Email Authentication

Contents

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 6). Están disponibles los siguientes métodos:

- Validación SPF (Sender Policy Framework) (véase Comprobación SPF en la página 6)
- Validación y firma DKIM (DomainKeys Identified Mail) (véase Validación DKIM y firma DKIM en la página 19)
- Validación DMARC (Domain-based Message Authentication, Reporting and Conformance (véase Validación DMARC en la página 25)

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 4).

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 6), la validación DKIM (véase Validación DKIM y firma DKIM en la página 19) y la validación DMARC (véase Validación DMARC en la página 25) 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 9.

Para saber cómo definir un registro CNAME, véase Definir un registro CNAME en la página 19.

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 1: 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 6).

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 6
- Validación DKIM y firma DKIM en la página 19
- Validación DMARC en la página 25

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 39).

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 41).

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 7.

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 9) 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 10) y configurar las opciones avanzadas (véase Configurar opciones avanzadas de comprobación SPF en la página 14).

En el capítulo Solución de problemas en la página 17 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 10). 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 1: 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 2: 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 3: 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 9). 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 9).
- 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 2: Activar la comprobación SPF

Se muestra un mensaje de advertencia.

5. Haga clic en **Confirmar**.

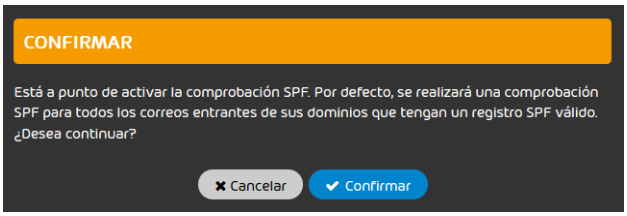

Figura 3: Confirmar

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.

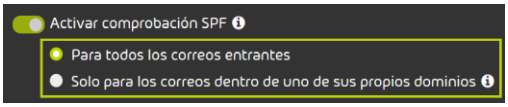

Figura 4: Elegir correos para la comprobación SPF

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 14).

Configurar opciones avanzadas de comprobación SPF

Ha activado la comprobación SPF (véase Activar la comprobación SPF en la página 10).

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 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** > **Email Authentication**.
4. Haga clic en **Opciones avanzadas**.

Figura 5: 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**.

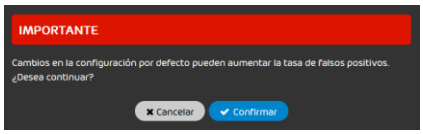

Figura 6: Confirmar

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.

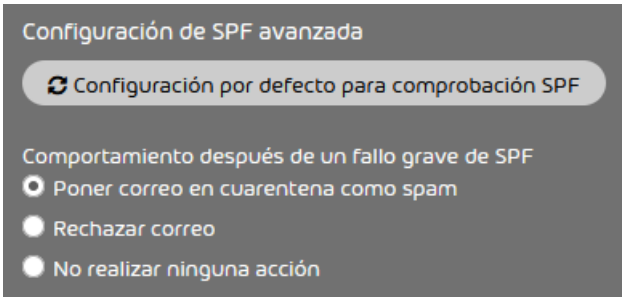

Figura 7: Seleccionar las acciones tras un fallo grave de SPF

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.

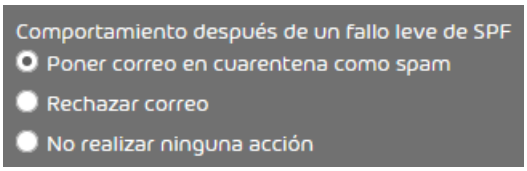

Figura 8: Seleccionar las acciones tras un fallo leve de SPF

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.

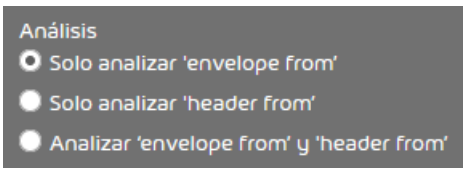

Figura 9: Configurar el análisis

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 17)
- Errores debidos a comprobaciones SPF al recibir correos (véase Solución de problemas: Problemas provocados por comprobaciones SPF al recibir correos en la página 18)

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 20) y, a continuación, configurar las opciones avanzadas (véase Configurar opciones avanzadas de validación DKIM en la página 21).

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 19). A continuación, los administradores deben activar las firmas DKIM para los correos salientes de sus dominios (véase Activar la firma DKIM en la página 24). 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 19). 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 20).

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 19) 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 10: 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 21).

Configurar opciones avanzadas de validación DKIM

Ha activado la validación mediante DKIM (véase Activar la validación DKIM en la página 20).

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 19).

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 11: 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**.

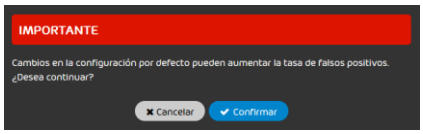

Figura 12: Confirmar

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.

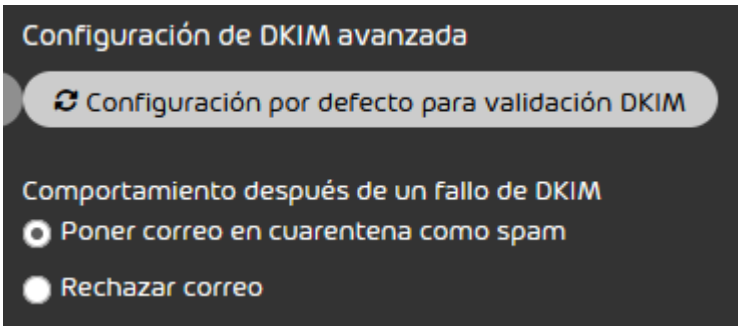

Figura 13: Seleccionar "Opciones avanzadas"

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 19). 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 14: 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 29.

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 25 y Etiquetas de los registros DMARC en la página 26), activar la validación DMARC (véase Activar la validación DMARC en la página 34) y, por último, configurar las opciones avanzadas (véase Configurar opciones avanzadas de validación DMARC en la página 35).

Añadir un registro DMARC

Los registros DMARC son imprescindibles para poder realizar validaciones DMARC (véase Validación DMARC en la página 25) 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 26 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 19). 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 6). 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 4: 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 6) o la validación DKIM (véase Validación DKIM y firma DKIM en la página 19) 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 35), 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 9, Definir un registro CNAME en la página 19 y Añadir un registro DMARC en la página 25). 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 6) y validaciones DKIM (véase Validación DKIM y firma DKIM en la página 19).

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 15: 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 35).

Configurar opciones avanzadas de validación DMARC

Ha activado la validación DMARC (véase Activar la validación DMARC en la página 34).

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 25).

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 16: 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**.

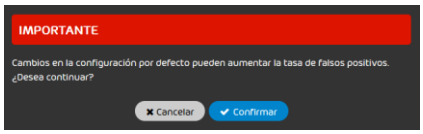

Figura 17: Confirmar

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.

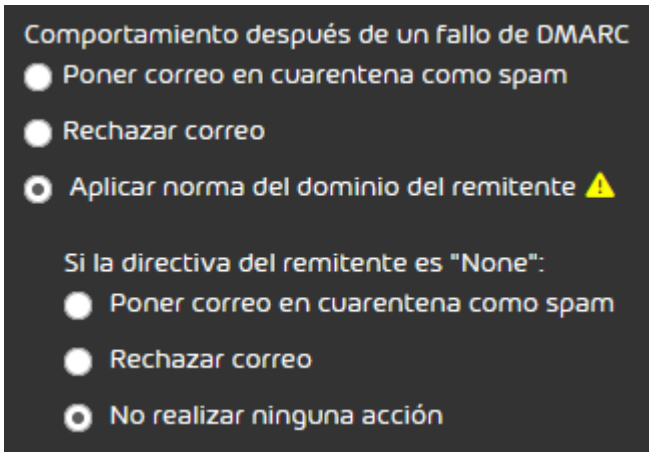

Figura 18: Seleccionar acciones tras un fallo de DMARC

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.

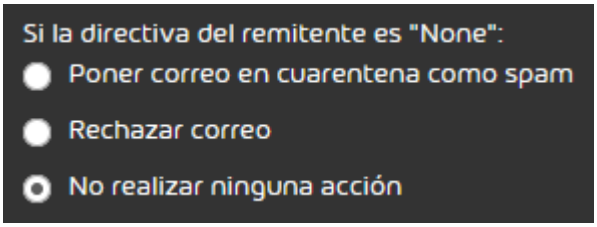

Figura 19: Acciones en caso de directiva de remitente ajustada a "None"

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 25), 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 6).

Si ha activado la comprobación SPF (véase Comprobación SPF en la página 6), la validación DKIM (véase Validación DKIM y firma DKIM en la página 19) y/o la validación DMARC (véase Validación DMARC en la página 25) 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 20: agregar excepción

Se abre una vista avanzada.

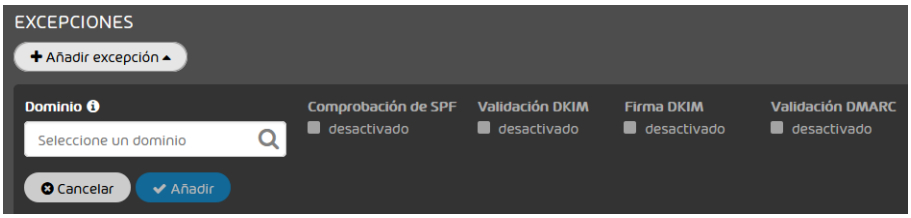

Figura 21: Vista avanzada

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 14), 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 35), 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 35), 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.

Index

A

C

D

E

F

I

M

R

S

T

V

U.S. SALES 1.800.734.9905

INTERNATIONAL SALES +1.206.613.0895

www.watchguard.com | pandasecurity.com