Compliance Filter

Contents

Convenciones lingüísticas y símbolos en la documentación..... 4

Acerca de Compliance Filter.....6

Orden de las reglas de todos los servicios.....8

Activar Compliance Filter.....11

Reglas de filtrado..... 12

Crear reglas de filtrado para correos entrantes.....13
Crear reglas de filtrado para correos salientes.....20
Visualización de reglas de filtrado.....27
Acciones para reglas de filtrado.....29
Tipos de reglas de filtrado.....32
Editar reglas de filtrado.....39
Cambiar la prioridad de una regla de filtrado.....41
Orden de las reglas de filtrado.....43
Activar reglas de filtrado.....50
Desactivar reglas de filtrado de Compliance Filter.....51
Eliminar reglas de filtrado de Compliance Filter.....52

Diccionarios.....55

Crear un diccionario.....56
Editar un diccionario.....59
Eliminar un diccionario.....61

Expresiones regulares.....64

Explicación de las expresiones regulares.....65
Excepciones en las expresiones regulares.....73
Usos frecuentes de las expresiones regulares.....74

Ejemplos de expresiones regulares complejas..... 76

Desactivar Compliance Filter..... 78

Índice.....80

Convenciones lingüísticas y símbolos en la documentación

Aclaración sobre el género empleado

Para mejorar la legilibilidad, en esta documentación se emplea el masculino genérico. Cabe señalar aquí que el uso exclusivo de la forma masculina debe entenderse como independiente del género.

Símbolos utilizados

Los siguientes símbolos se utilizan para identificar mejor los pasos relevantes dentro de los capítulos dedicados a instrucciones:

SÍMBOLO	SIGNIFICADO	EXPLICACIÓN
	Requisito	Condición que debe cumplirse antes del siguiente paso.
	Resultado intermedio	Resultado alcanzado provisionalmente tras un paso concreto.
	Resultado final	Resultado alcanzado una vez finalizada la secuencia de pasos de un capítulo de instrucciones.

Advertencias e indicaciones de seguridad

Las advertencias e indicaciones de seguridad se emplean para informar al usuario sobre riesgos residuales y peligros, así como sobre el procedimiento a emplear para evitarlos. En esta documentación se emplean las siguientes advertencias e indicaciones de seguridad:

SÍMBOLO	SIGNIFICADO	EXPLICACIÓN
	NOTA	Información adicional dentro de determinado párrafo, relevante para la realización de pasos posteriores.

SÍMBOLO	SIGNIFICADO	EXPLICACIÓN
	CONSEJO	Indicación sobre opciones de configuración.
	IMPORTANTE	Advertencias con información sobre limitaciones u opciones de configuración importantes del servicio.
	ATENCIÓN	Advertencia sobre costes adicionales que pueden surgir al contratar servicios.
	ADVERTENCIA	Advertencia sobre una posible pérdida de datos.
	PELIGRO	Advertencia sobre una posible infección de un sistema con malware.

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 8.

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 11), 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 64). 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 12. 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 55). 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 78).

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 6) se aplica antes que Content Control (véase Acerca de Content Control). 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 12).

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**.

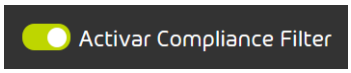


Figura 1: Activar Compliance Filter

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 12) y diccionarios (véase Diccionarios en la página 55) 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 13) y salientes (véase Crear reglas de filtrado para correos salientes en la página 20). Las reglas de filtrado creadas se muestran en dos tablas (véase Visualización de reglas de filtrado en la página 27).

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 29) 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 32) 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 39). Además, los administradores pueden cambiar la prioridad de las reglas de filtrado (véase Cambiar la prioridad de una regla de filtrado en la página 41). 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 43.

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 51). Las reglas de filtrado desactivadas pueden activarse de nuevo posteriormente (véase Activar reglas de filtrado en la página 50).

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 52).

Crear reglas de filtrado para correos entrantes

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 11).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede crear reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 6) 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**.

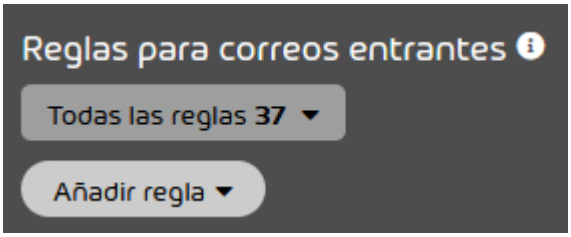


Figura 2: Añadir reglas

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 29 encontrará una explicación de las acciones.

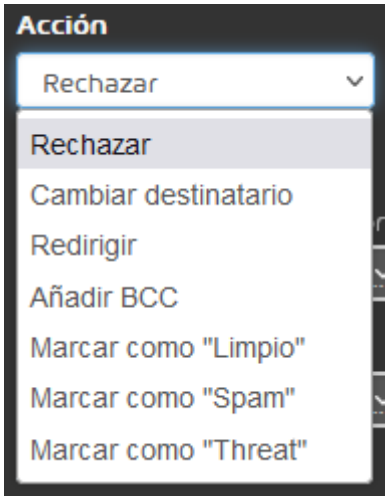


Figura 3: Seleccionar una acción

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 29.

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.

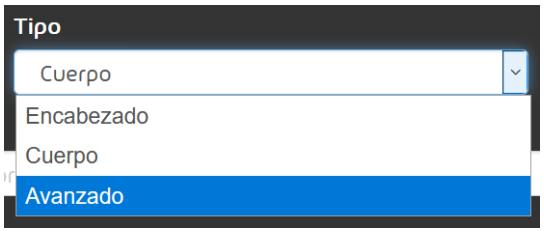


Figura 4: Seleccionar el tipo de regla de filtrado.

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 32 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 55) 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 55) 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 64 y Explicación de las expresiones regulares en la página 65. En Excepciones en las expresiones regulares en la página 73 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 5: Describir reglas de filtrado

11. Haga clic en **Añadir**.

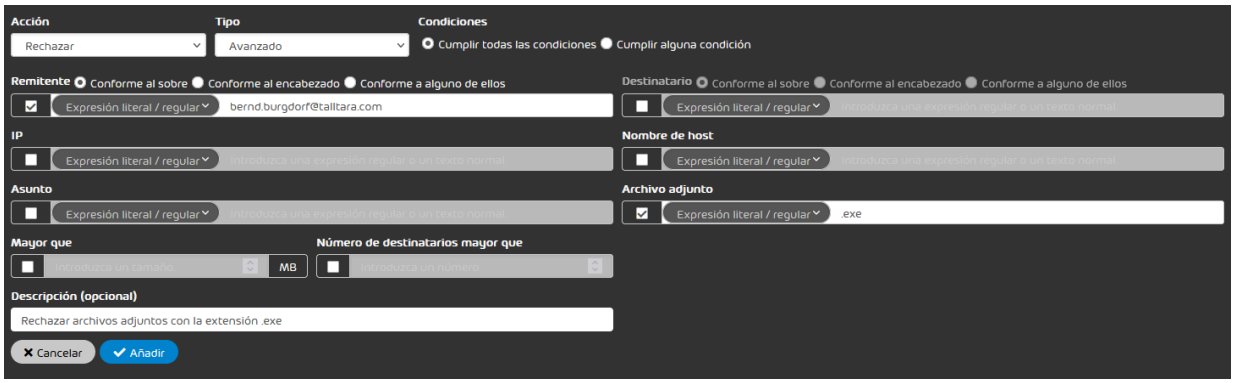


Figura 6: Añadir una regla de filtrado

La regla de filtrado se añade a la tabla bajo **Reglas para correos entrantes** (véase Visualización de reglas de filtrado en la página 27). 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 39), modificar su prioridad (véase Cambiar la prioridad de una regla de filtrado en la página 41), desactivarla temporalmente (véase Desactivar reglas de filtrado de Compliance Filter en la página 51) o eliminarla (véase Eliminar reglas de filtrado de Compliance Filter en la página 52).

Crear reglas de filtrado para correos salientes

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 11).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede crear reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 6) 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**.

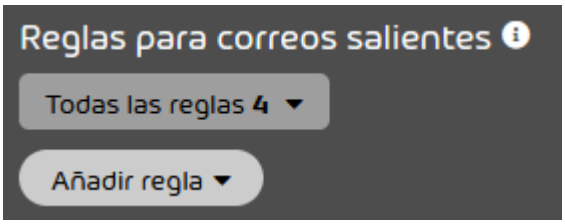


Figura 7: Añadir reglas

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 29 encontrará una explicación de las acciones.

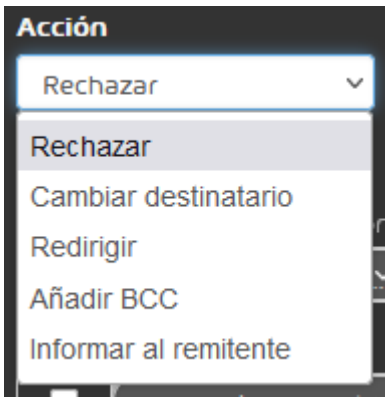


Figura 8: Seleccionar una acción

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 29.

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.

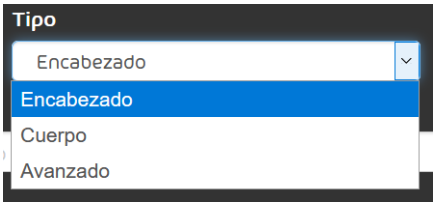


Figura 9: Seleccionar el tipo de regla de filtrado.

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 32 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 55) 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 55) 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 64 y Explicación de las expresiones regulares en la página 65. En Excepciones en las expresiones regulares en la página 73 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 10: Describir reglas de filtrado

11. Haga clic en **Añadir**.

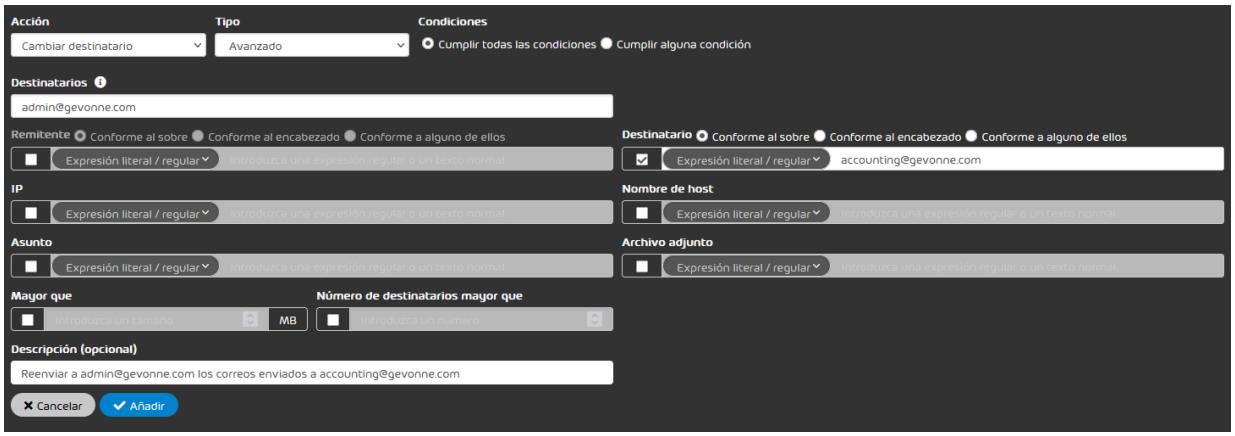


Figura 11: Añadir una regla de filtrado

La regla de filtrado se añade a la tabla bajo **Reglas para correos salientes** (véase Visualización de reglas de filtrado en la página 27). 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 39), modificar su prioridad (véase Cambiar la prioridad de una regla de filtrado en la página 41), desactivarla temporalmente (véase Desactivar reglas de filtrado de Compliance Filter en la página 51) o eliminarla (véase Eliminar reglas de filtrado de Compliance Filter en la página 52).

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 29.
- **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 32). 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 6) 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 1: 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 6), 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 64 y Explicación de las expresiones regulares en la página 65. El capítulo Excepciones en las expresiones regulares en la página 73 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 55.

Tabla 2: Tipo Encabezado

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Filtro: encabezado	El término de búsqueda introducido se busca en el encabezado del correo.	Factura

Tabla 3: 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 4: Tipo Avanzado

CAMPO	DESCRIPCIÓN	EJEMPLO DE VALORES
Remitente	El término de búsqueda o las expresiones del diccionario asignado (véase Diccionarios en la página 55) 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 11) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 13 o Crear reglas de filtrado para correos salientes en la página 20).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede editar reglas de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 6).

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.

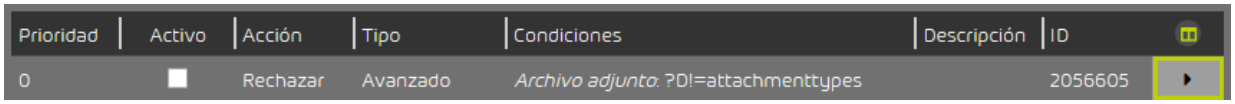


Figura 12: Abrir el menú

6. Haga clic en **Editar regla**.

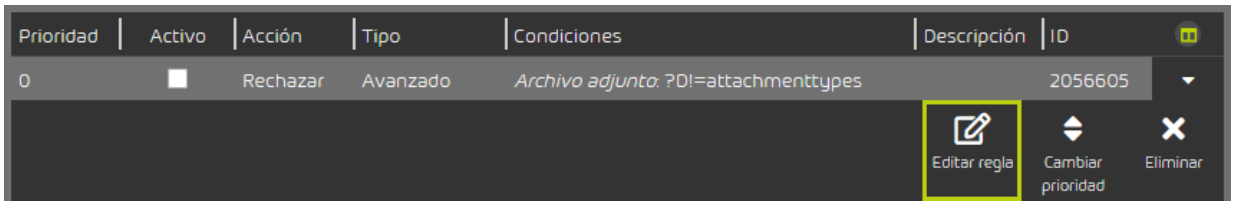


Figura 13: Editar reglas de filtrado

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 13 o Crear reglas de filtrado para correos salientes en la página 20.

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

Figura 14: 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 11) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 13 o Crear reglas de filtrado para correos salientes en la página 20).

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 6). 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 43).

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.

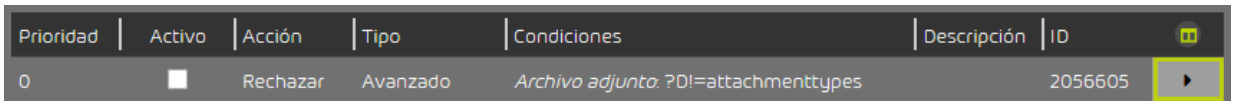


Figura 15: Abrir el menú

Se abre un menú.

6. Haga clic en **Cambiar prioridad**.

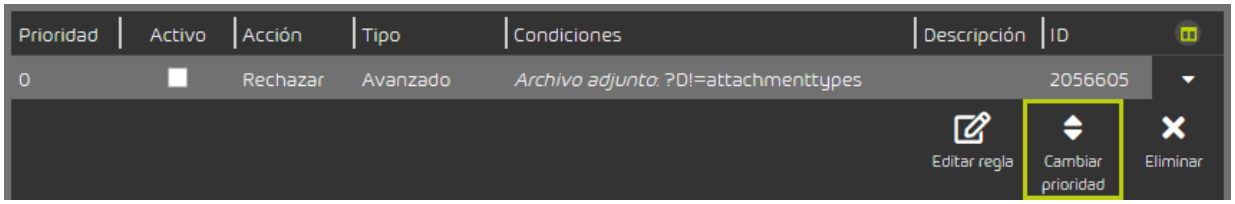


Figura 16: Cambiar la prioridad

Se abre un menú.

7. Introduzca la nueva prioridad de la regla de filtrado en **Prioridad**.

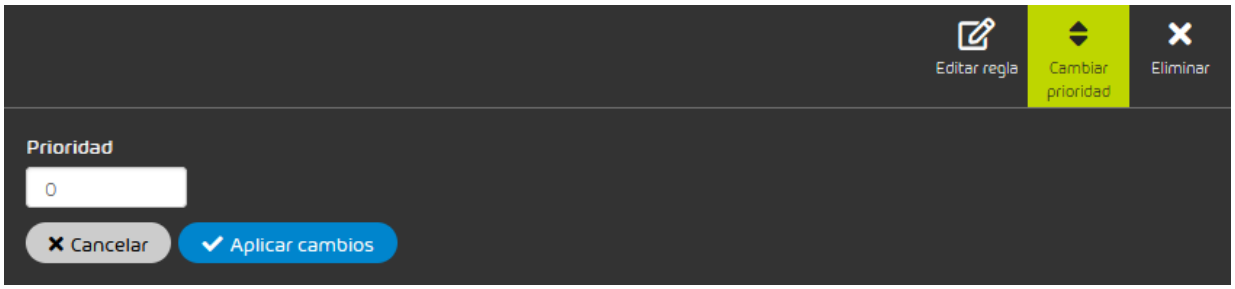


Figura 17: Indicar la prioridad

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 8). 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 6) se procesan conforme a su tipo (véase Tipos de reglas de filtrado en la página 32) en el siguiente orden:

1. **Cuerpo**
2. **Encabezado**
3. **Avanzado**

Figura 18: 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 41).

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.

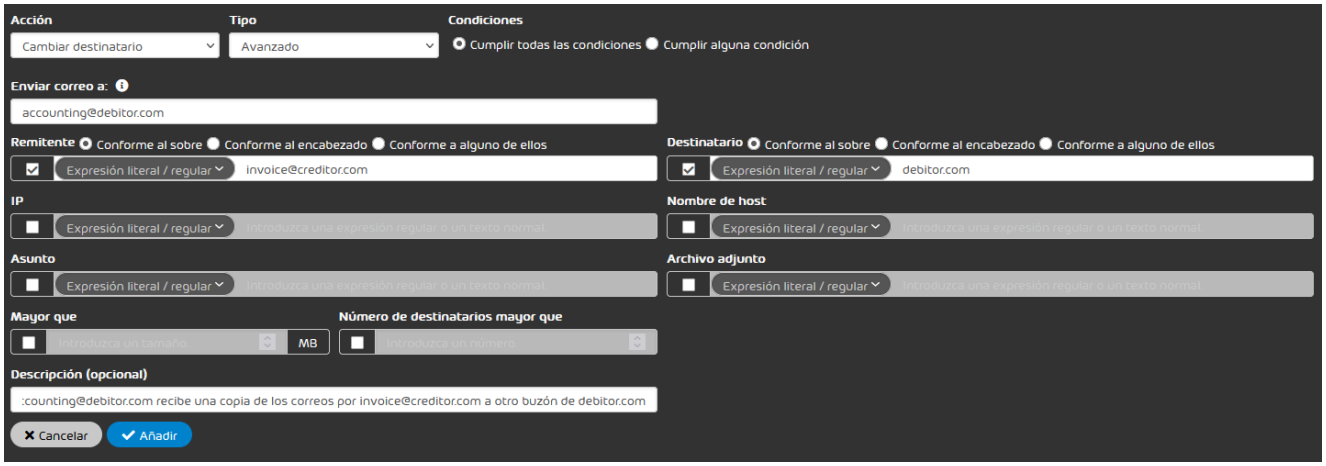


Figura 19: Regla de filtrado: Reenviar

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.

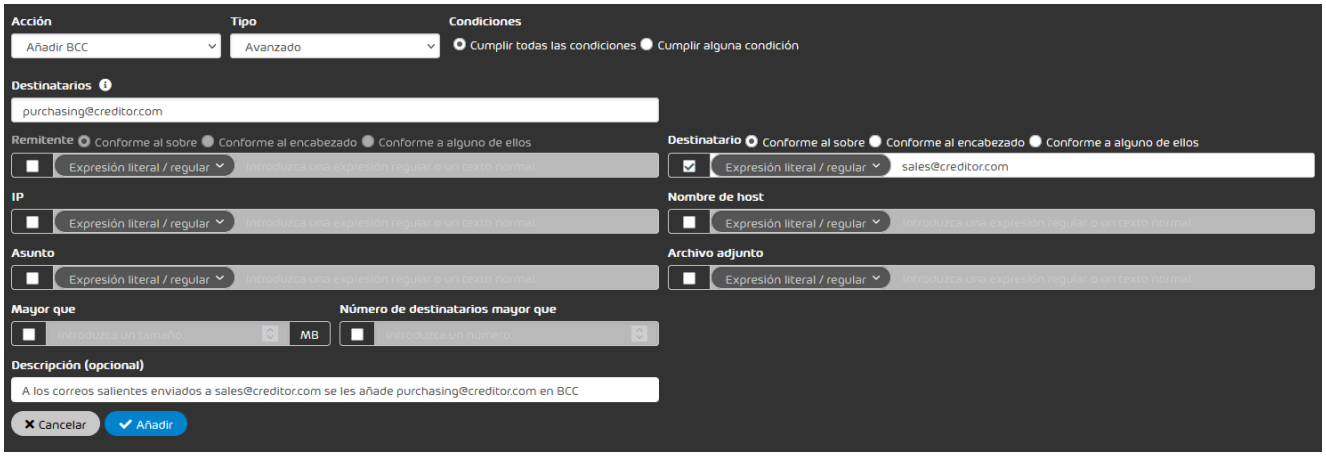


Figura 20: Regla de filtrado: añadir purchasing@creditor.com como destinatario de copia oculta

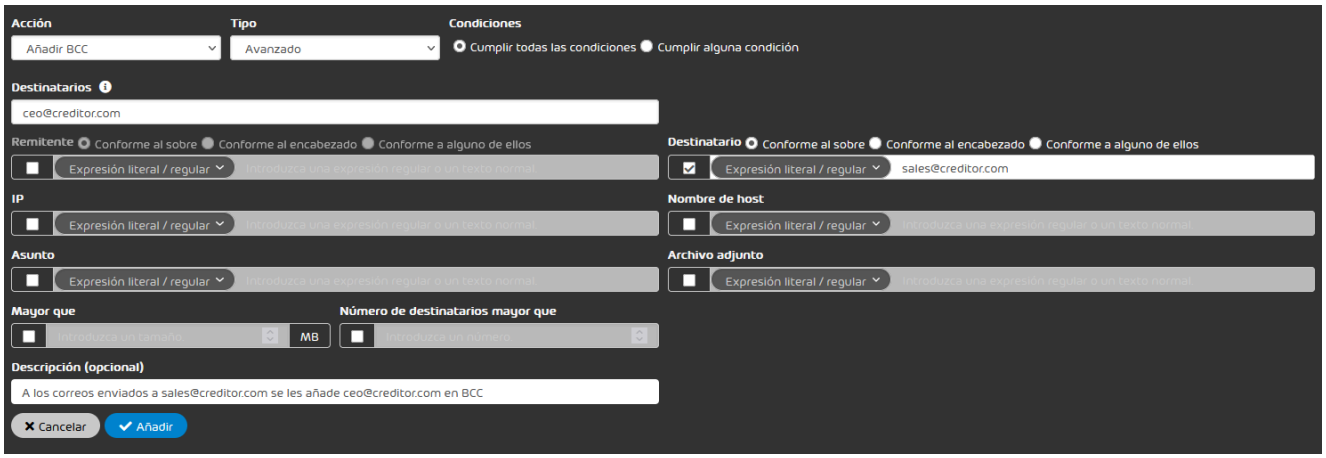
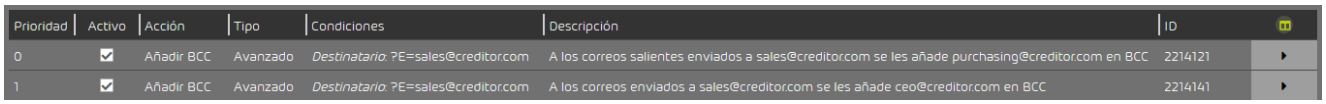


Figura 21: Regla de filtrado: añadir ceo@creditor.com como destinatario de copia oculta



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 22: 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.

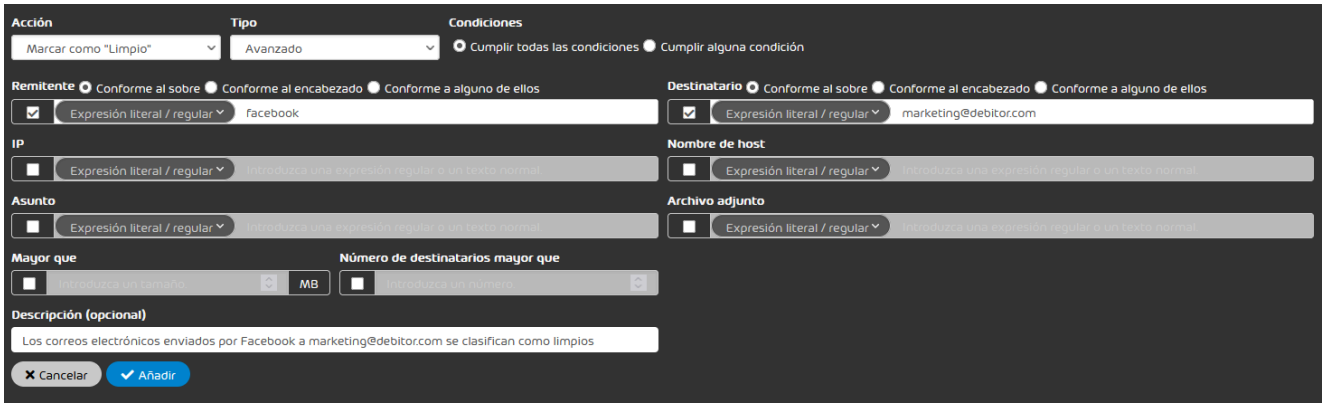


Figura 23: Regla de filtrado: Marcar como "limpio"

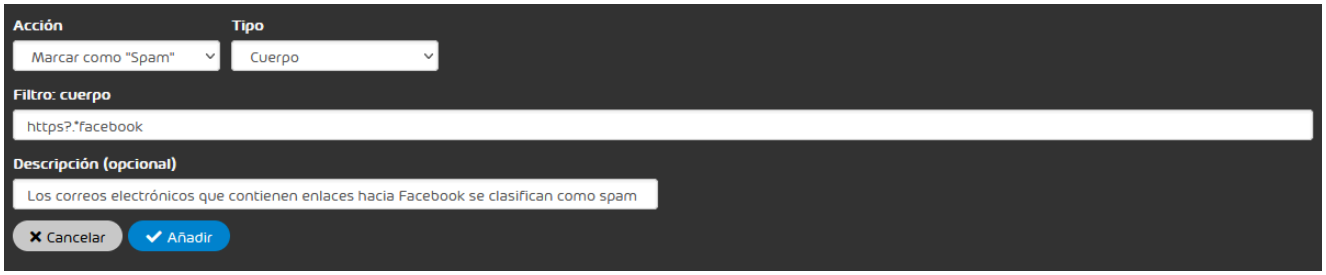


Figura 24: Regla de filtrado: Marcar como "spam"

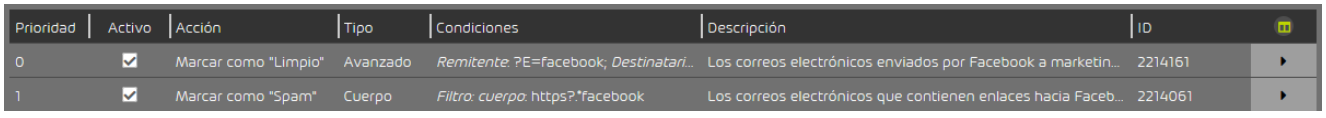


Figura 25: Orden de las reglas de filtrado

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.

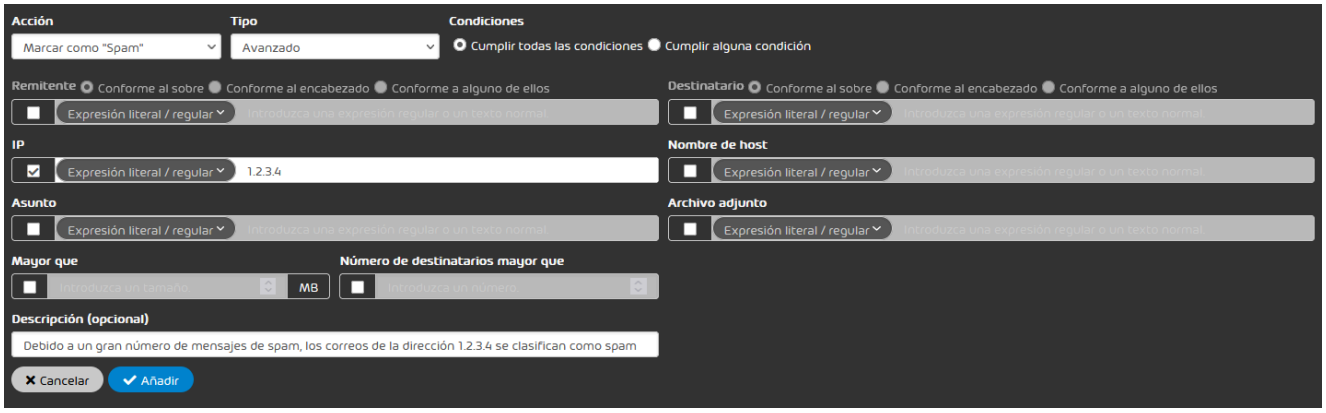


Figura 26: Regla de filtrado: Marcar correos de una dirección IPv4 como spam

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 51).

Si desea volver a aplicar una regla de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 6) 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**.

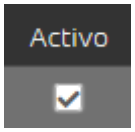


Figura 27: Activar reglas de filtrado

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 11) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 13 o Crear reglas de filtrado para correos salientes en la página 20).

Si desea utilizar una regla de filtrado de Compliance Filter (véase Acerca de Compliance Filter en la página 6) 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**.

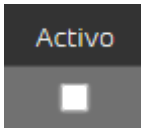


Figura 28: Desactivar reglas de filtrado

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 50).

Eliminar reglas de filtrado de Compliance Filter

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 11) y creado reglas de filtrado para Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 13 o Crear reglas de filtrado para correos salientes en la página 20).

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.

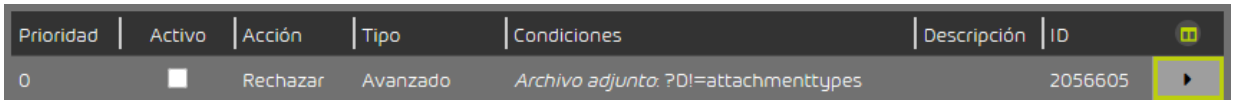


Figura 29: Abrir el menú

Se abre un menú.

6. Haga clic en **Eliminar**.

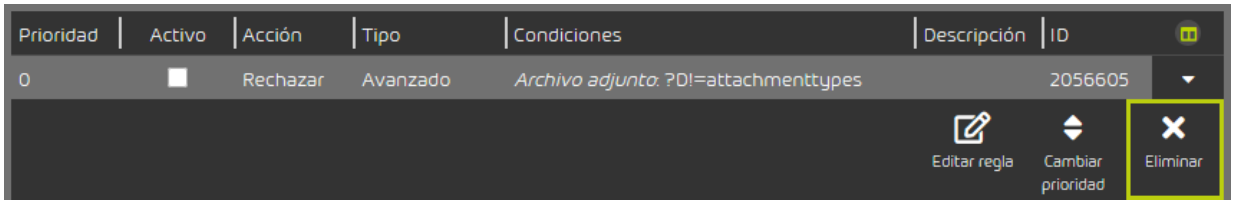


Figura 30: Eliminar reglas de filtrado

Se muestra un mensaje de advertencia.

7. Haga clic en **Confirmar**.

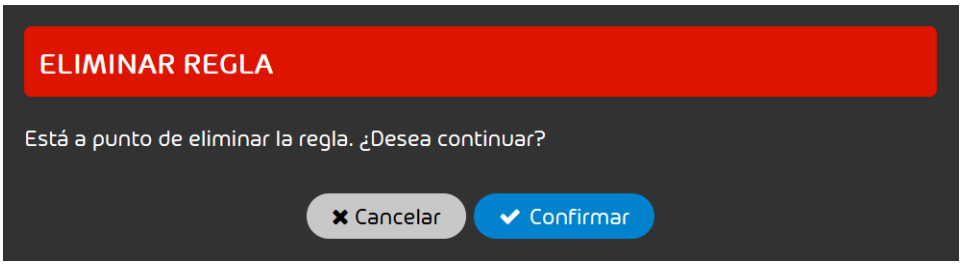


Figura 31: Confirmar la eliminación

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 6). 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 13 o Crear reglas de filtrado para correos salientes en la página 20), 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 32). 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 56), así como editar (véase Editar un diccionario en la página 59) y eliminar (véase Eliminar un diccionario en la página 61) diccionarios previos.

Crear un diccionario

Ha activado Compliance Filter para el dominio seleccionado (véase Activar Compliance Filter en la página 11).

En el módulo **Compliance Filter** > **Diccionarios** puede crear diccionarios (véase Diccionarios en la página 55) 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 13 y Crear reglas de filtrado para correos salientes en la página 20).

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**.

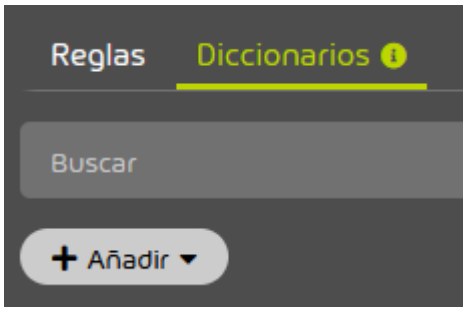


Figura 32: Añadir un diccionario

Se muestra un formulario para la creación de diccionarios.

Figura 33: 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 65) así como sus excepciones (véase Excepciones en las expresiones regulares en la página 73).

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 59) o eliminarlo (véase Eliminar un diccionario en la página 61). Puede vincular el diccionario a reglas de filtrado de Compliance Filter (véanse Crear reglas de filtrado para correos entrantes en la página 13 y Crear reglas de filtrado para correos salientes en la página 20).

Editar un diccionario

Ha creado un diccionario (véase Crear un diccionario en la página 56).

En el módulo **Configuración de seguridad** > **Compliance Filter** puede editar diccionarios (véase Diccionarios en la página 55) de Compliance Filter (véase Acerca de Compliance Filter en la página 6).

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.

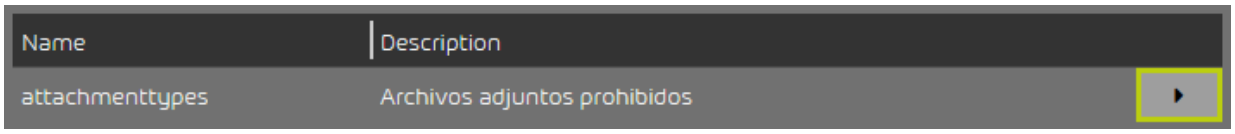


Figura 34: Abrir el menú

6. Haga clic en **Editar**.

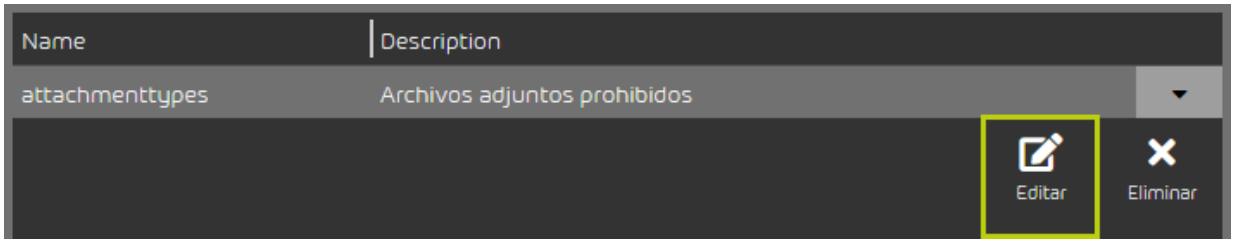


Figura 35: Editar un diccionario

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 56.

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

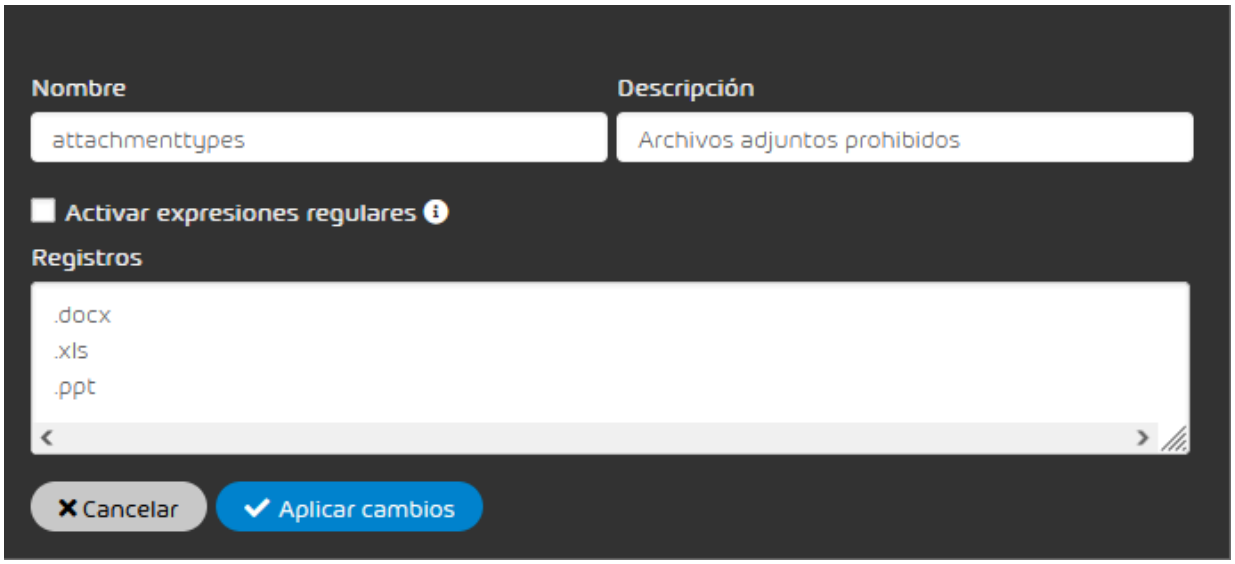


Figura 36: Aplicar los cambios

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 56). El diccionario no está vinculado a ninguna regla de filtrado de Compliance Filter.

Si deja de necesitar un diccionario (véase Diccionarios en la página 55) de Compliance Filter (véase Acerca de Compliance Filter en la página 6) 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.

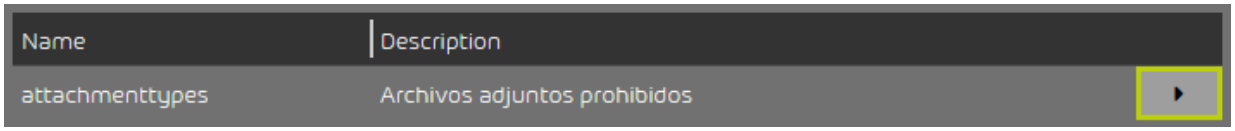


Figura 37: Abrir el menú

Se abre un menú.

6. Haga clic en **Eliminar**.

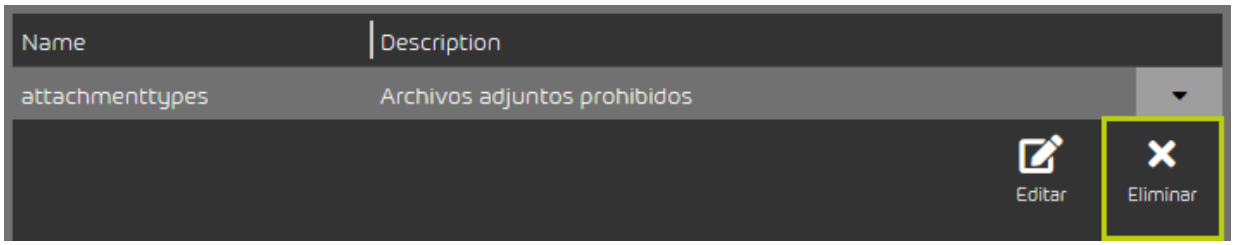


Figura 38: Eliminar un diccionario

Se muestra un mensaje de advertencia.

7. Haga clic en **Confirmar**.

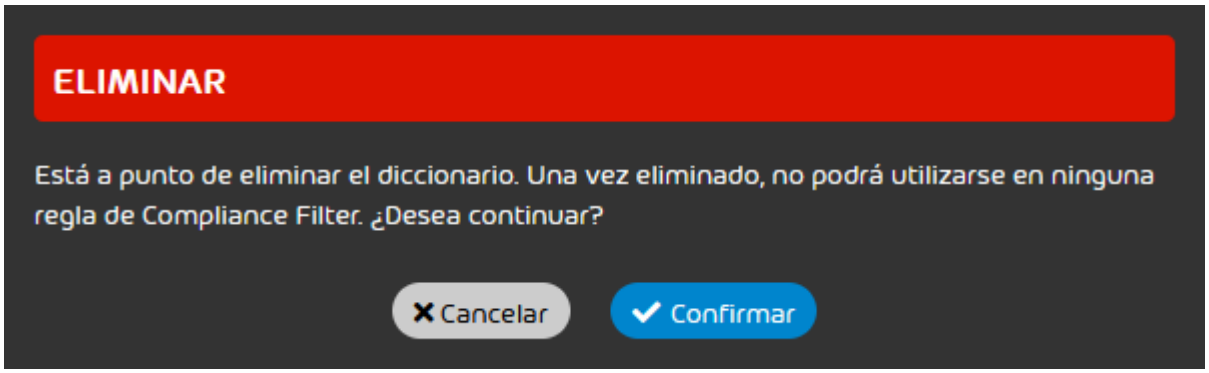


Figura 39: Confirmar la eliminación

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 12) 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 65) 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 32) y en diccionarios (véase Diccionarios en la página 55).

En los capítulos Explicación de las expresiones regulares en la página 65 y Ejemplos de expresiones regulares complejas en la página 76 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 73.

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 "p0rn", que Compliance Filter no marca. En estos casos resulta más efectivo emplear una expresión regular:

Figura 40: 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 5: Búsqueda de letras

TEXTO	REGEX
abcdef	**abc**
abcde	
Abcd	

Las letras permiten encontrar letras en cualquier posición de un texto.

Tabla 6: 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 7: 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 8: 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 9: 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 10: 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 11: 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 12: 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 13: 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 14: Caracteres opcionales

TEXTO	REGEX
3 users online	**\d+ users? online**
150 users online	

TEXTO	REGEX
20 users online	
1 user online	
no user online	

El signo de interrogación "?" marca el carácter anterior como opcional.

grupos

Tabla 15: 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 16: Selección de varias opciones

TEXTO	REGEX
data.csv	**.*\.(exe|xlsx)**
bild.jpg	

TEXTO	REGEX
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 17: 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 18: Elementos sintácticos

COMODÍN/CLASE DE CARACTERES	FUNCIÓN
abc…	Letras

COMODÍN/CLASE DE CARACTERES	FUNCIÓN
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
\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

COMODÍN/CLASE DE CARACTERES	FUNCIÓN
(.*)	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 6 y Reglas de filtrado en la página 12) 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 55) 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 65) para supuestos frecuentes de Compliance Filter (véase Acerca de Compliance Filter en la página 6).

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 65) dentro de reglas de filtrado para Compliance Filter (véase Acerca de Compliance Filter en la página 6).

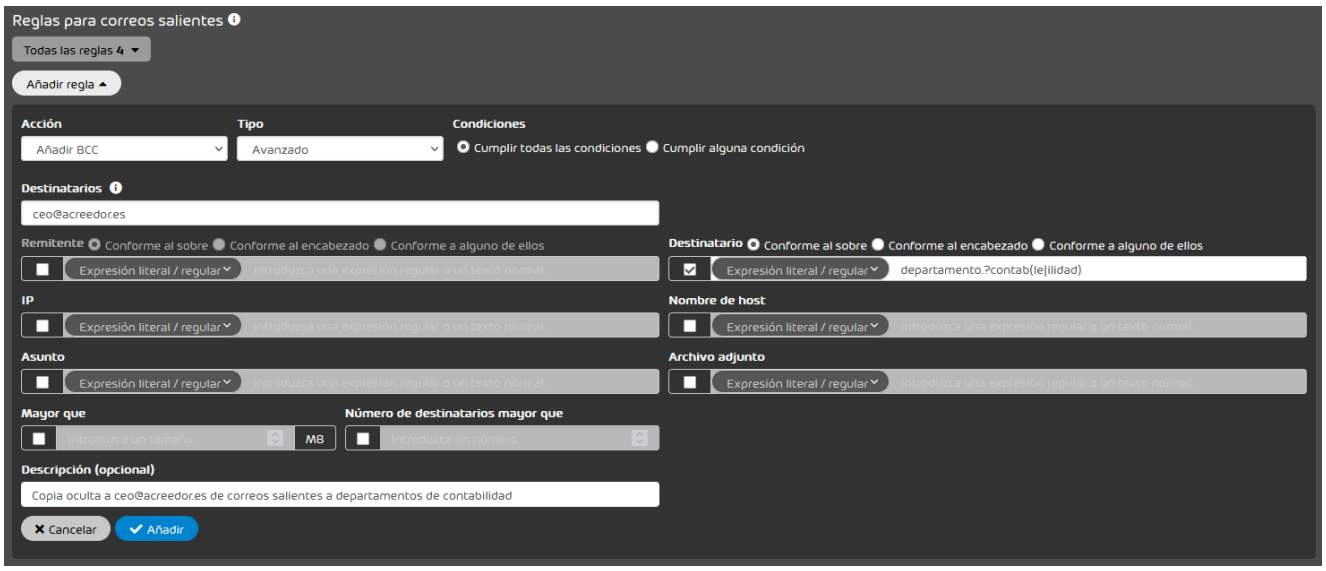


Figura 41: Búsqueda de destinatarios

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 42: 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 6), 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**.

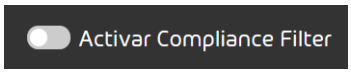


Figura 43: Desactivar Compliance Filter

Aparece una ventana de confirmación.

5. Haga clic en **Confirmar**.

Figura 44: 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.

Índice

A

acciones
    explicación 29
activar
    Compliance Filter 11
    regla de filtrado 50
advertencias
    explicación 4

B

borrar
    diccionario, *Ver* diccionario borrar
    regla de filtrado, *Ver* regla de filtrado borrar

C

cambiar
    prioridad de una regla de filtrado 41
campos
    tipo, *Ver* tipo campos
Compliance Filter
    activar 11
    desactivar 78
    explicación 6
condición
    regla de filtrado, *Ver* regla de filtrado condición
crear
    diccionario, *Ver* diccionario crear
    reglas de filtrado para correos entrantes 13
    reglas de filtrado para correos salientes 20

D

desactivar
    Compliance Filter 78
    regla de filtrado 51
diccionario
    borrar 61
    crear 56
    editar 59
    explicación 55
documentación
    indicaciones 4

símbolos 4

E

editar
diccionario, *Ver* diccionario editar
regla de filtrado 39
ejemplo
expresión regular compleja 76
Ejemplo
expresión regular, *Ver* expresión regular Ejemplo
excepción
expresión regular 73
explicación
acciones 29
advertencias 4
diccionario 55
expresión regular 65
indicaciones de seguridad 4
expresión regular
Ejemplo 74
excepción 73
explicación 65
uso, *Ver* expresión regular Ejemplo
expresión regular compleja
ejemplo 76

I

indicaciones
documentación 4
indicaciones de seguridad
explicación 4

O

orden
reglas de filtrado, *Ver* reglas de filtrado orden
Orden de las reglas de todos los servicios 8

P

prioridad de una regla de filtrado
cambiar 41

R

regla de filtrado
    activar 50
    borrar 52
    condición 32
    desactivar 51
    editar 39
    tipo 32
reglas de filtrado
    orden 43
reglas de filtrado para correos entrantes
    crear 13
reglas de filtrado para correos salientes
    crear 20

S

símbolos
    documentación 4

T

tipo
    campos 32
    regla de filtrado, *Ver* regla de filtrado tipo

U

uso
    expresión regular, *Ver* expresión regular Ejemplo

U.S. SALES 1.800.734.9905

INTERNATIONAL SALES +1.206.613.0895

www.watchguard.com | pandasecurity.com