SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Ayuda (iOS)

Versión del producto: 9.6

Contenido

1 Accesibilidad

Sophos Intercept X for Mobile cumple con las Directrices de accesibilidad para el contenido web (WCAG) 2.1 Nivel AA. Puede encontrar más información sobre estas directrices en la información relacionada.

Le recomendamos que utilice Sophos Intercept X for Mobile con el lector de pantalla VoiceOver y el software magnificador Zoom incluido en los dispositivos iOS. Puede encontrar enlaces para utilizar VoiceOver y Zoom en la información relacionada. Si necesita más ayuda con VoiceOver o Zoom, puede ponerse en contacto con el soporte técnico de Apple.

Si desea utilizar productos de tecnología de asistencia con nuestro software, le recomendamos que esté familiarizado con el funcionamiento del producto elegido y los comandos de teclado disponibles.

Información relacionada

Directrices de accesibilidad para el contenido web

Manual del usuario del iPhone: Activar VoiceOver y practicar gestos en el iPhone

Manual del usuario del iPhone: Acercar la imagen en la pantalla del iPhone

2 Acerca de Sophos Intercept X for Mobile

Sophos Intercept X for Mobile le ayuda a trabajar de forma segura en su iPhone o iPad.

Puede obtener un menú de acciones rápidas si mantiene pulsado el icono Sophos. En un dispositivo con 3D Touch, pulse brevemente el icono para ver el menú.

3 Panel de control

El panel de control de Sophos Intercept X for Mobile le ofrece una visión general del estado de seguridad del dispositivo.

Las funciones tienen colores diferentes en función de su estado:

- Verde: No se han detectado problemas
- Rojo: Se han encontrado problemas
- Azul: Función activada
- Gris: La función está desactivada o no está configurada

4 Seguridad de dispositivos

En **Seguridad de dispositivos** puede ver el estado de seguridad del dispositivo.

Sophos Intercept X for Mobile muestra la información siguiente:

- Información general del dispositivo, como el nombre del modelo y la versión de iOS.
- Recomendaciones de actualizaciones si no tiene instalada la última versión de iOS disponible.
- Información de "jailbreaking" si Sophos Intercept X for Mobile ha detectado un desbloqueo en el dispositivo.

5 Filtrado web

Su empresa puede utilizar el filtrado web para protegerle contra la navegación en sitios con contenido malicioso, no deseado o ilegal.

Si su empresa gestiona su dispositivo, puede especificar los tipos de sitios web de los que debe ser advertido antes de abrirlos o bloquearlos. Esto le protege contra la navegación en sitios con contenido malicioso, no deseado o ilegal.

En el panel de control, el filtrado web está disponible en **Seguridad de red**.

Nota

- Su empresa debe activar esta función.

Lista de permisos

Puede anular de forma permanente el aviso para determinadas páginas maliciosas o páginas que estén englobadas dentro de una categoría. Esto resulta útil cuando una de las páginas que visita frecuentemente está englobada dentro de una de las categorías que activan una advertencia. Deslice hacia abajo la notificación **Solicitud web bloqueada** y toque **Añadir a lista de permitidos**.

En la **Lista de permisos**, se muestra el número de páginas permitidas. Toque el contador para ver todas las páginas.

Las entradas que ha añadido personalmente y las predefinidas por su empresa se visualizan en secciones separadas.

Para filtrar una página de nuevo, deslice la entrada hacia la izquierda para eliminarla. Solo puede hacerlo para las entradas que ha añadido usted mismo.

Lista de bloqueo

Puede añadir páginas web para las que se genera un aviso a una lista de bloqueo para que siempre estén bloqueadas. Deslice hacia abajo la notificación **Solicitud web bloqueada** y toque **Añadir a lista de bloqueo**.

En la **Lista de bloqueo**, se muestra el número de páginas bloqueadas. Toque el contador para ver todas las páginas.

Las entradas que ha añadido personalmente y las predefinidas por su empresa se visualizan en secciones separadas.

Para generar una aviso de nuevo, deslice la entrada hacia la izquierda para eliminarla. Solo puede hacerlo para las entradas que ha añadido usted mismo.

6 Seguridad Wi-Fi

Seguridad Wi-Fi se utiliza para revisar su conexión Wi-Fi a fin de detectar amenazas basadas en red.

Nota
Si Sophos Intercept X for Mobile está inscrito en Sophos Mobile, esta función la administra la empresa.

En el panel de control, la seguridad Wi-Fi está disponible en **Seguridad de red**.

Tipos de problemas

Sophos Intercept X for Mobile detecta los siguientes problemas:

Suplantación ARP	La suplantación ARP consiste en que un atacante envía mensajes ARP (Protocolo de resolución de direcciones) maliciosos a su ordenador de forma que parece que la dirección MAC del atacante está asociada a la dirección IP de su puerta de enlace de red. Esto le permite acceder a la red privada del usuario, robar datos confidenciales y lanzar ataques adicionales como ataques de denegación de servicio o de tipo «Man in the middle». La suplantación ARP no se puede detectar en dispositivos con iOS 10.3 o posterior.
Portal cautivo	Un portal cautivo es una forma que tienen las redes Wi-Fi públicas de solicitar autenticación antes de otorgar acceso a la red. Dado que todo el tráfico se redirecciona al portal cautivo, es posible que reciba avisos adicionales.
Manipulación de contenido	La manipulación de contenido consiste en que un atacante manipula el contenido de un sitio web para forzarle a realizar acciones dañinas. Esto le permite hacer cosas como omitir la autenticación o borrar datos.
Interceptación de SSL	La interceptación de SSL es cuando un atacante utiliza un certificado de servidor falso para interceptar la conexión segura entre el equipo del usuario y un sitio web. El atacante puede descifrar datos sensibles mientras hace creer al usuario que la conexión sigue siendo segura.
Decapado de SSL	El decapado de SSL es cuando un atacante degrada la conexión a un sitio web de HTTPS seguro a HTTP no seguro. El atacante puede redireccionar todo el tráfico entre el equipo del usuario y el sitio web a través de su propio servidor proxy. Esto le permite descifrar datos

confidenciales mientras le hace creer que sigue conectado mediante HTTPS.

Ejecutar comprobaciones

- Para comprobar la red Wi-Fi a la que está conectado, toque **Comprobar Wi-Fi**.
- Para realizar comprobaciones de red automáticamente en segundo plano, active **Comprobación en segundo plano**. Esta opción ejecuta una comprobación cada vez que el dispositivo se conecta a una red Wi-Fi.

Ocultar problemas

Puede ocultar problemas de Wi-Fi para redes específicas. Los problemas ocultos no contribuyen al estado de seguridad del dispositivo.

Para volver a mostrar todos los problemas, seleccione **Mostrar todos los problemas de Wi-Fi** en la configuración de la app.

7 Authenticator

Authenticator se utiliza para generar contraseñas de un solo uso (o códigos de verificación) para iniciar sesión en sus cuentas que utilizan la autenticación multifactor.

Consulte a su proveedor de cuenta si se admite la autenticación multifactor y cómo habilitarla para su cuenta.

Authenticator admite contraseñas de un solo uso **basadas en tiempo** y **basadas en contador**. Consulte Acerca de las contraseñas de un solo uso (página 8).

Para iniciar Authenticator, mantenga pulsado el icono de Sophos y, a continuación, toque **Authenticator**.

Funciones:

- Para las contraseñas **basadas en tiempo,** Authenticator muestra la contraseña de un solo uso válida en ese momento junto con un icono animado que ilustra el tiempo que queda para que el código caduque y se calcule el siguiente código.
- Para las contraseñas **basadas en contador**, toque **Tocara para código** para crear el primer código o **Siguiente** para crear el siguiente código. Para impedir que pueda generar varios códigos seguidos de forma accidental, se aplica una latencia de varios segundos después de crearse un código hasta que pueda generarse el siguiente.
- Para copiar la contraseña de un solo uso actual para una cuenta en el portapapeles, tóquela.
- Para editar los detalles de la cuenta, toque **Editar**, seleccione el elemento de cuenta y luego toque **Modificar**. Por motivos de seguridad, no se puede mostrar ni editar la clave secreta.
- Para eliminar una cuenta, toque **Editar**, seleccione el elemento de cuenta y luego toque el icono **Eliminar** 🗑.

Aviso
Al eliminar una entrada de Authenticator, perderá la capacidad de generar contraseñas de un solo uso para esa cuenta. Esto no desactiva la autenticación multifactor. Si elimina la entrada de Authenticator, es posible que no pueda iniciar sesión en su cuenta.

Antes de eliminar la entrada, asegúrese de que dispone de un mecanismo alternativo para generar contraseñas de un solo uso, o bien un mecanismo alternativo para iniciar sesión en su cuenta sin la autenticación multifactor.

7.1 Acerca de las contraseñas de un solo uso

Las contraseñas de un solo uso (también llamadas códigos de verificación) están formadas por una serie de dígitos. Se calculan a partir de estos parámetros:

- Una clave secreta compartida que solo su proveedor de cuenta y usted conocen.
- Los valores de configuración específicos de su proveedor de cuenta.
- Un contador consecutivo.

Al utilizar una contraseña de un solo uso para autenticarse, su proveedor de cuenta espera una contraseña que se calcula a partir de un determinado valor del contador. Como Authenticator utiliza las mismas reglas que su proveedor de cuenta para determinar el valor del contador actual, el proveedor aceptará su contraseña de un solo uso.

Authenticator admite contraseñas de un solo uso **basadas en tiempo** y **basadas en contador**. Estos tipos se diferencian por la forma en que se determina el valor del contador actual:

- **Contraseñas de un solo uso basadas en tiempo** (TOTP, según RFC 6238): El valor del contador se incrementa de forma continua en función de la hora actual. El siguiente valor de la serie de códigos de verificación se genera cuando ha transcurrido un período de tiempo definido.
- **Contraseñas de un solo uso basadas en contador** (HOTP, según RFC 4226): El valor del contador se incrementa a demanda. El siguiente valor de la serie de códigos de verificación se genera cuando usted lo solicita.

7.2 Añadir una cuenta a partir de un código QR

Utilice este procedimiento si ha habilitado la autenticación multifactor para una cuenta y su proveedor de cuenta le ha proporcionado un código QR con los datos de configuración.

1. Seleccione **Crear > Escanear código QR**.
2. Escanee el código QR con el dispositivo.

Una vez que la app haya leído los detalles de configuración del código QR, creará una nueva cuenta de Authenticator.

7.3 Añadir una cuenta manualmente

Utilice este procedimiento si ha habilitado la autenticación multifactor para una cuenta y su proveedor de cuenta le ha proporcionado una lista con los datos de configuración.

1. Seleccione **Crear > Añadir manualmente**.
2. En el campo **Nombre**, escriba un nombre para la nueva cuenta de Authenticator.
3. En el campo **Clave**, escriba la clave secreta que le haya indicado su proveedor de cuenta. La clave es específica de su cuenta y constituye la base de cálculo para las contraseñas de un solo uso.
4. En el campo **Tipo**, seleccione el tipo de cálculo que le haya indicado su proveedor de cuenta.
5. Si su proveedor de cuenta ha especificado otros datos de configuración, introdúzcalos en los campos siguientes.

   Atención
   Rellene únicamente la información que le haya indicado su proveedor de cuenta.

   - En el campo **Período de tiempo**, introduzca el período de validez en segundos. Solo está disponible para las contraseñas de un solo uso basadas en tiempo.
   - En el campo **Longitud de código**, seleccione el número de dígitos de las contraseñas de un solo uso.
   - En el campo **Algoritmo hash**, seleccione el algoritmo hash para el cálculo de las contraseñas de un solo uso.
6. Opcional: En el campo **Color de fondo**, seleccione un color para la entrada de cuenta a fin de identificarla fácilmente en la lista de cuentas.
7. Cuando haya terminado, toque **Guardar**.

Así se configurará una nueva cuenta de Authenticator.

8 Cofre de contraseñas

El Cofre de contraseñas se utiliza para guardar todos los datos de su cuenta en un solo sitio protegido por una contraseña maestra.

Para iniciar el Cofre de contraseñas, mantenga pulsado el icono de Sophos y, a continuación, toque **Cofre de contraseñas**.

Tiene las opciones siguientes:

- Cree un nuevo archivo de Cofre de contraseñas.
- Importe un archivo KDBX de KeePass existente. Cuando edite entradas de contraseña, solo se cambiará la copia local.
- Abra un archivo KDBX de KeePass existente. Cuando edite entradas de contraseña, se cambiará el archivo original.

Activar Autorrellenar contraseñas

En iOS 12 y posterior, se puede utilizar el Cofre de contraseñas para autorrellenar contraseñas.

Para activar la opción **Autorrellenar contraseñas** en el Cofre de contraseñas:

1. Vaya a la app **Ajustes** y desplácese hacia abajo hasta **Contraseñas y cuentas**.
2. Toque **Autorrellenar contraseñas** y active la opción **Autorrellenar contraseñas**.
3. Seleccione **Intercept X** en **Permitir relleno desde:**.

Ahora puede acceder al Cofre de contraseñas con solo tocar **Contraseñas** en la barra QuickType situada sobre el teclado cuando se le pida que introduzca las credenciales.

8.1 Crear una entrada en el Cofre de contraseñas

Para añadir una entrada o grupo de entradas en un archivo de Cofre de contraseñas:

1. En Cofre de contraseñas, toque **Más** ⊕.
2. Seleccione el tipo de entrada que quiere crear:
   - **Añadir entrada de cuenta** crea una entrada con campos predefinidos adecuados para cuentas web y elementos similares.
   - **Añadir entrada de tarjeta de crédito** crea una entrada con campos predefinidos adecuados para tarjetas de crédito y elementos similares.
   - **Notas** crea una entrada para tomar una nota segura.
   - **Añadir grupo** crea una carpeta en el Cofre de contraseñas para organizar sus entradas.
3. Introduzca sus datos en los campos de la entrada.
4. Opcional: Toque **Más** ⊕ y luego **Añadir campo** para añadir un campo personalizado a la entrada.

   Si activa **Protegido** para un campo personalizado, debe tocar el botón del ojo situado junto al campo para ver el valor. Además, los campos protegidos no aparecen en los resultados de búsqueda.

   Con **Más** ⊕ también puede añadir un archivo o una imagen a la entrada.

5. Toque **Listo** para guardar la entrada.

Los datos de contraseña permiten iniciar sesión fácilmente en una página web o una app. Consulte Usar datos de contraseña para iniciar sesión (página 11).

Nota
Es posible que se produzcan problemas de rendimiento cuando adjunte archivos grandes o un gran número de archivos a una entrada. Le recomendamos que cifre estos archivos con la app Sophos Secure Workspace para guardarlos de forma segura.

8.2 Generar contraseñas

1. Abra la entrada de Cofre de contraseñas para la que quiere generar una contraseña.
2. Toque **Editar** para cambiar al modo de edición.
3. Toque el icono **Engranaje** para abrir el generador de contraseñas.
4. Defina la longitud de la contraseña y el tipo de caracteres que deban incluirse en la contraseña.
5. Toque **Actualizar** para generar una contraseña basada en las opciones que ha definido.
6. Si está de acuerdo con la contraseña generada, cierre el generador de contraseñas. La contraseña se actualiza con el valor generado.
7. Guarde la entrada.

8.3 Usar datos de contraseña para iniciar sesión

- Para copiar el valor de un campo al portapapeles, toque en el campo correspondiente.
- Para mostrar el valor de los campos protegidos, toque el icono **Ojo** junto al campo protegido.
- Para abrir una URL en Safari, toque el icono **Globo** junto al campo **URL**.

8.4 Administrar entradas del cofre de contraseñas

1. Toque y mantenga pulsada una entrada para cambiar al modo de selección.
2. Opcional: Seleccione las entradas adicionales para las que desee realizar la misma acción.
3. Toque un icono para realizar la acción correspondiente:
   - **Editar**: Editar el contenido de la entrada. Opción solo disponible cuando solo hay seleccionada una entrada.
   - **Cortar**: Mover las entradas seleccionadas a otro grupo en el archivo de Cofre de contraseñas.
   - **Copiar**: Copiar las entradas seleccionadas a otro grupo en el archivo de Cofre de contraseñas.
   - **Eliminar**: Mover las entradas seleccionadas al grupo especial **Papelera de reciclaje**.
     Para eliminar entradas de forma permanente, utilice **Eliminar** en las entradas en el grupo **Papelera de reciclaje**.

- Para pegar una entrada que haya cortado o copiado, navegue hasta la nueva ubicación y, a continuación, toque **Portapapeles** .

8.5 Buscar entradas en el cofre de contraseñas

En Cofre de contraseñas, puede buscar nombres de entradas y grupos, y valores de campos de entrada.

Nota
No puede buscar campos de contraseña o campos que haya configurado con la opción **Protegido**.

Sugerencia
Si no desea buscar en todo el archivo de Cofre de contraseñas, vaya al grupo o subgrupo. Todos los elementos de ese grupo se buscan recursivamente.

1. En Cofre de contraseñas, deslice hacia abajo para cambiar al modo de búsqueda.
2. Introduzca una cadena de búsqueda. La lista de resultados se actualiza según va escribiendo.

8.6 Realizar copia de seguridad de Cofre de contraseñas

Es importante que haga copias de seguridad del archivo de Cofre de contraseñas de forma periódica. Si pierde el archivo de Cofre de contraseñas porque lo elimina sin querer o pierde su dispositivo, por ejemplo, no podrá acceder a sus datos de contraseña a menos que tenga una copia de seguridad reciente.

1. En el cuadro Cofre de contraseñas del panel de control de la app, toque **Información** ⓘ.
2. Toque **Realizar copia de seguridad del archivo de Cofre de contraseñas**.
3. Seleccione la ubicación para crear la copia de seguridad.

Nota
Le recomendamos también que imprima una hoja de recuperación para que pueda acceder a sus datos de contraseña en el caso de que, por ejemplo, olvide la contraseña maestra o pierda del archivo de claves. Consulte Imprimir hoja de datos de recuperación de Cofre de contraseñas (página 12).

8.7 Imprimir hoja de datos de recuperación de Cofre de contraseñas

Si olvida la contraseña maestra de Cofre de contraseñas o pierde el archivo de claves, no podrá acceder a los datos almacenados en el Cofre de contraseñas. Para evitar esto, imprima una hoja de datos de recuperación que contenga la información necesaria.

Aviso
Es importante que haga copias de seguridad del archivo de Cofre de contraseñas de forma periódica. Si pierde el archivo de Cofre de contraseñas porque lo elimina sin querer o pierde su dispositivo, por ejemplo, la hoja de datos de recuperación no bastará para recuperar sus datos de contraseña. Consulte Realizar copia de seguridad de Cofre de contraseñas (página 12).

1. En el cuadro Cofre de contraseñas del panel de control de la app, toque **Información** ⓘ.
2. Toque **Imprimir hoja de datos de recuperación**.
3. Seleccione la impresora y el número de copias y luego toque **Imprimir**.
4. En el documento impreso, indique la información siguiente:
   - Su contraseña maestra
   - La ubicación de su archivo de Cofre de contraseñas
   - La ubicación de su copia de seguridad
5. Guarde la hoja de datos de recuperación en un lugar seguro.

   Cualquier persona que tenga acceso a la hoja de datos de recuperación y a su archivo de Cofre de contraseñas podrá leer sus datos de contraseña.

Si ha protegido el archivo de Cofre de contraseñas con un archivo de claves, la hoja de datos de recuperación incluye una huella de ese archivo en forma de código QR. Puede utilizar el código QR como alternativa al archivo de claves para abrir su archivo de Cofre de contraseñas.

9 Escáner de códigos QR

El Escáner de códigos QR se utiliza para escanear códigos QR y luego procesar la información asociada.

Para iniciar el Escáner de códigos QR, mantenga pulsado el icono de Sophos y, a continuación, toque **Escáner de códigos QR**.

Direcciones web

Al escanear un código QR, se comprueba la URL asociada por si incluye contenido malicioso o inadecuado en función de la clasificación proporcionada por SophosLabs.

- Cuando se indique que la URL es segura, toque **Continuar** para abrirla en Safari.

Contactos

Escanee el código QR y luego toque **Añadir** para crear una entrada en sus contactos con la información de tarjeta de presentación asociada.

Additional information
Sophos Intercept X for Mobile puede leer la información de tarjetas de visita en los formatos vCard 2.1 y 3.0.

Configuraciones Wi-Fi

Escanee el código QR y luego toque **Copiar** para copiar la contraseña en el portapapeles. En la app **Ajustes**, vaya a **Wi-Fi**, seleccione la red y pegue la contraseña cuando se le solicite.

Nota
Verá un aviso si intenta conectarse a una red no segura, por ejemplo, una red sin protección WPA o WPA2.

10 Filtrado de mensajes

Su empresa puede utilizar el filtrado de mensajes para comprobar si los mensajes SMS/MMS entrantes contienen direcciones URL de phishing.

Los mensajes sospechosos se filtran en una pestaña aparte llamada **SMS no deseados**.

Si ve **Activar filtrado de mensajes** en la configuración de la app, debe activar el filtrado de mensajes en la app **Ajustes** según lo requiera su empresa.

Activar el filtrado de mensajes

En la app **Ajustes** de iOS, vaya a **Mensajes**, toque **Desconocido y no deseado** y active **Intercept X** en **Filtrado de SMS**.

Pestaña SMS no deseados en la app Mensajes

Si un mensaje de un remitente desconocido se clasifica como spam, el mensaje se mueve a la pestaña **SMS no deseados** en la app Mensajes. Los mensajes existentes y posteriores del mismo remitente también se mueven a **SMS no deseados**.

Nota

- Los mensajes de un contacto conocido nunca se clasifican como spam.
- El filtrado de mensajes no funciona para iMessages.

11 Gestión corporativa

En un entorno corporativo, Sophos Mobile puede administrar Sophos Intercept X for Mobile. Esto permite a su empresa supervisar el estado de cumplimiento del dispositivo.

Para inscribir Sophos Intercept X for Mobile en Sophos Mobile, siga las instrucciones que le haya proporcionado su empresa.

Cuando Sophos Mobile administra Sophos Intercept X for Mobile, se aplican las siguientes diferencias:

- La configuración de la app es definida de forma centralizada por su empresa.
- Si su dispositivo infringe la política de cumplimiento de su empresa, es posible que se le restrinja el acceso a la red u otras funciones. Puede ver el estado de cumplimiento en el panel de control de la app. Consulte Resolver infracciones de cumplimiento (página 16).

11.1 Resolver infracciones de cumplimiento

Cuando Sophos Mobile administra Sophos Intercept X for Mobile, el panel de control muestra el estado de cumplimiento en función de la política de su empresa.

Para ver y resolver infracciones de cumplimiento:

1. En el panel de control, toque **Gestión corporativa**.
   Cuando hay infracciones de cumplimiento, la casilla tiene un icono rojo.
2. Toque la infracción de cumplimiento y siga las instrucciones indicadas para resolverla.

Nota
Cuando un dispositivo infringe reglas de cumplimiento, es posible que se le restrinja el acceso a la red u otras funciones.

11.2 Obtener asistencia

Cuando Sophos Mobile administra Sophos Intercept X for Mobile, puede mostrar información sobre cómo ponerse en contacto con el departamento de TI y cualquier otra información proporcionada.

En el panel de control, toque **Gestión corporativa**.

Los datos de contacto se muestran en **Contacto de TI** e **Información adicional**.

12 Configuración

Opción de configuración	Descripción
Activar filtrado de mensajes	Compruebe si hay URL de phishing en mensajes SMS/MMS entrantes. Su empresa debe activar esta función. Consulte Filtrado de mensajes (página 15).
Active el filtrado web	Bloquee las conexiones a páginas web maliciosas o categorizadas. Su empresa debe activar esta función. Consulte Filtrado web (página 5).
Mostrar todos los problemas de Wi-Fi	Muestre todos los problemas de Wi-Fi, incluidos los que ha ocultado anteriormente.
Nivel de registro	Si se lo solicita el soporte de Sophos, seleccione el nivel de información de registro.
Enviar archivos de registro	Toque esta opción para enviar un correo electrónico con el archivo de registro de la aplicación adjunto. La dirección de correo electrónico de soporte de Sophos se inserta por defecto.
Seguimiento de datos	Permita que Sophos recopile datos de uso anónimos para mejorar la aplicación.

13 Crear una copia de seguridad y restaurar

Puedes realizar una copia de seguridad de sus cuentas de Authenticator para moverlas a un nuevo dispositivo iOS o Android.

Realizar copias de seguridad de cuentas

1. En el menú de la app, seleccione **Copia de seguridad y restaurar**.
2. Toque **Realizar copia de seguridad**.
3. Introduzca un nombre para el archivo de copia de seguridad
4. Especifique una contraseña, confírmela y toque **Aceptar**.
5. Seleccione la ubicación para crear la copia de seguridad.

   Sugerencia
   Guarde la copia de seguridad en la nube para que pueda utilizarla en otros dispositivos.

6. Toque **Añadir**.

Restaurar cuentas

1. En la página **Copia de seguridad y restaurar**, toque **Restaurar**.
2. Vaya a la ubicación donde ha guardado el archivo y toque la copia de seguridad.
3. Especifique la contraseña para la copia de seguridad y toque **Aceptar**.

14 Aviso legal