

2025-07-21



HORNETSECURITY

EMAIL ENCRYPTION

[www.hornetsecurity.com](http://www.hornetsecurity.com)

THE CLOUD SECURITY PIONEER

# Contents

|                                                               |    |
|---------------------------------------------------------------|----|
| Convenciones lingüísticas y símbolos en la documentación..... | 3  |
| Email Encryption.....                                         | 5  |
| Activar Email Encryption.....                                 | 5  |
| Cifrado, directivas de.....                                   | 6  |
| Comprobar capacidades de cifrado de interlocutores.....       | 7  |
| Métodos de cifrado.....                                       | 9  |
| Reglas de cifrado.....                                        | 20 |
| Usuarios con S/MIME.....                                      | 35 |
| Añadir un usuario con S/MIME.....                             | 36 |
| Cancelar una suscripción.....                                 | 41 |
| Adquirir una suscripción.....                                 | 42 |
| Datos de usuarios con S/MIME.....                             | 44 |
| Exportar usuarios con S/MIME en formato CSV.....              | 47 |
| Palabras clave para usuarios con S/MIME.....                  | 50 |
| Desactivar Email Encryption.....                              | 51 |
| Índice.....                                                   | 53 |



## Convenciones lingüísticas y símbolos en la documentación

### Aclaración sobre el género empleado

Para mejorar la legibilidad, 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                                                                             | DESCRIPCIÓN          | 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                                                                             | DESCRIPCIÓN | EXPLICACIÓN                                                                                              |
|-------------------------------------------------------------------------------------|-------------|----------------------------------------------------------------------------------------------------------|
|  | NOTA        | Información adicional dentro de determinado párrafo, relevante para la realización de pasos posteriores. |
|  | CONSEJO     | Indicación sobre opciones de configuración.                                                              |



| SÍMBOLO                                                                            | DESCRIPCIÓN | EXPLICACIÓN                                                                                           |
|------------------------------------------------------------------------------------|-------------|-------------------------------------------------------------------------------------------------------|
|   | 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.                                    |



## Email Encryption

En el módulo **Email Security > Email Encryption**, los administradores pueden decidir los métodos de cifrado a emplear en el tráfico de correo de sus dominios. Esto se regula mediante directivas de cifrado (véase [Cifrado, directivas de](#) en la página 6). Adicionalmente, Email Encryption permite a los administradores adquirir certificados S/MIME para sus usuarios y administrarlos (véase [Usuarios con S/MIME](#) en la página 35). Mediante palabras clave en el asunto de los correos salientes es posible ejecutar diversas acciones relacionadas con el cifrado (véase [Palabras clave para usuarios con S/MIME](#) en la página 50).

Email Encryption debe activarse por separado por parte de un administrador (véase [Activar Email Encryption](#) en la página 5), que también puede desactivarlo (véase [Desactivar Email Encryption](#) en la página 51).

## Activar Email Encryption



Ha activado Spam and Malware Protection (véase [#unique\\_8](#)).

En el módulo **Email Security > Email Encryption** puede activar Email Encryption para su dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Accione el interruptor **Activar Email Encryption**.

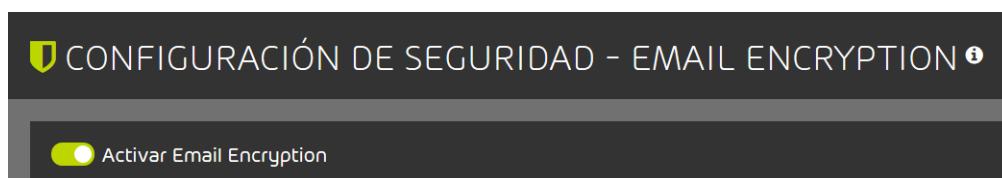


Figura 1: Activar Email Encryption



Se muestra una ventana de confirmación.



5.

**ATENCIÓN:**

Una vez activado Email Encryption, comenzará un periodo de prueba gratuito de 30 días. Al finalizar el periodo de prueba, el servicio se volverá de pago.

Haga clic en **Confirmar**.

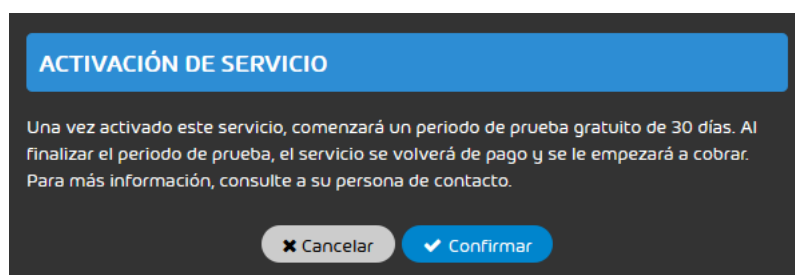


Figura 2: Confirmar



Los ajustes del módulo se habilitan.



Email Encryption se ha activado para el dominio.

**Nota:**

La firma y el cifrado de correos en el contexto de Email Encryption solo se aplica a los correos que se envíen a través de las direcciones de servidores de redireccionamiento definidas en Spam and Malware Protection (véase [#unique\\_9](#)).

A continuación puede comprobar las capacidades de cifrado de sus interlocutores (véase [Comprobar capacidades de cifrado de interlocutores](#) en la página 7) o seleccionar directamente el método de cifrado a emplear (véase [Activar métodos de cifrado](#) en la página 16), así como administrar los certificados S/MIME de sus usuarios (véase [Usuarios con S/MIME](#) en la página 35).

## Cifrado, directivas de

Una vez activado Email Encryption (véase [Activar Email Encryption](#) en la página 5), los administradores a nivel de cliente pueden comprobar qué métodos de cifrado permiten sus interlocutores (véase [Comprobar capacidades de cifrado de interlocutores](#) en la página 7).



Sabiendo esto pueden seleccionar entre una serie de métodos de cifrado (véase [Métodos de cifrado](#) en la página 9) y activarlos para su dominio (véase [Activar métodos de cifrado](#) en la página 16). Los métodos de cifrado se procesan en un orden determinado (véase [Orden de los métodos de cifrado](#) en la página 15) y, en algunos casos, pueden combinarse los unos con los otros (véase [Combinación de métodos de cifrado](#) en la página 14). También es posible hacer que se añadan indicaciones sobre el método de cifrado empleado a los asuntos de correos entrantes (véase [#unique\\_15](#)).

Los administradores a nivel de cliente pueden definir reglas para el cifrado del tráfico de correo entrante y saliente de sus dominios (véase [Añadir reglas](#) en la página 22) con los métodos de cifrado activados. Las reglas se ordenan por prioridad y se procesan en el orden establecido (véase [Orden de las reglas](#) en la página 21). Dichas reglas pueden editarse (véase [Editar reglas](#) en la página 26), activarse (véase [Activar reglas](#) en la página 29) y desactivarse (véase [Desactivar reglas](#) en la página 30). Si una regla deja de ser necesaria, es posible eliminarla (véase [Eliminar reglas](#) en la página 33).

Además, los usuarios pueden emplear palabras clave en los asuntos de los correos salientes para iniciar determinadas acciones relativas al cifrado y/o la firma S/MIME de dichos correos (véase [Palabras clave para usuarios con S/MIME](#) en la página 50).

## Comprobar capacidades de cifrado de interlocutores



Ha activado Email Encryption (véase [Activar Email Encryption](#) en la página 5).

Para averiguar qué métodos de cifrado (véase [Métodos de cifrado](#) en la página 9) permite un interlocutor externo, puede comprobar las capacidades de cifrado del mismo en el módulo **Email Security > Email Encryption**.

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. Haga clic en **Comprobar capacidad de cifrado**.  
 Se abre una vista avanzada.
6. Introduzca en **Direcciones de correo a comprobar** las direcciones de correo electrónico de los interlocutores cuyas capacidades de cifrado desee comprobar.

**Nota:**

Puede introducir un máximo de diez direcciones de correo electrónico al mismo tiempo. Separe las direcciones entre sí mediante punto y coma.

**Figura 3: Introducir direcciones de correo de los interlocutores**

7. Haga clic en **Añadir**.



Las direcciones de correo electrónico de los interlocutores se añaden a la tabla. Se comprueba qué métodos de cifrado son compatibles con los interlocutores. Una marca en la columna de un método de cifrado indica que el interlocutor permite el método de cifrado. Si el método de cifrado TLS es compatible con el interlocutor, se comprueba mediante un protocolo de enlace con su servidor SMTP. La columna **Respuesta de servidor** contiene la respuesta del servidor SMTP. Las columnas **S/MIME** y **PGP** solo están marcadas si disponemos de la clave pública del interlocutor.

**Nota:**

Recibimos la clave S/MIME pública de un interlocutor cuando éste envíe un correo firmado a un usuario de Control Panel. Alternativamente, los clientes pueden comunicar las claves S/MIME públicas de interlocutores a nuestro soporte técnico.

Solo disponemos de la clave PGP pública de un interlocutor si ésta se ha comunicado a nuestro soporte técnico.

Si las columnas **S/MIME** y **PGP** no están marcadas, no conocemos la clave pública del interlocutor. Sin embargo, es posible que el método de cifrado sea compatible con el interlocutor.

El método de cifrado Websafe siempre es compatible.

8. Opcional: Para vaciar la tabla, haga clic en **Borrar**.



➔ La tabla se vacía.

9. Opcional: Para cerrar la vista avanzada, haga clic en **Cerrar**.



Se han comprobado las capacidades de cifrado de un interlocutor.

A continuación puede activar métodos de cifrado para su dominio (véase [Activar métodos de cifrado](#) en la página 16).

## Métodos de cifrado

El módulo **Email Encryption** (véase [Email Encryption](#) en la página 5) ofrece diversos métodos de cifrado para activar (véase [Activar métodos de cifrado](#) en la página 16) y emplear en reglas (véase [Reglas de cifrado](#) en la página 20). Están disponibles los siguientes métodos de cifrado:

- **TLS:** TLS (Transport Layer Security) cifra los correos entre el servidor de origen y el servidor de destino. Este método de cifrado está siempre activado. TLS es compatible con diversos algoritmos y certificados de cifrado descritos en el capítulo [TLS](#) en la página 10.
- **EmiG:** EmiG (E-Mail made in Germany) es una forma de cifrado TLS con requisitos para interlocutores con certificación TÜV, la seguridad de sus servidores y los certificados empleados para el cifrado. EmiG consiste en un cifrado TLS especialmente seguro dentro de una red cerrada de proveedores de correo electrónico certificados con normas de seguridad especialmente estrictas. Para poder utilizar EmiG no es necesario realizar ningún tipo de ajustes especiales en Control Panel.
- **S/MIME:** S/MIME (Secure/Multipurpose Internet Mail Extensions) es un estándar de cifrado y firma de correos electrónicos encapsulados en MIME mediante un método de cifrado híbrido. La autoridad de certificación (CA) garantiza la autenticidad de la dirección de correo electrónico y del nombre del remitente.
- **PGP:** PGP (Pretty Good Privacy) es un estándar de cifrado asimétrico con claves públicas y privadas. El remitente cifra el correo con la clave pública del destinatario. A continuación, el destinatario puede descifrar el correo recibido con su clave privada.
- **Websafe:** Websafe permite enviar correos cifrados a destinatarios que no permiten ningún otro método de cifrado. El correo no se entrega directamente a su destinatario, sino que se deriva a Websafe, donde queda almacenado para el mismo. El destinatario puede registrarse en Websafe con sus datos de acceso personales y desbloquearlo con un PIN entregado por el remitente. Para más información, véase [Websafe](#) en la página 13.



Los administradores a nivel de cliente pueden definir reglas para el cifrado de correos entrantes y salientes de sus dominios (véase [Añadir reglas](#) en la página 22) con los métodos de cifrado TLS, S/MIME, PGP y Websafe. EmiG se aplica automáticamente una vez activado si el interlocutor ofrece dicho método de cifrado. Algunos métodos de cifrado pueden combinarse entre sí (véase [Combinación de métodos de cifrado](#) en la página 14), aplicándose en tal caso en un orden determinado (véase [Orden de los métodos de cifrado](#) en la página 15).

En el módulo **Email Live Tracking** se muestran los métodos de cifrado empleados en cada correo (véase [#unique\\_25](#)). Para poder distinguir el método de cifrado empleado en correos entrantes fuera de Control Panel, Email Encryption ofrece la opción de añadir a sus asuntos una indicación sobre el método de cifrado (véase [Activar métodos de cifrado](#) en la página 16).

## TLS



### IMPORTANTE:

Esta configuración solo es posible para las conexiones mediante TLS 1.2. Todas las versiones anteriores de TLS se desactivaron a principios del año 2022.

El cifrado TLS puede emplear diversos conjuntos de cifrado y certificados. Los administradores a nivel de cliente pueden crear reglas para el cifrado de correos con TLS (Transport Layer System) (véase [Añadir reglas](#) en la página 22) en el módulo **Email Encryption** (véase [Email Encryption](#) en la página 5). Los administradores pueden determinar los requisitos que ha de cumplir el servidor de correo del interlocutor para que pueda establecerse una conexión cifrada mediante TLS entre el mismo y un usuario de Control Panel. Esos requisitos se refieren tanto a conjuntos de cifrado como a certificados. Las diversas opciones se enumeran y describen en la siguiente tabla.



### Nota:

La conexión mediante TLS entre dos servidores suele emplear el conjunto de cifrado más fuerte del que dispongan ambos servidores. Los conjuntos de cifrado aparecen ordenados por su seguridad de mayor a menor.



Tabla 1: Opciones de TLS

| OPCIÓN               | DESCRIPCIÓN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Todos los algoritmos | <p>Es posible establecer conexiones mediante TLS con todos los conjuntos de cifrado que ofrecemos. Ofrecemos conjuntos de cifrado seguros y muy extendidos. Por tanto, esta opción ofrece la máxima compatibilidad con diversos servidores de correo de interlocutores. La conexión TLS solo se establece si el servidor de correo del interlocutor dispone de uno de los siguientes conjuntos de cifrado:</p> <ul style="list-style-type: none"><li>• ECDHE-ECDSA-AES256-GCM-SHA384</li><li>• ECDHE-RSA-AES256-GCM-SHA384</li><li>• DHE-RSA-AES256-GCM-SHA384</li><li>• ECDHE-ECDSA-CHACHA20-POLY1305</li><li>• ECDHE-RSA-CHACHA20-POLY1305</li><li>• DHE-RSA-CHACHA20-POLY1305</li><li>• ECDHE-ECDSA-AES256-CCM8</li><li>• ECDHE-ECDSA-AES256-CCM</li><li>• DHE-RSA-AES256-CCM8</li><li>• DHE-RSA-AES256-CCM</li><li>• ECDHE-ECDSA-AES256-SHA384</li><li>• ECDHE-RSA-AES256-SHA384</li><li>• DHE-RSA-AES256-SHA256</li><li>• AES256-GCM-SHA384</li><li>• AES256-CCM8</li><li>• AES256-CCM</li><li>• AES256-SHA256</li><li>• ECDHE-ECDSA-AES128-GCM-SHA256</li><li>• ECDHE-RSA-AES128-GCM-SHA256</li><li>• DHE-RSA-AES128-GCM-SHA256</li><li>• ECDHE-ECDSA-AES128-CCM8</li><li>• ECDHE-ECDSA-AES128-CCM</li><li>• DHE-RSA-AES128-CCM8</li><li>• DHE-RSA-AES128-CCM</li><li>• ECDHE-ECDSA-AES128-SHA256</li></ul> |

**OPCIÓN****Algoritmos seguros****DESCRIPCIÓN**

El cifrado TLS solo puede realizarse con conjuntos de cifrado recomendados como seguros por la Oficina Federal de Seguridad de la Información alemana (Bundesamt für Sicherheit in der Informationstechnik). La conexión TLS solo se establece si el servidor de correo del interlocutor dispone de uno de los siguientes conjuntos de cifrado:

- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-CCM
- DHE-RSA-AES256-CCM
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-CCM
- DHE-RSA-AES128-CCM
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256

**OPCIÓN****DESCRIPCIÓN****Certificados fiables****Nota:**

Esta opción solo está disponible para correos salientes.

La conexión TLS solo puede establecerse con interlocutores cuyo servidor de correo disponga de un certificado fiable.

**Certificados fiables + algoritmos seguros****Nota:**

Esta opción solo está disponible para correos salientes.

La conexión TLS solo puede establecerse con interlocutores cuyo servidor de correo disponga de un certificado fiable y un conjunto de cifrado seguro.

## Websafe

Hornetsecurity Websafe es un método para enviar correos electrónicos cifrados a destinatarios que no permitan ningún otro método de cifrado. El correo se reenvía a Hornetsecurity Websafe y se almacena allí. El destinatario del correo electrónico obtiene los datos de acceso a su cuenta personal de Websafe. A continuación, el destinatario debe introducir un PIN, una contraseña y la respuesta a una pregunta de seguridad para finalizar el registro de su cuenta de Websafe. En general, el destinatario introduce además su número de teléfono móvil para obtener el PIN con el que registrar su cuenta de Websafe. Este número de teléfono móvil se puede usar posteriormente para enviar otros PINs con los que recuperar el acceso a la cuenta de Websafe en determinadas situaciones.

El acceso a Websafe queda establecido para el destinatario y se mantiene para futuros mensajes enviados mediante Websafe. Los mensajes se almacenan en Websafe durante tres meses, eliminándose automáticamente al cabo de dicho periodo.

**Nota:**

El remitente recibe notificaciones por correo en diversas ocasiones. Algunos de estos correos incluyen datos que el remitente debe comunicar al destinatario a través de otro medio de su elección:

- Si el destinatario se registra sin comunicar su número de teléfono móvil, el PIN necesario para el registro de la cuenta de Websafe lo recibe el remitente. El remitente debe comunicar dicho PIN al destinatario.
- Si el destinatario ha cambiado su número de teléfono móvil y ha olvidado la respuesta a su pregunta de seguridad, el remitente recibe un correo con un enlace que permite al destinatario restaurar el acceso a su cuenta. El remitente debe comunicar dicho enlace al destinatario.
- Si el remitente ha solicitado un acuse de recibo al enviar un correo, recibirá una notificación en cuanto el destinatario haya leído el correo dentro de Websafe.

**Nota:**

Si un cliente o su partner ha realizado ajustes en el módulo **Configuración y auditoría > Configuración > Personalización**, las notificaciones por correo electrónico de Websafe se adaptarán a dichos ajustes. Para los clientes con Control Panel personalizado, Websafe se muestra con un diseño neutro. Para el resto de clientes, Websafe se muestra con nuestro diseño habitual. Para más información acerca los ajustes del módulo **Configuración y auditoría > Configuración > Personalización**, véase "[Personalización](#)" en el manual de Control Panel.

## Combinación de métodos de cifrado

En las reglas del módulo **Email Encryption** (véase [Reglas de cifrado](#) en la página 20) es posible combinar entre sí diversos métodos de cifrado. La siguiente tabla muestra las opciones de combinación de los métodos de cifrado. La x indica que los métodos de cifrado son compatibles entre sí.



Tabla 2: Combinaciones posibles

| CIFRADO | TLS | EMIG | S/MIME | PGP | WEBSAFE |
|---------|-----|------|--------|-----|---------|
| TLS     | -   | -    | x      | x   | -       |
| EmiG    | -   | -    | x      | x   | -       |
| S/MIME  | x   | x    | -      | -   | -       |
| PGP     | x   | x    | -      | -   | -       |
| WEBSAFE | -   | -    | -      | -   | -       |

**Nota:**

Websafe (véase [Websafe](#) en la página 13) puede combinarse con todos los métodos de cifrado. Websafe se utiliza como último recurso en caso de que el interlocutor no permita ningún otro método de cifrado.

**Nota:**

Si se han seleccionado varios métodos de cifrado para una regla, éstos se procesarán en un orden fijo (véase [Orden de los métodos de cifrado](#) en la página 15). Durante el procesamiento se tienen en cuenta todas las combinaciones posibles.

## Orden de los métodos de cifrado

Si una regla del módulo **Email Encryption** (véase [Reglas de cifrado](#) en la página 20) incluye varios métodos de cifrado, éstos se procesarán en un orden fijo. Para comprobar cuáles de los métodos de cifrado seleccionados pueden aplicarse a sus correos, se emplea la siguiente secuencia:

**S/MIME → PGP → EmiG → TLS → WEBSAFE**

Desde que se encuentra un método de cifrado aplicable a un correo, solo se tienen en cuenta los métodos de cifrado compatibles con el mismo (véase [Combinación de métodos de cifrado](#) en la página 14).



Todos los métodos de cifrado posibles se aplican al correo.

## Activar métodos de cifrado



Ha activado el servicio Email Encryption (véase [Activar Email Encryption](#) en la página 5).

En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede activar los métodos de cifrado con los que desee cifrar los correos entrantes y/o salientes de su dominio. A partir de los métodos de cifrado activados, puede usted posteriormente definir reglas (véase [Reglas de cifrado](#) en la página 20) para el cifrado de correos entrantes y salientes de su dominio. También puede hacer que se añada una indicación acerca del método de cifrado empleado a los asuntos de correos cifrados con TLS, S/MIME, PGP o Websafe. Puede elegir libremente los textos correspondientes. Las indicaciones se añaden automáticamente al asunto de todos los correos entrantes cifrados con los métodos de cifrado correspondientes.

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. En la sección **Métodos de cifrado y referencias a métodos de cifrado en el asunto**, marque la casilla del método de cifrado que desee activar.



### Nota:

El método de cifrado TLS siempre está activado. Este método de cifrado no se puede desactivar.

El método de cifrado Websafe está activado por defecto.



**TLS**  
☒ Sin referencia

**S/MIME**  
☐ Sin referencia

**PGP**  
☐ Sin referencia

**Websafe**  
☒ Sin referencia

☐ EmiG

✓ Guardar

Figura 4: Activar método de cifrado

- ➔ Se muestra una ventana de confirmación.

6. Haga clic en **Confirmar**.

**ACTIVAR S/MIME**

Está a punto de activar el método de cifrado S/MIME. Debe guardar la configuración para que este cambio entre en vigor. ¿Desea continuar?

✕ Cancelar    ✓ Confirmar

Figura 5: Confirmar la activación

- ➔ El método de cifrado se selecciona para la activación.

**IMPORTANTE:**

La activación solo se hará efectiva cuando se guarden las modificaciones en **Métodos de cifrado y referencias a métodos de cifrado en el asunto** (véase el paso 8 en la página 18).

7. Opcional: Si el método de cifrado debe indicarse en los asuntos de correos entrantes, introduzca el texto de la indicación en el campo de introducción del método de cifrado.

**Nota:**

Solo se pueden redactar indicaciones para métodos de cifrado activados.

Las indicaciones solo se añaden al asunto de los correos entrantes cifrados con el método de cifrado.



Figura 6: Introducir indicación

8. En **Métodos de cifrado y referencias a métodos de cifrado en el asunto**, haga clic en **Guardar**.



Los cambios se guardan.



Se ha activado un método de cifrado.

**IMPORTANTE:**

Para aplicar los métodos de cifrado activados a correos entrantes y/o salientes de su dominio, defina reglas para el cifrado (véase [Añadir reglas](#) en la página 22).

No es posible definir reglas para el método de cifrado EmiG. EmiG se aplica automáticamente tan pronto usted lo active y su interlocutor permita dicho método de cifrado.

**Nota:**

Si no hay ninguna regla aplicable a un correo concreto, dicho correo se trata del siguiente modo:

- Si es posible utilizar TLS, el correo se cifra con TLS.
- Si no es posible cifrarlo con TLS, el correo se envía con SMTP. Si ha activado S/MIME y se dispone de la clave pública del destinatario, el correo se cifra adicionalmente con S/MIME.

A continuación puede definir reglas para el cifrado de correos entrantes y salientes de su dominio (véase [Añadir reglas](#) en la página 22) con los métodos de cifrado activados. Si no



desear seguir aplicando un método de cifrado, puede desactivarlo (véase [Desactivar métodos de cifrado](#) en la página 19).

## Desactivar métodos de cifrado

 Ha activado un método de cifrado para Email Encryption (véase [Activar métodos de cifrado](#) en la página 16).

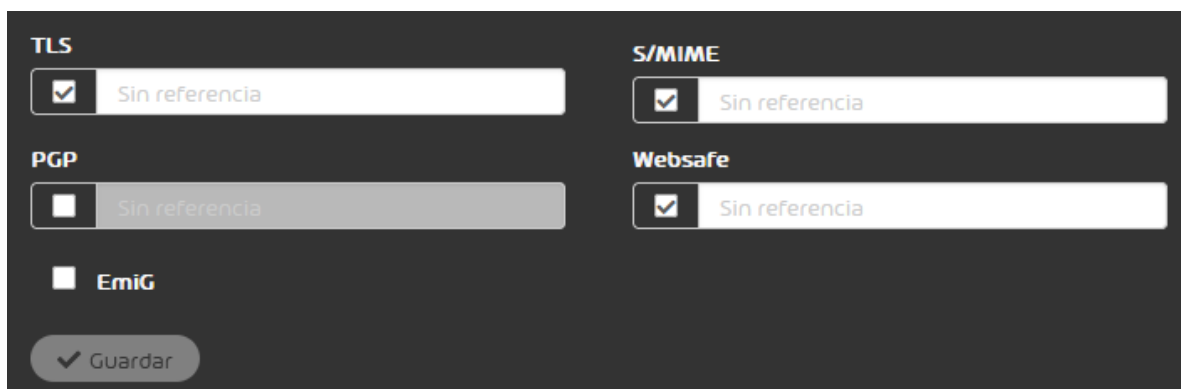
En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede desactivar los métodos de cifrado que ya no desee seguir empleando para el tráfico de correo de su dominio.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. En la sección **Métodos de cifrado y referencias a métodos de cifrado en el asunto**, desmarque la casilla del método de cifrado que desee desactivar.



### Nota:

El método de cifrado TLS siempre está activado. Este método de cifrado no se puede desactivar.



The screenshot shows a configuration interface for email encryption methods. It is divided into four sections: TLS, S/MIME, PGP, and Websafe. Each section has a checkbox and a text field labeled 'Sin referencia'. The TLS checkbox is checked. The S/MIME checkbox is checked. The PGP checkbox is unchecked. The Websafe checkbox is checked. At the bottom, there is a 'Guardar' button with a checkmark icon.

| Método  | Estado                              | Referencia     |
|---------|-------------------------------------|----------------|
| TLS     | <input checked="" type="checkbox"/> | Sin referencia |
| S/MIME  | <input checked="" type="checkbox"/> | Sin referencia |
| PGP     | <input type="checkbox"/>            | Sin referencia |
| WebSafe | <input checked="" type="checkbox"/> | Sin referencia |

☒ EmiG

Figura 7: Desactivar métodos de cifrado



Se muestra una ventana de confirmación.



6.

**IMPORTANTE:**

Tan pronto como desactive un método de cifrado, todas las reglas relativas al mismo se desactivarán también. Si vuelve a activar el método de cifrado más tarde, las reglas permanecen desactivadas. Puede volver a activar las reglas manualmente (véase [Activar reglas](#) en la página 29).

Haga clic en **Confirmar**.

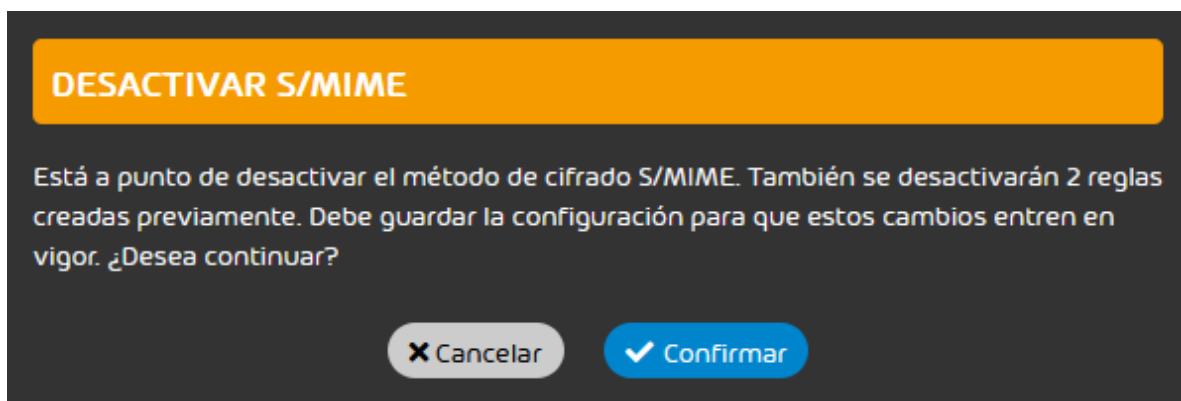


Figura 8: Confirmar la desactivación



El método de cifrado se selecciona para la desactivación.

**IMPORTANTE:**

La desactivación solo se hará efectiva cuando se guarden las modificaciones en **Métodos de cifrado y referencias a métodos de cifrado en el asunto** (véase el paso 7 en la página 20).

7. Haga clic en **Guardar**.



Los cambios se guardan. El método de cifrado se desactiva. Todas las reglas relativas al método de cifrado se desactivan también.



Se ha desactivado un método de cifrado.

## Reglas de cifrado

Los administradores a nivel de cliente pueden crear reglas de cifrado para configurar el cifrado de los correos entrantes y salientes de sus dominios.



Las reglas se procesan en un orden determinado (véase [Orden de las reglas](#) en la página 21).

Una vez añadidas (véase [Añadir reglas](#) en la página 22), las reglas pueden editarse, y sus prioridades pueden cambiarse (véase [Modificar la prioridad de una regla](#) en la página 27).

Si no es preciso aplicar una regla temporalmente, es posible desactivarla (véase [Desactivar reglas](#) en la página 30) y volver a activarla con posterioridad (véase [Activar reglas](#) en la página 29).

Es posible exportar las reglas existentes en formato CSV (véase [Exportar reglas en formato CSV](#) en la página 30).

Si una regla deja de ser necesaria, es posible eliminarla (véase [Eliminar reglas](#) en la página 33).

Los administradores a nivel de cliente pueden buscar un término de búsqueda en las reglas existentes (véase [Buscar reglas](#) en la página 34).

## Orden de las reglas

Las reglas del módulo **Email Security > Email Encryption** están ordenadas por prioridad y se procesan en dicho orden. Cada regla tiene asignado un número que representa su prioridad. Cuanto mayor sea el número, menor será la prioridad de la regla. Las reglas están ordenadas por prioridad en las listas de **Email Security > Email Encryption**.

| Prioridad | Activo                              | Acción               | Criterio                                              |   |
|-----------|-------------------------------------|----------------------|-------------------------------------------------------|---|
| 0         | <input checked="" type="checkbox"/> | Cifrar siempre       | Remitente: admin@gevonne.com                          | ► |
| 2         | <input checked="" type="checkbox"/> | Permitir sin cifrado | Remitente: marketing@gevonne.com; Destinatario: sa... | ► |
| 3         | <input checked="" type="checkbox"/> | Cifrar siempre       | Destinatario: finance@gevonne.com                     | ► |

Figura 9: Orden de las reglas

Para cada correo entrante y saliente de su dominio se comprueba si hay alguna regla activa aplicable al mismo. Las reglas se procesan en orden descendente de prioridad. Tan pronto como se encuentra una regla aplicable al correo, se aplica. El procesamiento de las demás reglas se detiene y no se le aplica ninguna regla más al correo.

**Nota:**

Si no hay ninguna regla aplicable a un correo concreto, dicho correo se trata del siguiente modo:

- Si es posible utilizar TLS, el correo se cifra con TLS.
- Si no es posible cifrarlo con TLS, el correo se envía con SMTP. Si S/MIME está activado y se dispone de la clave pública del destinatario, el correo se cifra adicionalmente con S/MIME.

## Añadir reglas



✓ Ha activado Email Encryption (véase [Activar Email Encryption](#) en la página 5) y métodos de cifrado para su dominio (véase [Activar métodos de cifrado](#) en la página 16).

A partir de los métodos de cifrado que haya activado para su dominio, puede definir reglas para el cifrado de correos entrantes o salientes en el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5).

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
- 5.

**Nota:**

Las reglas para correos entrantes se aplican a correos enviados a su servidor desde un servidor externo.

Seleccione la dirección del tráfico de correo.

- Para añadir una regla para correos entrantes, haga clic en **Añadir regla** en la sección **Reglas para correos entrantes**.
- Para añadir una regla para correos salientes, haga clic en **Añadir regla** en la sección **Reglas para correos salientes**.



Se abre un menú.

6. En el menú desplegable de **Acción**, seleccione la acción que aplicar a los correos afectados por la regla.



- Para cifrar siempre los correos afectados por la regla, seleccione **Cifrar siempre**.
- Para permitir que los correos afectados por la regla se envíen sin cifrar, seleccione **Permitir sin cifrado**.



Figura 10: Seleccionar una acción

- ➔ Si ha seleccionado la opción **Cifrar siempre**, los métodos de cifrado disponibles para la regla se mostrarán en el menú desplegable.

7.



**Nota:**

Solo puede seleccionar métodos de cifrado activados (véase [Activar métodos de cifrado](#) en la página 16).

Si ha seleccionado la opción **Cifrar siempre**, marque las casillas de los métodos de cifrado que desee emplear en la regla.

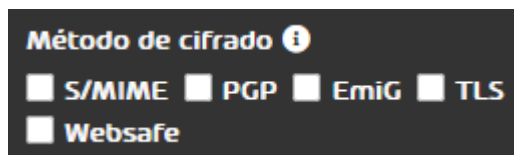


Figura 11: Seleccionar métodos de cifrado

8. Si ha seleccionado el método de cifrado TLS, seleccione los conjuntos de cifrado o certificados a emplear. Puede elegir entre las siguientes opciones:
- Todos los algoritmos
  - Algoritmos seguros
  - Certificados fiables
  - Certificados fiables + algoritmos seguros

**i Nota:**

Las opciones **Certificados fiables** y **Certificados fiables + algoritmos seguros** solo están disponibles para correos salientes.

Las opciones de TLS se detallan en el capítulo [TLS](#) en la página 10.

9.

**i Nota:**

Si define una regla para correos entrantes, no podrá elegir criterios. Dispone de los siguientes campos:

- **Remitente**
- **Destinatario**
- **IP**
- **Nombre de host**

Si define una regla para correos salientes, seleccione el criterio para determinar los correos a los que se aplicará dicha regla en el menú desplegable de **Criterio**.

- **Encabezado:** La regla se aplica a todos los correos que contengan determinado término de búsqueda en su encabezado.
- **Cuerpo:** La regla 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. Para los correos salientes, además, puede determinar términos de búsqueda adicionales para el asunto y los archivos adjuntos. La regla se aplica a todos los correos que presenten las características definidas.
- **Complemento:** Este criterio se refiere a Hornetsecurity Outlook Add-in (versión 4.0.3 o anterior). Puede determinar el remitente, el destinatario, la dirección IPv4 y el nombre de host de los correos. Para los correos salientes, además, puede determinar términos de búsqueda adicionales para el asunto y los archivos adjuntos. La regla se aplica a todos los correos que presenten las características definidas.

**Nota:**

Actualmente, Hornetsecurity Outlook Add-in no permite el cifrado con Websafe. Por tanto, no es posible seleccionar la opción **Complemento** en el menú desplegable y seleccionar **Websafe** como método de cifrado.

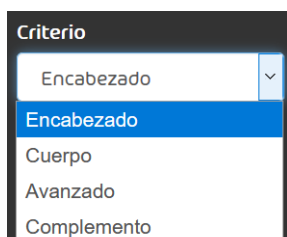


Figura 12: Seleccionar un criterio

- ➔ La configuración del criterio se muestra bajo el menú desplegable.
10. Si selecciona el criterio **Encabezado** o **Cuerpo**, indique en **Filtro: encabezado** o **Filtro: cuerpo** el término de búsqueda que deberá contener el encabezado o el cuerpo de los correos.

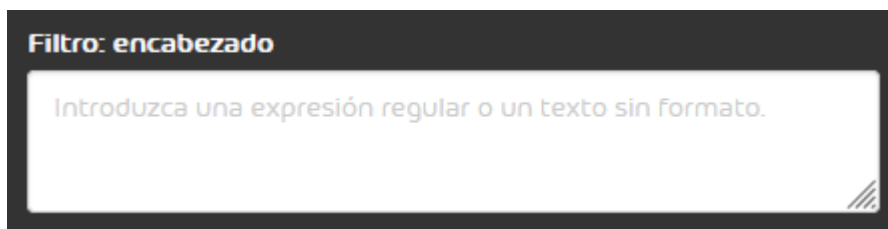


Figura 13: Introducir término de búsqueda

**Nota:**

El término de búsqueda se encontrará incluso si está rodeado de texto.

11. Si ha seleccionado el criterio **Avanzado** o **Complemento**, marque las casillas de las características deseadas e introduzca un término de búsqueda en los campos correspondientes.



|                                                                                                                  |                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| <b>Absender</b>                                                                                                  | <b>Empfänger</b>                                                                                                 |
| <input checked="" type="checkbox"/> <input type="text" value="gevonne.com"/>                                     | <input checked="" type="checkbox"/> <input type="text" value="talltara.com"/>                                    |
| <b>IP</b>                                                                                                        | <b>Hostname</b>                                                                                                  |
| <input type="checkbox"/> <input type="text" value="Geben Sie einen regulären Ausdruck oder einfachen Text ein"/> | <input type="checkbox"/> <input type="text" value="Geben Sie einen regulären Ausdruck oder einfachen Text ein"/> |
| <b>Betreff enthält</b>                                                                                           | <b>Anhang enthält</b>                                                                                            |
| <input type="checkbox"/> <input type="text" value="Geben Sie einen regulären Ausdruck oder einfachen Text ein"/> | <input type="checkbox"/> <input type="text" value="Geben Sie einen regulären Ausdruck oder einfachen Text ein"/> |

Figura 14: Determinar las características

**Nota:**

El término de búsqueda se encontrará incluso si está rodeado de texto.

**Nota:**

Como remitente o destinatario puede introducir, por ejemplo, dominios o direcciones de correo electrónico.

12. Opcional: Introduzca una descripción de la regla en **Descripción (opcional)**.

**Descripción (opcional)**

Figura 15: Describir la regla

13. Haga clic en **Añadir**.



La regla se añade a la lista de reglas definidas. La nueva regla obtiene la prioridad más baja de todas las reglas definidas y se coloca al final de la lista. La regla se activa.



Se ha añadido una regla de cifrado.

A continuación puede editar la regla (véase [Editar reglas](#) en la página 26) o cambiar su prioridad (véase [Modificar la prioridad de una regla](#) en la página 27).

## Editar reglas



Ha añadido reglas a Email Encryption.



En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede editar reglas de cifrado.

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. Haga clic en la lista de reglas para correos entrantes o salientes en la flecha de menú junto a la regla que desee editar.

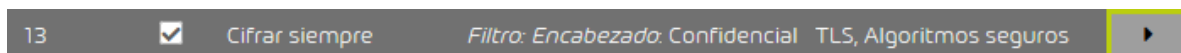


Figura 16: Seleccionar una regla

- ➔ Se abre un menú.
6. Haga clic en **Editar**.

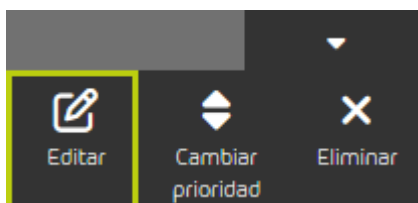


Figura 17: Editar reglas

- ➔ Se abre un menú con la configuración actual de la regla.
7. Ajuste la configuración del modo deseado. Para saber más, véase [Añadir reglas](#) en la página 22.
  8. Haga clic en **Aplicar cambios**.

- ➔ Los cambios se aplican.

✓ Se ha editado una regla de cifrado.

## Modificar la prioridad de una regla

✓ Ha añadido reglas a Email Encryption (véase [Añadir reglas](#) en la página 22).



En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede cambiar el orden en que se procesan las reglas de cifrado. Para cambiar el orden de las reglas es preciso cambiar su prioridad.

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. Haga clic en la lista de reglas para correos entrantes o salientes en la flecha de menú junto a la regla cuya prioridad desee modificar.

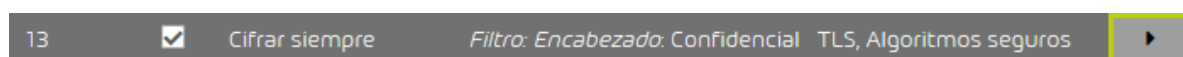


Figura 18: Seleccionar una regla

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

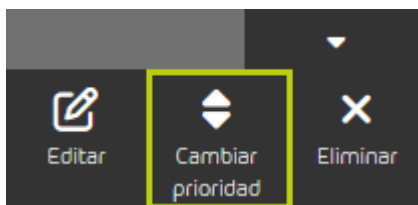


Figura 19: Seleccionar una regla

- ➔ Se abre un menú.
7. Introduzca la nueva prioridad de la regla en **Prioridad**.

**i Nota:**

Cuanto mayor sea el número, menor será la prioridad de la regla.

Figura 20: Indicar la prioridad



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



La nueva prioridad se asigna a la regla. La regla se mueve hasta la posición de la lista correspondiente a la nueva prioridad.



Se ha cambiado la prioridad de una regla. De este modo, se ha modificado el orden en que se procesan las reglas.

## Activar reglas



Ha desactivado una regla previamente añadida a Email Encryption (véase [Desactivar reglas](#) en la página 30). Ha activado todos los métodos de cifrado a los que se refiere la regla (véase [Activar métodos de cifrado](#) en la página 16).

Para que vuelvan a aplicarse reglas de cifrado desactivadas, puede volver a activarlas en el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5).

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
- 5.



### Nota:

Solo puede activar una regla cuando haya activado todos los métodos de cifrado empleados en la misma (véase [Activar métodos de cifrado](#) en la página 16).

Seleccione la regla para correos entrantes o salientes deseada de la lista y marque la casilla de la columna **Activo**.



Figura 21: Activar reglas



Se ha activado una regla de cifrado.



## Desactivar reglas



Ha añadido una regla a Email Encryption y ésta se encuentra activada (véase [Añadir reglas](#) en la página 22).

Si no desea aplicar temporalmente reglas de cifrado, puede desactivarlas en el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5).

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. Seleccione las reglas para correos entrantes o salientes deseadas en la lista y desmarque las casillas de la columna **Activo**.

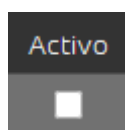


Figura 22: Desactivar reglas



Se ha desactivado una regla de cifrado.

## Exportar reglas en formato CSV



Ha añadido reglas de cifrado (véase [Añadir reglas](#) en la página 22).

En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede exportar las reglas de cifrado (véase [Reglas de cifrado](#) en la página 20) de un cliente en formato CSV. Puede exportar por separado las reglas de cifrado para correos entrantes y salientes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio cuyas reglas de cifrado desee exportar.
3. Vaya a **Email Security > Email Encryption**.
4. En **Reglas para correos entrantes**, haga clic en **Reglas para correos salientes** o **Exportar como CSV**.

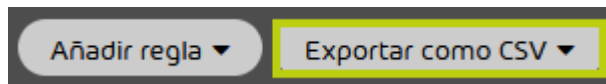


Figura 23: Exportar en formato CSV

- ➔ Se muestran los ajustes para la exportación en formato CSV.

**Nota:**

Los ajustes en **Exportación de datos** son diferentes para las reglas de cifrado para correos entrantes y salientes porque las opciones de configuración de las reglas de cifrado son diferentes (véase [Añadir reglas](#) en la página 22).

**EXPORTACIÓN DE DATOS**

|                                                                    |                                               |                                                  |                                                    |                                                       |                                                 |
|--------------------------------------------------------------------|-----------------------------------------------|--------------------------------------------------|----------------------------------------------------|-------------------------------------------------------|-------------------------------------------------|
| <input checked="" type="checkbox"/> Prioridad                      | <input checked="" type="checkbox"/> Activa    | <input checked="" type="checkbox"/> IP           | <input checked="" type="checkbox"/> Nombre de host | <input checked="" type="checkbox"/> Acción            | <input checked="" type="checkbox"/> Descripción |
| <input checked="" type="checkbox"/> Dirección                      | <input checked="" type="checkbox"/> Remitente | <input checked="" type="checkbox"/> Destinatario | <input checked="" type="checkbox"/> ID             | <input checked="" type="checkbox"/> Método de cifrado |                                                 |
| <input checked="" type="checkbox"/> Seleccionar/deseleccionar todo |                                               |                                                  |                                                    |                                                       |                                                 |

**TIPO DE EXPORTACIÓN**

☐ Descargar ☐ Por correo electrónico

Figura 24: Ajustes para la exportación en formato CSV de las reglas de cifrado para correos entrantes

**EXPORTACIÓN DE DATOS**

|                                                                    |                                               |                                                  |                                                    |                                                       |                                                                 |
|--------------------------------------------------------------------|-----------------------------------------------|--------------------------------------------------|----------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------|
| <input checked="" type="checkbox"/> Prioridad                      | <input checked="" type="checkbox"/> Activa    | <input checked="" type="checkbox"/> IP           | <input checked="" type="checkbox"/> Nombre de host | <input checked="" type="checkbox"/> Acción            | <input checked="" type="checkbox"/> Descripción                 |
| <input checked="" type="checkbox"/> Dirección                      | <input checked="" type="checkbox"/> Remitente | <input checked="" type="checkbox"/> Destinatario | <input checked="" type="checkbox"/> ID             | <input checked="" type="checkbox"/> Método de cifrado | <input checked="" type="checkbox"/> El archivo adjunto contiene |
| <input checked="" type="checkbox"/> El asunto contiene             |                                               |                                                  |                                                    |                                                       |                                                                 |
| <input checked="" type="checkbox"/> Seleccionar/deseleccionar todo |                                               |                                                  |                                                    |                                                       |                                                                 |

**TIPO DE EXPORTACIÓN**

☐ Descargar ☒ Por correo electrónico

Figura 25: Ajustes para la exportación en formato CSV de las reglas de cifrado para correos salientes

5. Marque las casillas de los datos que desee exportar en **Exportación de datos**.
- **Prioridad**
  - **Activa**
  - **IP**
  - **Nombre de host**
  - **Acción**



- **Descripción**
- **Dirección**
- **Remitente**
- **Destinatario**
- **ID**
- **Método de cifrado**
- **El archivo adjunto contiene:** Esta opción solo está disponible para la exportación CSV de las reglas de cifrado para correos salientes.
- **El asunto contiene:** Esta opción solo está disponible para la exportación CSV de las reglas de cifrado para correos salientes.
- **Seleccionar/deseleccionar todo:** Se marcan o desmarcan todas las casillas anteriormente descritas.

**Nota:**

Por defecto, todas las opciones están seleccionadas.

Las opciones corresponden a campos durante la creación de reglas de cifrado. Para más información, véase [Añadir reglas](#) en la página 22.

6. En **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o enviarlo por correo electrónico.
  - **Descargar:** El archivo CSV se facilita para su descarga.
  - **Por correo electrónico:** El archivo CSV se envía por correo electrónico.



Figura 26: Seleccionar el tipo de exportación

-  Si se elige la opción **Por correo electrónico**, se muestra un campo de introducción de datos.
7. Opcional: Si elige la opción **Por correo electrónico**, introduzca la dirección de correo electrónico a la que enviar el archivo CSV en el campo de introducción de datos.

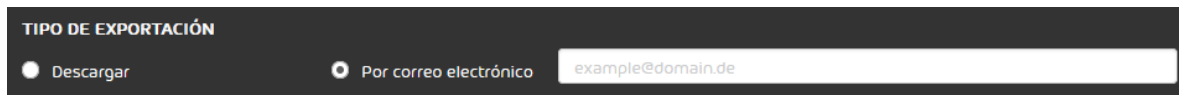


Figura 27: Introducir una dirección de correo electrónico

8. Haga clic en **Exportar**.



Las reglas de cifrado se exportan en formato CSV. El archivo CSV se presenta para su descarga o se envía por correo electrónico.



Todas las reglas de cifrado para los correos entrantes o salientes del cliente se han exportado en formato CSV.

## Eliminar reglas



Ha añadido reglas a Email Encryption (véase [Eliminar reglas](#) en la página 33).

En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede eliminar las reglas de cifrado 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 para el cual desee activar Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Normas de cifrado**.
5. Haga clic en la lista de reglas para correos entrantes o salientes en la flecha de menú junto a la regla que desee eliminar.

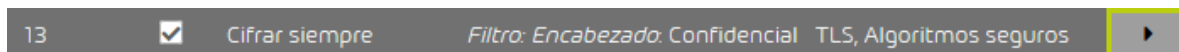


Figura 28: Seleccionar una regla



Se abre un menú.

6. Haga clic en **Eliminar**.

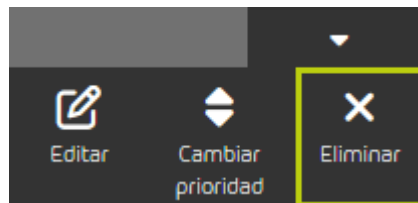


Figura 29: Eliminar reglas

- ➔ Aparece un mensaje de advertencia.
- 7. Para eliminar la regla, haga clic en **Confirmar**.

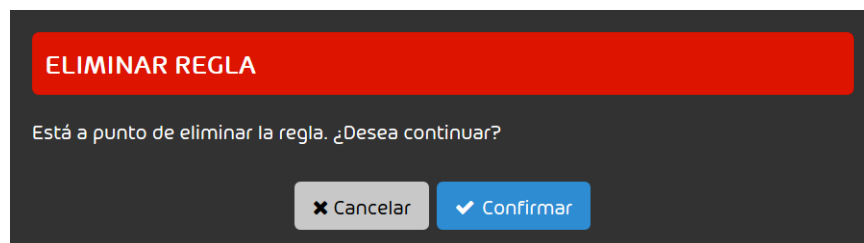


Figura 30: Confirmar la eliminación

- ➔ La regla se elimina de modo definitivo.
- ✓ Se ha eliminado una regla de cifrado.

## Buscar reglas

En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede buscar un término de búsqueda en las reglas de cifrado (véase [Reglas de cifrado](#) en la página 20). Puede buscar por separado en las reglas de cifrado para correos entrantes y salientes.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio en cuyas reglas de cifrado desee buscar.
3. Vaya a **Email Security > Email Encryption**.
4. Introduzca el término de búsqueda en la barra de búsqueda bajo **Reglas para correos entrantes** o **Reglas para correos salientes**.

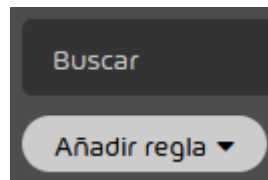


Figura 31: Introducir término de búsqueda

**i Nota:**

Es posible buscar un carácter individual o una cadena de caracteres. La búsqueda no distingue entre mayúsculas y minúsculas.

El término de búsqueda se busca en las columnas **Criterio**, **Descripción** y **ID**.

En las columnas **Criterio** y **Descripción** se encuentran todos los valores que contengan el término de búsqueda. Por el contrario, en la columna **ID** solo se obtiene un resultado si el término de búsqueda coincide con el ID entero.

5. Pulse la tecla Intro o el botón izquierdo del ratón.

➔ La búsqueda se efectúa. En la lista solo se muestran las reglas de cifrado cuyo ID, cuyo criterio o cuya descripción contengan el término de búsqueda.

6. Opcional: Si desea cancelar la búsqueda, vacíe la barra de búsqueda y pulse la tecla Intro o el botón izquierdo del ratón.

➔ Se vuelven a mostrar todas las reglas de cifrado existentes en la lista.

✓ Se ha buscado un término de búsqueda en las reglas de cifrado.

## Usuarios con S/MIME

En **Email Security > Email Encryption > Usuarios con S/MIME**, los administradores a nivel de cliente pueden administrar los certificados S/MIME de sus usuarios.

Para solicitar un certificado S/MIME para usuarios de un dominio, los usuarios deben añadirse como usuarios con S/MIME (véase [Añadir un usuario con S/MIME](#) en la página 36). Al solicitar el certificado, para cada usuario con S/MIME se adquiere una suscripción que es posible cancelar anualmente. Las suscripciones se facturan anualmente. Las suscripciones permiten renovar automáticamente los certificados S/MIME. Mientras un usuario de su dominio tenga



una suscripción activa, sus certificados S/MIME se renovarán automáticamente según vayan caducando. Los administradores a nivel de cliente pueden cancelar la suscripción hasta tres meses antes de que finalice el periodo de suscripción actual (véase [Cancelar una suscripción](#) en la página 41). En tal caso, la suscripción solo será válida hasta que finalice el periodo actual.

Una vez cancelada una suscripción, puede adquirir otra en cualquier momento (véase [Adquirir una suscripción](#) en la página 42). Los certificados S/MIME que haya sin caducar se mantendrán.

Los datos sobre los usuarios con S/MIME se reúnen en una tabla (véase [Datos de usuarios con S/MIME](#) en la página 44). Los administradores a nivel de cliente pueden exportar los datos de los usuarios con S/MIME en formato CSV (véase [Exportar usuarios con S/MIME en formato CSV](#) en la página 47).

**Nota:**

Los usuarios con certificados S/MIME pueden emplear palabras clave en los asuntos de sus correos para ejecutar diversas acciones relacionadas con el cifrado (véase [Palabras clave para usuarios con S/MIME](#) en la página 50).

## Añadir un usuario con S/MIME



Ha activado Email Encryption (véase [Activar Email Encryption](#) en la página 5).

Para adquirir un certificado S/MIME para un usuario de su dominio debe añadirlo como usuario con S/MIME en el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5).

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Usuarios con S/MIME**.
5. Haga clic en **Añadir usuario con S/MIME**.

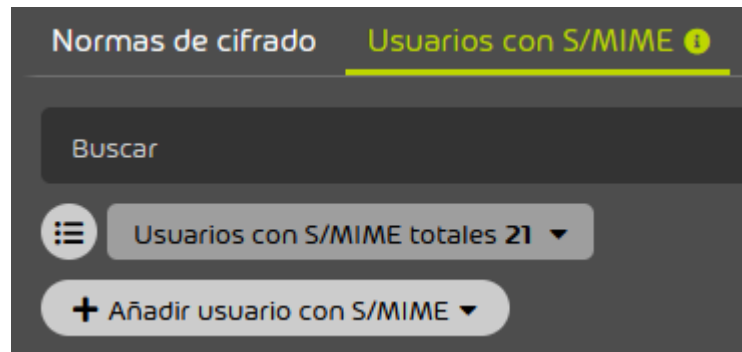


Figura 32: Añadir un usuario con S/MIME

- ➔ Se abre una vista avanzada.
6. En **Dirección de correo**, introduzca la dirección de correo del usuario que desee añadir como usuario con S/MIME. Para iniciar la búsqueda automática, introduzca al menos tres caracteres seguidos.



Figura 33: Introducir una dirección de correo electrónico

7. Haga clic en **Añadir**.
- ➔ La dirección de correo electrónico se añade a la tabla de abajo.

8. **! IMPORTANTE:**  
El certificado solo es válido como firma electrónica con el nombre correcto.

Introduzca el nombre del usuario en **Nombre**, y sus apellidos en **Apellidos**.



| Dirección de correo | Nombre | Apellidos |
|---------------------|--------|-----------|
| admin@gevonne.com   |        |           |

Figura 34: Introducir nombre y apellidos del usuario

9. Opcional: Repita las instrucciones a partir del [paso 6](#) para introducir más usuarios que desee añadir como usuarios con S/MIME.

10.



**IMPORTANTE:**

La solicitud de certificados S/MIME conlleva costes adicionales conforme a la lista de precios.

Haga clic en **Pedir certificado S/MIME**.



Aparece un aviso sobre costes adicionales.

11. Para solicitar certificados S/MIME para los usuarios añadidos, haga clic en **Confirmar**.

**PEDIR CERTIFICADO**

Está a punto de pedir un certificado S/MIME a modo de suscripción. Esta suscripción conlleva costes conforme a la lista de precios. ¿Desea continuar?

Figura 35: Confirmar



Los usuarios se añaden a la lista de usuarios con S/MIME (véase [Datos de usuarios con S/MIME](#) en la página 44). Para dichos usuarios se adquieren certificados S/MIME a modo de suscripción. Tan pronto como la suscripción se activa, su estado cambia de **Pedido** a **Activo en Suscripción**, y la fecha de caducidad del certificado S/MIME actual se muestra



en **Fecha de caducidad de certificado**. La firma S/MIME se activa para todos los usuarios con S/MIME añadidos.

**IMPORTANTE:**

Las suscripciones de usuarios con S/MIME activas se renuevan anualmente. Para evitar la renovación de la suscripción, es necesario cancelarla 3 meses antes de que finalice el periodo de suscripción actual (véase [Cancelar una suscripción](#) en la página 41).

Independientemente de los datos básicos actuales de un usuario (véase [Editar los datos básicos de un buzón de correo](#)), una suscripción siempre se renueva para la dirección de correo electrónico, el nombre y los apellidos registrados en el módulo **Configuración de seguridad > Email Encryption**. Estos datos no pueden editarse para una suscripción existente. Sin embargo, si los datos para un usuario han cambiado en Control Panel, un administrador a nivel de cliente puede volver a añadir el usuario como usuario con S/MIME y adquirir un nuevo certificado S/MIME con coste adicional.

**IMPORTANTE:**

Un certificado S/MIME está vinculado a la dirección de correo principal de un usuario. Si la dirección de correo electrónico del usuario cambia, el certificado S/MIME ya no es válido para el usuario. Sin embargo, en este caso, el certificado S/MIME existente se continúa mostrando en el módulo **Configuración de seguridad** > **Email Encryption** y sigue asignado a la dirección de correo electrónico anterior. El estado de la suscripción también se mantiene. Para impedir la renovación automática de la suscripción, un administrador a nivel de cliente debe cancelar la suscripción (véase [Cancelar una suscripción](#) en la página 41). Para que el usuario con la dirección de correo electrónico renombrada vuelva a recibir un certificado S/MIME válido, un administrador a nivel de cliente debe volver a añadir el usuario como usuario con S/MIME y adquirir un nuevo certificado con coste adicional.

Si la dirección de correo electrónico de un usuario con S/MIME de un cliente de 365 Total Protection se renombra en Microsoft 365, también se renombrará en Control Panel durante la siguiente sincronización. Si al menos un usuario con S/MIME de un cliente se ha renombrado en Control Panel durante la sincronización, los administradores del cliente serán informados por correo electrónico de qué usuarios con S/MIME se han renombrado últimamente y ya no disponen de un certificado S/MIME válido. Los administradores son informados una vez al día sobre cambios de nombre.

12. Opcional: Si desea desactivar la firma S/MIME para el usuario, desmarque la casilla de la fila correspondiente en **Firma S/MIME**.
13. Opcional: Para que los correos del usuario se cifren con S/MIME siempre que sea posible, marque la casilla bajo **Cifrar (si es posible)**.



Se han añadido usuarios con S/MIME y se han solicitado certificados S/MIME para ellos.

A continuación puede rescindir suscripciones sobre certificados S/MIME (véase [Cancelar una suscripción](#) en la página 41) y exportar los usuarios con S/MIME de su dominio en formato CSV (véase [Exportar usuarios con S/MIME en formato CSV](#) en la página 47).



## Cancelar una suscripción

 Ha adquirido una suscripción para un usuario con S/MIME (véanse [Añadir un usuario con S/MIME](#) en la página 36 y [Adquirir una suscripción](#) en la página 42).

Las suscripciones sobre certificados S/MIME activas se renuevan automáticamente cada año por un año adicional. Para impedir la renovación automática de una suscripción, puede cancelarla en el módulo **Email Security > Email Encryption** al menos 3 meses antes de que finalice el periodo de suscripción actual (véase [Email Encryption](#) en la página 5).



### IMPORTANTE:

La suscripción de un usuario con S/MIME no se cancelará automáticamente cuando su buzón de correo se elimine de Control Panel (véase [Quitar un buzón de correo](#)). Por tanto, un administrador debe cancelar la suscripción antes de que el buzón de correo se elimine de Control Panel.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee activar Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Usuarios con S/MIME**.
5. En la tabla de usuarios con S/MIME, haga clic en la flecha de menú junto al usuario cuya suscripción desee cancelar.



Figura 36: Abrir el menú



Se abre un menú.

6. Haga clic en **Cancelar suscripción**.

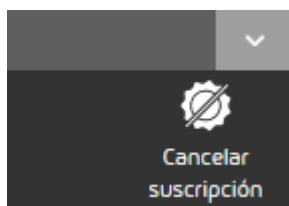


Figura 37: Cancelar una suscripción



➔ Aparece un mensaje de advertencia.

7. Haga clic en **Confirmar**.

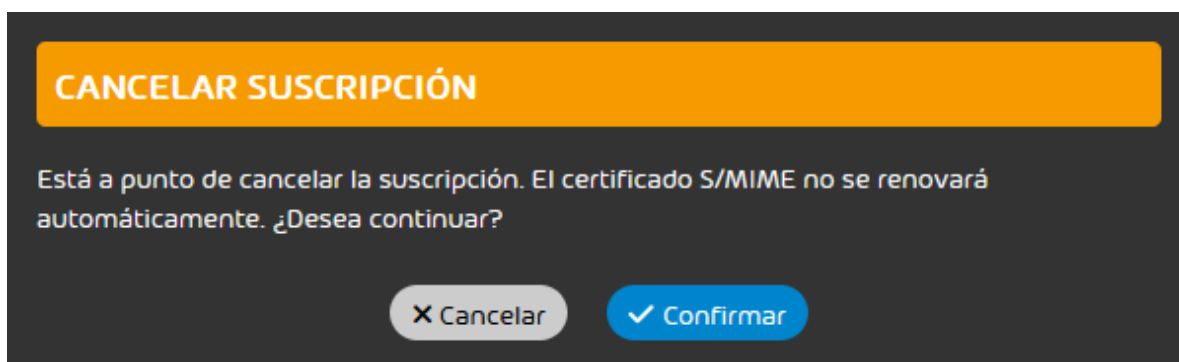


Figura 38: Confirmar

➔ La suscripción del usuario está desactivada. La fecha de caducidad de la suscripción se muestra en **Suscripción**. La suscripción no se renovará más allá de esa fecha.

✓ Se ha cancelado la suscripción de un usuario. La suscripción es válida hasta su fecha de caducidad y no se renueva automáticamente.

A continuación puede volver a adquirir una suscripción rescindida (véase [Adquirir una suscripción](#) en la página 42).

## Adquirir una suscripción

✓ Ha cancelado la suscripción de un usuario con S/MIME (véase [Cancelar una suscripción](#) en la página 41).

Para que una suscripción rescindida sobre un certificado S/MIME de un usuario se renueve automáticamente cada año, puede adquirir una nueva suscripción para el usuario en el módulo **Email Security > Email Encryption**.

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Usuarios con S/MIME**.



5. En la tabla de usuarios con S/MIME, haga clic en la flecha de menú junto al usuario para el cual desee adquirir una suscripción.



Figura 39: Abrir el menú

- ➔ Se abre un menú.
6. Haga clic en **Renovar suscripción**.

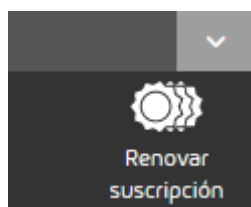


Figura 40: Renovar suscripción

- ➔ Aparece un mensaje de advertencia.
7. Haga clic en **Confirmar**.

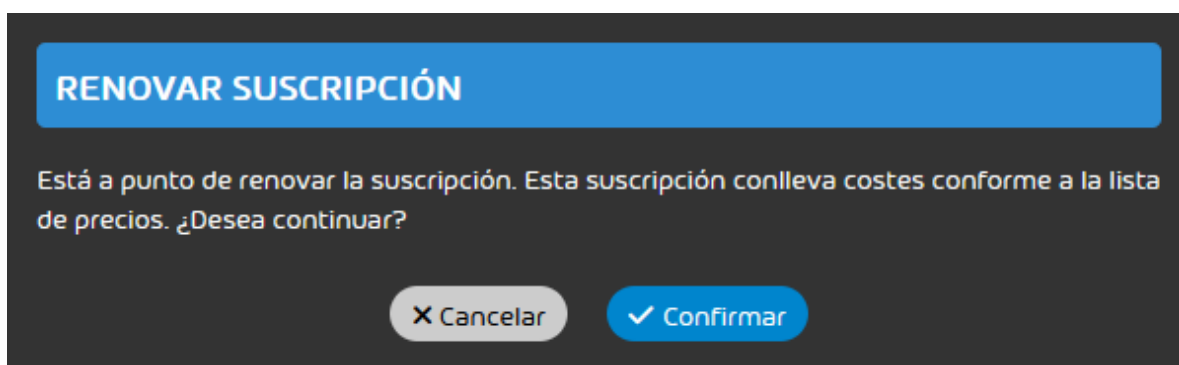


Figura 41: Confirmar

- ➔ Se adquiere y activa una suscripción para el usuario. En **Suscripción** se muestra el estado **Activo**.
- ✓ Se ha adquirido una suscripción para un usuario. Cada año, la suscripción se renueva automáticamente por otro año antes de su fecha de caducidad.

A continuación puede rescindir una suscripción cuando ya no sea necesaria (véase [Cancelar una suscripción](#) en la página 41).



## Datos de usuarios con S/MIME

En **Email Security > Email Encryption > Usuarios con S/MIME** se muestran los datos de los usuarios con S/MIME del dominio seleccionado.

La cantidad de usuarios con S/MIME se muestra en el menú desplegable **Usuarios con S/MIME totales**. En el menú desplegable pueden seleccionarse las siguientes opciones:

- **Usuarios con S/MIME totales:** Se muestra la cantidad de usuarios con un certificado S/MIME válido o para los que se ha solicitado un certificado S/MIME.
- **Usuarios con S/MIME activos:** Se muestra la cantidad de usuarios que poseen un certificado S/MIME válido.

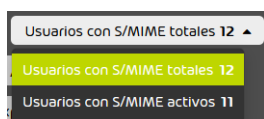


Figura 42: Cantidad de usuarios con S/MIME

El resto de datos sobre los usuarios con S/MIME se muestran en una tabla. Dicha tabla muestra los usuarios seleccionados en el menú desplegable.

La tabla contiene los siguientes datos.



### Nota:

Por defecto, no se muestran todos los datos. Con  es posible seleccionar los datos a mostrar en la tabla.



### Nota:

Los registros de la tabla pueden ordenarse por los valores de las columnas **Dirección de correo**, **Nombre** y **Apellidos** haciendo clic en el encabezado de la columna correspondiente.



Tabla 3: Datos de usuarios con S/MIME

| INFORMACIÓN         | EXPLICACIÓN                                                |
|---------------------|------------------------------------------------------------|
| Dirección de correo | Se muestra la dirección de correo electrónico del usuario. |
| Nombre              | Se muestra el nombre del usuario.                          |
| Apellidos           | Se muestran los apellidos del usuario.                     |



## INFORMACIÓN

## Suscripción

## EXPLICACIÓN

Se muestra el estado de la suscripción.

**Nota:**

Los certificados de S/MIME se adquieren a modo de suscripción. Mientras la suscripción se mantenga activa, se renovará por otro año tres meses antes de finalizar.

Están disponibles los siguientes estados:

- **Pedido:** La suscripción se ha solicitado, pero aún no está activa. El usuario aún no tiene ningún certificado S/MIME.
- **Activo:** La suscripción está activa. El usuario tiene un certificado S/MIME. La suscripción se renueva anualmente.
- **Caduca el:** Se ha cancelado la suscripción. Se muestra la fecha de caducidad de la suscripción.

**Nota:**

La suscripción se renueva durante otro año si se cancela menos de tres meses antes de su finalización. De lo contrario, finalizará al final de su periodo de validez actual.

## Cifrar (si es posible)

Indica si los correos del usuario se cifran con S/MIME siempre que sea posible.

## Firma S/MIME

Indica si la firma S/MIME se encuentra activada para el usuario.



## INFORMACIÓN

## Fecha de caducidad de certificado

## EXPLICACIÓN

Indica la fecha de caducidad del certificado S/MIME actual.

**Nota:**

La fecha de caducidad se refiere únicamente al certificado S/MIME actual y no a la suscripción. Esta fecha es irrelevante para la cancelación de la suscripción.

## Exportar usuarios con S/MIME en formato CSV



Ha añadido usuarios con S/MIME (véase [Añadir un usuario con S/MIME](#) en la página 36).

En el módulo **Email Security > Email Encryption** (véase [Email Encryption](#) en la página 5) puede exportar los datos de todos los usuarios con S/MIME o una selección de los mismos en formato CSV.

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 Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Seleccione la pestaña **Usuarios con S/MIME**.
5. Haga clic en **Exportar como CSV**.



Se abre una vista avanzada.

6. En la sección **Exportación de datos**, marque las casillas correspondientes a los datos que desee exportar.
  - **Dirección de correo:** La dirección de correo del usuario se exporta.
  - **Nombre:** El nombre del usuario se exporta.
  - **Apellidos:** Los apellidos del usuario se exportan.
  - **Suscripción:** El estado de la suscripción se exporta. Se distingue entre los estados **Pedido** y **Activo**.



- **Firma S/MIME:** El estado de la firma S/MIME se exporta. Se indica si la firma S/MIME se encuentra activa.
- **Fecha de caducidad de certificado:** Se exporta la fecha de vencimiento del certificado S/MIME.
- **Pedir de nuevo:** Se exporta información relativa a si el certificado S/MIME habrá de renovarse automáticamente antes de su fecha de vencimiento o no.
- **Cifrar (si es posible):** Se exporta información relativa a si el cifrado con S/MIME habrá de emplearse para un usuario siempre que sea posible.
- **Fecha de vencimiento de suscripción:** Se exporta la fecha más próxima para la que puede hacerse efectiva la cancelación de una suscripción activa, o bien la fecha en la que vence una suscripción cancelada.

Figura 43: Seleccionar datos para la exportación



**Nota:**

Para marcar todas las casillas, marque la casilla **Seleccionar/deseleccionar todo**.

Para desmarcar todas las casillas, desmarque la casilla **Seleccionar/deseleccionar todo**.

7. Opcional: Si solo desea exportar datos de usuarios con S/MIME seleccionados, proceda del siguiente modo:
  - a) En el módulo, haga clic en

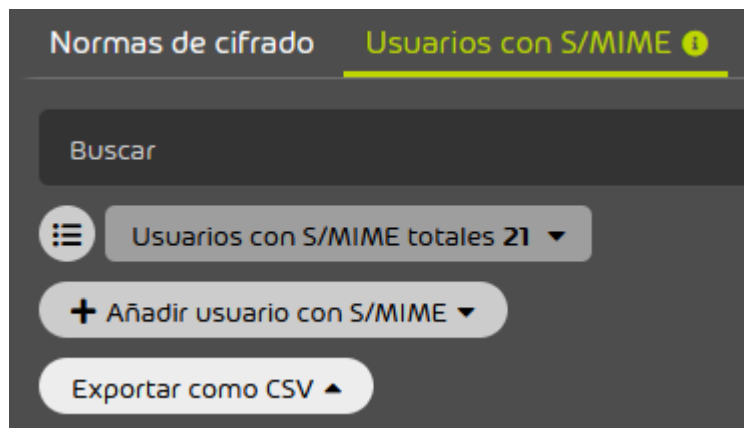


Figura 44: Activar la selección

- ➔ En la tabla de usuarios con S/MIME se muestra una columna con casillas.
- b) Marque las casillas de las filas cuyos datos desee exportar.

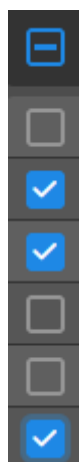


Figura 45: Seleccionar filas

- ➔ La casilla **Exportar solo líneas seleccionadas** se habilita en la vista avanzada.
- c) Marque la casilla **Exportar solo líneas seleccionadas**.

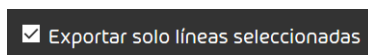


Figura 46: Exportar las filas seleccionadas



8. En la sección **Tipo de exportación**, seleccione entre obtener el archivo CSV mediante descarga o correo electrónico.

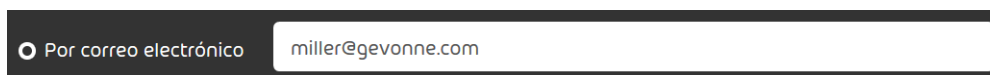


TIPO DE EXPORTACIÓN

☒ Descargar ☐ Por correo electrónico

Figura 47: Seleccionar el tipo de exportación

- ➔ Si elige la opción **Por correo electrónico**, se mostrará un campo de introducción de datos.
9. Si elige la opción **Por correo electrónico**, introduzca la dirección de correo electrónico a la que enviar el archivo CSV en el campo de introducción de datos.



☒ Por correo electrónico

Figura 48: Introducir una dirección de correo electrónico

10. Haga clic en **Exportar**.

- ➔ El archivo CSV se facilita para su descarga o se envía a la dirección de correo electrónico indicada.

✓ Se han exportado datos de usuarios con S/MIME en formato CSV.

## Palabras clave para usuarios con S/MIME

Si el servicio Email Encryption (véase [Email Encryption](#) en la página 5) está activado para un dominio, los usuarios con S/MIME de dicho dominio (véase [Usuarios con S/MIME](#) en la página 35) pueden emplear palabras clave en los asuntos de sus correos salientes. Dichas palabras clave provocan la ejecución de determinadas acciones. Los usuarios con S/MIME pueden emplear las siguientes palabras clave:

- **CRYPT**: El correo se envía cifrado con S/MIME.
- **NOCRYPT**: El correo se envía sin cifrado S/MIME.
- **SIGN**: El correo se envía con una firma S/MIME.
- **NOSIGN**: El correo se envía sin firma S/MIME.

**IMPORTANTE:**

Las palabras clave solo provocan la ejecución de acciones cuando se escriben en mayúsculas. La palabra clave **CRYPT** debe, además, figurar exclusivamente al comienzo del asunto. El resto de palabras clave, por el contrario, pueden incluirse en cualquier parte del asunto.

La palabra clave **CRYPT** puede emplearse incluso si el remitente no dispone de certificado S/MIME. Para cifrar un correo, basta con disponer de la clave pública (public key) del destinatario. Sin embargo, si se desea firmar un correo mediante la palabra clave **SIGN**, el remitente deberá disponer de un certificado S/MIME válido.

## Desactivar Email Encryption



Ha activado Email Encryption (véase [Activar Email Encryption](#) en la página 5).

Si no desea continuar cifrando correos con Email Encryption, puede desactivar Email Encryption deactivieren. Los ajustes del módulo **Email Security > Email Encryption** se guardarán por si desea volver a activar Email Encryption con posterioridad.

1. Inicie sesión en Control Panel con sus datos de acceso de administrador.
2. En la selección de ámbitos, seleccione el dominio para el cual desee desactivar Email Encryption.
3. Vaya a **Email Security > Email Encryption**.
4. Accione el interruptor **Activar Email Encryption**.

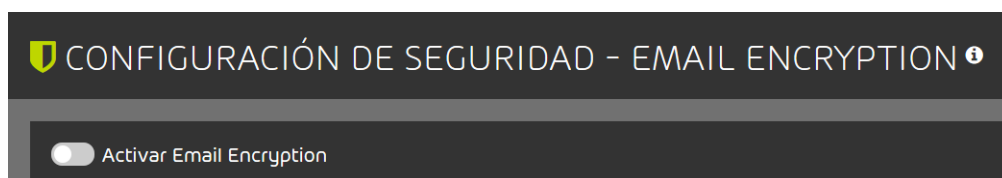


Figura 49: Desactivar Email Encryption

5. Aparece una ventana de confirmación.
5. Haga clic en **Confirmar**.
- ➔ Los ajustes del módulo **Email Encryption** se bloquean. Ya no es posible modificar datos.



Email Encryption se ha deshabilitado.



**Nota:**

La desactivación de Email Encryption no supone la rescisión del contrato sobre dicho servicio. Esto aplica también, particularmente, a los contratos relativos a certificados S/MIME. Para rescindir un contrato deberá ponerse en contacto con su interlocutor.

# Índice

## A

### activar

- Email Encryption [5](#)
- método de cifrado, *Ver* método de cifrado activar
- regla de cifrado [29](#)

### advertencias

- explicación [3](#)

### algoritmos de cifrado

- TLS, *Ver* TLS conjuntos de cifrado

### añadir

- usuario con S/MIME [36](#)

### asunto

- indicación de métodos de cifrado, *Ver* método de cifrado indicación en el asunto

## B

### buscar

- reglas de cifrado, *Ver* reglas de cifrado buscar

## C

### certificado S/MIME

- solicitar [36](#)

### certificados

- TLS, *Ver* TLS certificados

### cifrado

- excepción, *Ver* crear regla de cifrado

### cifrado, capacidades

- comprobar [7](#)

### cifrado, directivas de [6](#)

### cifrado, métodos

- combinación [14](#)
- compatibilidad, *Ver* cifrado, métodos combinación
- del interlocutor, comprobar, *Ver* cifrado, capacidades comprobar
- desactivar [19](#)
- explicación [9](#)
- orden [15](#)
- procesamiento, *Ver* orden de los métodos de cifrado

### combinación

- cifrado, métodos [14](#)

### compatibilidad

- cifrado, métodos, *Ver* combinación cifrado, métodos

### comprobar

- cifrado, capacidades [7](#)
- métodos de cifrado del interlocutor, *Ver* comprobar cifrado, capacidades

### conjuntos de cifrado

- TLS, *Ver* TLS conjuntos de cifrado

### crear

- regla de cifrado [22](#)

### CSV, exportación

- reglas de cifrado, *Ver* reglas de cifrado exportar

## D

### desactivar

- cifrado, métodos, *Ver* cifrado, métodos desactivar
- Email Encryption [51](#)
- regla de cifrado [30](#)

### documentación

- indicaciones [3](#)
- símbolos [3](#)

## E

### editar

- regla de cifrado [26](#)

### eliminar

- regla de cifrado [33](#)

### Email Encryption

- activar [5](#)
- desactivar [51](#)

### EmiG [9](#)

### emplear

- palabra clave en el asunto [50](#)

### excepción

- cifrado, *Ver* regla de cifrado crear

### explicación

- advertencias [3](#)
- indicaciones de seguridad [3](#)

### exportar

- reglas de cifrado, *Ver* reglas de cifrado exportar

## I

### indicaciones

- documentación [3](#)

### indicaciones de seguridad

- explicación [3](#)

## M

### método de cifrado

- activar [16](#)
- indicación en el asunto [16](#)

## O

### orden

- de los métodos de cifrado [15](#)

## P

### palabra clave

- emplear en el asunto [50](#)

### PGP [9](#)

### prioridad

- regla de cifrado [27](#)

procesamiento  
cifrado, métodos, *Ver* cifrado, métodos orden

## R

regla de cifrado  
  activar [29](#)  
  crear [22](#)  
  desactivar [30](#)  
  editar [26](#)  
  eliminar [33](#)  
  prioridad [27](#)  
reglas de cifrado  
  buscar [34](#)  
  exportar [30](#)

## S

S/MIME [9](#)  
símbolos  
  documentación [3](#)  
solicitar  
  certificado S/MIME [36](#)

## T

TLS [9](#)  
  certificados [10](#)  
  conjuntos de cifrado [10](#)

## U

usuario con S/MIME  
  añadir [36](#)

## W

Websafe [9](#)  
  explicación [13](#)



**HORNETSECURITY**

Hornetsecurity GmbH  
Am Listholze 78 | 30177 Hannover | Germany  
Phone: +49 511 515 464-0 | [info@hornetsecurity.com](mailto:info@hornetsecurity.com)  
[www.hornetsecurity.com](http://www.hornetsecurity.com)