

**Correo  
electrónico  
seguro**

**Preguntas frecuentes**

## Preguntas frecuentes

### Contenido

[Respuestas a preguntas generales sobre el correo electrónico seguro](#)

[Respuestas a preguntas sobre Forced TLS](#)

[Respuestas a preguntas sobre SecureMail](#)

[Glosario](#)

[Soporte](#)

### Respuestas a preguntas generales

#### **1. ¿Cuál es la política de seguridad de HSBC respecto al correo electrónico?**

La seguridad tiene una prioridad alta para HSBC, en especial cuando estamos tratando con la información de nuestros clientes y socios comerciales.

Es política de seguridad de HSBC cifrar todos los correos electrónicos que contienen información que pudiera representar un riesgo para nuestros clientes, socios comerciales o para HSBC.

#### **2. Ya recibo correos de HSBC que están cifrados con PGP. ¿Seguiré recibiendo correos seguros de esta manera?**

Si ya hay un acuerdo para usar Pretty Good Protection (PGP) entre HSBC y usted, entonces podemos seguir utilizando PGP para cifrar sus correos. En el futuro, pudiéramos cambiar y usar únicamente Forced TLS y SecureMail, pero de ser así se le avisaría con anticipación. Si desea que sus mensajes sean cifrados con Forced TLS o SecureMail, entonces póngase en contacto con su ejecutivo de cuenta o representante HSBC.

#### **3. Recibo correos seguros mediante otra solución. ¿Seguiré recibiendo correos de esta manera?**

Sí, pero a su debido tiempo, puede que cambiemos a usar únicamente Forced TLS y SecureMail cuando necesitemos enviar información privada o delicada a su correo electrónico personal o laboral.

El intercambio de mensajes mediante correo electrónico es un método para comunicarse con seguridad con usted. Seguirá recibiendo mensajes a través de su banca en línea normal u otros canales de comunicación segura existentes.

#### **4. ¿Qué pasa si mi empresa usa un tercero para procesar mi correo electrónico?**

Si el correo de HSBC pasa para su procesamiento por un tercero que gestione todos o algunos de los aspectos de su servicio de correo p. ej. filtrado de correo no deseado o detección de malware, entonces si el correo ha sido cifrado con Forced TLS únicamente podemos garantizar que llegue al tercero en cuestión (ya que es ahí que termina nuestra conexión). Usted o un representante de su empresa deberá hablar con el tercero que procesa su correo si desea mantener una información segura entre ellos y ustedes.

No es necesario involucrar al tercero que funja como empresa de servicio de correo si el mensaje ha sido enviado cifrado con SecureMail, ya que usted solo necesita su cuenta de correo, una conexión a internet y acceso a un navegador para ver su mensaje de manera segura.

#### **5. Mi empresa tiene su propia solución de cifrado de correo, la cual se debe usar de conformidad con la política de seguridad interna. ¿Qué hago?**

Si es HSBC quien inicia el mensaje, entonces usaremos Forced TLS si contamos con él para la comunicación con usted. TLS se está convirtiendo rápidamente en una norma en la industria y es soportado ahora por la mayoría de aplicaciones de servidor de correo. Cuando

no tengamos disponible Forced TLS para la comunicación con usted, usaremos SecureMail u otra solución aprobada.

Si busca utilizar su propia solución de cifrado de correo para iniciar o responder mensajes, entonces le pedimos nos lo informe con anticipación. Hable con su ejecutivo de cuenta o representante HSBC quien lo consultará con los equipos correspondientes en HSBC. Será necesario que HSBC evalúe la solución. Su ejecutivo de cuenta o representante HSBC confirmará el resultado y los pasos a seguir.

#### **6. ¿Qué pasa si no deseo recibir correos cifrados seguros?**

HSBC se toma en serio la protección de la información y va contra nuestra política de seguridad enviar información sin las medidas de seguridad establecidas, no hacerlo pudiera representar un riesgo para usted o para HSBC en caso de ser interceptada por un destinatario no autorizado.

Únicamente le enviaremos correo seguro si estamos respondiendo a una solicitud o si debemos enviar información privada o delicada que usted prefiera recibir por correo electrónico. Hable con su ejecutivo de cuenta o representante HSBC para analizar otros canales seguros de transferencia de información a la medida de sus necesidades si no desea recibir correos cifrados seguros.

## **Respuestas a preguntas sobre Forced TLS**

#### **7. ¿Qué es Forced TLS?**

Transport Layer Security (TLS) es una característica de servidor de correo que, una vez habilitada, cifra la transmisión de correo electrónico de una organización a otra a través de internet. Forced TLS es una configuración que se asegura que el correo se envíe únicamente si se puede transmitir de forma segura.

#### **8. ¿Quién puede usar Forced TLS?**

TLS está instalado/configurado en los servidores de correo y, por ende, regularmente lo usan las organizaciones comerciales/de negocios. TLS se está convirtiendo rápidamente en una norma en la industria y es soportado ahora por la mayoría de los servidores de correo. HSBC se ha unido al creciente número de organizaciones que lo han implementado.

Puesto que TLS es una función del servidor de correo, es necesario que usted o su empresa puedan configurar TLS en su servidor de correo. Si no puede hacerlo, entonces no podremos utilizar TLS con usted. Por ejemplo, si usa un servicio de correo en red, no podrá gestionar dichos servidores de correo.

Si recurre a un tercero para gestionar sus correos, entonces pudiera hablar con él acerca de establecer un vínculo TLS entre usted y HSBC.

#### **9. ¿El uso de TLS tiene algún costo para mí?**

Para enviar o recibir correos electrónicos con seguridad a través de TLS, se debe configurar su servidor de correo para aceptar tráfico de correo TLS. Pudiera tener un costo para usted si su infraestructura de correo actual no soporta TLS y se necesita comprar software nuevo o si necesita pagar personal informático para configurar su software existente. Una vez que se hayan hecho los ajustes necesarios, el único costo continuo será la renovación anual de los certificados de seguridad. No se le cobrará por el correo seguro que envíe o reciba.

#### **10. ¿Tendré que descargar o comprar algún software para recibir correo seguro mediante TLS?**

El método preferido de HSBC para enviar correo seguro es Forced TLS, mismo que funcionará si está habilitado Transport Layer Security (TLS) tanto en el servidor de correo del remitente como en el del destinatario. Es necesario contar con el software de servidor correcto para habilitar TLS y puede que usted o su empresa tuvieran que comprar nuevo

software si su infraestructura de correo actual no soporta TLS. Si su empresa está recurriendo a un tercero para la gestión de su correo, entonces puede que sea necesario que negocie con dicho tercero el establecimiento de conexiones TLS.

Si HSBC no puede hacer los arreglos para una conexión Forced TLS con usted, no podremos enviarle el correo seguro mediante TLS. En este caso, HSBC escogerá una solución alternativa aprobada para enviar la información de manera segura.

#### **11. ¿Cómo configuro una conexión Forced TLS con ustedes?**

Una vez que haya confirmado tener habilitado TLS en sus servidores de correo, infórmelo a su ejecutivo de cuenta o representante HSBC, quien seguirá el proceso interno y hará los arreglos necesarios. Este proceso puede tomar varios días para permitir que nuestro equipo de IT complete los procedimientos y las pruebas de implementación junto con usted o un representante de IT de su empresa.

#### **12. ¿Cómo veré el mensaje seguro si está cifrado con TLS?**

Si recibe un correo cifrado con TLS, no necesitará emprender una acción específica. El mensaje le llegará descifrado a su bandeja de entrada de correo como cualquier otro.

#### **13. ¿Cómo sé que TLS está funcionando?**

HSBC usa Forced TLS cuando es posible para asegurar los correos. Forced TLS garantiza que el correo será cifrado con TLS y se enviará con seguridad. Esto significa que si TLS no está funcionando, el correo no se enviará. Cabe destacar que esto únicamente se aplica cuando está configurado Forced TLS.

#### **14. ¿Qué pasa si no se puede enviar un correo mediante TLS o si TLS está descompuesto?**

Cuando está configurado Forced TLS, siempre que no se pueda establecer una conexión TLS con usted, no se enviará el correo y recibiremos un mensaje de error de entrega. Primero trataremos nuevamente durante un cierto plazo en caso que fueran problemas temporales de TLS o bien nos pondremos en contacto con usted en caso que esté teniendo problemas con TLS de su lado. Pudiera ser necesario tener asistencia técnica y consultaremos con nuestra mesa de ayuda de IT para obtener asesoría.

Cuando **no** se cuente con Forced TLS, el correo irá cifrado con SecureMail u otra solución aprobada.

## **Respuestas a preguntas sobre SecureMail**

[Para recibir un mensaje de SecureMail](#)

[Para responder un mensaje de SecureMail](#)

[Para reenviar un mensaje de SecureMail](#)

[Para redactar un mensaje de SecureMail](#)

[Respuestas a preguntas generales sobre SecureMail](#)

### **Para recibir un mensaje de SecureMail**

#### **15. Recibí un mensaje de SecureMail pero no puedo encontrar el adjunto message\_zdm.htm mencionado en mi correo. ¿Qué hago?**

Dependiendo del lector de correo que tenga, el adjunto aparecerá en la parte superior o inferior del correo. Si de todas maneras no puede encontrar el adjunto, consulte la [Ayuda de lectura de correo](#) o póngase en contacto con su ejecutivo de cuenta o representante HSBC que le haya enviado el correo.

### 16. ¿Cómo doy de alta mi cuenta de SecureMail?

Usted podrá dar de alta una cuenta de SecureMail cuando su ejecutivo de cuenta o representante HSBC le envíe un correo por primera vez usando SecureMail. Si su organización ya utiliza la solución SecureMail provista por Voltage, entonces no será necesario que dé de alta una cuenta.

Para ver una guía paso a paso de cómo dar de alta una cuenta SecureMail, consulte la Guía del usuario de SecureMail que está disponible en [www.hsbc.com/secureemail](http://www.hsbc.com/secureemail).

### 17. ¿Cómo leo un correo seguro enviado mediante SecureMail?

Para leer su correo seguro, descargue y abra el **adjunto message\_zdm.html**. En la página que se abre en su navegador, haga clic en el **botón Sign in and Read Message** (Iniciar sesión y lea el mensaje).

Si ya tiene una cuenta, verifique su dirección de correo y capture su contraseña para iniciar sesión en SecureMail. Si no tiene una cuenta, puede crear una si sigue las instrucciones en la pantalla o vea la Guía de usuario SecureMail disponible en [www.hsbc.com/secureemail](http://www.hsbc.com/secureemail). Después de que haya iniciado sesión, el mensaje seguro aparece en su navegador.

### 18. ¿Cómo accedo a los adjuntos que se me envíen en el mensaje seguro?

Una vez que haya iniciado sesión y aparezca su mensaje, puede abrir los adjuntos al hacer clic en las ligas **View** (Ver) o **Download** (Descargar) junto al nombre del archivo adjunto. Si el programa es conocido, se abre automáticamente el adjunto; de lo contrario, se abre el adjunto en una nueva ventana del navegador. También le pudiera aparecer una ventana emergente donde se le dan opciones para abrir o guardar el archivo adjunto.

### 19. ¿Qué significa que la firma de mi mensaje SecureMail aparece marcada como válida con un ?

Cada correo seguro está firmado por el remitente del mensaje para asegurar la autenticidad del remitente y la integridad de los datos del mensaje. El  significa que la firma asociada con este correo es válida y se puede confiar en el mensaje.

### 20. ¿Qué significa que la firma de mi mensaje SecureMail aparezca marcada como inválida con un ?

Cada mensaje de correo seguro está firmado por el remitente para asegurar la autenticidad del remitente y la integridad de los datos del mensaje. El  significa que la firma asociada con este mensaje no es válida y cabe la posibilidad que el mensaje haya sido falsificado. Le recomendamos ponerse en contacto con su ejecutivo de cuenta o representante HSBC para verificar si el correo es genuino.

### 21. ¿Puedo leer mi correo cifrado de SecureMail en mi Smartphone?

Los mensajes de SecureMail están diseñados para leerse únicamente desde computadoras portátiles o de escritorio. Dependiendo del navegador de su teléfono, pudiera de todas maneras acceder al mensajes desde su Smartphone; sin embargo, HSBC no recomienda hacerlo ni ofrece soporte para ello.

## Para responder un mensaje de SecureMail

### 22. ¿Cómo respondo un mensaje seguro en SecureMail?

Puede responder a la persona que originó el mensaje como se describe a continuación:

1. Haga clic en **Reply Secure** (Respuesta segura) en la parte superior del mensaje seguro. Esto lo llevará a la pantalla de respuesta. La dirección de la persona que originó el correo ya estará en el campo **To:** (Para:) y no podrá agregar más nombres a dicho campo.
2. Escriba su respuesta. El mensaje original ya habrá sido incluido en el área de redacción.

3. Haga clic en **Send Secure** (Enviar con seguridad) para enviar su respuesta.

Cabe destacar que si está enviando una respuesta a nombre de su empresa, no aparecerá el texto de renuncia de responsabilidad (disclaimer) de su empresa en la respuesta a menos que lo inserte manualmente.

### **23. ¿Cómo agrego adjuntos a mi mensaje de respuesta en SecureMail?**

Para agregar adjuntos a su respuesta:

1. Haga clic en **Choose File...** (Seleccione archivo) en el campo **Attach** (Adjuntar) y seleccione un archivo.  
El archivo seleccionado se carga de inmediato.
2. Para quitar adjuntos, haga clic en **Remove** (Quitar).

### **24. ¿Cómo obtengo una copia de la respuesta que redacté en SecureMail?**

Para hacer que se le envíe una copia de la respuesta a su bandeja de entrada, haga clic en **Send a Copy to my Inbox** a la derecha del campo **To:** (Para:). Cuando envía el mensaje, se envía una copia exacta de su respuesta en forma segura a su cuenta de correo. Si ya no desea recibir una copia en su bandeja de entrada, haga clic en **Do not send a copy to my inbox** a la derecha del campo 'To:' (Para:) antes de enviar la respuesta.

## Para reenviar un mensaje de SecureMail

### **25. ¿Puedo reenviar mi mensaje seguro a otras personas?**

Por razones de seguridad, no podrá reenviar mensajes ni a HSBC ni a otras personas.

## Para redactar mensajes en SecureMail

### **26. ¿Puedo usar SecureMail en cualquier momento para comunicarme con usted con seguridad?**

SecureMail le permite responder a la persona que originó el mensaje seguro; sin embargo, por razones de seguridad, no podrá redactar ni reenviar mensajes a HSBC ni a otras personas.

## Respuestas a preguntas generales sobre SecureMail

### **27. ¿Qué es SecureMail?**

SecureMail es una solución de cifrado de correo electrónico provista por Voltage Security Inc. que se puede usar con cualquier aplicación de correo electrónico. SecureMail es compatible con computadoras de escritorio, portátiles y netbooks.

Si recibe un mensaje seguro de esta manera, será necesario que dé de alta una cuenta de SecureMail. Para darla de alta y ver su mensaje, será necesario que tenga una conexión a internet y acceso a un navegador.

### **28. ¿Qué tan seguros son los mensajes de SecureMail?**

El correo seguro está cifrado con una llave de 1024 bits. Usa un cifrado de identidad revolucionario para asegurar la privacidad de la información confidencial sin comprometer la facilidad de uso. Cada mensaje está firmado también por el remitente a fin de asegurar la autenticidad del remitente y la integridad de los datos del mensaje.

Además, todos los mensajes de correo descifrados se ven a través de su navegador con una conexión SSL/TLS.

### **29. ¿Es la solución SecureMail adecuada para todos?**

Los mensajes enviados a través de SecureMail se pueden recibir en forma segura a través de cualquier aplicación de correo electrónico. Para ver el mensaje seguro, debe estar conectado también a la internet y tener acceso a un navegador.

**30. Cuando use SecureMail en el pasado, descargué una aplicación para mi BlackBerry. Esta aplicación ya no funciona. ¿Por qué?**

Debido a la cambiante tecnología de BlackBerry y la retroalimentación de los clientes, se decidió que se debía retirar esta aplicación. Dependiendo del navegador de su teléfono, pudiera de todas maneras acceder al mensaje desde su BlackBerry; sin embargo, HSBC no recomienda ver mensajes de SecureMail desde su BlackBerry y ya no ofrece soporte alguno al respecto.

**31. ¿La utilización de SecureMail para leer mis mensajes me genera algún costo?**

No hay costo alguno implicado en la recepción o respuesta de correos cifrados mediante SecureMail.

**32. ¿Tendré que descargar o comprar algún software para recibir correo seguro mediante SecureMail?**

No hay requisitos de descargar o comprar software nuevo alguno cuando se usa SecureMail.

**33. No tengo configurado TLS en mi servidor de correo y no tengo un navegador para ver un mensaje SecureMail. ¿Cómo podré ver el mensaje seguro?**

Si no puede aceptar tráfico de correo TLS y no tiene un navegador para usar SecureMail, no podremos enviarle la información en forma segura por correo electrónico con Forced TLS o SecureMail. Póngase en contacto con la persona que originó el mensaje con quien puede analizar soluciones adecuadas para enviar la información mediante un método seguro alternativo.

Recuerde, va contra la política de HSBC enviar información de forma no segura si dicha información pudiera representar un riesgo para usted, HSBC y otros clientes de ser interceptada por otra persona.

**34. ¿Cómo sabré que el correo proviene de HSBC mediante SecureMail?**

Cada correo que su destinatario reciba mediante SecureMail contendrá la misma imagen antiphishing que le fue asignada en el primer correo de SecureMail proveniente de su ejecutivo de cuenta o representante HSBC. Si tiene alguna duda, póngase en contacto con su ejecutivo de cuenta o representante HSBC por teléfono en lugar de por correo electrónico.

**35. ¿Puede mi empresa dar de alta una sola cuenta de SecureMail para todos sus empleados?**

Por cuestiones técnicas y de seguridad, cada destinatario de correo debe tener una cuenta de SecureMail para asegurarse que el mensaje vaya a cada persona autorizada. Por lo tanto, su empresa no puede dar de alta una sola cuenta de SecureMail para todos los empleados.

Si el correo se envía a una cuenta de correo compartida, será necesario que el titular de la cuenta dé de alta una cuenta de SecureMail y comparta los detalles de acceso de la misma de conformidad con las políticas de seguridad de su empresa.

**36. ¿Qué pasa con la posibilidad de que los filtros de correo no deseado bloqueen los mensajes de SecureMail?**

Los filtros de correo no deseado funcionan de distintas maneras. Pueden filtrar correos con base en el encabezado, el asunto, el contenido del correo o simplemente viendo la frecuencia con que se recibe un correo de una fuente que usted no ha autorizado. Dependiendo del filtro que use su prestador de servicios de correo electrónico, el correo de HSBC cifrado con SecureMail pudiera ser bloqueado o mandado a su carpeta de correo no deseado. Si está esperando un correo y no lo ve en su bandeja de entrada, verifique primero su carpeta de correo no deseado o si ya ha recibido notificación de que se ha bloqueado un correo, verifique la dirección de correo del remitente. Si confía en la fuente, puede proceder a recuperar el correo de la manera que normalmente lo hace. Puede que también necesite cambiar las configuraciones de su propio filtro: por ejemplo, hay configuraciones que evitan la recepción de correos cifrados.

**37. ¿Todos los correos de HSBC estarán cifrados con SecureMail?**

Los correos estarán cifrados únicamente si la información que contienen pudiera representar un riesgo para usted o para HSBC de ser interceptada por destinatarios no autorizados. Si no cuenta con una conexión Forced TLS, su correo será cifrado con SecureMail o una solución aprobada alternativa que asegure la información que se le envía.

**38. Ya recibo correo mediante Forced TLS. ¿Recibiré ahora correos seguros mediante SecureMail?**

Forced TLS es la solución de cifrado de correo preferida de HSBC. Si ya tenemos disponible Forced TLS con usted, no cifraremos el correo con SecureMail.

**39. ¿Dónde puedo encontrar más información sobre SecureMail?**

Visite [www.hsbc.com/secureemail](http://www.hsbc.com/secureemail) para obtener más información sobre SecureMail.

**40. ¿A quién puedo acudir para obtener más ayuda sobre SecureMail?**

Si no encuentra las respuestas que está buscando aquí ni en la información provista en el sitio web [www.hsbc.com/secureemail](http://www.hsbc.com/secureemail), póngase en contacto con el ejecutivo de cuenta o representante HSBC que le envió el correo.

## Glosario

### **Dominio de correo electrónico**

Dominio de correo electrónico es la parte después del signo @ en una dirección de correo p. ej. [nombre@sudominiodecorreo.com](mailto:nombre@sudominiodecorreo.com)

### **Servidor de correo**

Un servidor de correo procesa los mensajes entrantes de alguna manera (p. ej. filtro de correo no deseado) antes de enviarlos a la bandeja de entrada de los destinatarios.

### **Cifrado**

El cifrado es el proceso de transformar los datos de manera que no los pueda leer nadie salvo la contraparte autorizada para recibirlos.

### **Forced TLS – Transport Layer Security**

Transport Layer Security (TLS) es una manera transparente para el usuario de cifrar la transmisión de correo electrónico de una organización a otra a través de internet. TLS es un protocolo de seguridad basado en el protocolo Secure Sockets Layer (SSL) 3.0 que ha existido desde 1996. Forced TLS es una configuración que se tiene que configurar en los servidores de correo electrónico del remitente y el destinatario para que se pueda transportar con seguridad el correo electrónico.

### **Correo electrónico seguro**

Correo electrónico seguro es un correo que ha sido cifrado para que se pueda enviar con seguridad a través de internet.

### **Servidor**

Un servidor es un sistema o dispositivo de cómputo que gestiona los recursos de red. Con frecuencia, los servidores actúan como dispositivos de almacenamiento para los archivos.

### **SSL – Secure Socket Layer**

Secure Socket Layer (SSL) proporciona una seguridad mejorada para las comunicaciones en internet. Utiliza el **cifrado** (vea definición anterior) para garantizar la confidencialidad de la información delicada –tal como números de tarjeta de crédito, saldos de cuenta y otros datos financieros y personales– que se envía entre el navegador y un **servidor** de red (vea definición anterior).

### **Navegador**

Un **navegador** es una aplicación de software para recuperar, presentar y desplazar recursos de información en la red mundial.

## Soporte

Para más información acerca de nuestras soluciones de correo electrónico, póngase en contacto con su ejecutivo de cuenta o representante HSBC quien lo ayudará o canalizará su consulta.

**Publicado por HSBC Holdings plc**

Somos un miembro importante del Grupo HSBC, una de las organizaciones de servicios bancarios y financieros más grandes del mundo con cerca de 8,000 oficinas en 87 países y territorios.

**Publicado por Riesgo de Seguridad de la Información del Grupo**

8 Canada Square, London, United Kingdom E14 5HQ

© HSBC Holdings plc. 2011

Todos los derechos reservados.