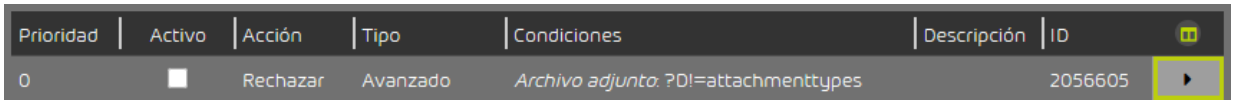


Figura 391: Abrir el menú

Se abre un menú.

6. Haga clic en **Eliminar**.

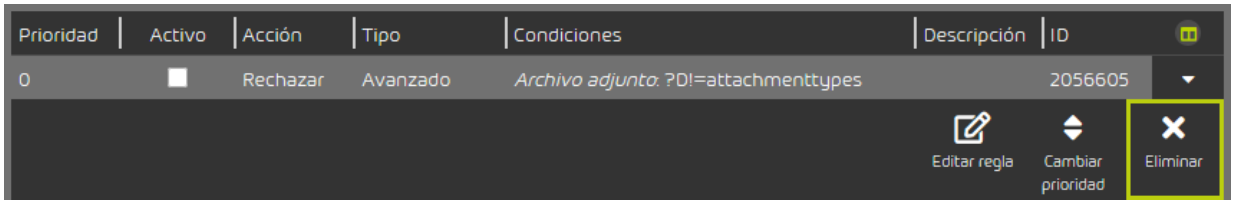


Figura 392: Eliminar reglas de filtrado

Se muestra un mensaje de advertencia.

7. Haga clic en **Confirmar**.

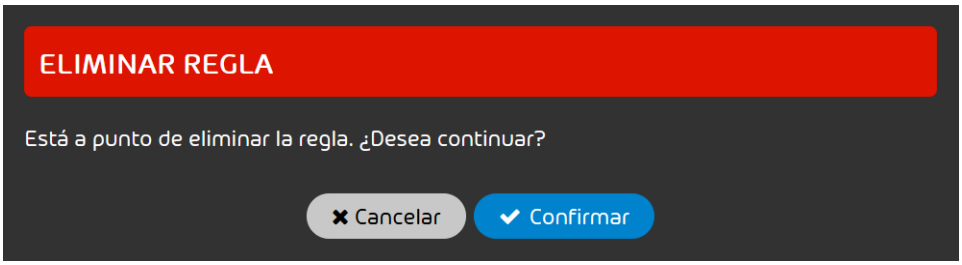


Figura 393: Confirmar la eliminación

La regla de filtrado se elimina.

Se ha eliminado una regla de filtrado de Compliance Filter.

Diccionarios

Los diccionarios son colecciones de expresiones que pueden emplearse para crear reglas de filtrado en el módulo **Configuración de seguridad** > **Compliance Filter** (véase Acerca de Compliance Filter en la página 516). Las expresiones de un diccionario pueden interpretarse, o bien todas como expresiones literales, o bien todas como expresiones regulares. Estas últimas ofrecen una mayor precisión de búsqueda y reducen la cantidad de registros que definir y mantener.

Nota:

Es posible crear un máximo de 250 diccionarios por dominio principal.

Los diccionarios de expresiones regulares pueden contener un máximo de 1000 registros, mientras que los diccionarios con expresiones literales pueden contener hasta 15000.

Al crear reglas de filtrado con de tipo **Avanzado** (véase Crear reglas de filtrado para correos entrantes en la página 521 o Crear reglas de filtrado para correos salientes en la página 528), los administradores a nivel de cliente pueden vincular diccionarios a algunas condiciones en lugar de introducir expresiones individuales. Para vincular un diccionario, los administradores deben introducir su nombre en el campo de la condición correspondiente y seleccionar en un menú desplegable el modo en que se deben interpretar las expresiones del diccionario. Con la opción **Dentro de diccionario**, la regla de filtrado se aplica de encontrarse al menos una expresión del diccionario en el correo correspondiente. Por tanto, dentro de la condición, las expresiones del diccionario están unidas entre sí por la conjunción OR. Con la opción **Fuera de diccionario**, la regla de filtrado se aplica de no encontrarse en el correo ninguna de las expresiones del diccionario.

Los diccionarios simplifican la creación de reglas de filtrado de Compliance Filter, ya que permiten aplicar una única regla a correos con diferentes valores en algún atributo. Así, con una sola regla es posible, por ejemplo, marcar como válidos los correos enviados por **@facebook**, **@instagram** o **@tiktok** a direcciones de correo del departamento de marketing creando un diccionario con dichos tres términos y vinculándolo a la condición **Remitente** (véase Tipos de reglas de filtrado

en la página 540). Para obtener el mismo efecto con Compliance Filter sin hacer referencia a un diccionario, habría que emplear tres reglas de filtrado distintas con una expresión literal cada una en el campo de remitente, o bien una única regla de filtrado con conjunciones OR entre los distintos remitentes. Esta última opción podría dificultar la comprensión de la regla en caso de que los remitentes fuesen muchos.

Otro ejemplo del uso de diccionarios es para rechazar todos los correos entrantes que contengan palabras malsonantes. Para ello, los administradores a nivel de cliente pueden crear un diccionario de insultos y enlazarlo en una única regla de filtrado para correos entrantes. Si en su lugar hubiese que crear y mantener una regla de filtrado para cada insulto, sería mucho más laborioso.

Los administradores a nivel de cliente pueden crear diccionarios (véase Crear un diccionario en la página 563), así como editar (véase Editar un diccionario en la página 566) y eliminar (véase Eliminar un diccionario en la página 568) diccionarios previos.

Crear un diccionario

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 519).

En el módulo **Compliance Filter** > **Diccionarios** puede crear diccionarios (véase Diccionarios en la página 562) de Compliance Filter. Con ayuda de diccionarios es posible crear reglas de filtrado complejas con poco esfuerzo (véanse Crear reglas de filtrado para correos entrantes en la página 521 y Crear reglas de filtrado para correos salientes en la página 528).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee crear un diccionario.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Diccionarios**.

5. Haga clic en **Añadir**.

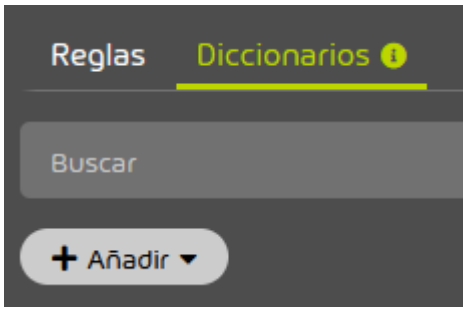


Figura 394: Añadir un diccionario

Se muestra un formulario para la creación de diccionarios.

Figura 395: Formulario de diccionario

6. Introduzca un nombre para el diccionario en el campo **Nombre**.

> **Nota:**
>
> El nombre puede contener los siguientes caracteres:
>
> - Letras minúsculas del alfabeto latino (a-z)
> - Cifras (0-9)
> - Los caracteres especiales **- _ . , =**
>
> No se permite emplear espacios ni dos puntos.

7. Opcional: Introduzca una descripción del diccionario en el campo **Descripción**.
8. Opcional: Si los términos del diccionario deben interpretarse como expresiones regulares, marque la casilla **Activar expresiones regulares**.

> **Nota:**
>
> Si se selecciona esta opción, es preciso respetar las reglas sobre expresiones regulares (véase Explicación de las expresiones regulares en la página 572) así como sus excepciones (véase Excepciones en las expresiones regulares en la página 580).

9. Introduzca las expresiones deseadas en el campo **Registros**.

> **Nota:**
>
> Cada fila es un registro. La longitud máxima de cada fila asciende a 1000 caracteres. La cantidad de filas por diccionario asciende a 15000 en el caso de expresiones literales, y a 1000 en el caso de expresiones regulares. Las líneas vacías y los registros duplicados se ignoran y se eliminan al guardar el diccionario.

10. Haga clic en **Aplicar cambios**.

    Si se ha marcado la casilla **Activar expresiones regulares**, se comprueba la validez de las expresiones regulares.

    El formulario se cierra, el diccionario se guarda y se añade a la tabla de diccionarios.

Se ha creado un diccionario.

A continuación puede editar el diccionario (véase Editar un diccionario en la página 566) o eliminarlo (véase Eliminar un diccionario en la página 568). Puede vincular el diccionario a reglas de filtrado de Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 521 y Crear reglas de filtrado para correos salientes en la página 528).

Editar un diccionario

Ha creado un diccionario (véase Crear un diccionario en la página 563).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede editar diccionarios (véase Diccionarios en la página 562) de Compliance Filter (véase Acerca de Compliance Filter en la página 516).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee editar un diccionario.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Diccionarios**.
5. En la lista de diccionarios, haga clic en la flecha de menú junto al diccionario que desee editar.

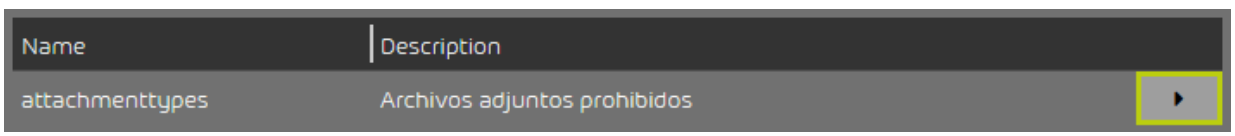


Figura 396: Abrir el menú

6. Haga clic en **Editar**.

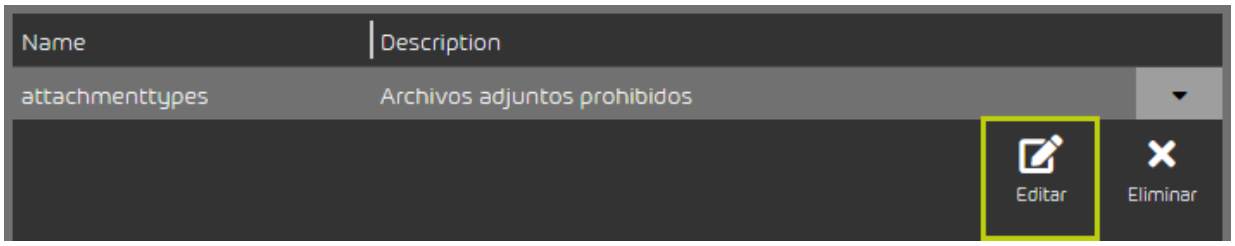


Figura 397: Editar un diccionario

Se abre un formulario con la configuración actual del diccionario.

7. Ajuste la configuración del modo deseado.

> **Nota:**
>
> Para más información, véase Crear un diccionario en la página 563.

8. Haga clic en **Aplicar cambios**.

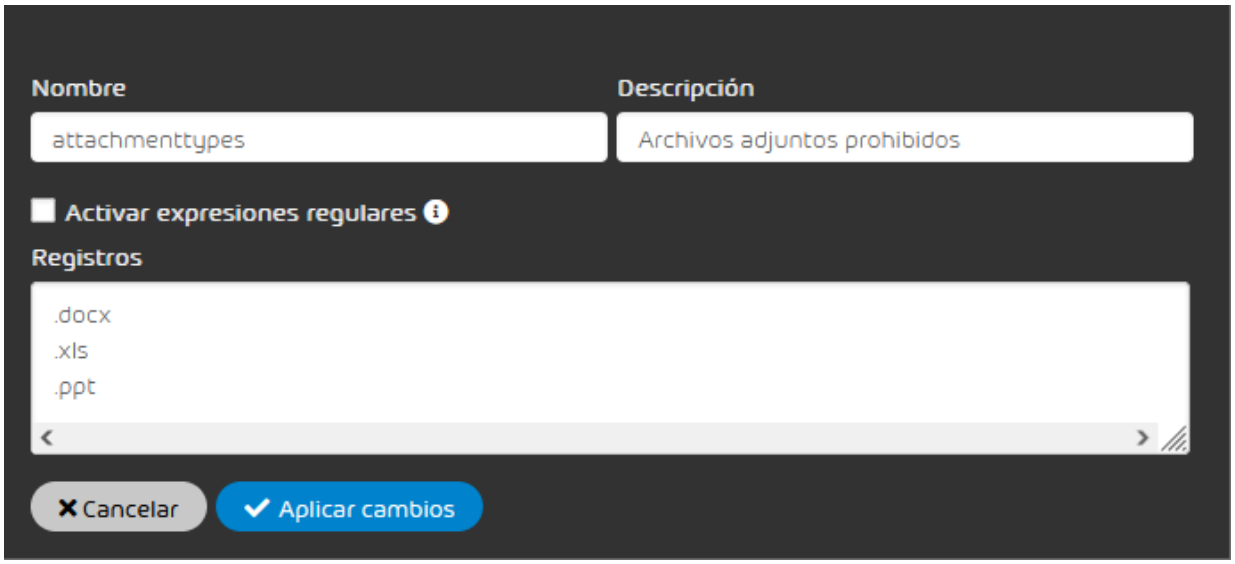


Figura 398: Aplicar los cambios

Los cambios se aplican.

Nota:

Si se ha cambiado el nombre del diccionario y éste ya está vinculado a alguna regla de filtrado, el nombre del diccionario se actualizará también en dicha regla de filtrado.

Se ha editado un diccionario.

Eliminar un diccionario

Ha creado un diccionario (véase Crear un diccionario en la página 563). El diccionario no está vinculado a ninguna regla de filtrado de Compliance Filter.

Si deja de necesitar un diccionario (véase Diccionarios en la página 562) de Compliance Filter (véase Acerca de Compliance Filter en la página 516) puede eliminarlo en el módulo **Configuración de seguridad** > **Compliance Filter**.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee eliminar un diccionario.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Seleccione la pestaña **Diccionarios**.
5. En la lista de diccionarios, haga clic en la flecha de menú junto al diccionario que desee eliminar.

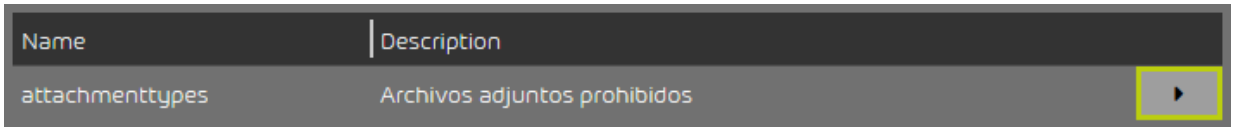


Figura 399: Abrir el menú

Se abre un menú.

6. Haga clic en **Eliminar**.

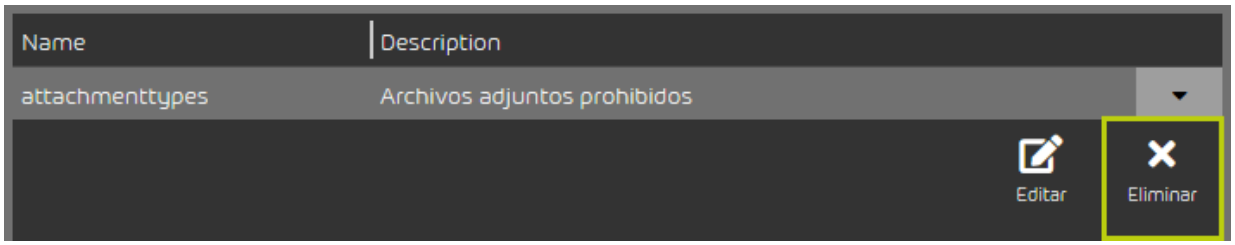


Figura 400: Eliminar un diccionario

Se muestra un mensaje de advertencia.

7. Haga clic en **Confirmar**.

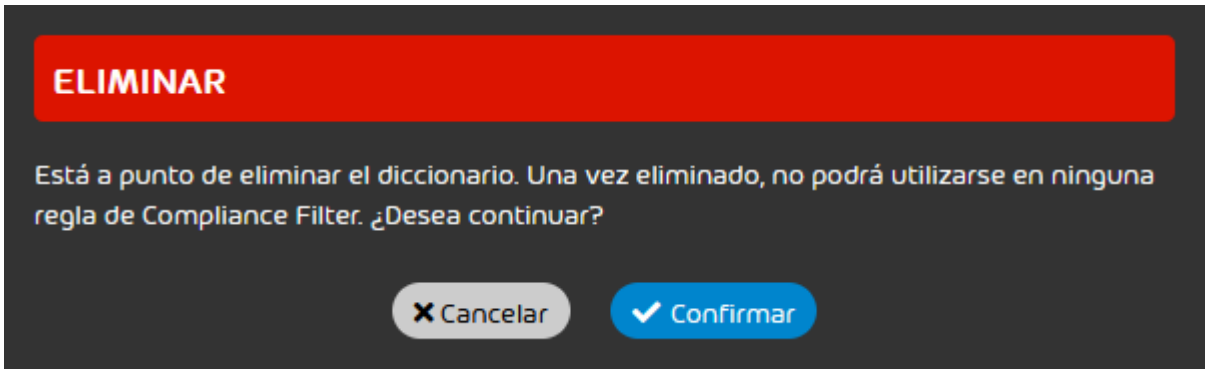


Figura 401: Confirmar la eliminación

Se comprueba si el diccionario está vinculado a reglas de Compliance Filter. Si no está vinculado a ninguna regla, el diccionario se elimina.

Se ha eliminado un diccionario.

Expresiones regulares

En las reglas de filtrado de Compliance Filter (véase Reglas de filtrado en la página 520) es posible emplear expresiones regulares (RegEx) para extraer información de cadenas de caracteres. Con ellas es posible reconocer patrones en el asunto u otras partes de un correo y filtrar por dichos patrones.

Nota:

El sistema añade automáticamente la secuencia **.*** delante y detrás de las expresiones regulares en el módulo **Compliance Filter**, a no ser que éstas comiencen con **^** o terminen con **$**.

Nota:

Los cuantificadores **+** y ***** (véase la tabla Elementos sintácticos y caracteres especiales en el capítulo Explicación de las expresiones regulares en la página 572) se convierten automáticamente en perezosos añadiendo un signo de interrogación a continuación de los mismos antes de evaluarse las expresiones regulares.

"Perezoso" es lo contrario de "codicioso", y quiere decir que la búsqueda finaliza al encontrarse la coincidencia más breve posible. Por ejemplo, en la cadena **aabcaabcdf**, la expresión regular codiciosa **a.*b** encontraría el término **aabcaab**. Por el contrario, la expresión perezosa **a.*?b** encontraría en la misma cadena dos veces la expresión **aab**.

Importante:

En el módulo **Compliance Filter** solo es posible emplear expresiones regulares en reglas de filtrado de tipo **Avanzado** (véase Tipos de reglas de filtrado en la página 540) y en diccionarios (véase Diccionarios en la página 562).

En los capítulos Explicación de las expresiones regulares en la página 572 y Ejemplos de expresiones regulares complejas en la página 582 se ofrecen explicaciones y ejemplos de expresiones regulares.

En Compliance Filter pueden emplearse expresiones regulares compatibles con Perl (PCRE). No se admiten otras bibliotecas. Para más información, véase: http://www.pcre.org/. Además, existen limitaciones especiales que se explican en Excepciones en las expresiones regulares en la página 580.

Ejemplo: Uso de expresiones regulares en Compliance Filter

A menudo, los usuarios recibían correos con la palabra "porn" en el asunto. Para marcarlos como spam, se definió una regla de filtrado. Sin embargo, últimamente se han recibido, cada vez más a menudo, correos que emplean expresiones similares para eludir el filtro. Por ejemplo, se reciben correos con el asunto "pOrn", que Compliance Filter no marca. En estos casos resulta más efectivo emplear una expresión regular:

Figura 402: Uso de una expresión regular en Compliance Filter

En lugar del punto, cualquier carácter se interpreta como válido. Por lo tanto, el filtro no se limita a buscar una "o", sino que encuentra cualquier letra, dígito y carácter especial.

Explicación de las expresiones regulares

En los siguientes ejemplos, la columna derecha muestra expresiones regulares que aplicar a los textos de la columna izquierda. En negrita se resaltan los segmentos de texto encontrados por la expresión regular correspondiente.

Caracteres individuales

Tabla 31: Búsqueda de letras

TEXTO	REGEX
abcdef	**abc**
abcde	
Abcd	

Las letras permiten encontrar letras en cualquier posición de un texto.

Tabla 32: Búsqueda de clases de caracteres

TEXTO	REGEX
ac**bde**f	**[abc]de**
adefg	

Con las clases de caracteres se encuentra uno de los caracteres contenido entre dos corchetes.

Tabla 33: Búsqueda de caracteres dentro de rangos

TEXTO	REGEX
1 Palabra	**[1-5] [A-Z]**
7 Palabras	
2 palabras distintas	

Los corchetes también permiten indicar rangos de caracteres. El primer y el último carácter del rango se escriben separados por un guión. El orden de los caracteres se corresponde con el orden de la tabla ASCII, por lo que las mayúsculas van antes que las minúsculas. Por tanto, la expresión regular **[A-z]** encuentra todos los caracteres ASCII desde la A mayúscula hasta la z minúscula. La expresión regular **[a-Z]**, por el contrario, es incorrecta y no encuentra nada.

Importante:

El rango de caracteres **[A-z]** contiene únicamente letras latinas. Los siguientes caracteres no forman parte del rango:

- Vocales con diéresis (äöü)
- Vocales con acentos (por ejemplo, áéíóú)
- Letras especiales de determinados idiomas (por ejemplo, ñ o ß)

Tabla 34: Búsqueda de cifras

TEXTO	REGEX
number - **123**	**123** o **\d\d\d**
var number - **123**	
ab**123**fg	

Las cifras funcionan igual que las letras. En lugar de una cifra concreta, puede emplearse la clase de caracteres'**\d** para encontrar cualquier cifra.

Tabla 35: Búsqueda de letras

TEXTO	REGEX
a12**b**34**c**	**\w**

La expresión **\w** busca cualquier letra latina de la A a la z (véase arriba) sin caracteres especiales ni letras específicas de determinados idiomas.

Tabla 36: Búsqueda de cualquier carácter

TEXTO	REGEX
bob.	**…\.**
tom.	
?!a.	
abc1	

Con un solo punto (".") se obtiene un resultado por cada carácter. Para comprobar la presencia de un punto, éste debe enmascararse con "\.".

Tabla 37: Búsqueda de caracteres repetidos

TEXTO	REGEX
abcc	**ab*c**
a**abbbbbc**c	
bb**ac**cc	

Repeticiones

El asterisco se utiliza para indicar que el carácter anterior puede aparecer cualquier número de veces. Por tanto, el símbolo puede no aparecer, aparecer una vez o aparecer varias veces.

Tabla 38: Búsqueda de caracteres repetidos al menos una vez

TEXTO	REGEX
aaaaaaaaa**abc**	**ab+c**
a**abbbc**	
ac	

El signo más escrito después de un carácter indica que este carácter puede aparecer una vez o varias. Si el carácter no se encuentra en el texto, no se obtienen resultados.

Tabla 39: Determinar la cantidad de repeticiones de caracteres

TEXTO	REGEX
12 **123 4544 1564**14	**\d{3,4}**

Con las llaves, es posible indicar la cantidad de repeticiones del símbolo precedente mediante un número fijo o un intervalo. En el ejemplo de arriba se buscan cadenas de caracteres que solo contengan cifras y tengan una longitud de entre 3 y 4 caracteres. Es posible emplear las siguientes combinaciones:

- {m}: El símbolo precedente debe aparecer exactamente m veces.
- {m,}: El símbolo precedente debe aparecer m veces como mínimo.
- {m,n}: El símbolo precedente debe aparecer m veces como mínimo y n veces como máximo.

Tabla 40: Caracteres opcionales

TEXTO	REGEX
3 users online	**\d+ users? online**
150 users online	
20 users online	
1 user online	
no user online	

El signo de interrogación "?" marca el carácter anterior como opcional.

grupos

Tabla 41: División de expresiones regulares en grupos

TEXTO	REGEX
dump025.csv	**\w+\d+\.(\w+)**
dump026.csv	

Mediante paréntesis es posible crear grupos dentro de una expresión. En el ejemplo superior, la extensión del archivo se registra como un grupo. Los operadores tratan los grupos como si fueran caracteres. Así, cuantificadores como ?, *, + o las llaves se aplican al grupo al completo en lugar de únicamente a su último carácter. Por ejemplo, todo el grupo **(abc)?** sería opcional. Además, los grupos permiten operaciones avanzadas como la referencia hacia atrás (véase más abajo). Otra ventaja de los grupos es que aportan claridad a las expresiones.

Tabla 42: Selección de varias opciones

TEXTO	REGEX
data.csv	**.*\.(exe|xlsx)**
bild.jpg	
moving.gif	
document.pdf	
virus.exe	
locky.xlsx	

Con una barra vertical | dentro de un paréntesis es posible separar cadenas de caracteres alternativas que buscar.

Tabla 43: Referencia hacia atrás

TEXTO	REGEX
From: "local@dominio.es" <local@dominio.es>	**From: "(.*@.*\.de)" <\1>**
From: "local@dominio.es" <hacker@dominiohackeado.es>	

La referencia hacia atrás \1 adquiere el valor del grupo definido (.*@.*\.de). Solo se obtiene un resultado si el texto del grupo vuelve a aparecer en el punto en el que se establece la referencia.

Elementos sintácticos y caracteres especiales

Para definir expresiones regulares en Compliance Filter se permiten los siguientes elementos sintácticos:

Tabla 44: Elementos sintácticos

COMODÍN/CLASE DE CARACTERES	FUNCIÓN
abc…	Letras
123…	Cifras
[abc]	a, b o c
[a-z]	Un símbolo ASCII dentro del rango indicado
\d	Cualquier cifra
.	Cualquier carácter
\. \/ \ *	Enmascaramiento de los caracteres impresos en negrita

COMODÍN/CLASE DE CARACTERES	FUNCIÓN
\w	Cualquier carácter alfanumérico
*	0 o más repeticiones de la expresión precedente
+	1 o más repeticiones de la expresión precedente
?	La expresión precedente es opcional
{m}	Exactamente m repeticiones de la expresión precedente
{m,}	Al menos m repeticiones de la expresión precedente
{m, n}	De m a n repeticiones de la expresión precedente
\s	Cualquier espacio en blanco
(…)	Grupo de extracción
(.*)	Todo
(abc|def)	abc o def
^	Comienzo de la cadena
$	Final de la cadena

Los caracteres especiales de la tabla anterior se interpretan normalmente como elementos especiales de una expresión regular. Sin embargo, también es posible buscar dichos caracteres especiales literalmente. Para ello es necesario omitir las funciones de los mismos precediéndolos de

una barra invertida \. Por ejemplo, la expresión **a*** no encuentra un número ilimitado de aes, sino la cadena de caracteres **a***.

Excepciones en las expresiones regulares

Las expresiones regulares creadas para reglas de Compliance Filter (véanse Acerca de Compliance Filter en la página 516 y Reglas de filtrado en la página 520) se diferencian de las expresiones PCRE, ya que en Compliance Filter no es posible emplear todos sus elementos sintácticos. Básicamente están permitidos los símbolos de la tabla ASCII extendida. Al evaluar expresiones regulares no se distingue entre mayúsculas y minúsculas.

Las expresiones introducidas en los campos de reglas de filtrado en el módulo **Compliance Filter** y las expresiones incluidas en diccionarios (véase Diccionarios en la página 562) están sometidas a limitaciones distintas.

Los siguientes símbolos **no** pueden introducirse en los campos de las reglas de filtrado del módulo **Compliance Filter** cuyos valores se interpreten como expresiones regulares:

- Punto y coma ;
- Símbolo de grado °
- El asterisco * al principio de una expresión
- Barra / (a no ser que se enmascare con \)

Los siguientes símbolos **no** pueden introducirse en los diccionarios del módulo **Compliance Filter** cuyos registros se interpreten como expresiones regulares:

- Símbolo de grado °
- Barra / (a no ser que se enmascare con \)

Nota:

Tanto en los campos de las reglas de filtrado como en los diccionarios, la barra vertical | (pleca) solo se permite dentro de grupos rodeados por paréntesis. Además, siempre se utiliza una sola barra vertical | para el significado OR. Dos barras verticales || se interpretan como un carácter comodín y hacen que se acepten todos los caracteres.

Usos frecuentes de las expresiones regulares

A continuación se presentan ejemplos de expresiones regulares (véase Explicación de las expresiones regulares en la página 572) para supuestos frecuentes de Compliance Filter (véase Acerca de Compliance Filter en la página 516).

Nombres de host diferentes con el mismo final

Al crear reglas de filtrado para correos enviados o recibidos por servidores de correo de diversos subdominios de un dominio determinado, es posible emplear la condición **Nombre de host** para buscar cadenas que terminen de un modo determinado en el módulo **Configuración de seguridad** > **Compliance Filter**.

Esta búsqueda puede realizarse con la siguiente expresión regular:

Cadena$

El signo del dólar significa que la cadena de caracteres buscada debe encontrarse al final del nombre de host. Así, por ejemplo, la expresión **.*dominio\.tld$** encontraría correos enviados desde o dirigidos al servidor de correo del dominio **dominio.tld** y todos sus subdominios (p. ej. **marketing.dominio.tld**, **ventas.dominio.tld**, **contabilidad.dominio.tld**).

Nombres de host numerados de servidores de correo

A menudo, los servidores de correo de un dominio solo se diferencian en su numeración. Para procesar correos enviados desde o dirigidos a dichos servidores de correo con reglas de filtrado de Compliance Filter, es posible emplear la condición **Nombre de host** para buscar cadenas de caracteres que solo se diferencien en su numeración.

Esta búsqueda puede realizarse con la siguiente expresión regular:

(cadena antes de numeración)\d+(cadena tras numeración)

Nota:

Los paréntesis son opcionales en esta expresión y solo se han añadido para mayor claridad.

La secuencia **\d+** significa "al menos una cifra". Así, por ejemplo, la expresión **mx\d+\.dominio\.tld** encontraría correos enviados por o dirigidos a los siguientes servidores de correo: **mx3.dominio.tld**, **mx30.dominio.tld**, **mx100.dominio.tld**.

Varias direcciones de correo de un domino

Para que una regla de filtrado pueda aplicarse a correos correspondientes a una pequeña cantidad de direcciones de correo de un dominio, es posible introducir una expresión regular para las condiciones **Remitente** o **Destinatario** según el siguiente patrón:

(usuario1|usuario2|usuario3)@dominio

El símbolo **|** separa cadenas de caracteres alternativas, debiendo encontrarse una de ellas. Las cadenas de caracteres alternativas deben ir entre paréntesis. Así, por ejemplo, la expresión regular **(klaus|peter|petra)@dominio.com** encontrará correos enviados por o dirigidos a las siguientes direcciones de correo: **klaus@dominio.com**, **peter@dominio.com**, **petra@dominio.com**.

Ejemplos de expresiones regulares complejas

Por último veremos ejemplos de uso de expresiones regulares complejas (véase Explicación de las expresiones regulares en la página 572) dentro de reglas de filtrado para Compliance Filter (véase Acerca de Compliance Filter en la página 516).

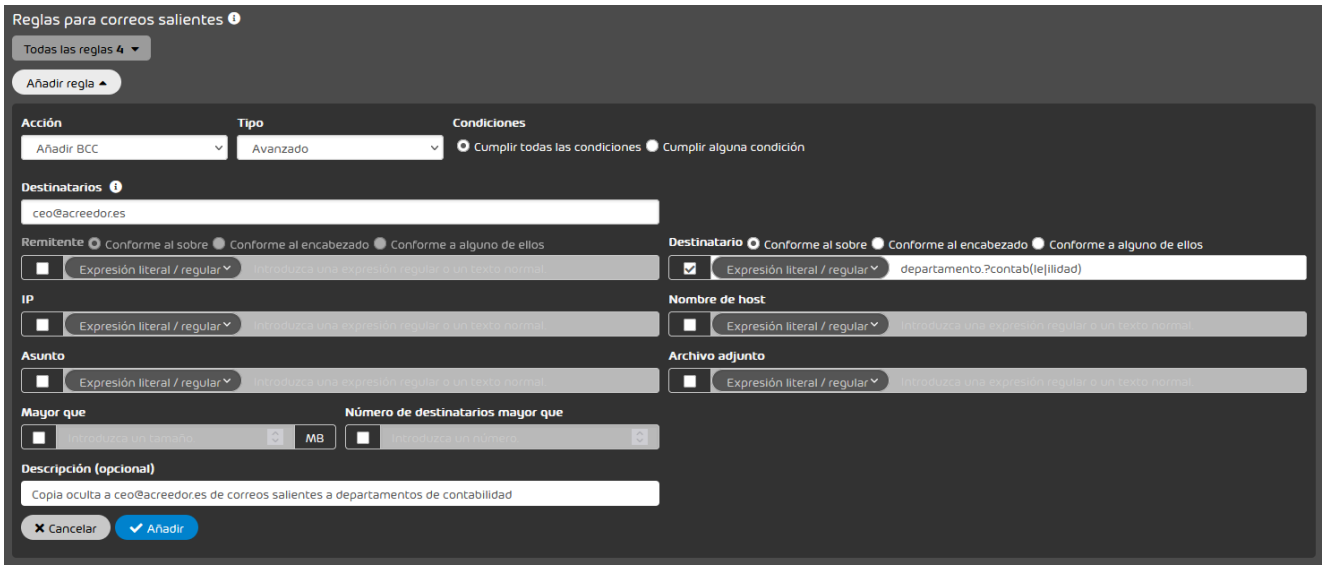


Figura 403: Búsqueda de destinatarios

En este ejemplo, un cliente desea que su administrador reciba una copia oculta de los correos salientes enviados a los departamentos de contabilidad de los clientes de su empresa. Sus direcciones de correo presentan determinada estructura. Con la expresión regular **departamento.?contab(le|ilidad)** se pueden encontrar los siguientes segmentos de texto y muchas otras combinaciones:

- **departamentocontable@prueba.es**
- **departamento_contable@prueba.es**
- **departamento.contabilidad@prueba.es**
- **departamento.contabilidad@otraprueba.es**

Figura 404: Búsqueda de IBAN en el cuerpo de un correo

En este ejemplo, un cliente alemán desea reenviar a su departamento de contabilidad todos los correos que contengan números de cuenta IBAN en su texto. La expresión regular **(DE\d{2} ?)(\d{4} ?){4}(\d{2})** permite buscar números de cuenta IBAN alemanes. Esta expresión regular encuentra números de cuenta IBAN alemanes tanto cuando se escriben sin espacios como cuando se escriben, como es habitual, en bloques de cuatro caracteres con un bloque final de dos caracteres.

- **DE12345678901234567890**
- **DE12 3456 7890 1234 5678 90**

Desactivar Compliance Filter

Si ya no desea utilizar las reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 516), puede desactivar Compliance Filter en el módulo **Configuración de seguridad > Compliance Filter**. En el proceso se eliminan todas las reglas.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.

2. En la selección de ámbitos, seleccione el dominio para el cual desee desactivar Compliance Filter.
3. Vaya a **Configuración de seguridad** > **Compliance Filter**.
4. Accione el interruptor **Activar Compliance Filter**.

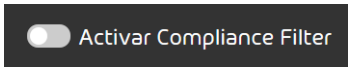


Figura 405: Desactivar Compliance Filter

Aparece una ventana de confirmación.

5. Haga clic en **Confirmar**.

Figura 406: Confirmar

Compliance Filter se desactiva. Todas las reglas se eliminan. Los ajustes del módulo **Compliance Filter** se bloquean. Ya no es posible modificar datos.

Compliance Filter se ha desactivado.

Signature and Disclaimer

Acerca de Signature and Disclaimer

Signature and Disclaimer controla la adición automática y centralizada de firmas y notas legales a correos. Las firmas y notas legales pueden crearse, o bien para todos los buzones de correo de un dominio, o bien para los buzones de correo de un grupo determinado (véase "Grupos" en el manual de Control Panel). Mediante sincronización con Active Directory, la herramienta genera de modo dinámico firmas específicas de usuario basadas en una plantilla elaborada previamente y que se añaden automáticamente detrás del texto del correo. Para ello se emplean variables de Active Directory (variables de AD), que permiten integrar datos de los atributos de Active Directory correspondientes en la firma o la nota legal. Para buzones de correo creados manualmente en Control Panel y que no se sincronizan mediante LDAP (véase el capítulo "Tipos de buzón de correo" en el manual de Control Panel), las variables de AD se emplean para obtener los datos básicos del buzón.

Las variables de AD solo están disponibles para clientes cuyos usuarios y grupos se sincronicen mediante LDAP con un Active Directory de Microsoft. No se pueden utilizar con otros servicios de directorio.

Nota:

Las firmas y notas legales se añaden a todos los correos enviados mediante nuestro servidores de retransmisión. Por tanto, las firmas y notas legales también se añaden a correos enviados dentro de una empresa siempre que éstos se transmitan a través de nuestra infraestructura.

Los administradores a nivel de cliente y los usuarios con el rol **Marketing** (véase Acceso al módulo Signature and Disclaimer en la página 587) pueden configurar firmas y notas legales. Las funciones de Signature and Disclaimer también están disponibles para teléfonos móviles (véase Uso móvil de Signature and Disclaimer en la página 587).

Antes de poder emplear Signature and Disclaimer es preciso activar dicho servicio (véase Activar Signature and Disclaimer en la página 588). A continuación es posible crear firmas y notas

legales para grupos en un editor (véase Crear firmas y notas legales en la página 589), editarlas o eliminarlas (véase Editar o eliminar una firma o nota legal en la página 597). La prioridad de los grupos se puede modificar (véase Modificar prioridades de grupos en la página 594). En el editor, las firmas y notas legales se muestran tal y como se verán posteriormente (véase Editor WYSIWYG en la página 600). También es posible añadir imágenes a firmas y notas legales (véase Adición de imágenes en Signature and Disclaimer en la página 616). Si se crean firmas y notas legales para grupos, es posible modificar las prioridades de los grupos (véase Modificar prioridades de grupos en la página 594).

Si no se desea seguir utilizando Signature and Disclaimer, es posible desactivar el servicio (véase Desactivar Signature and Disclaimer en la página 598).

Para más información sobre cómo solucionar errores frecuentes, véase Solución de problemas en la página 632.

Uso móvil de Signature and Disclaimer

Con Signature and Disclaimer activado, las firmas y notas legales se añaden también a los correos enviados desde dispositivos móviles.

Nota:

Este servicio es compatible con la versión más reciente de los sistemas operativos Android e iOS. Es posible que las firmas y notas legales no se muestren correctamente en versiones antiguas.

Acceso al módulo Signature and Disclaimer

Si es preciso que algún usuario sin derechos administrativos cree y edite firmas y notas legales, los administradores a nivel de cliente pueden asignarle el rol **Marketing** (véase "Roles" en el manual de Control Panel). El rol **Marketing** concede a los usuarios acceso al módulo **Signature and Disclaimer** (véase Acerca de Signature and Disclaimer en la página 586).

Activar Signature and Disclaimer

Usted ha activado la sincronización mediante LDAP para el dominio (véase «Activar la conexión mediante LDAP» en el manual de Control Panel) para el que desee activar Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede desactivar Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee activar Signature and Disclaimer.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Marque la casilla **Activate Signature and Disclaimer**.

Figura 407: Activar Signature and Disclaimer

Se muestra una ventana de confirmación.

5. Haga clic en **Confirm**.

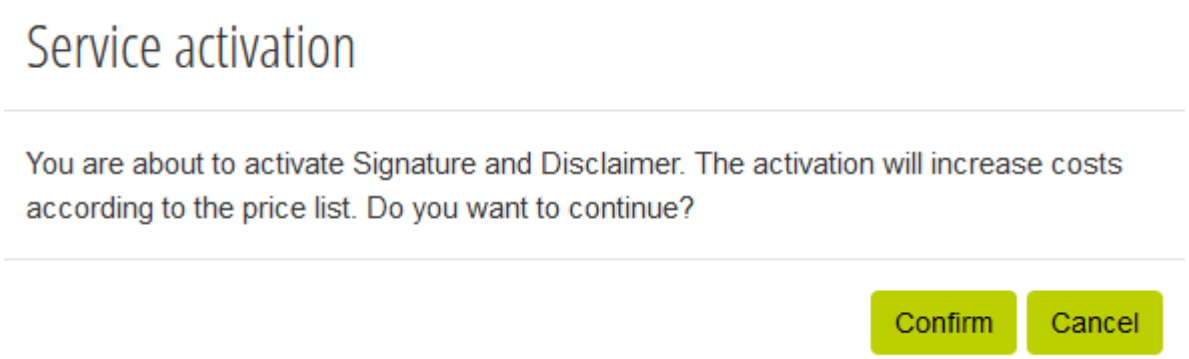


Figura 408: Confirmar la activación

Signature and Disclaimer se activa.

Signature and Disclaimer se ha activado.

A continuación puede cambiar la prioridad de los grupos (véase Modificar prioridades de grupos en la página 594). A continuación puede crear firmas y notas legales (véase Crear firmas y notas legales en la página 589), editarlas o eliminarlas (véase Editar o eliminar una firma o nota legal en la página 597). Si no desea seguir utilizando Signature and Disclaimer, puede desactivar dicho servicio (véase Desactivar Signature and Disclaimer en la página 598).

Crear firmas y notas legales

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede crear firmas o notas legales para distintos grupos. Los grupos se muestran en el lado izquierdo de la pantalla. Si no ha

creado grupos para el dominio, podrá seleccionar el grupo **default** para asignar la misma firma o la misma nota legal a todos los usuarios.

> **Nota:**
>
> Puede crear grupos nuevos en la sección **Configuración de cliente** > **Grupos** de Control Panel. Para más información, véase el capítulo "Grupos" del manual de Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear firmas y notas legales.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. En la sección **Grupos**, situada en el lado izquierdo de la vista general, añada un grupo de la selección de grupos.

> **Nota:**
>
> Haciendo clic en el campo **búsqueda** podrá ver un menú desplegable con todos los grupos creados. También puede emplearlo para buscar grupos.

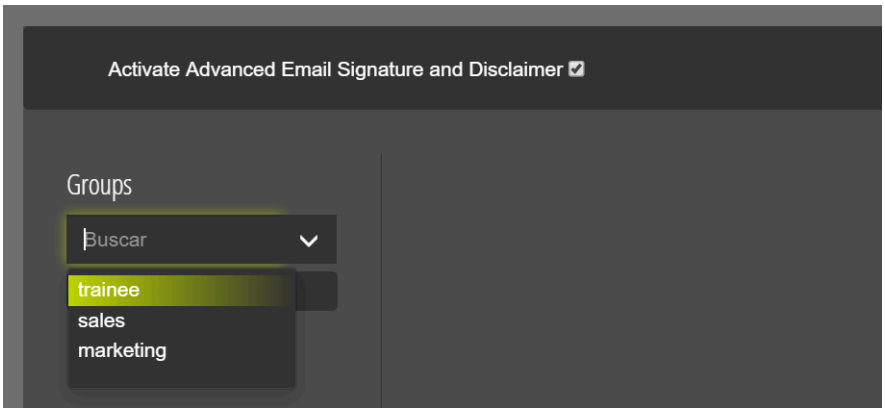


Figura 409: Añadir grupos

5. Seleccione el grupo añadido.

Figura 410: Seleccionar un grupo

En el lado derecho de la vista general aparecerá la selección de notas legales y firmas.

6. En el lado derecho, haga clic en **+** bajo **Disclaimer** o **Signature** para crear una nueva plantilla.

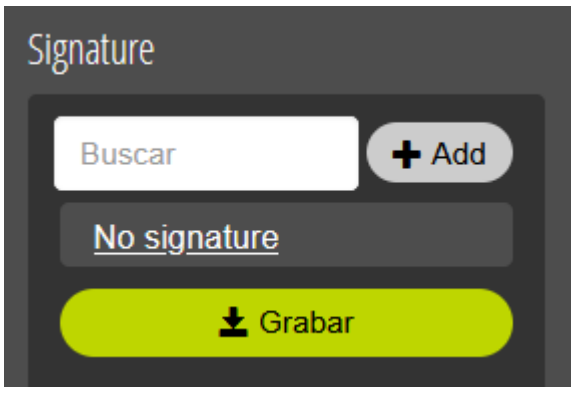


Figura 411: Añadir una nueva plantilla

7. Asigne un nombre a su nueva plantilla.

Puede crear la plantilla para firmas o notas legales tanto en formato HTML como sin formato al mismo tiempo. Las plantillas se crean por separado.

8. Elija el formato para de correo para el que desee crear la plantilla.
   - HTML
   - Plain

   Nota:

   Puede cambiar de formato durante la edición.

9. Defina su plantilla en el editor gráfico con vista preliminar (editor WYSIWYG) (véase Editor WYSIWYG en la página 600):

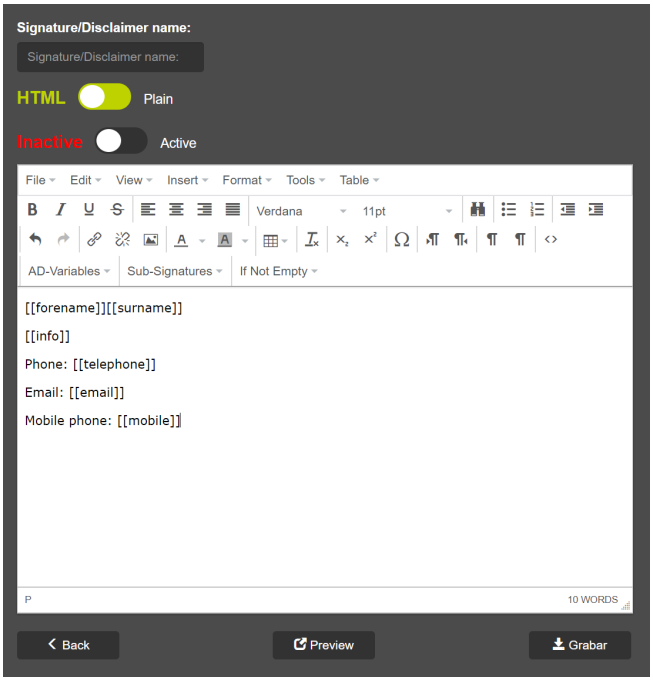


Figura 412: Crear una plantilla en el editor WYSIWYG

10. Guarde la plantilla.

11. Seleccione la plantilla en la vista general.

Figura 413: Selección de firma en la vista general

12. En la vista general, haga clic en **Guardar** para asignar la plantilla seleccionada al grupo seleccionado.

Se ha creado una firma y/o una nota legal y se ha asignado a un grupo.

Nota:

Las firmas y notas legales solo se añaden a correos enviados por servidores de redireccionamiento a través de las direcciones indicadas en **Spam and Malware Protection** (véase "Configuración del entorno primario" en el manual de Control Panel).

Nota:

La firma y la nota legal de un usuario solo se añaden a su primer correo en cada hilo de correo. En lo posible, se evita repetir la firma y la nota legal en el transcurso de los hilos de correo.

Modificar prioridades de grupos

Ha añadido varios grupos al módulo **Signature and Disclaimer** (véase Crear firmas y notas legales en la página 589).

En el módulo **Signature and Disclaimer**, los grupos se ordenan por su prioridad. Las prioridades de los grupos se muestran en la columna **Grupos** de la tabla de grupos. Cuanto menor es el número, mayor es la prioridad de un grupo. Si un buzón de correo pertenece a varios grupos añadidos al módulo **Signature and Disclaimer**, los correos salientes del buzón de correo se enviarán con la firma y la nota legal del grupo que tenga la prioridad más alta.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para cuyos grupos desee modificar las prioridades en el módulo **Signature and Disclaimer**.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. En **Grupos**, seleccione el grupo cuya prioridad desee cambiar.

5. Opcional: Cambie la prioridad del grupo desplazándolo a otra posición de la lista.

   a) Haga clic en el icono de los nueve puntos junto al grupo y mantenga el botón izquierdo del ratón pulsado.

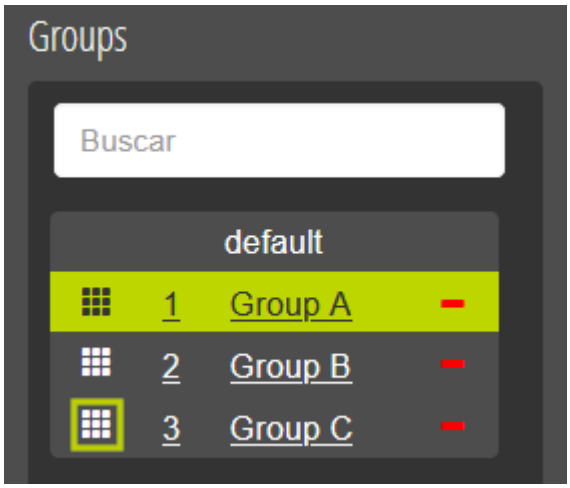


Figura 414: Desplazar un grupo

   b) Desplace el grupo hasta la posición correspondiente a la prioridad deseada.

   c) Suelte el botón izquierdo del ratón.

El grupo se deposita en la nueva posición. Las prioridades de todos los grupos que se hayan visto desplazados en la tabla se actualizan.

6. Sobrescriba la prioridad del grupo.

   a) Haga doble clic sobre la prioridad del grupo.

   El número se vuelve editable.

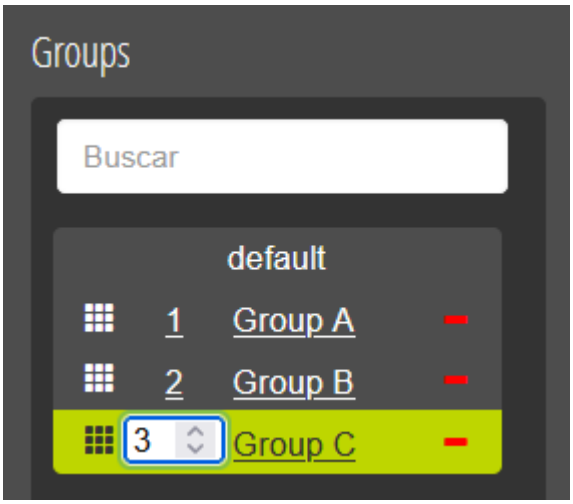


Figura 415: Campo de introducción de prioridad

   b) Introduzca el número correspondiente a la nueva prioridad en el campo o selecciónelo con las flechas.

   c) Confirme la nueva prioridad con la tecla Intro.

   La prioridad del grupo se guarda. El grupo se desplaza hasta la posición correspondiente a su nueva prioridad. Las prioridades de todos los grupos que se hayan visto desplazados en la tabla se actualizan.

Se han modificado las prioridades de los grupos.

Editar o eliminar una firma o nota legal

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588) y creado una firma o una nota legal (véase Crear firmas y notas legales en la página 589).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede editar o eliminar firmas o notas legales.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee editar o eliminar una firma o nota legal.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. En la ventana general, haga clic en el campo **Buscar** de debajo de **Disclaimer** o **Signature** y seleccione la plantilla deseada.

Figura 416: Selección de firma en la vista general

5. Seleccione una de las siguientes acciones:

   - Para editar la plantilla seleccionada, haga clic en el icono del lápiz junto al nombre de la plantilla. El editor se abrirá y usted podrá editar su plantilla.

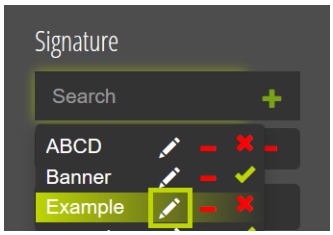


Figura 417: Editar una plantilla

   - Para eliminar la plantilla seleccionada, haga clic en el guion rojo (**–**). Confirme el mensaje con **OK**.

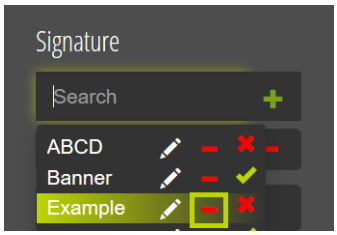


Figura 418: Eliminar una plantilla

Se ha editado o eliminado una firma o una nota legal.

Desactivar Signature and Disclaimer

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588).

Si no desea seguir utilizando Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586), puede desactivar este servicio. Sus ajustes de grupos, firmas y notas legales se guardarán por si desea volver a activar Signature and Disclaimer con posterioridad.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.

2. En la selección de ámbitos, seleccione el dominio para el cual desee desactivar Signature and Disclaimer.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Desmarque la casilla **Activate Signature and Disclaimer**.

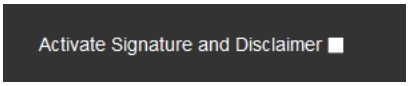


Figura 419: Desactivar Signature and Disclaimer

Aparece una ventana de confirmación.

5. Haga clic en **Aceptar**.

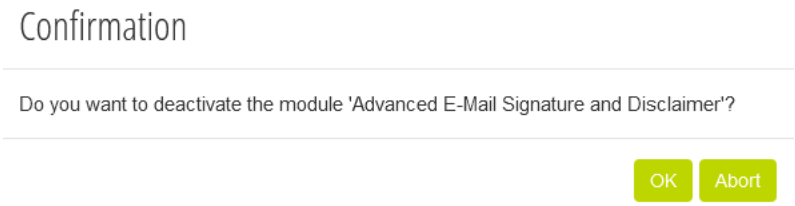


Figura 420: Confirmar la desactivación

Signature and Disclaimer se desactiva.

Signature and Disclaimer se ha deshabilitado.

Nota:

La desactivación de Signature and Disclaimer no supone la rescisión del contrato sobre dicho servicio. Para rescindir un contrato deberá ponerse en contacto con su interlocutor.

Editor WYSIWYG

El editor WYSIWYG permite crear y editar fácilmente plantillas de firmas y notas legales.

Para ello, los administradores a nivel de cliente y usuarios con el rol **Marketing** (véase Acceso al módulo Signature and Disclaimer en la página 587) disponen de sencillas opciones de formato, como cambiar la alineación del párrafo o el tipo de letra. Además, es posible emplear variables de Active Directory para acceder a atributos del Active Directory o a datos básicos de buzones de correo creados manualmente (véase el capítulo "Tipos de buzón de correo" en el manual de Control Panel) para, por ejemplo, añadir el nombre y los apellidos asignados al buzón de correo correspondiente a las firmas o notas legales. Los atributos disponibles dependen de las circunstancias de uso:

- Con una conexión mediante LDAP activada (véase "Conexión mediante LDAP" en el manual de Control Panel) se dispone de numerosos atributos de Active Directory (véase Atributos sincronizados desde Active Directory en la página 601). Si hay algún atributo al que no se haya asignado ningún valor, es posible ocultarlo en las firmas y notas legales (véase Ocultar elementos vacíos de Active Directory en la página 607).
- Para buzones de correo creados manualmente, están disponibles los datos básicos de los buzones de correo (véase Consulta de datos básicos con variables de AD en la página 605).

> **Importante:**
>
> Para poder utilizar variables de AD, éstas deberán estar definidas en el Active Directory.

Las firmas y notas legales pueden formatearse mediante código fuente HTML (véase Introducir código fuente HTML en la página 614). Además, es posible añadir firmas a otras firmas a modo de subfirmas (véase Añadir subfirmas en la página 610) así como imágenes a firmas y notas legales (véase Adición de imágenes en Signature and Disclaimer en la página 616). Mediante una función de vista previa es posible ver el aspecto que tendrá más tarde una firma o nota legal (véase Ver una vista previa de una firma o una nota legal en la página 615).

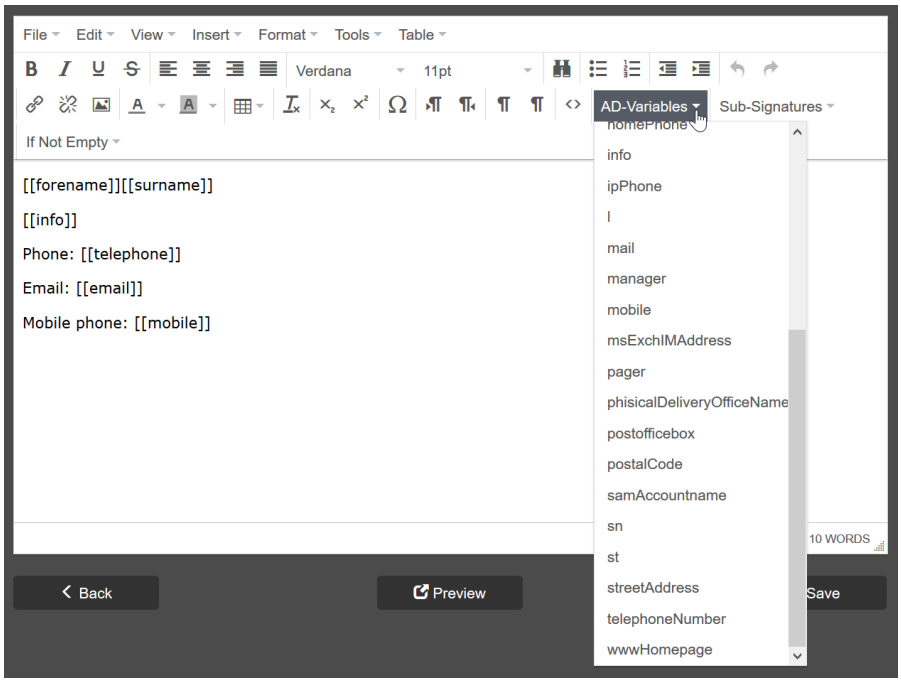


Figura 421: Editor WYSIWYG

Atributos sincronizados desde Active Directory

Si la conexión mediante LDAP (véase "Conexión mediante LDAP" en el manual de Control Panel) se encuentra activada, se sincronizarán numerosos atributos con el Active Directory de Microsoft que pueden emplearse en el módulo **Signature and Disclaimer** (véase Acerca de Signature and Disclaimer en la página 586). Si se modifican datos en el Active Directory, los cambios se actualizarán también en Control Panel (véase Sincronización de datos mediante LDAP en la página 603).

Los siguientes atributos de Active Directory se sincronizan para buzones de correo LDAP (véase el capítulo "Tipos de buzón de correo" en el manual de Control Panel) y pueden emplearse para crear firmas y notas legales:

VARIABLE DE AD	SIGNIFICADO
cn	"Common name", nombre común

VARIABLE DE AD	SIGNIFICADO
company	Empresa
countryCode	País/región
department	Departamento
description	Descripción
directReports	Empleado
displayName	Nombre para mostrar – nombre completo
facsimileTelephoneNumber	Fax
givenName	Nombre
homePhone	Número de teléfono personal
info	Función/cargo
ipPhone	Número de teléfono IP
l (L minúscula)	Municipio
mail	Dirección de correo
manager	Superior

Nota:

El campo "title" se emplea para otras muchas cosas. Por tanto, para el atributo de LDAP "Title" (función/cargo) se emplea aquí la denominación "info".

VARIABLE DE AD	SIGNIFICADO
mobile	Número de teléfono móvil
msExchIMAddress	Dirección IM
pager	Número de buscapersonas
physicalDeliveryOfficeName	Oficina
postalCode	Código postal
postOfficeBox	Buzón de correo
samAccountName	Nombre de cuenta del usuario
sn	Apellido
st	Estado/cantón
streetAddress	Calle
telephoneNumber	Número de teléfono
wwwHomepage	Página web

Sincronización de datos mediante LDAP

Si efectúa cambios en el Active Directory, dichos cambios se sincronizarán.

Los cambios del Active Directory se registran mediante el atributo **USNChangedNr**. Si cambia su valor, se efectúa la sincronización de los datos.

Importante:

Si aplica una copia de seguridad, el **USNChangedNr** no se incrementa, sino que se devuelve a un estado anterior. En tal caso, los datos también vuelven a sincronizarse.

Atributos sincronizados desde Azure Active Directory

Determinados atributos para Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586) se sincronizan con Azure Active Directory de Microsoft.

Importante:

Para los buzones creados manualmente se emplean los datos básicos (véase Consulta de datos básicos con variables de AD en la página 605). Los atributos de LDAP no se sincronizan y no pueden emplearse.

Los siguientes atributos se sincronizan y pueden emplearse para crear firmas y notas legales:

VARIABLE DE AD	SIGNIFICADO
countryCode	País/región
department	Departamento
displayName	Nombre para mostrar – nombre completo
givenName	Nombre

VARIABLE DE AD	SIGNIFICADO
info	Función/cargo **Nota:** El campo "title" se emplea para otras muchas cosas. Por tanto, para el atributo de LDAP "title" (función/cargo) se emplea aquí la denominación "info".
l (L minúscula)	Municipio
mail	Dirección de correo
mobile	Número de teléfono móvil
postalCode	Código postal
sn	Apellido
st	Estado/cantón
streetAddress	Calle
telephoneNumber	Número de teléfono

Consulta de datos básicos con variables de AD

Importante:

Para buzones de correo creados manualmente, los datos básicos aquí descritos pueden consultarse mediante variables de AD.

Entre las variables de AD y los datos básicos de un buzón de correo existen las siguientes correspondencias.

VARIABLE DE AD	DATO BÁSICO
countryCode	**País/región**
department	**Departamento**
displayName	**Nombre para mostrar**
facsimileTelephoneNumber	**Fax**
givenName	**Nombre**
l (L minúscula)	**Municipio**
mail	Dirección de correo electrónico del buzón
mobile	**Teléfono móvil**
postalCode	**Código postal**
physicalDeliveryOfficeName	**Oficina**
sn	**Apellidos**
st	**Estado**
streetAddress	**Calle, número**
telephoneNumber	**Teléfono (profesional)**

Ocultar elementos vacíos de Active Directory

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede ocultar contenidos de firmas y notas legales si determinadas variables de AD de los usuarios están vacías con la función **If Not Empty** del editor WYSIWYG (véase Editor WYSIWYG en la página 600).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear firmas y notas legales.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Cree o edite una firma o una nota legal (véase Crear firmas y notas legales en la página 589 o Editar o eliminar una firma o nota legal en la página 597).
5. En el editor, seleccione la línea a la que desee añadir la variable de AD.
6. Haga clic en **If Not Empty**.

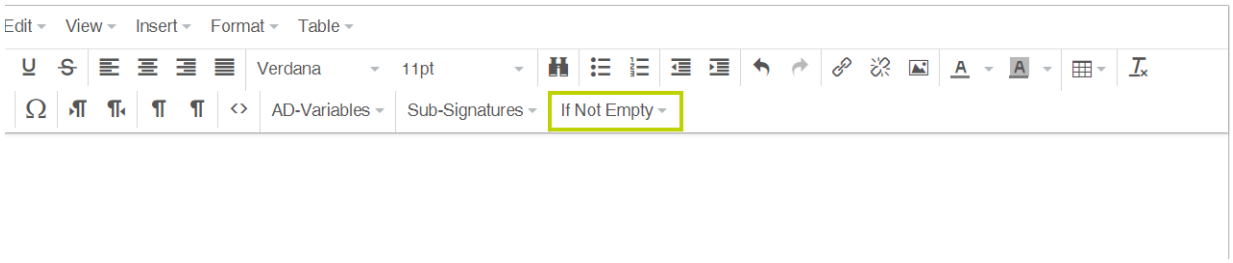


Figura 422: Abrir la selección

7. Seleccione la variable de AD deseada en el campo "Variable".

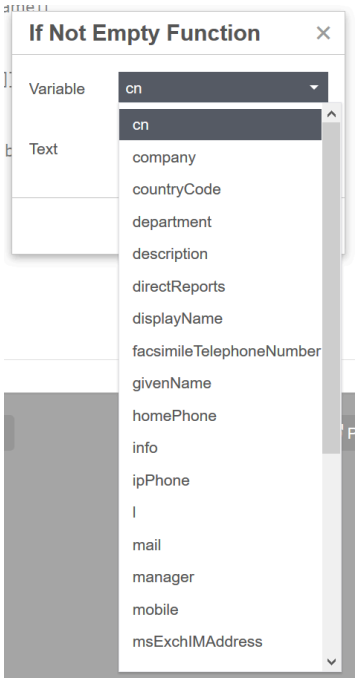


Figura 423: Seleccionar una variable de AD

8. Introduzca el texto a ocultar si el elemento está vacío para el usuario.
9. Confirme con **Aceptar**.

10. También es posible incluir una variable de AD en el texto a ocultar:

    a) En el editor, haga clic en el punto entre etiquetas "If not empty" en el que desee introducir la variable de AD a ocultar.

    b) Seleccione la variable de AD en el menú desplegable.

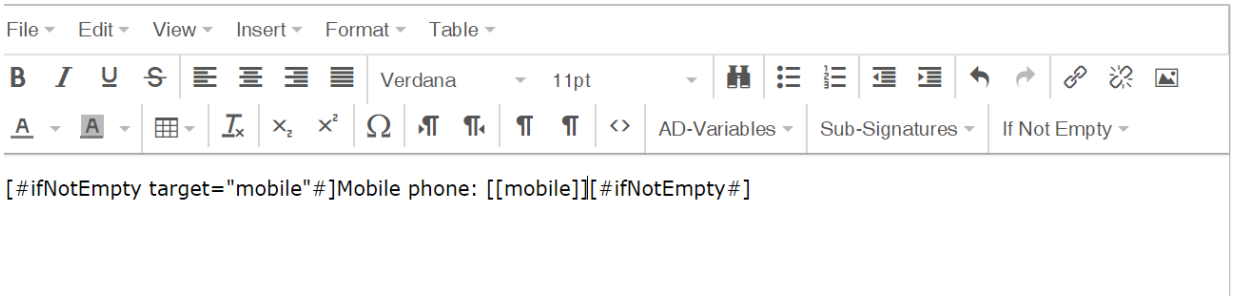


Figura 424: If not empty - Número de teléfono móvil

11. Haga clic en **Guardar** para guardar la firma o nota legal.

Se han ocultado elementos vacíos del Active Directory en una firma o nota legal.

Ejemplo: Ocultación de variables de AD vacías

Se crea la siguiente firma para todos los usuarios:

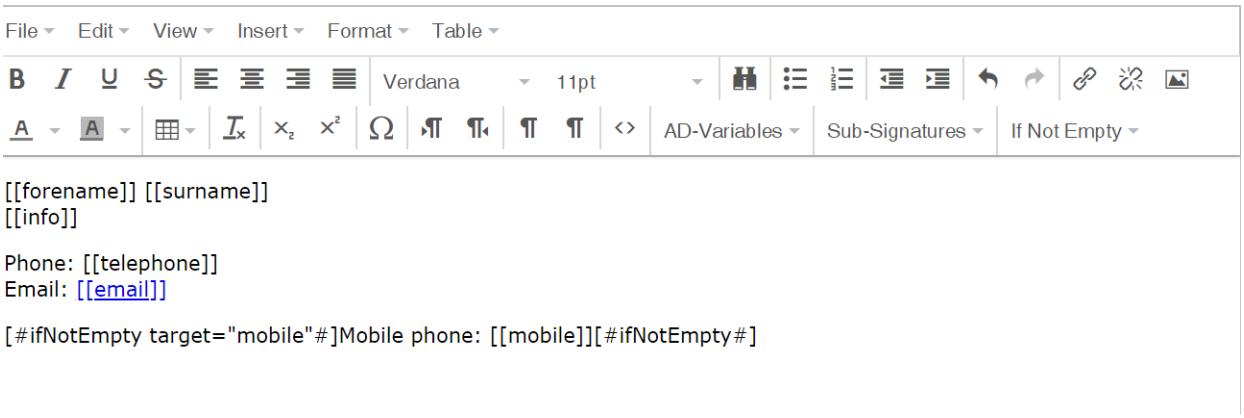


Figura 425: Firma en el editor

La siguiente firma se emite para usuarios con número de teléfono móvil:

Figura 426: Firma con número de teléfono móvil

La siguiente firma se emite para usuarios sin número de teléfono móvil:

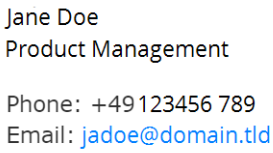


Figura 427: Firma sin número de teléfono móvil

Añadir subfirmas

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588). Ha creado un firma (véase Crear firmas y notas legales en la página 589).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede emplear la función **Sub-Signatures** del editor WYSIWYG (véase Editor WYSIWYG en la página 600) para añadir una firma a otra firma de Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586) a modo de subfirma.

Importante:

Las subfirmas solo pueden emplearse en firmas. Además, debe existir al menos una firma que añadir a otra en calidad de subfirma.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en el que desee crear una firma.

3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Cree o edite una firma (véase Crear firmas y notas legales en la página 589 o Editar o eliminar una firma o nota legal en la página 597).
5. En el editor, seleccione la línea de la firma en la que desee añadir la subfirma.
6. Haga clic en **Sub-Signatures** y seleccione la subfirma deseada de entre las firmas disponibles.

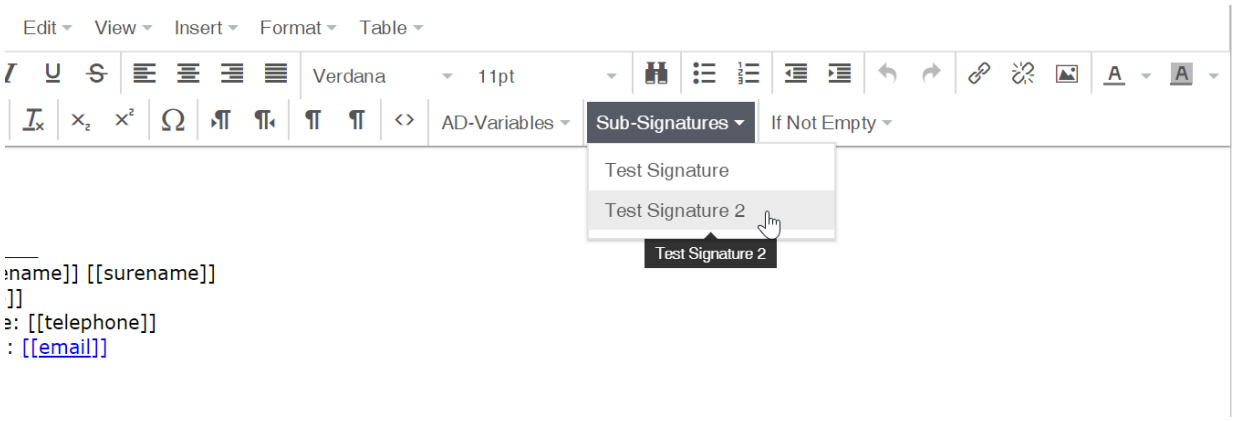


Figura 428: Seleccionar una subfirma

Se añade un comodín para la subfirma.

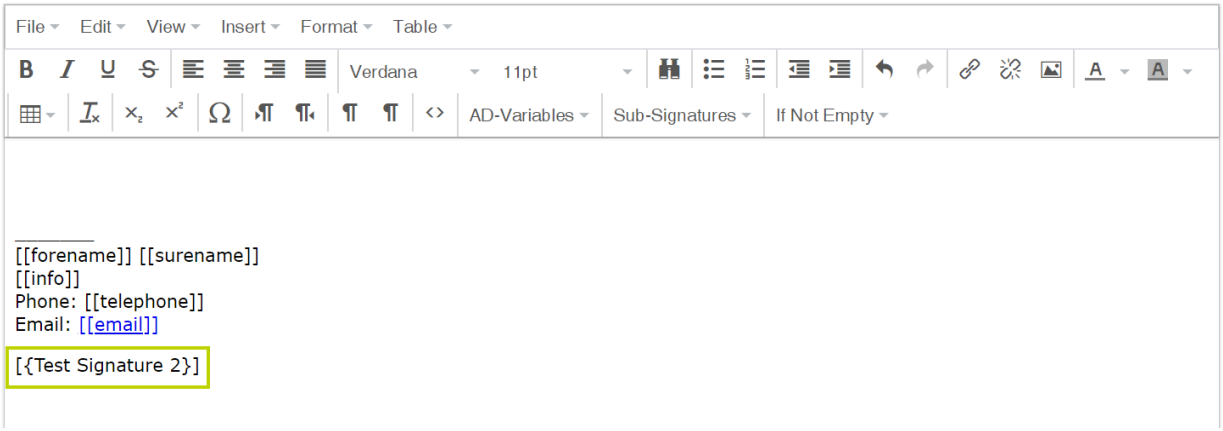


Figura 429: Comodín de subfirma

7. Haga clic en **Guardar** para guardar la firma con subfirma.

8. **Importante:**

   Para poder emplear una firma como subfirma, es necesario activarla previamente.

Para activar una firma para su uso como subfirma, proceda del siguiente modo:

a) Abra el modo de edición de la firma que desee emplear como subfirma.

b) Ponga el interruptor en posición **Cifrado activo**.

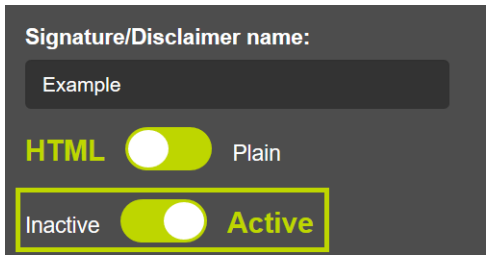


Figura 430: Activar subfirmas

Las firmas activadas y desactivadas están marcadas como tales en la selección de firmas.

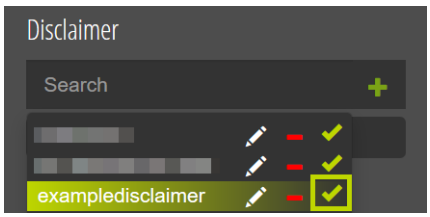


Figura 431: Firma activada en la selección

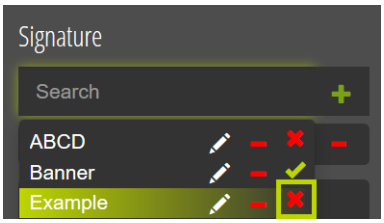


Figura 432: Firma desactivada en la selección

Se ha añadido una subfirma a una firma.

Introducir código fuente HTML

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede añadir código fuente HTML a firmas y notas legales con el editor WYSIWYG.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear un firma o nota legal.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Cree o edite una firma o una nota legal (véase Crear firmas y notas legales en la página 589 o Editar o eliminar una firma o nota legal en la página 597).
5. En el editor WYSIWYG, haga clic en el punto de menú **Tools** y seleccione el punto **Source Code**.

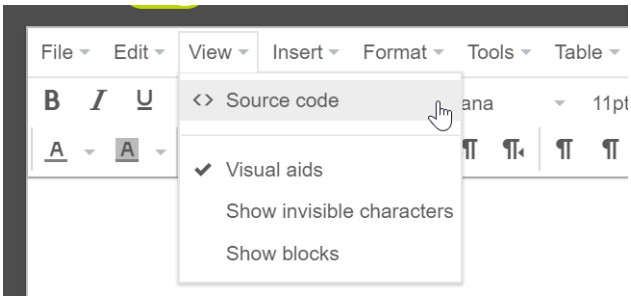


Figura 433: Editor de código fuente

Se abre una nueva ventana de introducción de texto.

6. Introduzca el código fuente HTML deseado y confírmelo con **OK**.

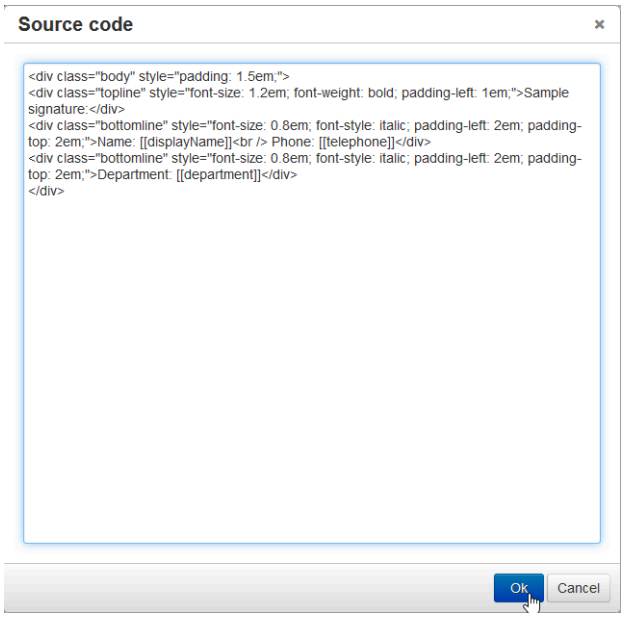


Figura 434: Introducir código fuente

7. A continuación, guarde su plantilla haciendo clic en **Guardar**.

Se ha añadido código fuente HTML a una firma o nota legal.

Ver una vista previa de una firma o una nota legal

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede generar una vista previa de una firma o una nota legal.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear un firma o nota legal.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.

4. Cree o edite una firma o una nota legal (véase Crear firmas y notas legales en la página 589 o Editar o eliminar una firma o nota legal en la página 597).
5. En la parte inferior del editor WYSIWYG, haga clic en **Preview**.

   Se abre una ventana para la previsualización de firmas y notas legales.
6. Seleccione un buzón de correo de la lista situada en el lado izquierdo de la ventana.

   En el lado derecho de la ventana se muestra una vista previa de la firma y/o de la nota legal del usuario seleccionado.

Se ha generado una vista previa de una firma y/o de una nota legal.

Adición de imágenes en Signature and Disclaimer

Con el editor WYSIWYG es posible añadir imágenes a firmas y notas legales. Las imágenes que han de emplearse para todos los buzones de correo de un grupo pueden, o bien añadirse directamente en el editor WYSIWYG con la función de "arrastrar y soltar" (véase Añadir imágenes y añadirles enlaces mediante arrastrar y soltar en la página 621) o bien incrustarse como URL mediante una ventana de introducción de datos (véase Incrustar imágenes mediante una URL en la página 616). También es posible añadir imágenes diferentes a las firmas y notas legales de distintos buzones de correo de un grupo (véase Añadir imágenes distintas para buzones de correo distintos en la página 624).

Incrustar imágenes mediante una URL

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588).

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede añadir una imagen a una firma o nota legal de Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586) mediante una URL.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear un firma o nota legal.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Cree o edite una firma o una nota legal (véase Crear firmas y notas legales en la página 589 o Editar o eliminar una firma o nota legal en la página 597).
5. Durante la creación o edición de la nota legal o firma en el editor WYSIWYG, haga clic en la posición en la que desee añadir la imagen.
6. Desde la barra de menú del editor, vaya a **Insert** > **Image**.

   Se abre un formulario con parámetros adicionales.

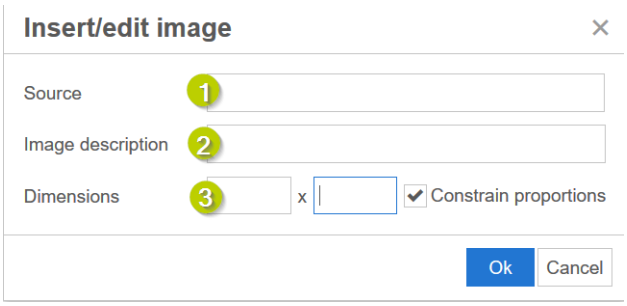


Figura 435: Formulario para imágenes

7. En **Source** (1), introduzca la dirección de la imagen que desee mostrar como elemento representativo para su enlace. Busque la imagen que desee en Internet y copie su dirección.

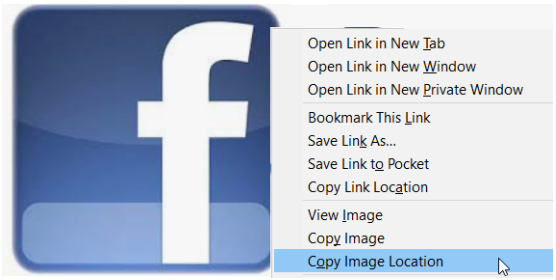


Figura 436: Copiar la dirección de la imagen representativa y añadirla en Source

La dirección la imagen deseada se ha guardado.

8. Si lo desea, introduzca una descripción en **Image description** (2).
9. Ajuste el tamaño de la imagen en **Dimensions** (3) y guarde los ajustes con **Ok**.

Figura 437: Ajustar el tamaño de la imagen

Los parámetros se almacenan y la imagen se muestra en el editor.

10. Haga clic con el botón derecho del ratón en la imagen introducida y seleccione **Enlace** para asignarle una dirección URL.

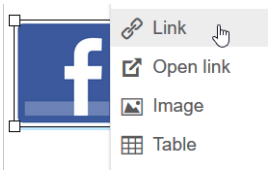


Figura 438: Añadir un enlace a la imagen

Se abre un formulario con parámetros adicionales.

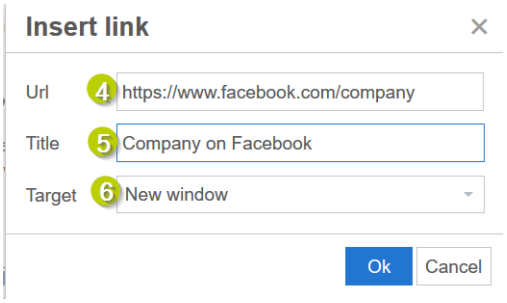


Figura 439: Introducir la URL

11. Indique la dirección de destino de la página web deseada en **URL** (4).
12. Si lo desea, introduzca en **Title** (5) un texto que se mostrará cuando el puntero del ratón se detenga sobre la imagen.
13. Para que la página web enlazada se abra en una nueva pestaña, seleccione la opción **Target** en **New window** (6).
14. Para guardar todos los cambios, haga clic en **Ok** y, a continuación, en **Guardar**.

Nota:

Si desea añadir más imágenes, repita los pasos 1 a 10.

Se ha añadido una imagen a una firma o nota legal mediante una URL.

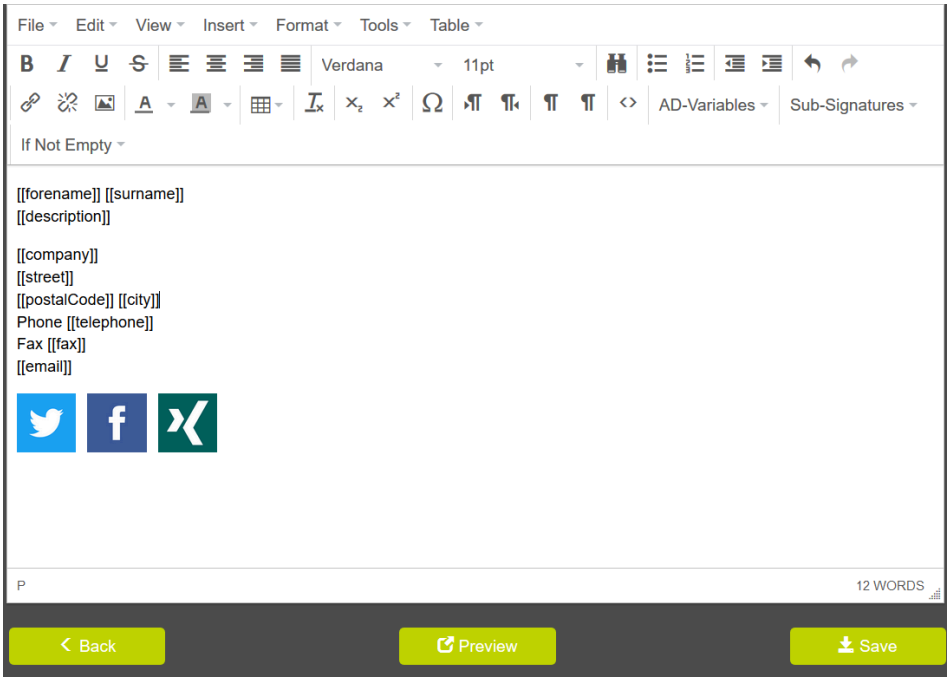


Figura 440: Asignación de variables con imágenes provistas de enlaces

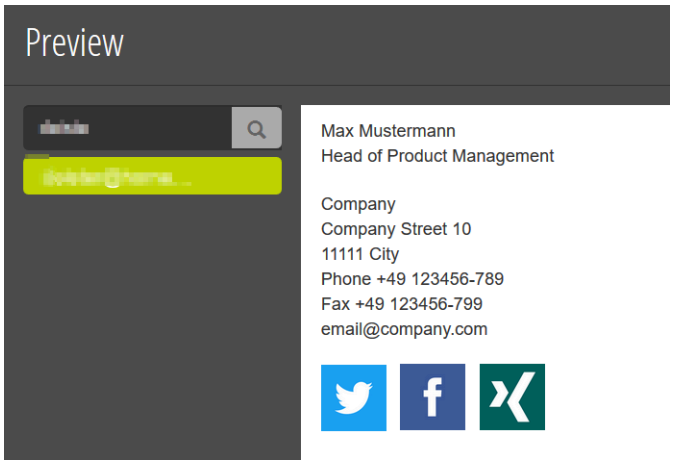


Figura 441: Vista previa de una firma con imágenes provistas de enlaces

Añadir imágenes y añadirles enlaces mediante arrastrar y soltar

En el módulo **Configuración de seguridad** > **Signature and Disclaimer** puede añadir y enlazar una imagen a una firma o nota legal de Signature and Disclaimer (véase Acerca de Signature and Disclaimer en la página 586) mediante "arrastrar y soltar".

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee crear un firma o nota legal.
3. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.
4. Cree o edite una firma o una nota legal (véase Crear firmas y notas legales en la página 589 o Editar o eliminar una firma o nota legal en la página 597).
5. Durante la creación o edición de la nota legal o firma en el editor WYSIWYG, haga clic en la posición en la que desee añadir la imagen.
6. Arrastre la imagen en el editor hasta la posición deseada.

   La imagen se añade en la posición deseada mediante "arrastrar y soltar".

7. Haga clic con el botón derecho del ratón en la imagen introducida y seleccione **Enlace** para asignarle una dirección URL.

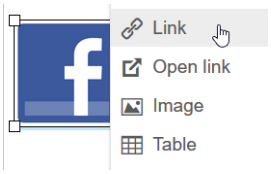


Figura 442: Añadir un enlace a la imagen

Se abre un formulario con parámetros adicionales.

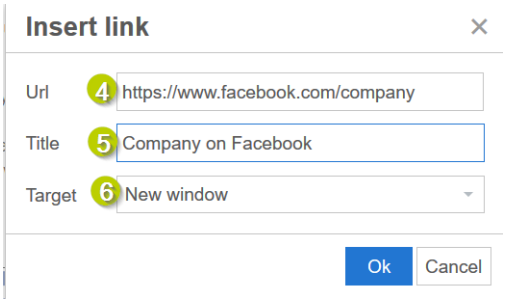


Figura 443: Introducir la URL

8. Indique la dirección de destino de la página web deseada en **URL** (4).
9. Si lo desea, introduzca en **Title** (5) un texto que se mostrará cuando el puntero del ratón se detenga sobre la imagen.
10. Para que la página web enlazada se abra en una nueva pestaña, seleccione la opción **Target** en **New window** (6).
11. Haga clic en **Ok** y cierre el formulario.

Se añade un enlace a la imagen.

12. Opcional: Haga clic en la imagen introducida con el botón derecho del ratón y seleccione **Image** para ajustar su tamaño en el campo **Dimensions**.

13. Para guardar todos los cambios, haga clic en **Ok** y, a continuación, en **Guardar**.

> **Nota:**
>
> Si desea añadir más imágenes, repita los pasos 1 a 9.

Se ha añadido una imagen a una firma o nota legal mediante "arrastrar y soltar".

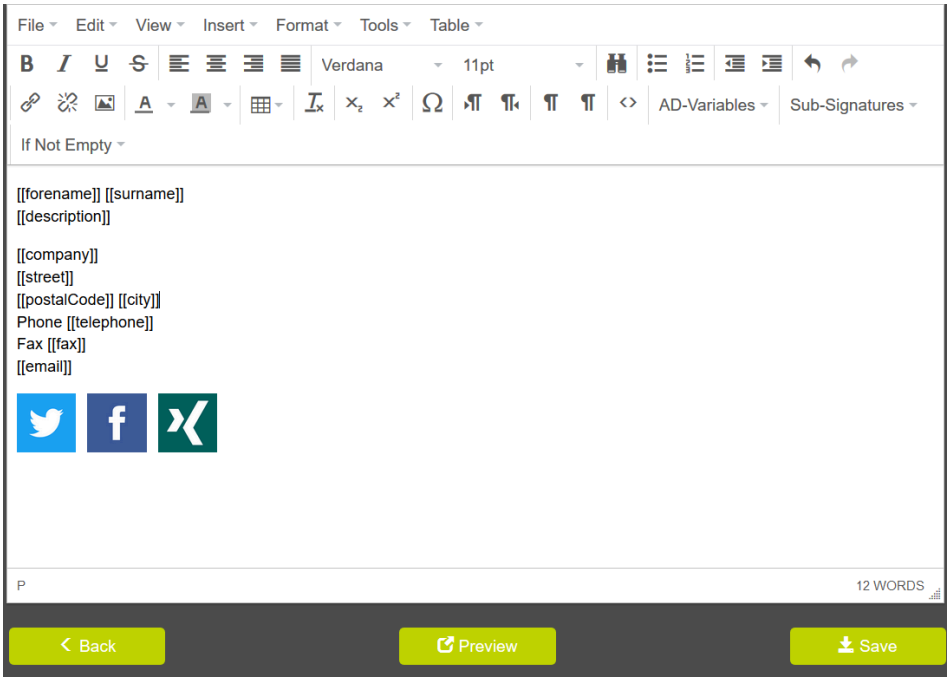


Figura 444: Asignación de variables con imágenes provistas de enlaces

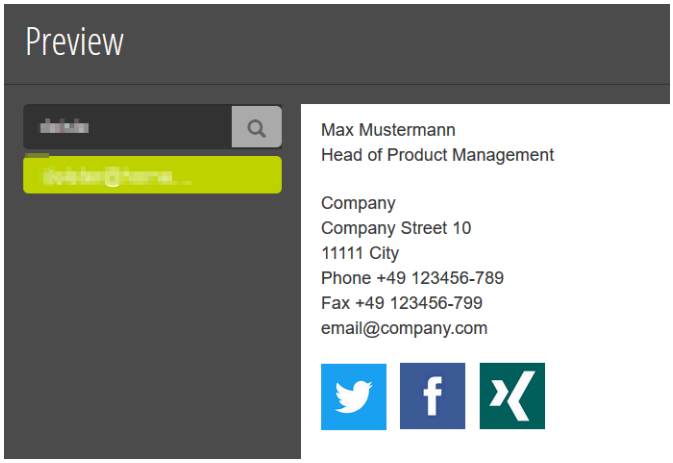


Figura 445: Vista previa de una firma con imágenes provistas de enlaces

Añadir imágenes distintas para buzones de correo distintos

Ha activado Signature and Disclaimer (véase Activar Signature and Disclaimer en la página 588). Ha creado un buzón de correo (véase "Añadir un buzón de correo" en el manual de Control Panel) y lo ha añadido a un grupo (véase "Añadir un buzón de correo a un grupo" en el manual de Control Panel).

Mediante los módulos **Configuración de cliente** > **Buzones** y **Configuración de seguridad** > **Signature and Disclaimer** (véase Acerca de Signature and Disclaimer en la página 586) puede añadir distintas imágenes a las firmas de los distintos buzones de correo de un grupo.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio deseado en la selección de ámbitos.
3. Vaya a **Configuración de cliente** > **Buzones**.

4. Haga clic en la flecha de menú del buzón de correo deseado.

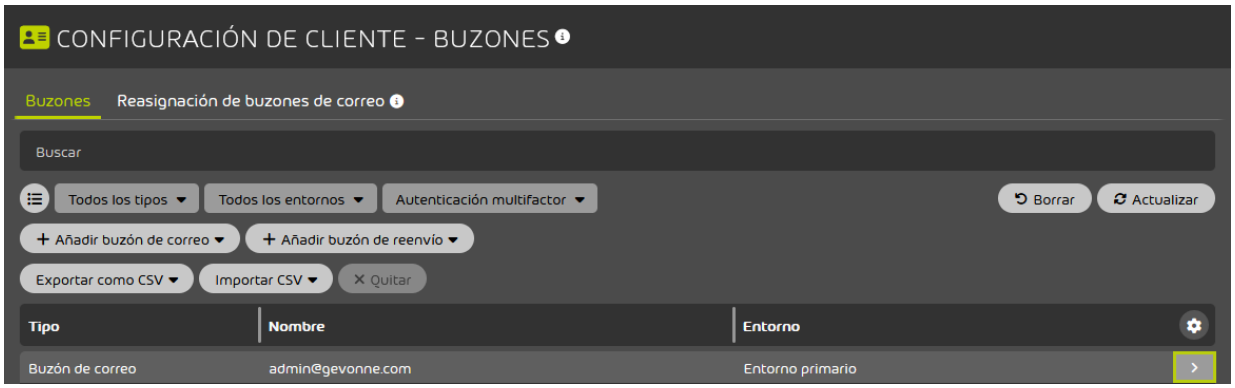


Figura 446: Abrir el menú

Se abre un menú.

5. Haga clic en **Información básica**.

Se despliega un menú desplegable.

6. Introduzca la URL de una imagen en cualquier campo vacío de **Información básica**.

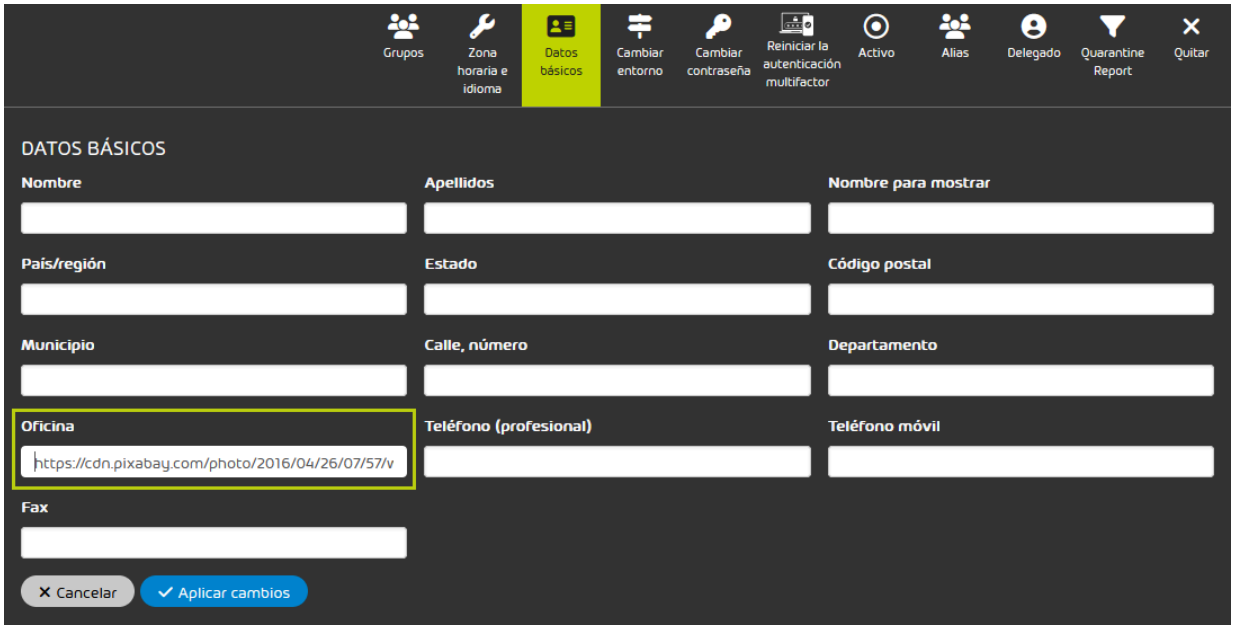


Figura 447: Ejemplo de introducción de dirección de imagen en Oficina

7. Haga clic en **Aplicar cambios**.

Los cambios se guardan.

8. Repita el procedimiento para cada buzón de correo del grupo.
9. Vaya a **Configuración de seguridad** > **Signature and Disclaimer**.

10. Seleccione el grupo en el que se encuentre el buzón editado previamente.

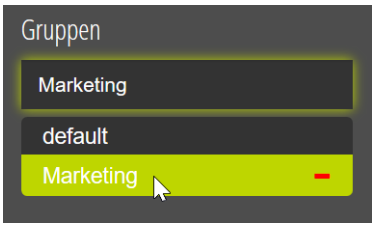
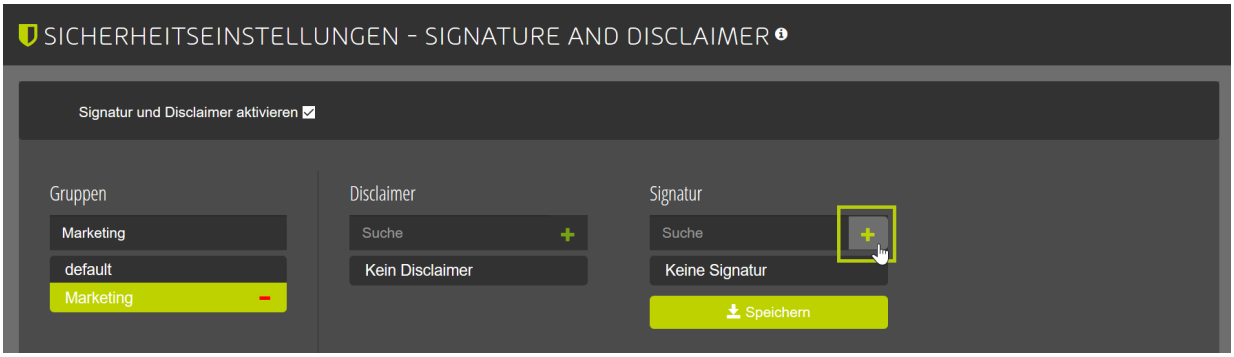


Figura 448: Seleccionar un grupo

El grupo se selecciona.

11. Haga clic en el botón con el símbolo de suma bajo el rótulo **Signature**.



Se abre la ventana **Signature**.

12. Haga clic en el botón **Source code** de la ventana **Signature**.

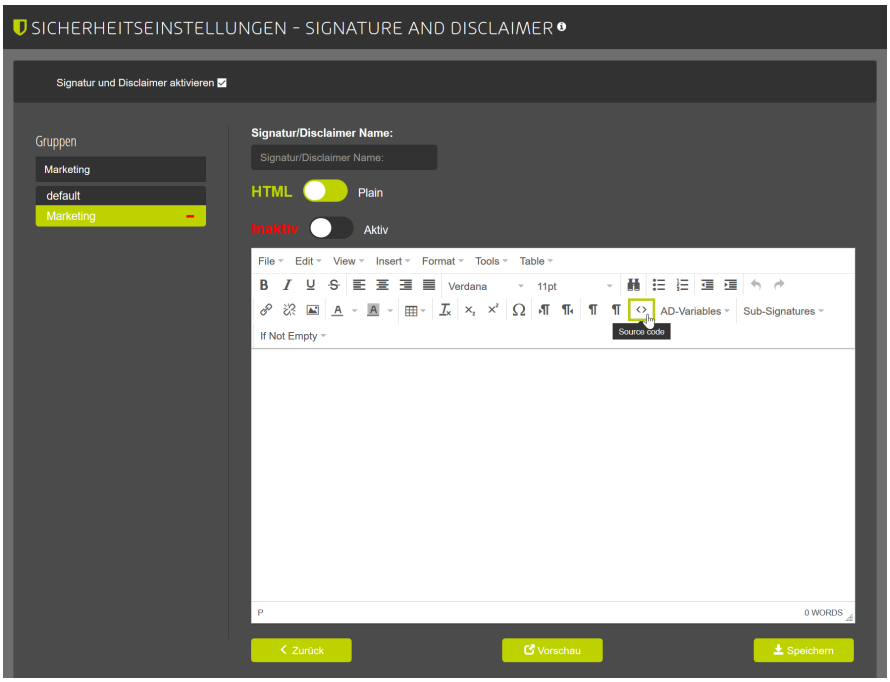


Figura 449: Mostrar código fuente

13.

Nota:

En el atributo **src**, introduzca el nombre del campo de datos básicos en el cual haya introducido la dirección de la imagen. He aquí algunos ejemplos de nombres de campo:

- **Departamento**: department
- **Nombre para mostrar**: displayname
- **Oficina**: office
- **Estado**: state
- **Fax**: fax
- **País/región**: country
- **Municipio**: city
- **Código postal**: postalcode
- **Calle, número**: street
- **Teléfono (profesional)**: telephone
- **Teléfono móvil**: mobile

Introduzca código HTML conforme al siguiente patrón para añadir imágenes:****.

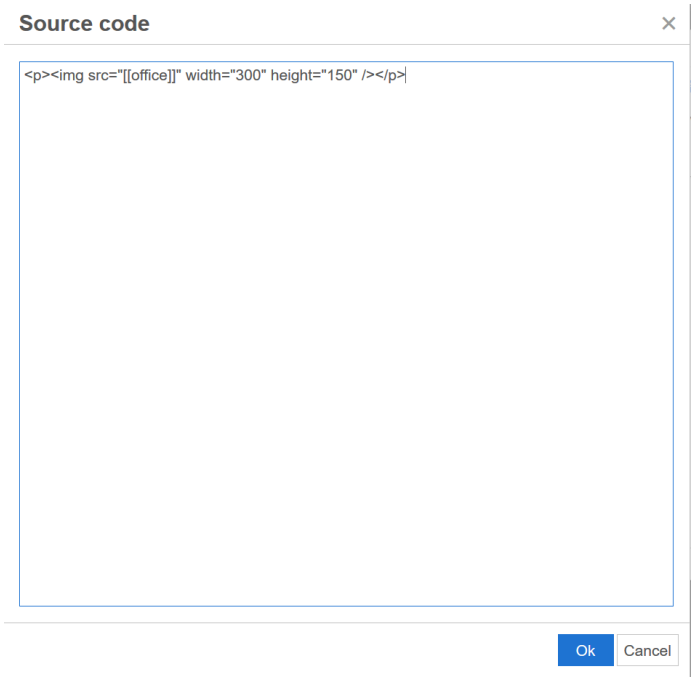


Figura 450: Ejemplo de inserción de una URL de imagen del campo Oficina en la ventana Signature

14. Haga clic en **Aceptar**.

La ventana **Source code** se cierra y aparece la ventana **Signature**.

15. Opcional: Haga clic en el botón **Ver** y seleccione el buzón cuya firma haya editado en último lugar.

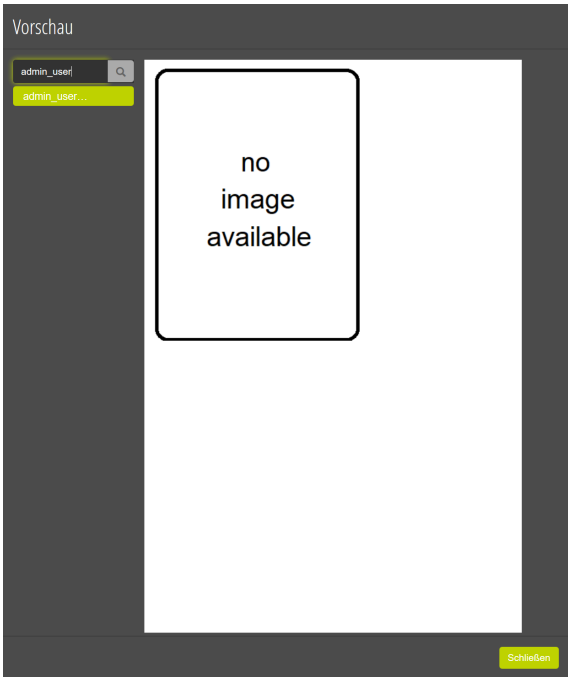


Figura 451: Vista previa de la nueva firma

16. Opcional: Haga clic en **Cerrar**.

    La vista previa se cierra.

17. Introduzca un nombre para la firma creada en el campo **Signature/Disclaimer name**.
18. Haga clic en **Guardar**.

    La firma se guarda.

Se han incrustado distintas imágenes en las firmas de los distintos buzones de correo de un grupo.

Solución de problemas

Al emplear Signature and Disclaimer pueden producirse errores debido a defectos en la configuración. En los siguientes capítulos se explican las causas de errores frecuentes y cómo solucionarlos:

- Solución de problemas: en la página 632
- Solución de problemas: Falta la firma HTML en correos de Mail (Apple) o Thunderbird en la página 633

Solución de problemas:

Condición:

Ha añadido una variable de AD o una subfirma (véase Añadir subfirmas en la página 610) y ésta se muestra de modo incorrecto en la firma creada.

Causa: Variable de AD no disponible

La variable no está creada en el Active Directory.

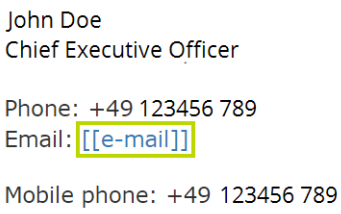


Figura 452: Ejemplo de variable de AD no disponible

Solución

Seleccione las variables de AD de la lista de selección del editor.

Causa: Subfirma no disponible

La firma a la que se hace referencia no se encuentra disponible, o se le ha cambiado el nombre. Por eso no puede integrarse.

Figura 453: Ejemplo de integración de una firma no disponible

Solución

Vuelva a seleccionar la firma a incorporar en el menú desplegable **Sub-Signatures**.

Solución de problemas: Falta la firma HTML en correos de Mail (Apple) o Thunderbird

Estado

A los correos enviados a través de Thunderbird o Mail (Apple) no se les añade la firma HTML, sino la firma en texto sin formato. Si no dispone de una firma en texto sin formato, el mensaje se enviará sin firma.

Causa

Por defecto, algunos clientes de correo, como Mail (Apple) o Thunderbird, envían sus correos como texto sin formato, y no en formato HTML. En tal caso se utiliza la plantilla en texto sin formato definida en **Signature and Disclaimer**.

Solución para Mail (Apple) con MacOS

Lea Usar texto normal o texto con formato en correos electrónicos en Mail en el Mac y siga las instrucciones del fabricante.

Truco para Mail (Apple) con iOS

Escriba uno o varios caracteres del texto de su correo en negrita, cursiva o subrayado.

El cliente enviará el correo en formato HTML, y **Signature and Disclaimer** le añadirá la firma en HTML.

Solución para Thunderbird

- Para correos individuales: Seleccione **Redactar** > **Opciones** > **Formato de entrega** > **Solo texto enriquecido (HTML)**.

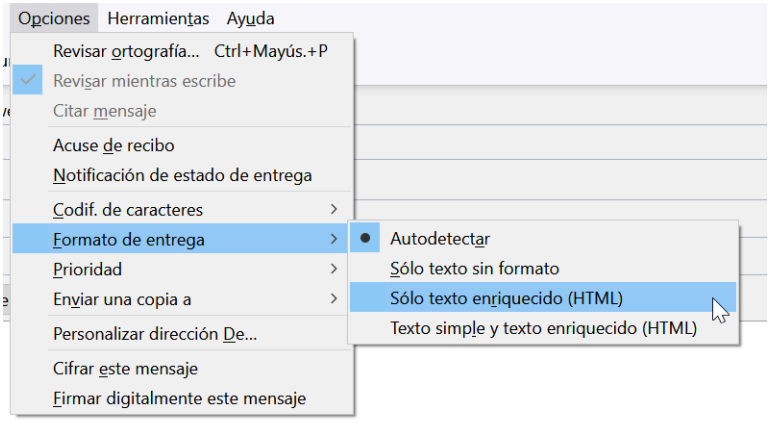


Figura 454: Ajustes para un solo correo

- Para todos los correos: Seleccione **Redactar** > **Herramientas** > **Configuración de cuenta** > **Redacción y direcciones** y marque la casilla **Redactar mensajes en formato HTML**.

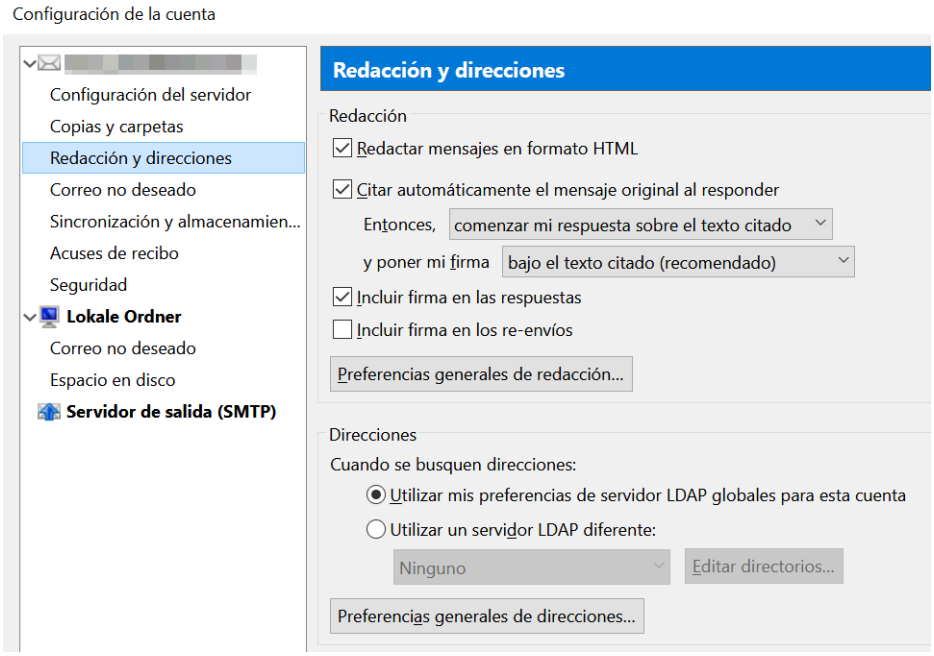


Figura 455: Ajustes para todos los correos:

Solución de problemas: Problemas al reservar salas en Microsoft 365

Estado

No es posible reservar salas en Microsoft 365 después de haber activado Signature and Disclaimer.

Causa

Para reservar las salas, Microsoft 365 emplea buzones de correo especiales denominados "buzones de sala" que solo admiten correos procedenetes de su misma organización. Tras activar Signature and Disclaimer, sus correos se desvían a nuestros servidores para que sea posible adjuntarles las firmas y notas legales. Los correos desviados a nuestros servidores se consideran correos externos y no son aceptados por los buzones de sala.

Solución

1. Abra la shell de administración de Exchange.
2. Ejecute la siguiente orden:

   Set-CalendarProcessing "" -ProcessExternalMeetingMessages $True

   Se permite la aceptación de correos externos por parte de los buzones de sala.

Continuity Service

Sobre Continuity Service

Con Continuity Service, los usuarios pueden seguir recibiendo y enviando mensajes de correo electrónico en caso de avería de su propio servidor de correo electrónico. Una vez configurado Continuity Service para un dominio o un usuario suelto, Continuity Service se activará automáticamente en caso de avería del servidor de correo electrónico.

Si los usuarios se sincronizan mediante LDAP, es preciso que definan una contraseña de emergencia (véase Activar la contraseña de emergencia) para poder acceder al servicio de correo web de Continuity Service.

Importante:

Continuity Service es un sistema en modo de espera. Si un cliente activa el servicio solo después de que su propio servidor de correo electrónico haya fallado, Continuity Service tardará unas horas en hacerse efectivo. Por tanto, los correos enviados mientras tanto se pueden perder. Para poder mantener el tráfico de correo de manera fiable, Continuity Service debe estar permanentemente activado.

Para los dominios con Continuity Service activado, los correos de los últimos tres meses se almacenan en el archivo de correos electrónicos. Además, en el módulo **Email Live Tracking** (véase

"Email Live Tracking" en el manual de Control Panel), el usuario puede ver cuáles de sus correos se han entregado mediante Continuity Service.

Nota:

Los correos entregados mediante Continuity Service mantienen el estado **Aplazado** incluso tras su entrega.

A continuación se describen las opciones de configuración de Continuity Service:

- Activar Continuity Service (véase Activar Continuity Service)
- Añadir todos los usuarios de un dominio a Continuity Service (véase Añadir todos los usuarios de un dominio a Continuity Service en la página 637)
- Añadir usuarios sueltos a Continuity Service (véase Añadir usuarios sueltos a Continuity Service en la página 638)
- Excluir usuarios de Continuity Service (véase Excluir usuarios de Continuity Service en la página 640)
- Activar la contraseña de emergencia (véase Activar la contraseña de emergencia)
- Desactivar Continuity Service (véase Desactivar Continuity Service)

Añadir todos los usuarios de un dominio a Continuity Service

Ha activado Continuity Service (véase Activar Continuity Service).

En el módulo **Configuración de seguridad** > **Continuity Service** puede añadir todos los usuarios de un dominio a Continuity Service (véase Sobre Continuity Service en la página 636) para poder mantener el tráfico de correo de sus buzones en caso de avería de su propio servidor de correo electrónico.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Continuity Service**.

4. **Importante:**

   Si cambia de la opción **Solo usuarios seleccionados** a la opción **Todos los usuarios**, se quitarán todos los usuarios introducidos hasta el momento.

   Para activar Continuity Service para todos los usuarios del dominio, marque la casilla **Todos los usuarios**.

   Si ha añadido anteriormente usuarios sueltos a Continuity Service, aparecerá un mensaje de advertencia.

5. Si aparece un mensaje de advertencia, haga clic en **Confirmar**.

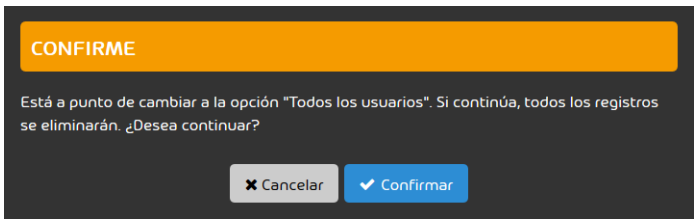


Figura 456: Confirmar

Continuity Service comienza a aplicarse a todos los usuarios del dominio.

Todos los usuarios de un dominio se han añadido a Continuity Service.

Añadir usuarios sueltos a Continuity Service

Ha activado Continuity Service (véase Activar Continuity Service).

En el módulo **Configuración de seguridad** > **Continuity Service** puede añadir usuarios concretos de un dominio a Continuity Service (véase Sobre Continuity Service en la página 636) para poder

mantener el tráfico de correo de sus buzones en caso de avería de su propio servidor de correo electrónico.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Continuity Service**.
4. Marque la casilla **Solo usuarios seleccionados**.
5. En **Usuarios de Continuity Service**, haga clic en **Añadir**.

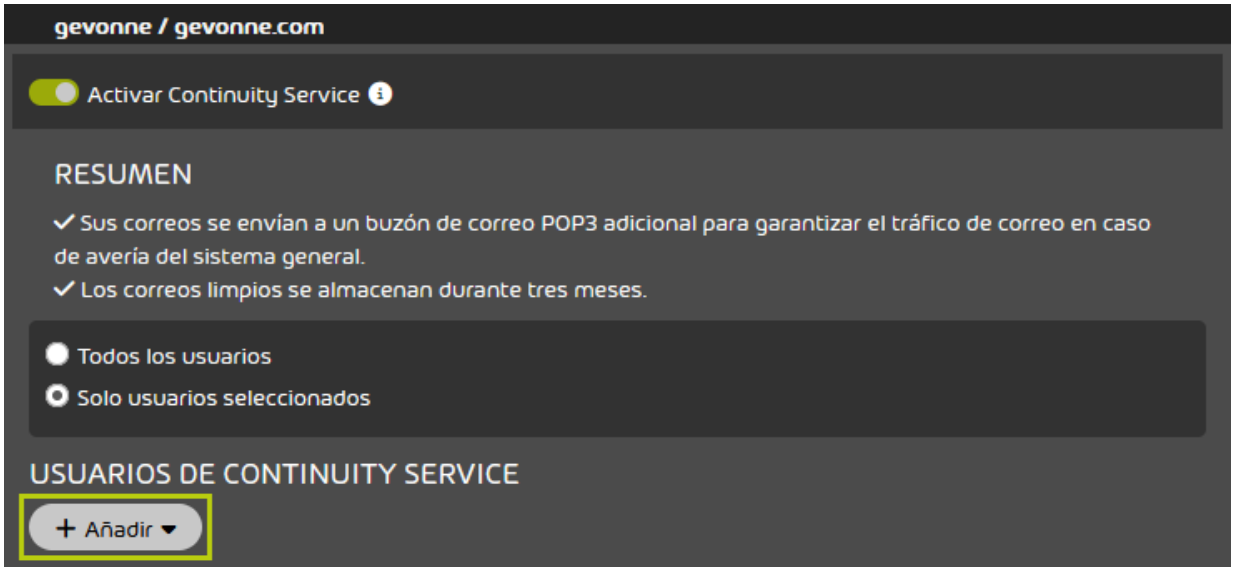


Figura 457: Añadir usuarios

Se abre una vista avanzada.

6. Introduzca la dirección de correo del usuario que desee añadir en **Seleccionar usuario**.

> **Nota:**
>
> Para activar la función de sugerencias automáticas, introduzca al menos tres caracteres seguidos.

7. Haga clic en **Añadir**.

Figura 458: Indicar usuario

El usuario se añade y aparece en la tabla. Continuity Service deja de aplicarse a dicho usuario.

Se ha añadido un usuario suelto a Continuity Service.

Excluir usuarios de Continuity Service

Ha añadido usuarios individuales a Continuity Service (véase Añadir usuarios sueltos a Continuity Service en la página 638).

En el módulo **Configuración de seguridad** > **Continuity Service** puede usted excluir usuarios que no necesite asegurar mediante Continuity Service.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. Seleccione el dominio en la selección de ámbitos.
3. Vaya a **Configuración de seguridad** > **Continuity Service**.

4. Para excluir un usuario de Continuity Service, haga clic sobre la cruz de la columna **Quitar usuario** del mismo.

Figura 459: Quitar un usuario

El usuario se retira de la lista. Continuity Service deja de aplicarse a dicho usuario.

Se ha excluido un usuario de Continuity Service.

Personalización

Personalización de Control Panel

En el módulo **Personalización**, los administradores pueden personalizar Control Panel a dos niveles.

Por una parte, los administradores pueden determinar la apariencia de los correos enviados por Control Panel (véase Personalizar la plantilla de correos electrónicos en la página 649) y registrar los datos de contacto a incluir en ellos (véase Personalizar datos mostrados en correos electrónicos en la página 646).

Nota:

También las notificaciones por correo electrónico de Websafe (véase "Websafe en el manual de Control Panel) se adaptan mediante estos ajustes.

Por la otra, los administradores pueden personalizar la apariencia tanto de la página web de Control Panel como de la aplicación web dinámica y definir un URL para la primera y un nuevo nombre para la segunda (véase Personalizar Control Panel en la página 653).

Los ajustes se muestran para todos los usuarios que inicien sesión en el dominio registrado.

Atención:

La activación de un Control Panel personalizado conlleva costes adicionales conforme a la lista de precios.

Importante:

Si un administrador a nivel de cliente no ha guardado ajustes para su dominio en alguna de las pestañas del módulo **Personalización**, se aplicarán a dicho dominio los ajustes que el partner más inmediato haya realizado en dicho módulo. Si no se han guardado ajustes a nivel de su partner o del partner de su partner, no se aplicará ninguna personalización.

Importante:

Los datos de soporte técnico (véase Añadir datos de soporte técnico a Control Panel en la página 643) deben registrarse incluso si no se emplea ninguna otra opción de personalización. Los datos de soporte técnico se muestran a los usuarios en Control Panel.

Añadir datos de soporte técnico a Control Panel

En la pestaña **Información de soporte técnico** del módulo **Personalización** (véase Personalización de Control Panel en la página 642) puede registrar la información de soporte técnico de su empresa para mostrarla a los usuarios en Control Panel. Esta opción es independiente de la personalización de Control Panel, la cual conlleva costes adicionales. Los datos introducidos se muestran también en la versión estándar de Control Panel.

Nota:

Los ajustes de un partner se aplican también a sus partners subordinados y clientes siempre que éstos no hayan realizado sus propios ajustes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee realizar ajustes.

3. Vaya a **Personalización** > **Información de soporte técnico**.

Figura 460: Seleccionar "Información de soporte"

4. En el campo **Número de teléfono de soporte**, introduzca el número de teléfono destinado a consultas de soporte técnico en su empresa.

> **Nota:**
>
> Si uno de los campos aquí descritos se encuentra vacío en la configuración de un cliente o partner, se empleará el valor que haya introducido en el mismo el siguiente partner que lo preceda en la jerarquía. Si dicho campo está vacío en las configuraciones de todos sus partners superiores, se emplearán los valores por defecto de Control Panel.

5. En el campo **Dirección de correo electrónico de soporte**, introduzca la dirección de correo electrónico destinada a consultas de soporte técnico en su empresa.

Figura 461: Introducir información de soporte

6. Haga clic en **Guardar**.

Los datos de soporte técnico se han registrado en Control Panel.

A continuación puede adaptar los correos enviados por Control Panel a su empresa (véase Personalizar correos electrónicos de Control Panel en la página 645) y personalizar el aspecto de Control Panel (véase Personalizar Control Panel en la página 653).

Personalizar correos electrónicos de Control Panel

Control Panel envía correos automáticamente en determinadas situaciones (por ejemplo, cuando un usuario solicita una nueva contraseña en Control Panel (véase "Restablecer la contraseña" en el manual de Control Panel)). Puede adaptar a su empresa tanto la apariencia de los correos enviados por Control Panel como los datos que éstos contienen.

1. Adapte los datos de correo electrónico a su empresa (véase Personalizar datos mostrados en correos electrónicos en la página 646).

   Los correos enviados por Control Panel contienen una nota legal personalizada, el nombre de un interlocutor de la empresa y una dirección de remitente personalizada.

2. Adapte la apariencia de los correos electrónicos a su empresa (véase Personalizar la plantilla de correos electrónicos en la página 649).

   El color de los pies de página, la paleta cromática (tema) de los correos y el logotipo del encabezado se personalizan.

La apariencia de los correos enviados por Control Panel y sus datos se han personalizado.

A continuación puede personalizar la apariencia de Control Panel (véase Personalizar Control Panel en la página 653).

Personalizar datos mostrados en correos electrónicos

En la pestaña **Información de correo electrónico** del módulo **Personalización** (véase Personalización de Control Panel en la página 642) puede definir un saludo, una dirección de contacto, una dirección de remitente y una nota legal para los correos enviados por Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee realizar ajustes.

3. Vaya a **Personalización** > **Información de correo electrónico**.

Se muestra un formulario.

Figura 462: Información de correo electrónico

4. Cumplimente el formulario. Los campos tienen los siguientes significados:

   - **Nombre de partner**: Aquí se introduce el nombre de la empresa mencionada en el saludo al principio de los correos (p. ej., "Estimado cliente de <Nombre de empresa>:").
   - **Contacto**: Aquí se introduce el texto para la firma que se muestra en los correos bajo la fórmula de despedida (p. ej., "Su equipo de Control Panel").
   - **Dirección de remitente para plantillas de correos**: Aquí se introduce la dirección del remitente de los correos enviados por Control Panel.

     Nota:

     Esta dirección de remitente no se aplica a los correos enviados por Websafe (véase el capítulo "Websafe" en el manual de Control Panel).

     Nota:

     Si un cliente ha activado la comprobación SPF (véase el capítulo "Activar la comprobación SPF" en el manual de Control Panel), nuestro registro SPF debe estar registrado en la zona de DNS del dominio de la dirección del remitente (véase el capítulo "Definir un registro SPF" en el manual de Control Panel). De lo contrario, las comprobaciones SPF de los correos enviados por Control Panel acabarán en error (véase el capítulo "Lógica de la comprobación SPF" en el manual de Control Panel).

   - **Nombre de remitente**: Aquí se introduce el nombre para mostrar del remitente.
   - **Nota legal**: Aquí se introduce la nota legal de la empresa.

     Nota:

     Si alguno de estos campos se encuentra vacío en la configuración de un cliente o partner, se empleará el valor que haya introducido en el mismo el siguiente partner que lo preceda en la jerarquía. Si dicho campo está vacío en las configuraciones de todos sus partners superiores, se emplearán los valores por defecto de Control Panel.

5. Haga clic en **Guardar**.

Los datos de correo electrónico se han personalizado.

A continuación puede adaptar la apariencia de los correos enviados por Control Panel a su imagen corporativa (véase Personalizar la plantilla de correos electrónicos en la página 649) y personalizar el aspecto de Control Panel (véase Personalizar Control Panel en la página 653).

Personalizar la plantilla de correos electrónicos

En la pestaña **Plantilla de correos** del módulo **Personalización** (véase Personalización de Control Panel en la página 642) puede adaptar la apariencia de los correos enviados por Control Panel a su imagen corporativa. Personalizar la plantilla de correos electrónicos es una opción sin coste adicional que no requiere personalizar el propio Control Panel, que sí conlleva costes adicionales. Sin embargo, si personaliza Control Panel, el color primario, el tema y el logotipo de la pestaña **Plantilla de correos** se emplearán también en Control Panel (véase Personalizar la apariencia y el URL de Control Panel en la página 654).

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee realizar ajustes.
3. Vaya a **Personalización** > **Plantilla de correos**.

Figura 463: Seleccionar una pestaña

4. Seleccione un color para el pie de página de los correos enviados por Control Panel.

a) Haga clic en el campo bajo **Color principal**.

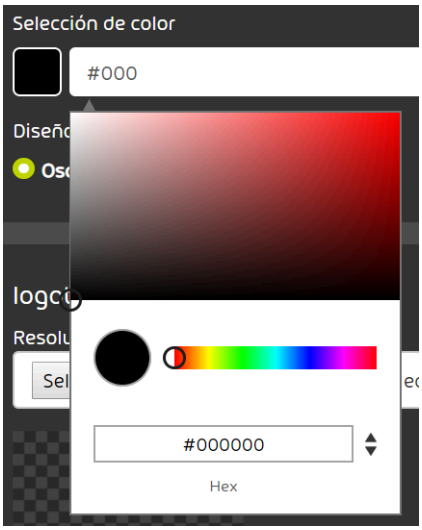


Figura 464: Seleccionar un color

b) Seleccione un color. Puede, o bien seleccionar el color deseado en el selector de colores, o bien introducir el código del mismo en HEX, RGB o HSL dentro del campo.

> **Nota:**
>
> Si personaliza también Control Panel, el color seleccionado se empleará también como color primario de Control Panel (véase Personalizar la apariencia y el URL de Control Panel en la página 654).

El color seleccionado se muestra dentro del círculo, y su código se muestra en HEX, RGB o HSL.

Figura 465: Pie de página en color en un informe de cuarentena

5. Seleccione un tema para sus correos en **Diseño**. Tiene dos opciones:

   - **Oscuro**: Se selecciona un tema oscuro. Los correos se muestran en colores oscuros.

Figura 466: Correo con tema oscuro

   - **Claro**: Se selecciona un tema claro. Los correos se muestran en colores claros.

Figura 467: Correo con tema claro

6. Haga clic en el botón **Buscar** bajo **Logotipo** y seleccione su logotipo.

> **Nota:**
>
> Los mejores resultados se obtienen con logotipos de 160 × 80 píxeles de resolución.
>
> Solo se admite el formato .png.
>
> El logotipo se mostrará en el encabezado de los correos enviados por Control Panel.

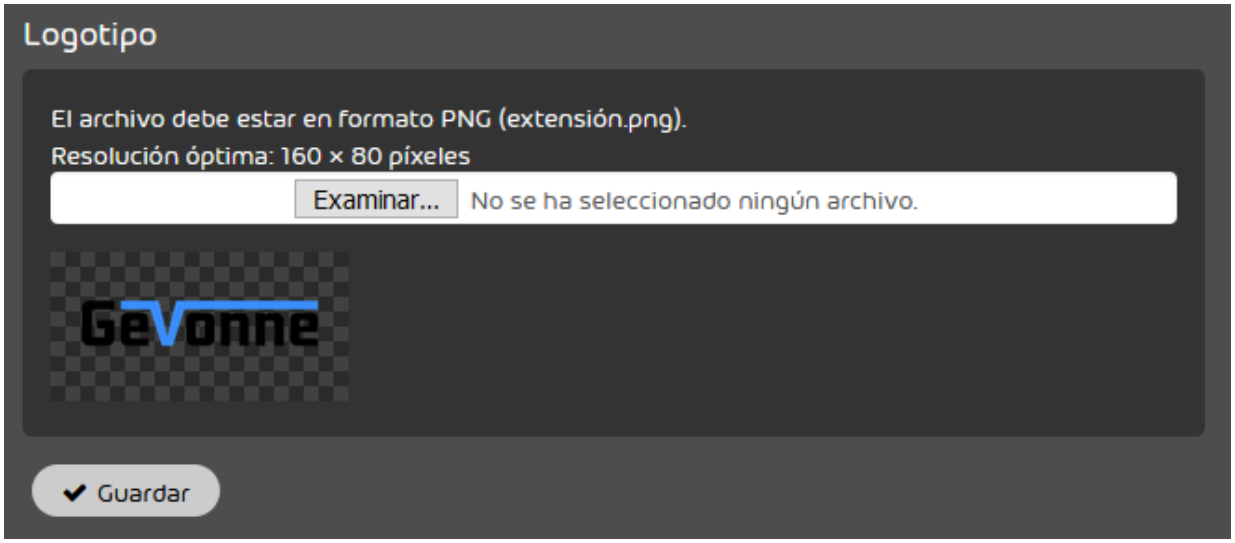


Figura 468: Seleccionar logotipo

7. Haga clic en **Guardar**.

Ha personalizado la apariencia de los correos electrónicos enviados por Control Panel.

A continuación puede cambiar los datos mostrados en los correos enviados por Control Panel por los de su empresa (véase Personalizar datos mostrados en correos electrónicos en la página 646) y personalizar la apariencia de Control Panel (véase Personalizar Control Panel en la página 653).

Personalizar Control Panel

Puede personalizar el aspecto de Control Panel indicando un URL de su dominio e incorporando los colores, el logotipo y el Favicon de su empresa.

1. Defina un URL de su dominio para Control Panel y establezca un redireccionamiento a el URL estándar de Control Panel para ella mediante un registro CNAME en la zona de DNS de su domino.

   A continuación se define un registro CNAME para **controlpanel.dominiodecliente.es**:

   controlpanel.dominiodecliente.es IN CNAME <URL estándar>

   > **Nota:**
   >
   > Puede solicitar el URL estándar de Control Panel al soporte técnico.

2. Personalice la apariencia y el URL de la página web de Control Panel (véanse Personalizar la apariencia y el URL de Control Panel en la página 654 y Personalizar la plantilla de correos electrónicos en la página 649).
3. Personalice el nombre y el icono de la aplicación web dinámica con el diseño de su empresa (véase Personalizar la aplicación web dinámica en la página 658).
4. Defina los datos de soporte (número de teléfono y dirección de correo electrónico) que mostrar a los usuarios en Control Panel (véase Añadir datos de soporte técnico a Control Panel en la página 643).

> **Nota:**
>
> Esta opción es independiente de la personalización de Control Panel, la cual conlleva costes adicionales. Los datos de contacto introducidos se muestran también en la versión estándar de Control Panel.

Figura 469: Datos de contacto en Control Panel

5. **Atención:**

   La creación de una versión personalizada de Control Panel conlleva costes adicionales conforme a la lista de precios.

   PRECAUCIÓN:

   Asegúrese de haber introducido todos los datos y el URL para su Control Panel personalizado en el módulo **Personalización**.

   Para personalizar Control Panel conforme a la información y datos aportados, póngase en contacto con nuestro soporte técnico.

Control Panel se ha personalizado.

Personalizar la apariencia y el URL de Control Panel

Ha personalizado con éxito la plantilla de correos electrónicos (véase Personalizar la plantilla de correos electrónicos en la página 649).

En la pestaña **Control Panel** del módulo **Personalización** (véase Personalización de Control Panel en la página 642) puede adaptar la apariencia de Control Panel a su imagen corporativa. El color primario, el tema y el logotipo del Control Panel personalizado se obtienen de los ajustes de la pestaña **Plantilla de correos**.

Nota:

He aquí algunos ejemplos de los efectos que tienen los ajustes de la pestaña **Plantilla de correos** sobre el Control Panel personalizado (véase Personalizar la plantilla de correos electrónicos en la página 649).

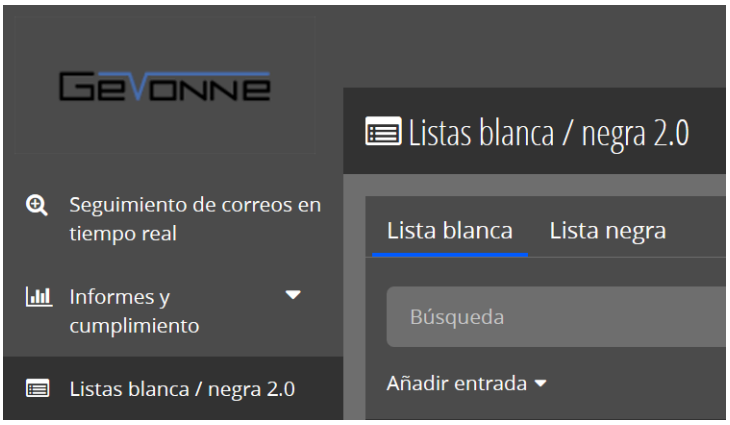


Figura 470: Vista de Control Panel con tema oscuro y logotipo personalizado

Figura 471: Vista de Control Panel con tema claro y logotipo personalizado

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee realizar ajustes.

3. Vaya a **Personalización** > **Control Panel**.

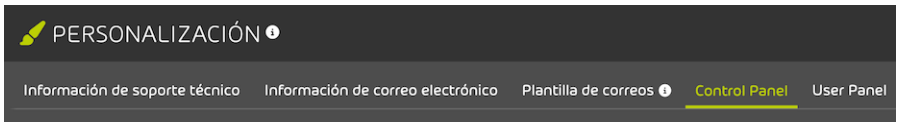


Figura 472: Seleccionar una pestaña

4. **Importante:**

   La personalización de Control Panel solo está disponible para partners o clientes con un mínimo de 5.000 usuarios.

   Accione el interruptor **Activar la personalización de Control Panel**.

   Se muestra una ventana de confirmación.

5. **Atención:**

   La personalización de Control Panel conlleva costes adicionales.

   Haga clic en **Confirmar**.

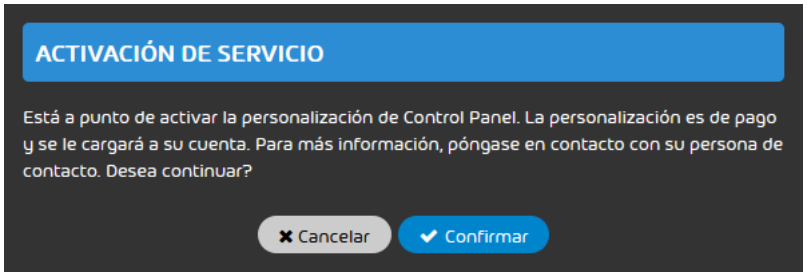


Figura 473: Confirmar

Los ajustes de la pestaña **Control Panel** se habilitan.

6. **PRECAUCIÓN:**

   La personalización de Control Panel solo funciona si el URL del Control Panel personalizado apunta al URL de la versión estándar de Control Panel mediante un registro CNAME.

   Asegúrese de que el URL apunte al URL de la versión estándar de Control Panel mediante un registro CNAME (véase Personalizar Control Panel en la página 653).

   Introduzca en **URL** el URL de su dominio a través del cual desee acceder a su Control Panel personalizado.

   El URL debe seguir el siguiente patrón: **controlpanel.dominiodecliente.es**

7. Bajo **Favicon**, haga clic en el botón **Buscar** y seleccione su favicon.

   Nota:

   El favicon debe cargarse en formato ICO (extensión *.ico). Para una calidad de visualización óptima se necesita una resolución de al menos 128 × 128 píxeles.

Figura 474: Seleccionar favicon

8. Personalice la aplicación web dinámica (véase Personalizar la aplicación web dinámica en la página 658).

9. Haga clic en **Guardar**.

   Nota:

   Los ajustes de Control Panel tardan un máximo de 5 minutos en surtir efecto.

10. Actualice la página web para que se muestren sus ajustes.

> **Nota:**
>
> Los cambios solo se verán a través del URL del Control Panel personalizado.

La apariencia y el URL de Control Panel se han personalizado con coste adicional.

A continuación puede personalizar la apariencia de la aplicación web dinámica (véase Personalizar la aplicación web dinámica en la página 658) y registrar datos de soporte técnico (véase Añadir datos de soporte técnico a Control Panel en la página 643).

Personalizar la aplicación web dinámica

Ha activado la personalización de Control Panel (véase Personalizar la apariencia y el URL de Control Panel en la página 654).

En la pestaña **Control Panel** del módulo **Personalización** (véase Personalización de Control Panel en la página 642) puede adaptar el nombre y el icono de la aplicación web dinámica a su imagen corporativa.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que desee realizar ajustes.
3. Vaya a **Personalización** > **Control Panel**.
4. En **Nombre de la aplicación**, introduzca el nombre que aparecerá en la ventana de inicio de los dispositivos móviles.

Figura 475: Introducir el nombre de la aplicación

5. Cargue una imagen en **Icono de la aplicación**.

> **Nota:**
>
> Solo se admite el formato .png.

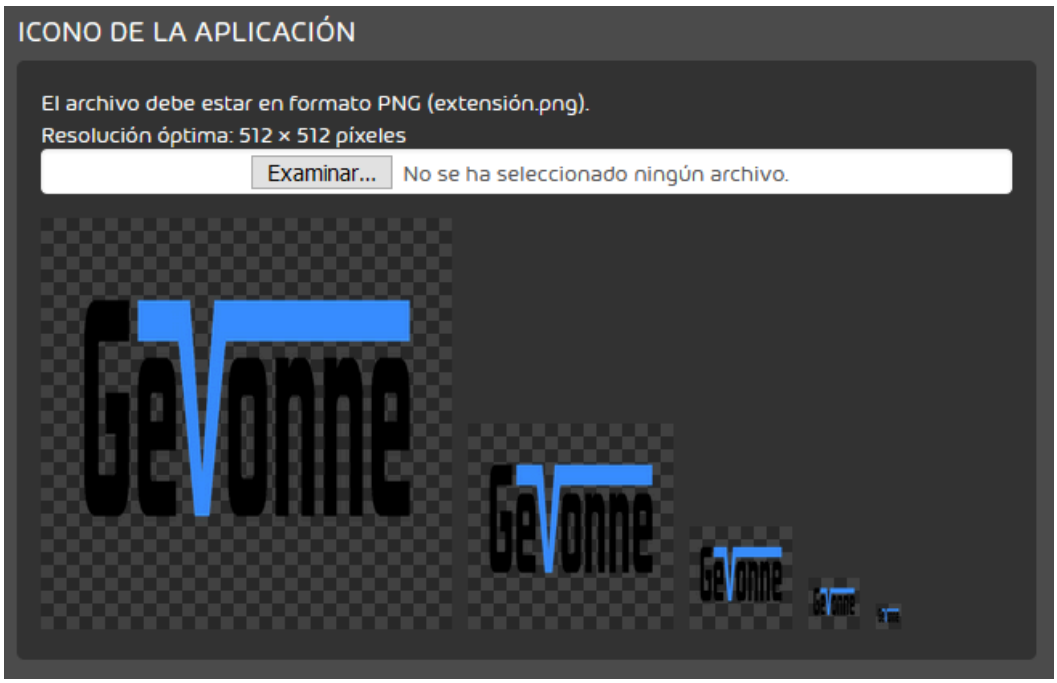


Figura 476: Cargar el icono de la aplicación

Bajo el botón de selección del icono de la aplicación se muestra una vista previa del icono en distintos tamaños. Además, en la sección **Pantalla de presentación** se muestra una vista

previa de la pantalla de presentación. Esta pantalla de presentación se muestra mientras se carga la aplicación web dinámica y contiene el archivo de imagen cargado en **Logotipo**.

Figura 477: Vista previa de la pantalla de presentación

6. Haga clic en **Guardar**.

El nombre y el logotipo de la aplicación web dinámica se han personalizado.

A continuación puede personalizar la apariencia de Control Panel (véase Personalizar la apariencia y el URL de Control Panel en la página 654) y registrar datos de soporte técnico (véase Añadir datos de soporte técnico a Control Panel en la página 643).

Modificar los módulos mostrados en User Panel

En la pestaña **User Panel** del módulo **Personalización** (véase Personalización de Control Panel en la página 642) puede modificar los módulos mostrados en User Panel.

Nota:

Si desea modificar la apariencia de User Panel, debe personalizar Control Panel (véase Personalizar Control Panel en la página 653). La personalización realizada allí se refiere tanto a Control Panel como a User Panel. Por tanto, el interruptor **Personalización de User Panel** en **Personalización** depende de la personalización de Control Panel y no se puede activar ni desactivar manualmente.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el que modificar los módulos mostrados en User Panel.
3. Vaya a **Personalización** > **User Panel**.

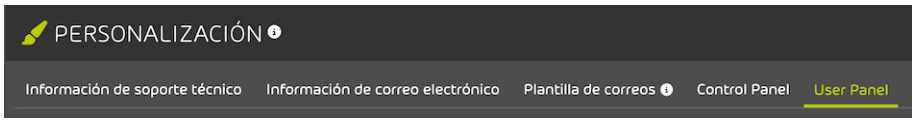


Figura 478: Seleccionar una pestaña

4. Accione los interruptores en **Funciones** para mostrar u ocultar módulos en User Panel.

   Los módulos con un interruptor verde se muestran User Panel, los módulos con un interruptor gris se ocultan en User Panel.

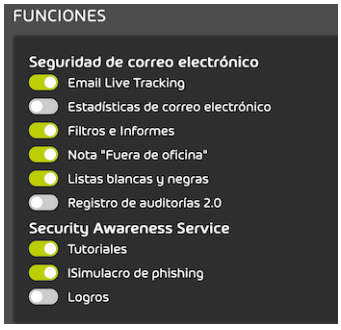


Figura 479: Mostrar u ocultar módulos en User Panel

Ha mostrado u ocultado módulos en User Panel.

Se han modificado los módulos mostrados para los usuarios en User Panel.

Motivos de clasificación de correos

Motivos de clasificación

En Control Panel se asigna una categoría a cada correo (véase "Categorías de correo electrónico" en el manual de Control Panel). Los motivos de clasificación de cada correo se indican en la columna **Motivo** del módulo **Email Live Tracking** (véase "Email Live Tracking" en el manual de Control Panel).

En la siguiente tabla se exponen y explican los motivos de clasificación junto a las categorías de correo electrónico correspondientes.

Tabla 45: Motivos de clasificación

CAUSA	CATEGORÍA	DEFINICIÓN
450 4.5.5 E-Mail deferred because of Spam sending to unlock goto {URL}	Rechazado	El correo se ha rechazado temporalmente por haberse enviado spam desde la dirección de correo electrónico del remitente. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
450 4.5.5 too many false recipients rate-limited;	Rechazado	El correo se ha rechazado temporalmente por contener demasiados destinatarios incorrectos.

CAUSA	CATEGORÍA	DEFINICIÓN
450 4.5.5 unblock {URL}	Rechazado	El correo se ha rechazado temporalmente debido al contenido de su encabezado. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
450 4.5.6 busy try again later;	Rechazado	El correo se ha rechazado temporalmente debido a un exceso de carga en el servidor.
450 4.5.7 busy try again later by {puerta de enlace}	Rechazado	El correo se ha rechazado temporalmente debido a un exceso de carga en el servidor. Se detalla el nombre de host de nuestra puerta de enlace.
450 4.5.7 loop detected, by {smarthost}	Rechazado	El correo se ha rechazado temporalmente por haberse detectado un bucle. Se detalla el nombre de host de nuestro smarthost.
450 4.5.8 no mail data, by {smarthost};	Rechazado	El correo se ha rechazado temporalmente por carecer de contenido. Se detalla el nombre de host de nuestro smarthost.
450 4.5.8 no mail data;	Rechazado	El correo se ha rechazado temporalmente por carecer de contenido.

CAUSA	CATEGORÍA	DEFINICIÓN
450 4.5.8 too much load try next hop;	Rechazado	El correo se ha rechazado temporalmente debido a un exceso de carga en el servidor. La entrega debería intentarse a través de otro dispositivo de red.
450 4.5.9 Connection PID broken $CLEANUPID by $(nombre de host);	Rechazado	El correo se ha rechazado temporalmente debido a un error en el sistema.
450 4.5.9 Greylisted, please try again later;	Rechazado	El correo se ha rechazado temporalmente debido a un proceso de greylisting.
450 4.5.9 no resources please take next hop. by {smarthost};	Rechazado	El correo se ha rechazado temporalmente por falta de recursos para la recepción. La entrega debería intentarse a través de otro dispositivo de red. Se detalla el nombre de host de nuestro smarthost.
450 4.5.9 no smtp resources, please take next hop. by {smarthost};	Rechazado	El correo se ha rechazado temporalmente por falta de recursos SMTP para la recepción. Se detalla el nombre de host de nuestro smarthost.
450 5.5.6 loop detected;	Rechazado	El correo se ha rechazado temporalmente por haberse detectado un bucle.

CAUSA	CATEGORÍA	DEFINICIÓN
454 4.7.1 [dirección de correo del remitente]: Relay access denied	Aplazado	El correo se ha aplazado por no haber sido enviado desde una de las direcciones IP de servidores de retransmisión definidas en el módulo **Spam and Malware Protection** (véase «Spam and Malware Protection» en el manual de Control Panel). Para que un correo pueda enviarse a través de nuestra infraestructura, deberá proceder de una de las direcciones IP registradas. La entrega del correo se detendrá al cabo de un día.
504 5.5.2 Recipient address rejected: need fully-qualified address	Rechazado	El correo se ha rechazado porque la dirección de correo electrónico del destinatario estaba incompleta.
523 5.2.3 E-Mail rejected, e-mail is too large by company rule [ID de regla];	Rechazado	El correo se ha rechazado por haber superado un límite de tamaño definido por el cliente. Se detalla el ID de la regla.
550 5.1.1 Recipient address rejected: undeliverable address	Rechazado	El correo se ha rechazado por no existir la dirección de correo electrónico del destinatario.

CAUSA	CATEGORÍA	DEFINICIÓN
552 5.2.2 Mailbox not available. For more information visit {URL};	Rechazado	El correo se ha rechazado debido a la dirección de correo electrónico del destinatario o del remitente. Se detalla el nombre de host de nuestra puerta de enlace.
552 5.5.2 Message size exceeds fixed maximum message size. Size: {tamaño del correo}, Max size: {tamaño máximo} by {puerta de enlace};	Rechazado	El correo se ha rechazado por superar el límite de tamaño en la puerta de enlace. Se detalla el nombre de host de nuestra puerta de enlace.
552 5.5.2 Size: {tamaño del correo}	Rechazado	El correo se ha rechazado mediante reglas de Content Control (véase «Acerca de Content Control» en el manual de Control Panel) por no respetar los límites de tamaño definidos. Se detalla el tamaño del correo.
552 5.5.8 utilize Smarthost instead of MX by {puerta de enlace};	Rechazado	El correo se ha rechazado porque debía haberse enviado a través de un smarthost y no directamente a la puerta de enlace. Se detalla el nombre de host de nuestra puerta de enlace.

CAUSA	CATEGORÍA	DEFINICIÓN
554 5.5.4 Your IP {dirección IP} address has a bad reputation. To unblock visit {URL};	Rechazado	El correo se ha rechazado porque su dirección IP tiene mala reputación. Puede desbloquear su dirección de correo electrónico haciendo clic en la URL indicada.
554 5.5.5 E-Mail rejected Spam found, for support contact {URL};	Rechazado	El correo se ha rechazado por contener spam. Haga clic en la URL indicada para realizar una solicitud al servicio técnico.
554 5.6.0 unblock {URL};	Rechazado	El correo se ha rechazado temporalmente debido a un tamaño de encabezado excesivo. Haga clic en la URL indicada para realizar una solicitud al servicio técnico.
554 5.6.1 E-Mail rejected because of Spam-Header to unlock goto {URL};	Rechazado	Su correo se ha rechazado por haber sido clasificado como spam debido a su encabezado. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
554 5.6.1 Your mailheader contains SPAM. To unblock visit {URL}	Rechazado	Su correo se ha rechazado por haber sido clasificado como spam debido a su encabezado. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.

CAUSA	CATEGORÍA	DEFINICIÓN
554 5.6.2 E-Mail rejected because of Spam-http-Link to unlock goto {URL};	Rechazado	El correo se ha rechazado por haber sido clasificado como spam debido a un enlace. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
554 5.6.2 Your mail contains a SPAM-LINK. To unblock visit {URL};	Rechazado	El correo se ha rechazado por haber sido clasificado como spam debido a un enlace. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
554 5.6.3 E-Mail rejected because of Spam-Body to unlock goto {URL};	Rechazado	El correo se ha rechazado por haber sido clasificado como spam debido a su texto. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
554 5.6.3 Your mail contains SPAM. To unblock visit {URL};	Rechazado	El correo se ha rechazado por contener spam. Puede desbloquear la dirección de correo electrónico haciendo clic en la URL indicada.
554 5.6.4 E-Mail rejected, forbidden attachment by company rule Attachments {ID de regla}	Rechazado	El correo se ha rechazado por contener un archivo adjunto prohibido por una regla del cliente. Se detalla el ID de la regla.

CAUSA	CATEGORÍA	DEFINICIÓN
554 5.6.4 E-Mail rejected Virus found, for support contact {URL}	Rechazado	El correo se ha rechazado por contener virus. Haga clic en la URL indicada para realizar una solicitud al servicio técnico.
554 5.6.9, customer rule based reject by antispameurope Compliancfilter ID-{ID de regla}	Rechazado	El correo ha sido rechazado por la regla de Compliance Filter indicada (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detalla el ID de la regla.
554 5.6.9 Compliance rule based reject by antispameurope Compliancefilter ID-{ID de regla} by {puerta de enlace};	Rechazado	El correo ha sido rechazado por la regla de Compliance Filter indicada del host indicado (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detallan el ID de la regla y el nombre de host de nuestra puerta de enlace.
554 5.6.9 Compliance rule based reject by Compliancefilter ID-{ID de regla} by {puerta de enlace};	Rechazado	El correo ha sido rechazado por la regla de Compliance Filter indicada del host indicado (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detallan el ID de la regla y el nombre de host de nuestra puerta de enlace.

CAUSA	CATEGORÍA	DEFINICIÓN
554 5.7.0 Sender address rejected: {dirección de remitente} sending out spam;	Rechazado	El correo se ha rechazado porque el remitente ha distribuido spam.
554 5.7.12 SPF fail by customer policy.	Rechazado	El correo se ha rechazado por un error SPF conforme a la configuración del cliente (véase «Comprobación SPF» en el manual de Control Panel). Se detalla el nombre de host de nuestra puerta de enlace.

CAUSA	CATEGORÍA	DEFINICIÓN
554 5.7.1 Domain / User unknown	Rechazado	El correo se ha rechazado porque el dominio indicado o el buzón de correo indicado no se encuentra disponible en Control Panel (véase «Dominios» en el manual de Control Panel y «Buzones de correo» en el manual de Control Panel). **Nota:** La creación y la sincronización de nuevos buzones de correo pueden tardar hasta 90 minutos. Si se envían correos a un buzón de correo antes de que haya finalizado su creación, los correos se rechazan.
554 5.7.2 Sender address rejected: Access denied;	Rechazado	El correo se ha rechazado porque la dirección IP del remitente no está registrada en nuestro sistema.

CAUSA	CATEGORÍA	DEFINICIÓN
Allowed by User Policy	Limpio	El remitente o host que remite el correo electrónico está incluido en la lista blanca del destinatario (véase "Acerca de las listas blancas y negras" en el manual de Control Panel).
Bad Host Reputation	Spam	El host que remite el correo electrónico tiene mala reputación.
Bad IP Reputation	Spam	La dirección IP del host que remite el correo electrónico tiene mala reputación.
Bad Sender Reputation	Spam	El remitente del correo electrónico tiene mala reputación.
Bad URL Reputation	Spam	El correo electrónico contiene al menos un enlace a un servidor web con mala reputación.
Block by Compliance Filter Policy ID-{ID de regla}	Rechazado	El correo se ha bloqueado como de tipo «Threat» mediante una regla de Compliance Filter (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detalla el ID de la regla.

CAUSA	CATEGORÍA	DEFINICIÓN
Business Email Compromise	AdvThreat	El correo es un correo fraudulento con remitente falso de la propia empresa.
Clean by Compliance Rule ID-{ID de regla}	Limpio	El correo se ha clasificado como «Limpio» mediante una regla de Compliance Filter (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detalla el ID de la regla.
Denied by User Policy	Spam	El remitente o host que remite el correo electrónico está incluido en la lista negra del destinatario (véase "Acerca de las listas blancas y negras" en el manual de Control Panel).
Detached by Content Control Policy	Contenido	Al menos un archivo adjunto es inválido conforme a los ajustes de Content Control (véase «Acerca de Content Control» en el manual de Control Panel).
DKIM Failure	Spam	La validación DKIM ha fracasado (véase «Validación DKIM y firma DKIM» en el manual de Control Panel).

CAUSA	CATEGORÍA	DEFINICIÓN
DMARC Failure	Spam	La validación DMARC ha fracasado (véase «Validación DMARC» en el manual de Control Panel).
Envelope SPF Failure	Rechazado , Spam	La comprobación SPF del sobre del correo ha fracasado (véase «Comprobación SPF» en el manual de Control Panel). Como acciones tras error se habían definido **Rechazar correo** o **Poner correo en cuarentena como spam**.
Good Sender Reputation	Limpio	El remitente o host que remite el correo electrónico tiene buena reputación.
Ham	Limpio	Ham es lo contrario de spam: un correo deseado que encaja con el patrón de un correo válido.

CAUSA	CATEGORÍA	DEFINICIÓN
Impersonation attempt by customer policy	AdvThreat , Threat	El nombre para mostrar del remitente del correo coincide con el de un usuario registrado en Control Panel, pero la dirección de correo electrónico del campo "From" del encabezado difiere de la dirección de correo electrónico registrada para dicho usuario.
infomail	Infomail, Spam	Es probable que el correo sea un boletín informativo. El remitente o el rango de direcciones IP del remitente del correo es una fuente conocida de boletines informativos, o bien el correo contiene palabras clave, cadenas de caracteres u otras características que, combinadas, son indicio de que se trate de un boletín informativo.
Malicious Attachment	AdvThreat , Rechazado, Threat	Al menos un archivo adjunto es malicioso.
Malicious Email Content	AdvThreat , Rechazado, Threat	El correo contiene contenidos maliciosos.

CAUSA	CATEGORÍA	DEFINICIÓN
Malicious URL	AdvThreat , Rechazado, Threat	El correo contiene enlaces a páginas web o documentos maliciosos.
Massive Attack Prevention	AdvThreat , Threat	El correo coincide con el patrón de una campaña de malware en curso.
Message Header SPF Failure	Rechazado , Spam	La comprobación SPF del encabezado del correo ha fracasado (véase «Comprobación SPF» en el manual de Control Panel). Como acciones tras error se habían definido **Rechazar correo** o **Poner correo en cuarentena como spam**.
Phishing	AdvThreat , Threat	El correo electrónico contiene características propias de un ataque de phishing.
RBL	Rechazado	El host que remite el correo electrónico tiene mala reputación.

CAUSA	CATEGORÍA	DEFINICIÓN
Rejected by Content Filter	Contenido	El correo se ha rechazado conforme a reglas de Content Control (véase «Acerca de Content Control» en el manual de Control Panel) por contener al menos un archivo adjunto prohibido.
Sandbox	AdvThreat	Al menos un archivo adjunto del correo ha sido analizado por el motor de sandbox de Advanced Threat Protection y considerado malicioso (véase "Descripción de los motores de ATP" en el manual de Control Panel).
Sender Allowed by Domain Policy	Limpio	El remitente o host que remite el correo electrónico está incluido en la lista blanca del administrador del cliente (véase "Acerca de las listas blancas y negras" en el manual de Control Panel).

CAUSA	CATEGORÍA	DEFINICIÓN
Sender Denied by Domain Policy	Spam	El remitente o host que remite el correo electrónico está incluido en la lista negra del administrador del cliente (véase "Acerca de las listas blancas y negras" en el manual de Control Panel).
Spam by Compliance Rule ID-{ID de regla}	Spam	El correo se ha clasificado como «Spam» mediante una regla de Compliance Filter (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detalla el ID de la regla.
Spam Content	Spam	El correo electrónico incluye contenidos clasificados como spam.
SPF Failure	Rechazado	El correo se ha rechazado debido a un error de SPF (véase «Comprobación SPF» en el manual de Control Panel).
Statusmail	Limpio	El correo es un mensaje de sistema generado automáticamente (por ejemplo, un informe de cuarentena) (véase "Acerca de Quarantine Report" en el manual de Control Panel).

CAUSA	CATEGORÍA	DEFINICIÓN
Targeted Fraud	AdvThreat	El correo coincide con el patrón de una campaña de fraude en curso.
Threat by Compliance Rule ID-{ID de regla}	Threat	El correo se ha clasificado como de tipo «Threat» mediante una regla de Compliance Filter (véase «Acerca de Compliance Filter» en el manual de Control Panel). Se detalla el ID de la regla.
Unsolicited Email	Spam	El correo se ha considerado no deseado (por ejemplo, por contener una oferta no solicitada).

Índice

Caracteres Especiales

ámbito
    Control Panel, *Ver* selección de ámbitos explicación
    seleccionar, *Ver* selección de ámbitos uso
ámbito de aplicación
    Control Panel, *Ver* selección de ámbitos explicación
    seleccionar, *Ver* selección de ámbitos uso

A

abrir
    configuración de usuario(Control Panel), *Ver* configuración de usuario, abrir(Control Panel)
    registro(Auditing), *Ver* registro(Auditing) abrir
    vista de correos(Email Live Tracking) 78
acciones
    explicación(Compliance Filter) 537
    filtrar(Auditing) 209
acciones de usuario
    permitir 496
    prohibir 496
acciones para correos
    en informes de cuarentena 451
    explicación(Email Live Tracking) 95
aceptación
    hacer obligatoria para el contrato de tratamiento de datos, *Ver* Condiciones Generales hacer obligatorio el contrato de tratamiento de datos
activar
    ATP 389
    buzón de correo, *Ver* buzón de correo activar
    Compliance Filter 519
    comprobación SPF 414
    Content Control 502
    DKIM, firma 426
    envío de correos del simulacro de phishing en su nombre como usuario, *Ver* suplantación de identidad activar como usuario
    filtro de infomail como usuario, *Ver* filtro de infomail activar como usuario
    LDAP, conexión, *Ver* LDAP, conexión activar
    Quarantine Report 455
    regla de filtrado(Compliance Filter) 558
    Secure Links 396
    Signature and Disclaimer 588
    suplantación de identidad como usuario, *Ver* suplantación de identidad activar como usuario
    Validación DKIM 423
    validación DMARC 437

Active Directory, atributos
explicación(Signature and Disclaimer) 600
Active Directory, variables, *Ver* Active Directory, atributos explicación(Signature and Disclaimer)
actividad de usuario
registro(Auditing), *Ver* Registro de auditorías 2.0 explicación
actualizar
búsqueda de correos(Email Live Tracking), *Ver* búsqueda de correos repetir(Email Live Tracking)
filtros(Email Live Tracking), *Ver* búsqueda de correos repetir(Email Live Tracking)
actualizar(Email Live Tracking)
filtros 77
administradores
forzar la autenticación multifactor, *Ver* autenticación multifactor forzar para administradores
administrar
miembros de un grupo, *Ver* grupo administrar miembros
Advanced Threat Protection
explicación 381
Ver también ATP
AdvThreat
motivos de clasificación(Control Panel) 663
ajustar
cierre de sesión automático, *Ver* cierre de sesión automático ajustar
CNAME, registro 422
DMARC, registro, *Ver* DMARC, registro ajustar
informes de cuarentena como usuario, *Ver* Quarantine Report configurar como usuario
Quarantine Report como usuario, *Ver* Quarantine Report configurar como usuario
TXT, registro para DMARC, *Ver* TXT, registro para DMARC ajustar
zona horaria e idioma por defecto(Control Panel), *Ver* zona horaria e idioma por defecto(Control Panel) ajustar
ajustes de búsqueda
reiniciar(Email Live Tracking), *Ver* búsqueda de correos reiniciar(Email Live Tracking)
alternar
datos de estadísticas(Threat Live Report) 200
añadir
buzón de correo, *Ver* buzón de correo añadir
buzón de correo a un grupo, *Ver* buzón de correo añadir a un grupo
buzón de reenvío, *Ver* buzón de reenvío añadir
código fuente HTML(Signature and Disclaimer) 614
contacto, *Ver* contacto asignar
datos de contacto, *Ver* contacto asignar
datos de correo electrónico(Personalización), *Ver* datos de correo electrónico(Personalización) personalizar
datos de soporte técnico(Personalización) 643
delegado, *Ver* delegado añadir
destinatario de informe mensual(Estadística de correo), *Ver* informe mensual añadir un destinatario(Estadística de correo)
destinatarios de notificaciones (ATP) 391
dirección alias, *Ver* dirección alias añadir
dominio, *Ver* dominio alias añadir
dominio alias, *Ver* dominio alias añadir
entorno secundario, *Ver* entorno secundario añadir
grupo a Content Control 503
LDAP, conexión, *Ver* LDAP, conexión añadir
rol, asignación de, *Ver* asignar rol

subfirma 610
usuario a Continuity Service 637, 638
añadir a lista blanca
IP, dirección 420, 421
Añadir a lista blanca 373
archivo CSV para un dominio(Listas blancas y negras), *Ver* CSV, archivo lista blanca de dominio(Listas blancas y negras)
CSV, archivo para usuarios(Listas blancas y negras), *Ver* CSV, archivo lista blanca para usuarios(Listas blancas y negras)
CSV, exportación(Listas blancas y negras), *Ver* CSV, exportación Añadir a lista blanca(Listas blancas y negras)
editar registro para un dominio(Listas blancas y negras) 371
Eliminar un registro(Listas blancas y negras) 375
Añadir a lista negra
archivo CSV para un dominio(Listas blancas y negras), *Ver* CSV, archivo lista para dominios(Listas blancas y negras)
CSV, archivo para usuarios(Listas blancas y negras), *Ver* CSV, archivo lista negra para usuarios(Listas blancas y negras)
CSV, exportación(Listas blancas y negras), *Ver* CSV, exportación Añadir a lista negra(Listas blancas y negras)
Eliminar un registro(Listas blancas y negras) 375
Exportar registros(Listas blancas y negras), *Ver* CSV, exportación Añadir a lista negra(Listas blancas y negras)
API
crear token(Control Panel), *Ver* token de API crear(Control Panel)
eliminar token(Control Panel), *Ver* token de API eliminar(Control Panel)
archivo adjunto 501
categoría 501
archivo, tipo, *Ver* archivo adjunto
asignar
contacto, *Ver* contacto asignar
contacto para la entrega de correos, *Ver* contacto para la entrega de correos asignar
rol 109
ataque, tipo
explicación(Threat Live Report) 195
ataque, vector de
explicación(Threat Live Report) 198
ATP 389
activar 389
explicación, *Ver* Advanced Threat Protection explicación
atributos de LDAP
configurar 130
auditoría
categorías, *Ver* Registro de auditorías 2.0 categorías
explicación, *Ver* Registro de auditorías 2.0 explicación
autenticación
configuración de cliente, *Ver* configuración de cliente autenticación
remitente, *Ver* Email Authentication explicación
autenticación multifactor
configurar como usuario 28
desactivar como usuario 33
desactivar para un dominio 327
forzar para administradores 325
habilitar para un dominio 323
reiniciar para un usuario 279
solución de problemas 21

B

borrar
- diccionario(Compliance Filter), *Ver* diccionario borrar(Compliance Filter)
- firma 597
- lista blanca, registro(Listas blancas y negras), *Ver* Añadir a lista blanca Eliminar un registro(Listas blancas y negras)
- regla de filtrado(Compliance Filter), *Ver* regla de filtrado borrar(Compliance Filter)

buscar
- correo electrónico(Email Live Tracking) 72
- lista blanca, registro(Listas blancas y negras), *Ver* lista blanca buscar registros(Listas blancas y negras)
- lista negra, registro(Listas blancas y negras), *Ver* lista negra buscar registros(Listas blancas y negras)
- registros(Auditing) 223

búsqueda de correos
- actualizar(Email Live Tracking), *Ver* búsqueda de correos repetir(Email Live Tracking)
- reiniciar(Email Live Tracking) 77
- repetir(Email Live Tracking) 77

búsqueda(Email Live Tracking)
- combinada, *Ver* función de búsqueda(Email Live Tracking)
- limitar 73

buzón de correo
- activar 260
- añadir 237
- añadir a un grupo 257
- configuración de cliente, *Ver* configuración de cliente buzones de correo
- CSV, exportación 251
- CSV, importación 240
- desactivar 260
- quitar 281
- quitar de un grupo 258
- sincronización de entornos secundarios, *Ver* entorno secundario sincronización
- tipos 235

Buzón de correo
- quitar 283

buzón de reenvío
- añadir 255
- CSV, importación 265

C

cambiar
- contraseña, *Ver* contraseña cambiar
- contraseña de emergencia de un buzón de correo, *Ver* contraseña de emergencia de un buzón de correo cambiar
- contraseña de emergencia(Control Panel), *Ver* contraseña de emergencia cambiar(Control Panel)
- contraseña(Control Panel), *Ver* contraseña cambiar(Control Panel)
- entorno, *Ver* entorno cambiar
- formato de fecha(Control Panel), *Ver* formato de fecha(Control Panel) cambiar
- formato de hora(Control Panel), *Ver* formato de hora(Control Panel) cambiar
- Idioma(Control Panel), *Ver* Idioma(Control Panel) cambiar
- nombre de un grupo, *Ver* grupo renombrar

posición de campos de correo(Email Live Tracking) 70
prioridad de una regla de filtrado(Compliance Filter) 549
zona horaria(Control Panel), *Ver* zona horaria(Control Panel) cambiar
campo de búsqueda(Email Live Tracking) 72
campos
tipo(Compliance Filter), *Ver* tipo campos(Compliance Filter)
categoría
de archivos adjuntos 501
seleccionar(Auditing) 206
Categoría
explicación(Auditing), *Ver* Registro de auditorías 2.0 categorías
categorías de correo electrónico
explicación(Control Panel) 90
cierre de sesión automático
ajustar 329
restaurar la configuración por defecto 331
cliente
eliminiar, *Ver* Dashboard de servicios eliminar un cliente propio
CNAME, registro
ajustar 422
código fuente HTML(Signature and Disclaimer)
añadir 614
Compliance Filter
activar 519
desactivar 584
explicación 516
comprobación SPF
activar 414
comprobar
DKIM, configuración 407
DMARC, configuración 407
SPF, configuración 407
condición
regla de filtrado(Compliance Filter), *Ver* regla de filtrado condición(Compliance Filter)
Condiciones Generales
crear un contrato de licencia de usuario final y un contrato de tratamiento de datos 159
desactivar 169
explicación 155
exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos 168
habilitar 157
hacer obligatorio el contrato de tratamiento de datos 158
configuración
entorno primario, *Ver* entorno primario configuración
usuarios, *Ver* configuración de usuario explicación
configuración de cliente
autenticación 319
buzones de correo 230
dominios 307

grupos 288
módulo 230
configuración de usuario
explicación 22
configuración de usuario, abrir(Control Panel) 23
configuración por defecto
cierre de sesión automático, *Ver* cierre de sesión automático restaurar la configuración por defecto
configuración(Auditing)
descartar 222
configurar 484
atributos de LDAP
atributos de LDAP
configurar 130
autenticación multifactor como usuario, *Ver* autenticación multifactor configurar como usuario
Content Control 506
DKIM, acciones tras validación 424
DMARC, acciones tras validación 438
inicio de sesión con LDAP, *Ver* inicio de sesión configurar con LDAP
Quarantine Report 456, 463
SPF, acciones tras comprobación 417
consultar
informe ATP (Advanced Threat Protection) 80, 403
versión, número de(Control Panel), *Ver* versión, número de consultar(Control Panel)
contacto 107
añadir, *Ver* contacto asignar
asignar 110
eliminar 117
filtrar 114
send_email_to_admin, *Ver* contacto para la entrega de correos asignar
explicación 108
contacto para la entrega de correos
asignar 113
contenido
motivos de clasificación(Control Panel) 663
Content Control
activar 502
configurar 506
Continuity Service
explicación 636
contraseña
cambiar 277
cambiar(Control Panel) 24
restablecer(Control Panel) 19
contraseña de emergencia
cambiar(Control Panel) 26
contraseña de emergencia de un buzón de correo
cambiar 274

contraseñas
definir longitud mínima, *Ver* longitud de contraseña definir
restablecer longitud mínima, *Ver* longitud de contraseña restablecer
contrato de licencia de usuario final
Condiciones Generales, *Ver* Condiciones Generales explicación
crear, *Ver* Condiciones Generales crear un contrato de licencia de usuario final y un contrato de tratamiento de datos
desactivar, *Ver* Condiciones Generales desactivar
exportar, *Ver* Condiciones Generales exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos
contrato de tratamiento de datos
Condiciones Generales, *Ver* Condiciones Generales explicación
crear, *Ver* Condiciones Generales crear un contrato de licencia de usuario final y un contrato de tratamiento de datos
desactivar, *Ver* Condiciones Generales desactivar
exportar, *Ver* Condiciones Generales exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos
hacer obligatorio, *Ver* Condiciones Generales hacer obligatorio el contrato de tratamiento de datos
Control Panel
ajustar color(Personalización) 654
ajustar Favicon(Personalización) 654
ajustar logotipo(Personalización) 654
ajustar tema(Personalización) 654
ajustar URL(Personalización) 654
ámbito, *Ver* selección de ámbitos explicación
ámbito de aplicación, *Ver* selección de ámbitos explicación
iniciar sesión, *Ver* iniciar sesión Control Panel
Control Panel(Personalización)
editar 642
correo electrónico
ajustar el tamaño de los campos(Email Live Tracking) 68
buscar(Email Live Tracking) 72
filtrar por categorías(Email Live Tracking) 71
modificar orden de campos(Email Live Tracking) 70
por categoría(Estadística de correo), *Ver* estadística de correos correos por tipo
por fecha(Estadística de correo), *Ver* estadística de correos correos por fecha
por tipo(Estadística de correo), *Ver* estadística de correos correos por tipo
por usuario(Estadística de correo), *Ver* estadística de correos correos por usuario
seleccionar(Email Live Tracking) 92
vista previa 99
Correo electrónico
Motivos de clasificación de Email Authentication, *Ver* motivos de clasificación Email Authentication
correo, campo de
explicación(Email Live Tracking) 86
seleccionar(Email Live Tracking) 66
correos(Personalización)
editar 645
crear
contrato de licencia de usuario final, *Ver* Condiciones Generales crear un contrato de licencia de usuario final y un contrato de tratamiento de datos
contrato de tratamiento de datos, *Ver* Condiciones Generales crear un contrato de licencia de usuario final y un contrato de tratamiento de datos

diccionario(Compliance Filter), *Ver* diccionario crear(Compliance Filter)
entorno secundario, *Ver* entorno secundario crear
firma 589
grupo, *Ver* grupo crear
lista blanca, registro(Listas blancas y negras), *Ver* lista blanca, registro crear(Listas blancas y negras)
lista negra, registro, *Ver* lista negra, registro crear
lista negra, registro para un dominio(Listas blancas y negras), *Ver* lista negra, registro crear para un dominio(Listas blancas y negras)
nota de "fuera de la oficina"(Control Panel) 47
nota legal 589
registro de lista blanca para un dominio, crear(Listas blancas y negras), *Ver* lista blanca, registro crear(Listas blancas y negras)
reglas de filtrado para correos entrantes(Compliance Filter) 521
reglas de filtrado para correos salientes(Compliance Filter) 528
token de API(Control Panel), *Ver* token de API crear(Control Panel)
CSV, archivo
destinatario de informe mensual(Estadística de correo) 186
exportar estadística de correo, *Ver* estadística de correos exportar en formato CSV
lista blanca de dominio(Listas blancas y negras) 356
lista blanca para usuarios(Listas blancas y negras) 356
lista negra para usuarios(Listas blancas y negras) 356
lista para dominios(Listas blancas y negras) 356
CSV, exportación
Añadir a lista blanca(Listas blancas y negras) 373
Añadir a lista negra(Listas blancas y negras) 373
buzón de correo, *Ver* buzón de correo CSV, exportación
dominio, *Ver* dominio CSV, exportación
dominio alias, *Ver* dominio CSV, exportación
grupo, *Ver* grupo CSV, exportación
Registro de auditorías 2.0(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
registro de auditorías(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
CSV, importación
buzón de correo, *Ver* buzón de correo CSV, importación
buzón de reenvío, *Ver* buzón de reenvío CSV, importación
destinatario de informe mensual(Estadística de correo) 184
dominio, *Ver* dominio alias CSV, importación
dominio alias, *Ver* dominio alias CSV, importación
grupo, *Ver* grupo CSV, importación
lista blanca de dominio(Listas blancas y negras), *Ver* CSV, archivo lista blanca de dominio(Listas blancas y negras)
lista blanca para usuarios(Listas blancas y negras), *Ver* CSV, archivo lista blanca para usuarios(Listas blancas y negras)
lista blanca(Listas blancas y negras) 351
lista negra para usuarios(Listas blancas y negras), *Ver* CSV, archivo lista negra para usuarios(Listas blancas y negras)
lista negra(Listas blancas y negras) 351
lista para dominios(Listas blancas y negras), *Ver* CSV, archivo lista para dominios(Listas blancas y negras)

D

Dashboard de servicios
eliminar un cliente propio 119

explicación 106
datos básicos
editar(Control Panel) 39
datos básicos de un buzón de correo
editar 271
datos de acceso
configurar para una conexión LDAP, *Ver* inicio de sesión configurar con LDAP
datos de contacto 107
añadir, *Ver* contacto asignar
datos de contacto(Personalización)
añadir, *Ver* datos de soporte técnico(Personalización) añadir
datos de correo electrónico(Email Live Tracking) 84
datos de correo electrónico(Personalización)
añadir, *Ver* datos de correo electrónico(Personalización) personalizar
personalizar 646
datos de estadísticas(Threat Live Report)
alternar 200
datos de soporte técnico(Personalización)
añadir 643
definier
SPF, registro 413
definir
IP, dirección, *Ver* IP, dirección definir
longitud mínima de contraseñas, *Ver* longitud de contraseña definir
registro TXT para SPF, *Ver*
delegado
añadir 263
derechos
usuarios(Control Panel), *Ver* derechos, administración rol(Control Panel)
derechos, administración
rol(Control Panel) 53
desactivar
autenticación multifactor como usuario, *Ver* autenticación multifactor desactivar como usuario
autenticación multifactor para un dominio, *Ver* autenticación multifactor desactivar para un dominio
buzón de correo, *Ver* buzón de correo desactivar
Compliance Filter 584
Condiciones Generales, *Ver* Condiciones Generales desactivar
contrato de licencia de usuario final, *Ver* Condiciones Generales desactivar
contrato de tratamiento de datos, *Ver* Condiciones Generales desactivar
envío de correos del simulacro de phishing en su nombre, *Ver* suplantación de identidad activar como usuario
filtro de infomail como usuario, *Ver* filtro de infomail desactivar como usuario
LDAP, conexión, *Ver* LDAP, conexión desactivar
Quarantine Report 472
regla de filtrado(Compliance Filter) 559
Signature and Disclaimer 598
Spam and Malware Protection 498
suplantación de identidad, *Ver* suplantación de identidad desactivar para un buzón de correo
suplantación de identidad como usuario, *Ver* suplantación de identidad desactivar como usuario
descartar
configuración(Auditing) 222

destinatario
CSV, archivo para informe mensual(Estadística de correo), *Ver* CSV, archivo destinatario de informe mensual(Estadística de correo)
CSV, importación para informe mensual(Estadística de correo), *Ver* CSV, importación destinatario de informe mensual(Estadística de correo)
de informe mensual, añadir(Estadística de correo), *Ver* informe mensual añadir un destinatario(Estadística de correo)
destinatario(Estadística de correo)
de informe mensual, eliminar 187
destinatarios de notificaciones (ATP)
añadir 391
eliminar 393
diagrama
correos por fecha(Estadística de correo), *Ver* estadística de correos correos por fecha
correos por tipo(Estadística de correo), *Ver* estadística de correos correos por tipo
filtrar(Estadística de correo), *Ver* estadística de correos filtrar
diccionario
borrar(Compliance Filter) 568
crear(Compliance Filter) 563
editar(Compliance Filter) 566
explicación(Compliance Filter) 562
dirección alias
añadir 261
direcciones IP
configuración de cliente, *Ver* configuración de cliente autenticación
disclaimer
crear 589
DKIM 407, 422
DKIM, acciones tras validación
configurar 424
DKIM, configuración
comprobar 407
DKIM, firma
activar 426
DMARC 407, 427
matriz de decisiones 432
DMARC, acciones tras validación
configurar 438
DMARC, configuración
comprobar 407
DMARC, registro
ajustar 428
Domain-based Message Authentication, Reporting & Conformance 427
DomainKeys Identified Mail 422
dominio
añadir, *Ver* dominio alias añadir
configuración de cliente, *Ver* configuración de cliente dominios
CSV, exportación 311
CSV, importación, *Ver* dominio alias CSV, importación
desactivar la autenticación multifactor, *Ver* autenticación multifactor desactivar para un dominio

eliminar, *Ver* dominio alias eliminar
habilitar la autenticación multifactor, *Ver* autenticación multifactor habilitar para un dominio
iniciar comprobación, *Ver* verificación iniciar
lista blanca, crear registro(Listas blancas y negras), *Ver* lista blanca, registro crear(Listas blancas y negras)
verificación 316
verificar, *Ver* dominio verificación
Dominio
lista blanca, editar registro(Listas blancas y negras), *Ver* Añadir a lista blanca editar registro para un dominio(Listas blancas y negras)
lista negra, crear registro(Listas blancas y negras), *Ver* lista negra, registro crear para un dominio(Listas blancas y negras)
dominio alias
añadir 307
CSV, exportación, *Ver* dominio CSV, exportación
CSV, importación 309
eliminar 314

E

editar
color de Control Panel(Personalización) 654
Control Panel(Personalización), *Ver* Control Panel(Personalización) editar
correos(Personalización), *Ver* correos(Personalización) editar
datos básicos de un buzón de correo, *Ver* datos básicos de un buzón de correo editar
datos básicos(Control Panel), *Ver* datos básicos editar(Control Panel)
diccionario(Compliance Filter), *Ver* diccionario editar(Compliance Filter)
entorno secundario, *Ver* entorno secundario editar
favicon de Control Panel(Personalización) 654
firma 597
LDAP, conexión, *Ver* LDAP, conexión editar
logotipo de Control Panel(Personalización) 654
registro de lista blanca para un dominio(Listas blancas y negras), *Ver* Añadir a lista blanca editar registro para un dominio(Listas blancas y negras)
regla de filtrado(Compliance Filter) 547
tamaño de campos de correo(Email Live Tracking) 68
tema de Control Panel(Personalización) 654
URL de Control Panel(Personalización) 654
editor WYSIWYG(Signature and Disclaimer) 600
ejemplo
expresión regular compleja(Compliance Filter) 582
Ejemplo
expresión regular(Compliance Filter), *Ver* expresión regular Ejemplo(Compliance Filter)
eliminar
cliente propio, *Ver* Dashboard de servicios eliminar un cliente propio
contacto, *Ver* contacto eliminar
destinatario de informe mensual(Estadística de correo), *Ver* informe mensual eliminar destinatarios(Estadística de correo)
destinatarios de notificaciones (ATP) 393
dominio, *Ver* dominio alias eliminar
dominio alias, *Ver* dominio alias eliminar

entorno secundario, *Ver* entorno secundario eliminar
grupo, *Ver* grupo eliminar
grupos de lista de grupos de TFFF 401
IP, dirección, *Ver* IP, dirección eliminar
LDAP, conexión 151
lista negra, registro(Listas blancas y negras), *Ver* Añadir a lista negra Eliminar un registro(Listas blancas y negras)
rol, *Ver* rol, asignación de eliminar
rol, asignación de, *Ver* rol, asignación de eliminar
token de API(Control Panel), *Ver* token de API eliminar(Control Panel)
usuarios de Continuity Service 640
varios buzones de correo, *Ver* Buzón de correo quitar
Email Authentication
excepción 442
explicación 407
motivos de clasificación, *Ver* motivos de clasificación Email Authentication
Email Live Tracking
estructura(Email Live Tracking) 64
Explicación(Email Live Tracking) 63
emplear
función "if not empty"(Signature and Disclaimer) 607
entorno
cambiar 276
entorno primario
configuración 483
configurar 484
entorno secundario
añadir 123
buzón de correo LDAP, *Ver* entorno secundario sincronización
buzón de correo Microsoft 365, *Ver* entorno secundario sincronización
buzón de correo sincronizado, *Ver* entorno secundario sincronización
crear 123
editar 125
eliminar 127
sincronización 121
tipos 121
Entorno secundario
explicación 120
envío de correos del simulacro de phishing en su nombre
activar como usuario, *Ver* suplantación de identidad activar como usuario
desactivar como usuario, *Ver* suplantación de identidad desactivar como usuario
escaneo ATP
explicación (Advanced Threat Protection) 402
escaneo ATP (Advanced Threat Protection)
iniciar 80, 403
estadística
correos por usuario(Estadística de correo), *Ver* estadística de correos correos por usuario
filtrar(Estadística de correo), *Ver* estadística de correos filtrar
estadística de amenazas
por tipo de ataque(Threat Live Report) 190

por vector de ataque(Threat Live Report) 191
estadística de ataques
tipos de ataque por fecha(Threat Live Report) 190
vector de ataque por fecha(Threat Live Report) 192
estadística de correos
correos por fecha 177
correos por tipo 176
correos por usuario 180
exportar en formato CSV 179
filtrar 173
informe mensual(Estadística de correo), *Ver* informe mensual estadística de correos(Estadística de correo)
evento(Auditing)
filtrar 211
Ex Post Alert (Advanced Threat Protection) 388
excepción
Email Authentication 442
expresión regular(Compliance Filter) 580
explicación
acciones(Compliance Filter) 537
Condiciones Generales, *Ver* Condiciones Generales explicación
diccionario(Compliance Filter) 562
expresión regular(Compliance Filter) 572
LDAP, conexión, *Ver* LDAP, conexión explicación
lista blanca(Listas blancas y negras), *Ver* lista blanca explicación(Listas blancas y negras)
lista negra(Listas blancas y negras), *Ver* lista negra explicación(Listas blancas y negras)
Signature and Disclaimer, *Ver* Signature and Disclaimer explicación
exportar
contrato de licencia de usuario final, *Ver* Condiciones Generales exportar el contrato de licencia de usuario final y el contrato de tratamiento de datos
estadística de correos en formato CSV, *Ver* estadística de correos exportar en formato CSV
Registro de auditorías 2.0(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
Registro de auditorías 2.0registro de auditoría(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
registros(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
expresión regular
Ejemplo(Compliance Filter) 581
excepción(Compliance Filter) 580
explicación(Compliance Filter) 572
uso(Compliance Filter), *Ver* expresión regular Ejemplo(Compliance Filter)
expresión regular compleja
ejemplo(Compliance Filter) 582

F

falsos positivos
correos entrantes 421
correos salientes 420
fecha(Control Panel)
formato, *Ver* formato de fecha(Control Panel) cambiar

filtrar
acciones(Auditing) 209
correo por categorías(Email Live Tracking) 71
diagrama(Estadística de correo), *Ver* estadística de correos filtrar
estadística de correos, *Ver* estadística de correos filtrar
evento(Auditing) 211
por contacto, *Ver* contacto filtrar
por rol, *Ver* rol filtrar
tipo de rol, *Ver* tipo de rol filtrar
filtro de infomail
activar como usuario 48
desactivar como usuario 48
filtros 77
explicación(Email Live Tracking) 75
reiniciar(Email Live Tracking), *Ver* búsqueda de correos reiniciar(Email Live Tracking)
firma
borrar 597
crear 589
editar 597
formato
fecha(Control Panel), *Ver* formato de fecha(Control Panel) cambiar
hora(Control Panel), *Ver* formato de hora(Control Panel) cambiar
formato de fecha(Control Panel)
ajustar valor por defecto, *Ver* zona horaria e idioma por defecto(Control Panel) ajustar
cambiar 37
formato de hora(Control Panel)
ajustar valor por defecto, *Ver* zona horaria e idioma por defecto(Control Panel) ajustar
cambiar 37
forzar
autenticación multifactor para administradores, *Ver* autenticación multifactor forzar para administradores
función "if not empty"(Signature and Disclaimer)
emplear 607
función de búsqueda(Email Live Tracking) 74

G

gestión de roles 107
grupo
administrar miembros 297
añadir a Content Control 503
añadir miembros 290
añadir un buzón de correo, *Ver* buzón de correo añadir a un grupo
configuración de cliente, *Ver* configuración de cliente grupos
crear 290
CSV, exportación 303
CSV, importación 292
eliminar 305
personalizar descripción 301
quitar buzón de correo de un ~, *Ver* buzón de correo quitar de un grupo

renombrar 299
grupos
eliminar de la lista de grupos de TFFF 401
sincronizar mediante LDAP, *Ver* LDAP sincronizar usuarios y grupos

H

habilitar
autenticación multifactor para un dominio, *Ver* autenticación multifactor habilitar para un dominio
Condiciones Generales, *Ver* Condiciones Generales habilitar
hora(Control Panel)
formato, *Ver* formato de hora(Control Panel) cambiar

I

idioma(Control Panel)
ajustar valor por defecto, *Ver* zona horaria e idioma por defecto(Control Panel) ajustar
Idioma(Control Panel)
cambiar 37
imagen personalizada
incrustar(Signature and Disclaimer) 624
importar
lista blanca, registros(Listas blancas y negras), *Ver* CSV, importación lista blanca(Listas blancas y negras)
lista negra, registros(Listas blancas y negras), *Ver* CSV, importación lista negra(Listas blancas y negras)
inactividad
cierre de sesión automático, *Ver* cierre de sesión automático ajustar
incrustar
imagen personalizada(Signature and Disclaimer) 624
Infomail
motivos de clasificación(Control Panel) 663
informe ATP
consultar (Advanced Threat Protection) 80, 403
explicación (Advanced Threat Protection) 82, 405
informe de cuarentena
acciones para correos, *Ver* acciones para correos en informes de cuarentena
informe mensual
añadir un destinatario(Estadística de correo) 182
CSV, archivo para destinatarios(Estadística de correo), *Ver* CSV, archivo destinatario de informe mensual(Estadística de correo)
CSV, importación de destinatarios(Estadística de correo), *Ver* CSV, importación destinatario de informe mensual(Estadística de correo)
eliminar destinatarios(Estadística de correo) 187
estadística de correos(Estadística de correo) 181
informes de cuarentena
configuración de usuario, *Ver* Quarantine Report configurar como usuario
configurar como usuario, *Ver* Quarantine Report configurar como usuario
iniciar
escaneo ATP (Advanced Threat Protection) 80, 403
verificación, *Ver* verificación iniciar

iniciar sesión
Control Panel 10
inicio de sesión
configurar con LDAP 142
IP, dirección
añadir a lista blanca 420, 421
definir 332
eliminar 333

J

jerarquía(Listas blancas y negras), *Ver* procesamiento de registros(Listas blancas y negras)

L

LDAP
entorno secundario, *Ver* entorno secundario sincronización
sincronizar usuarios y grupos, *Ver* LDAP, conexión añadir
LDAP, conexión
activar 150
añadir 132
configurar atributos, *Ver* atributos de LDAP configurar
configurar datos de acceso, *Ver* inicio de sesión configurar con LDAP
desactivar 148
editar 146
eliminar 151
explicación 129
limitar rango de direcciones IP, *Ver* servicio de directorio limitar rango de direcciones IP
limitar
búsqueda(Email Live Tracking) 73
rango de direcciones IP para un servicio de directorio, *Ver* servicio de directorio limitar rango de direcciones IP
limpio
motivos de clasificación(Control Panel) 663
lista blanca
buscar registros(Listas blancas y negras) 378
explicación(Listas blancas y negras) 335
importar registros(Listas blancas y negras), *Ver* CSV, importación lista blanca(Listas blancas y negras)
registro, buscar(Listas blancas y negras), *Ver* lista blanca buscar registros(Listas blancas y negras)
lista blanca, registro
buscar(Listas blancas y negras), *Ver* lista blanca buscar registros(Listas blancas y negras)
crear(Listas blancas y negras) 340, 344
editar para un dominio(Listas blancas y negras), *Ver* Añadir a lista blanca editar registro para un dominio(Listas blancas y negras)
eliminar(Listas blancas y negras), *Ver* Añadir a lista blanca Eliminar un registro(Listas blancas y negras)
lista negra
buscar registros(Listas blancas y negras) 378
explicación(Listas blancas y negras) 335
importar registros(Listas blancas y negras), *Ver* CSV, importación lista negra(Listas blancas y negras)
registro, buscar(Listas blancas y negras), *Ver* lista negra buscar registros(Listas blancas y negras)

lista negra, registro
borrar(Listas blancas y negras), *Ver* Añadir a lista negra Eliminar un registro(Listas blancas y negras)
buscar(Listas blancas y negras), *Ver* lista negra buscar registros(Listas blancas y negras)
crear 337
crear para un dominio(Listas blancas y negras) 342
Listas blancas y negras(Listas blancas y negras)
módulo 335
longitud de contraseña
definir 321
restablecer 322

M

métodos
remitentes, autenticación
remitentes, autenticación
métodos 409
Microsoft 365
entorno secundario, *Ver* entorno secundario sincronización
miembros
añadir a un grupo, *Ver* grupo añadir miembros
modificar
módulos mostrados en User Panel(Personalización) 660
módulo
Listas blancas y negras(Listas blancas y negras), *Ver* Listas blancas y negras(Listas blancas y negras) módulo
motivos de clasificación
Email Authentication 444
motivos de clasificación de correos
AdvThreat(Control Panel) 663
contenido(Control Panel) 663
Infomail(Control Panel) 663
limpio(Control Panel) 663
rechazado(Control Panel) 663
spam(Control Panel) 663
Threat(Control Panel) 663
motores de ATP
funcionamiento 384

N

navegador(Control Panel), *Ver* requisitos de sistema(Control Panel)
nota de "fuera de la oficina"
crear(Control Panel) 47
nota legal
borrar 597
editar 597
notificación (Advanced Threat Protection) 388

O

orden
reglas de filtrado(Compliance Filter), *Ver* reglas de filtrado orden(Compliance Filter)
Orden de las reglas de todos los servicios 478, 517
orden(Listas blancas y negras), *Ver* procesamiento de registros(Listas blancas y negras)

P

periodo
seleccionar(Auditing) 208
seleccionar(Threat Live Report) 201
periodo de visualización
seleccionar(Auditing) 208
periodo de visualización(Auditing), *Ver* seleccionar periodo(Auditing)
periodo de visualización(Threat Live Report)
seleccionar, *Ver* periodo seleccionar(Threat Live Report)
permitir
acciones de usuario 496
personalizar
datos de correo electrónico(Personalización), *Ver* datos de correo electrónico(Personalización) personalizar
descripción de un grupo, *Ver* grupo personalizar descripción
prioridad de una regla de filtrado
cambiar(Compliance Filter) 549
prioridad(Listas blancas y negras), *Ver* procesamiento de registros(Listas blancas y negras)
procesamiento
de registros(Listas blancas y negras) 379
prohibir
acciones de usuario 496
publicar
contrato de licencia de usuario final, *Ver* Condiciones Generales crear un contrato de licencia de usuario final y un contrato de tratamiento de datos
contrato de tratamiento de datos, *Ver* Condiciones Generales crear un contrato de licencia de usuario final y un contrato de tratamiento de datos

Q

Quarantine Report
activar 455
configuración 445
configuración de usuario, *Ver* Quarantine Report configurar como usuario
configurar 456, 463
configurar como usuario 48
desactivar 472
quitar
buzón de correo, *Ver* buzón de correo quitar
buzón de correo de un grupo, *Ver* buzón de correo quitar de un grupo

R

rango de direcciones IP
    limitar para un servicio de directorio, *Ver* servicio de directorio limitar rango de direcciones IP
rechazado
    motivos de clasificación(Control Panel) 663
registro
    actividad de usuario(Auditing), *Ver* Registro de auditorías 2.0 explicación
    exportar(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
registro de auditoría
    CSV, exportación(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
    exportar(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
Registro de auditorías 2.0
    categorías 204
    CSV, exportación(Auditing), *Ver* Registro de auditorías 2.0 exportar registros(Auditing)
    explicación 203
    exportar registros(Auditing) 226
registro(Auditing)
    abrir 224
registros(Auditing)
    buscar 223
regla de filtrado
    activar(Compliance Filter) 558
    borrar(Compliance Filter) 560
    condición(Compliance Filter) 540
    desactivar(Compliance Filter) 559
    editar(Compliance Filter) 547
    tipo(Compliance Filter) 540
reglas de filtrado
    orden(Compliance Filter) 551
reglas de filtrado para correos entrantes
    crear(Compliance Filter) 521
reglas de filtrado para correos salientes
    crear(Compliance Filter) 528
reglas para contraseñas
    configuración de cliente, *Ver* configuración de cliente autenticación
reiniciar
    ajustes de búsqueda(Email Live Tracking), *Ver* búsqueda de correos reiniciar(Email Live Tracking)
    autenticación multifactor para un usuario, *Ver* autenticación multifactor reiniciar para un usuario
    búsqueda de correos(Email Live Tracking), *Ver* búsqueda de correos reiniciar(Email Live Tracking)
    filtros(Email Live Tracking), *Ver* búsqueda de correos reiniciar(Email Live Tracking)
remitentes, autenticación
    métodos 409
renombrar
    grupo, *Ver* grupo renombrar
repetir
    búsqueda de correos(Email Live Tracking), *Ver* búsqueda de correos repetir(Email Live Tracking)
requisitos de sistema(Control Panel) 9
restablecer
    contraseña(Control Panel) 19

longitud mínima de contraseñas, *Ver* longitud de contraseña restablecer
rol
asignar 109
eliminar, *Ver* rol, asignación de eliminar
filtrar 114
usuarios(Control Panel) 53
rol, asignación de
añadir, *Ver* rol asignar
eliminar 117

S

SaD
explicación, *Ver* Signature and Disclaimer explicación
Secure Links
activar 396
selección de ámbitos
ámbito, *Ver* selección de ámbitos explicación
ámbito de aplicación, *Ver* selección de ámbitos explicación
explicación 58
uso 60
seleccionar
ámbito, *Ver* selección de ámbitos uso
ámbito de aplicación, *Ver* selección de ámbitos uso
categorías(Auditing) 206
correo electrónico(Email Live Tracking) 92
correo, campo de(Email Live Tracking) 66
periodo de visualización(Threat Live Report), *Ver* seleccionar periodo(Threat Live Report)
periodo(Auditing) 208
periodo(Threat Live Report) 201
send_email_to_admin
asignar, *Ver* contacto para la entrega de correos asignar
Sender Policy Framework 410
separador(Email Live Tracking), *Ver* función de búsqueda(Email Live Tracking)
servicio de directorio
limitar rango de direcciones IP 141
sincronizar usuarios y grupos, *Ver* LDAP sincronizar usuarios y grupos
Signature and Disclaimer
activar 588
desactivar 598
explicación 586
Signature and Disclaimer(Signature and Disclaimer)
vista previa 615
sincronización
entorno secundario, *Ver* entorno secundario sincronización
sincronizar
usuarios y grupos mediante LDAP, *Ver* LDAP sincronizar usuarios y grupos
solución de problemas
autenticación multifactor, *Ver* autenticación multifactor solución de problemas

correos entrantes 421
correos salientes 420
solución de problemas(Signature and Disclaimer) 632
firma HTML, falta de 633
variables sin referencia 632
spam
motivos de clasificación(Control Panel) 663
Spam and Malware Protection
desactivar 498
SPF 407, 410
lógica de 411
SPF, acciones tras comprobación
configurar 417
SPF, configuración
comprobar 407
SPF, registro
definir 413
subfirma
añadir 610
suplantación de identidad
activar como usuario 41
desactivar como usuario 41
desactivar para un buzón de correo 287

T

Threat
motivos de clasificación(Control Panel) 663
tipo
buzón de correo, *Ver* buzón de correo tipos
campos(Compliance Filter) 540
regla de filtrado(Compliance Filter), *Ver* regla de filtrado tipo(Compliance Filter)
tipo de rol
filtrar 114
token de API
crear(Control Panel) 43
eliminar(Control Panel) 46
TXT, registro
definir para SPF, *Ver* SPF, registro definir
erróneo 420, 421
TXT, registro para DMARC
ajustar 428

U

User Panel
modificar los módulos mostrados(Personalización) 660

uso
expresión regular(Compliance Filter), *Ver* expresión regular Ejemplo(Compliance Filter)
usuario
contacto, *Ver* contacto explicación
usuarios
añadir a Continuity Service 637, 638
configuración, *Ver* configuración de usuario explicación
configurar autenticación multifactor, *Ver* autenticación multifactor configurar como usuario
desactivar autenticación multifactor, *Ver* autenticación multifactor desactivar como usuario
lista blanca, crear registro(Listas blancas y negras), *Ver* lista blanca, registro crear(Listas blancas y negras)
lista negra, crear registro, *Ver* lista negra, registro crear
permisos(Control Panel), *Ver* derechos, administración rol(Control Panel)
quitar de Continuity Service 640
reiniciar la autenticación multifactor, *Ver* autenticación multifactor reiniciar para un usuario
rol(Control Panel), *Ver* derechos, administración rol(Control Panel)
sincronizar mediante LDAP, *Ver* LDAP sincronizar usuarios y grupos

V

Validación DKIM
activar 423
validación DMARC
activar 437
verificación
dominio, *Ver* dominio verificación
iniciar 318
verificar
dominio, *Ver* dominio verificación
versión, información de(Control Panel) 9
versión, número de
consultar(Control Panel) 9
Ver también versión, información de(Control Panel)
vista de correos
abrir(Email Live Tracking) 78
explicación(Email Live Tracking), *Ver* Email Live Tracking estructura(Email Live Tracking)
vista general de ataques(Threat Live Report) 189
vista general de correos(Email Live Tracking), *Ver* Email Live Tracking Explicación(Email Live Tracking)
vista previa
correo electrónico, *Ver* correo electrónico vista previa
Signature and Disclaimer(Signature and Disclaimer) 615

Z

zona horaria e idioma por defecto(Control Panel)
ajustar 153
zona horaria(Control Panel)
ajustar valor por defecto, *Ver* zona horaria e idioma por defecto(Control Panel) ajustar
cambiar 37

U.S. SALES 1.800.734.9905

INTERNATIONAL SALES +1.206.613.0895

www.watchguard.com | pandasecurity.com