Preguntas frecuentes

Contenido

Preguntas frecuentes

1. Su cuenta de Mobile Security está bloqueada porque introdujo su código PIN demasiadas veces

Problema

Si intenta iniciar sesión en McAfee Mobile Security **varias veces** con un **código PIN incorrecto**, verá este error:

Ha usado el código PIN incorrecto demasiadas veces y su cuenta está bloqueada.

Vuelva a intentarlo después de xx minutos.

Solución

Utilice una de estas cuatro opciones para desbloquear su dispositivo:

- **Opción 1: Desbloquee con Desbloqueo de huella digital**:

  NOTA: Esta función está disponible en McAfee Mobile Security **4.9** o versiones posteriores.

  1. Debajo de la opción **¿Ha olvidado el código PIN?**, pulse:

     Desbloquea tu dispositivo con tu huella digital.
  2. Coloque el dedo registrado donde se indica. El dispositivo se desbloqueará.

- **Opción 2: Desbloquee con ayuda de sus amigos**:
  1. Pulse **¿Ha olvidado el código PIN?**
  2. Pulse **Enviarlo a mis amigos**.
  3. Obtenga el código PIN temporal de uno de sus amigos registrados.
  4. Escriba el código PIN para desbloquear el dispositivo.

- **Opción 3: Desbloquee usando sus preguntas de seguridad**:
  1. Pulse **¿Ha olvidado el código PIN?**
  2. Pulse **Responder preguntas de seguridad**.
  3. Escriba sus respuestas.
  4. Pulse **Enviar**.
  5. Cuando se le indique, cree un nuevo código PIN.

     NOTAS:

     - Asegúrese de que su dispositivo tenga conexión de datos (Wi-Fi, 3G o 4G inalámbrico). Esto es necesario para enviar el nuevo código PIN a los servidores de McAfee.

- Para los dispositivos que utilizan tarjetas SIM, asegúrese de que el **número de teléfono** que se muestra en la sección **Rastreo** en la página **Bloquear** (en http://www.mcafeemobilesecurity.com) coincida con la **tarjeta SIM** insertada en el dispositivo.
- Encontrará más información sobre la función de preguntas de seguridad en el artículo TS101128.

- **Opción 4: Desbloquee desde el sitio web de McAfee**:
  1. Restablezca su código PIN usando uno de los métodos descritos en TS101237.
  2. Inicie sesión en http://www.mcafeemobilesecurity.com.
     Puede usar los detalles de su cuenta de McAfee o su número de teléfono para iniciar sesión.
  3. Seleccione su cuenta de McAfee Mobile Security.
  4. En la página **Bloquear**:

     Pulse **Desbloquear**. Se envía un comando de desbloqueo al dispositivo.

     NOTAS:
     - Para los dispositivos que utilizan tarjetas SIM, asegúrese de que el **número de teléfono** que se muestra en la sección **Rastreo** de la página **Bloquear** coincida con la **tarjeta SIM** insertada en el dispositivo.
     - Si el dispositivo no tiene conexión de datos, puede que demore un poco antes de que el comando de desbloqueo llegue al dispositivo. Esto es porque se utiliza un proceso adicional para enviar el comando de desbloqueo por SMS.
     - Si el dispositivo no tiene conexión de datos ni ningún otro medio de conectividad, el comando de desbloqueo no puede llegar al dispositivo. Deberá obtener su código PIN de soporte para desbloquear el dispositivo. Para hacerlo, póngase en contacto con el Servicio de atención al cliente.

2. El dispositivo se ha bloqueado y ha olvidado el código PIN de seis dígitos para Mobile Security

Resumen

Si el dispositivo está bloqueado porque **se le ha olvidado** el código PIN de seis dígitos para McAfee Mobile Security (MMS), siga los pasos a continuación.

Pasos preliminares:

- El **Desbloqueo de huella digital** está disponible en MMS 4.9 o versiones posteriores. Esto le permite desbloquear su dispositivo con su huella digital en caso de que olvide el código PIN. Para obtener instrucciones, consulte el artículo TS102658.
- Si aparece un mensaje para informarle de **que ha introducido un código PIN incorrecto demasiadas veces y la cuenta se ha bloqueado**, consulte el artículo TS101795 en lugar de seguir los pasos de este artículo.

Solución

Debe recuperar el código PIN antes de poder iniciar sesión en MMS. Puede recuperar el código PIN desde:

- Su **dispositivo** o
- El sitio web **MMS** (McAfeeMobileSecurity.com)

Utilice una de estas opciones para recuperar el código PIN:

Opción 1: Recuperar el código PIN desde el dispositivo

En la pantalla de bloqueo de MMS, pulse **He olvidado el código PIN** y seleccione una de estas opciones:

NOTA: Las opciones visibles dependerán de la versión de MMS y la versión de Android que utilice.

- **Enviarme un correo electrónico con código PIN**. Pulse esta opción y compruebe la dirección de correo electrónico registrada. Haga clic en el vínculo del correo electrónico para restablecer su código PIN.
- **Responda a la pregunta de seguridad en el dispositivo**. Para obtener más información acerca de la función de preguntas de seguridad, consulte TS101128.
- **Enviar código PIN a mis amigos**. Para obtener más información acerca de las opciones de amigos, consulte TS101136.

Opción 2: Recuperar el código PIN con su número de teléfono móvil

1. Vaya a McAfeeMobileSecurity.com.
2. Haga clic en **Encontrar dispositivo**.
3. Seleccione **Número de móvil**.
4. Haga clic en **¿Ha olvidado el código PIN?**
5. Especifique:
    - Su **número de móvil**
    - El **código de verificación** que se muestra
6. Si su dispositivo está bloqueado, seleccione **Mi dispositivo está bloqueado**.
7. Haga clic en **Enviarme un vínculo**.
8. Compruebe la dirección de correo electrónico registrada para obtener el código PIN de soporte. Puede usarlo para desbloquear su smartphone.

NOTA: No podrá usar el código PIN de Soporte para iniciar sesión en su cuenta web.

Opción 3: Recuperar el código PIN con su cuenta de McAfee

1. Vaya a McAfeeMobileSecurity.com.
2. Haga clic en **Encontrar dispositivo**.
3. Seleccione **Dirección de correo electrónico**.
4. Especifique:
    - La dirección de **correo electrónico** registrada
    - La **contraseña**
5. Haga clic en **Iniciar sesión**.
6. Haga clic en **Configuración**.
7. Haga clic en **Cambiar código PIN**.
8. Siga las indicaciones.

Opción 4: Desbloquear su dispositivo de manera remota, pruebe esta opción si no consigue recuperar su código PIN con los métodos indicados anteriormente:

1. Inicie sesión en McAfeeMobileSecurity.com como se describió anteriormente.
2. Asegúrese de que su dispositivo esté **encendido** y tenga conexión a Internet o celular.
3. Haga clic en **Desbloquear** para que se envíe un comando de desbloqueo a su dispositivo.

3. ¿Qué es la función Activar alarma de McAfee Mobile Security?

Resumen

McAfee Mobile Security incluye una función nueva que activa una alarma como ayuda para localizar un dispositivo extraviado.

La alarma se puede activar de dos formas:

- Enviando un mensaje de texto desde otro dispositivo: **Secure Alarm**
- Iniciando sesión en el portal web de Mobile Security (http://mcafeemobilesecurity.com) y usando el comando Activar alarma.

Cuando el dispositivo recibe el mensaje, emite una alarma sonora durante un minuto y muestra una notificación de alarma. Cuando encuentre el dispositivo, pulse **Detener alarma** en la pantalla del dispositivo para desactivarla.

Aparece una alerta de "Cambio de SIM no válido" pero no ha cambiado su tarjeta SIM

Problema

McAfee Mobile Security (MMS) puede avisarle si detecta que se ha cambiado la tarjeta SIM de su dispositivo. Esta alerta puede enviarse a la dirección de correo electrónico registrada con su cuenta de McAfee. Aunque normalmente esta alerta solo se envía cuando se detecta un cambio en su tarjeta SIM, también podría recibirla, aunque no haya realizado ningún cambio.

Solución

Tenga en cuenta que MMS utiliza la Identidad Internacional del Abonado Móvil (IMSI) para identificar las tarjetas SIM. Así pues, aunque sustituya su SIM original por una tarjeta SIM nueva con el **mismo número de teléfono**, para McAfee Mobile Security será igualmente una SIM nueva y le enviará una alerta. Esto se debe a que la IMSI es exclusiva para cada tarjeta SIM.

Si no ha cambiado su tarjeta SIM, póngase en contacto con el Soporte técnico y proporcione la siguiente información para ayudar a determinar el motivo de la alerta:

- ¿Se ha cambiado en algún momento la tarjeta SIM de este dispositivo? Si es así, ¿cuándo?

- ¿Ha cambiado de proveedor de red?
- ¿Ha intentado reactivar su cuenta de McAfee con otro número de teléfono móvil? Si es así, ¿cuándo?

También deberá facilitar estos datos al Soporte técnico:

- Su dirección de correo electrónico registrada con McAfee
- La Identidad Internacional de Equipo Móvil (IMEI) de su dispositivo. Si no sabe cómo obtenerlo, el equipo de Soporte técnico puede ayudarle.
- Su número de teléfono móvil registrado con McAfee
- Una copia del correo electrónico de alerta que ha recibido
- El número de alertas recibidas por correo electrónico

4. Cómo restablecer su código PIN en Mobile Security for iOS

Resumen

McAfee Mobile Security (MMS) utiliza un número de identificación personal (PIN) que solo usted debe conocer para proteger sus datos. Si sospecha que otras personas conocen su código PIN, puede cambiarlo en cualquier momento desde su dispositivo.

Cambiar el código PIN de MMS

Siga estos pasos para cambiar su código PIN:

1. Abra McAfee Mobile Security.
2. Pulse el icono de menú en la parte superior izquierda.
3. Pulse **Configuración**.
4. Pulse **Cambiar código PIN**.
5. Escriba su código PIN antiguo.
6. Escriba y confirme el código PIN nuevo.

Una vez completado este proceso, su nuevo código PIN estará activo.

Restablecer su código PIN de MMS

Con tantos códigos PIN y contraseñas que recordar, es fácil olvidarse de alguno. Si ha olvidado el código PIN de Mobile Security, siga estos pasos:

1. Abra McAfee Mobile Security.
2. Pulse el icono de menú en la parte superior izquierda.
3. Pulse **Configuración**.
4. Pulse **Cambiar código PIN**.
5. Pulse **¿Ha olvidado el código PIN?** Se enviará un correo electrónico con un código de acceso temporal a la dirección de correo electrónico que tenga registrada.
6. Cuando reciba el correo electrónico, escriba el código de acceso exactamente como se muestra en el campo de McAfee Mobile Security.
7. Escriba y confirme el código PIN nuevo.

Restablecer el código PIN de la caja fuerte

McAfee Mobile Security también le proporciona una **caja fuerte** protegida por un código PIN en la que puede guardar imágenes y otro contenido de forma segura. Si ha olvidado el código PIN de la caja fuerte, siga estos pasos para restablecerlo:

1. Abra McAfee Mobile Security.
2. Intente abrir la caja fuerte. Se le pedirá el código PIN.
3. Pulse **¿Ha olvidado el código PIN?** Se enviará un correo electrónico con un código de acceso temporal a la dirección de correo electrónico que tenga registrada.
4. Cuando reciba el correo electrónico, escriba el código de acceso exactamente como se muestra en el campo de McAfee Mobile Security.
5. Escriba y confirme el código PIN nuevo.

6. McAfee Mobile Security: preguntas frecuentes

Resumen

Instalación y suscripción

¿Cómo puedo obtener McAfee Mobile Security (MMS)?

Acceda a la tienda online de su dispositivo móvil (Google Play Store o Apple Store) y busque McAfee Mobile

Security (MMS).

También puede descargar MMS desde http://m.McAfeeMobileSecurity.com mediante el navegador del dispositivo móvil. Para obtener más información, consulte el artículo TS101406.

¿Cómo puedo empezar a utilizar MMS?

Tras descargar MMS, siga las instrucciones que aparecen en pantalla para instalar la aplicación. Puede usar la dirección de correo electrónico y la contraseña de su cuenta actual de McAfee o crear una cuenta nueva. Una vez hecho esto, su dispositivo y sus datos móviles estarán protegidos mientras dure la suscripción a Mobile Security. Para obtener más detalles sobre el registro de MMS, consulte el artículo TS101880.

¿Cómo puedo acceder a mi cuenta de MMS online?

Puede utilizar cualquiera de los métodos siguientes:

Desde el sitio web de McAfee (http://home.mcafee.com):

1. Inicie sesión con su dirección de correo electrónico y contraseña de McAfee.
2 Haga clic en **Mi cuenta**.
3. Seleccione el dispositivo que desea administrar.

NOTA: No todas las funciones de MMS están disponibles en esta ubicación, como por ejemplo: mostrar los datos de copia de seguridad. El botón **Ver datos de la copia de seguridad** le redirigirá a https://www.mcafeemobilesecurity.com/.

Desde el sitio web de Mobile Security (http://www.mcafeemobilesecurity.com/):

1. Inicie sesión con su dirección de correo electrónico y contraseña de McAfee.
2. Seleccione el dispositivo que desea administrar.

NOTA: Para cuentas antiguas, inicie sesión con el número de teléfono y el código PIN de 6 dígitos.

¿Puedo instalar MMS en mi tarjeta de memoria?

No. MMS no se instala en tarjetas de memoria. MMS se instala en la memoria integrada del dispositivo móvil.

Tengo varios teléfonos. ¿Puedo agregarlos todos a mi cuenta?

Su suscripción de MMS solo se puede utilizar en un dispositivo.

NOTA: Si tiene un paquete de MMS que se haya activado por primera vez con MMS 3.2 entre el 5 y el 20 de febrero de 2014, MMS le permitirá proteger varios dispositivos porque tiene varias licencias disponibles.

Voy a cambiar de teléfono. ¿Puedo usar la cuenta antigua en el teléfono nuevo?

Sí. Sin embargo, debe utilizar las mismas credenciales de la cuenta. Compruebe que dispone de todas las credenciales necesarias (la dirección de correo electrónico y la contraseña de McAfee) y el código PIN de MMS durante la activación. Para obtener más información, consulte el artículo TS101148.

IMPORTANTE: Tras cambiar el dispositivo asociado con la cuenta, el dispositivo anterior dejará de estar protegido por MMS.

Voy a cambiar de número de teléfono. ¿Puedo conservar mi cuenta de MMS?

Sí. Para obtener información, consulte el artículo TS101148.

¿Cómo puedo suscribirme a MMS?

Al terminar la prueba, se le pedirá que se suscriba. Puede ver las opciones de pago y suscribirse desde la aplicación del dispositivo móvil o mediante el sitio web de McAfee.

¿Cuánto cuesta suscribirse a MMS?

Para obtener detalles sobre los precios y la suscripción, diríjase a https://www.mcafeemobilesecurity.com/buy/.

¿Cómo se desinstala MMS?

- En Android, se puede establecer MMS como aplicación de administración del dispositivo. Esto hace que MMS resulte más fiable y que sea más complicado para cualquiera desinstalarlo sin un código PIN o una contraseña. Para desinstalar, abra **Configuración**, pulse **Aplicaciones**, seleccione **MMS** y pulse **Desinstalar**. Escriba su código PIN si se le solicita.
- En los dispositivos con Apple iOS, mantenga pulsada la aplicación no deseada hasta que los iconos empiecen a moverse. Pulse la X en la aplicación que desee eliminar.

Para obtener más información, consulte el artículo TS101407.

Uso de MMS

¿Funcionará MMS en mi teléfono?

MMS se ejecuta en los principales sistemas operativos para dispositivos móviles, entre ellos:

- Teléfonos y tablets Android
- iOS: iPhone y iPad

¿Durará menos la batería con MMS?

El uso de la batería es insignificante. Con un uso normal, la batería del dispositivo solo se agota un 5 % más rápido cuando se tiene instalado MMS. Si tiene una tableta Android no compatible con la inserción, es posible que la batería se agote más rápido porque el uso de datos será mayor. Asimismo, la batería podría agotarse antes si tiene el análisis automático activado.

¿Puedo personalizar MMS para que se adapte a mis preferencias?

Sí. MMS ofrece muchas opciones que se pueden configurar. Por ejemplo, puede hacer lo siguiente:

- Configurar MMS para que cree una copia de seguridad de forma automática de los datos importantes, como los contactos y los mensajes de texto.
- Modificar la opción de filtro de llamadas y SMS según sus preferencias.
- Personalizar la forma en que MMS le protege frente a los virus y el spyware. Puede decidir la frecuencia con la que MMS realizará análisis en busca de malware, qué partes del teléfono se analizan y qué eventos activan un análisis antivirus automático.
- Definir la frecuencia con que MMS actualiza la protección y otras muchas opciones.

¿Puede proteger también MMS mi tarjeta SIM?

No. MMS no ofrece seguridad para la tarjeta SIM. Sin embargo, si pierde el dispositivo y la tarjeta SIM, puede utilizar MMS para proteger el dispositivo. Después puede llamar a su proveedor de servicios inalámbricos para desactivar la tarjeta SIM.

¿Tengo garantizada la recuperación de mi teléfono?

Lamentablemente, McAfee no puede garantizarle que vaya a recuperar su dispositivo móvil. Le recomendamos crear una copia de seguridad de los datos automáticamente para que siempre pueda acceder a la información importante. Si pierde el dispositivo móvil, podrá bloquearlo de forma remota para que no se pueda acceder a él.

Análisis de seguridad

¿Qué tipo de software malicioso puede detectar MMS?

MMS protege su dispositivo móvil del malware para móviles y otras amenazas digitales, incluidos virus, gusanos, spyware, registradores de pulsaciones de teclado, bots y programas potencialmente no deseados.

NOTA: Si utiliza un dispositivo Android, MMS también bloqueará el acceso a los sitios peligrosos si emplea el navegador web predeterminado de Android.

¿Con qué frecuencia realiza análisis MMS en busca de virus?

MMS analiza automáticamente el dispositivo en tiempo real. Cuando se recibe un mensaje, se accede a un archivo o se instala una aplicación, se realiza un análisis instantáneo. Además, MMS analiza el dispositivo según una planificación establecida. Si sospecha que su dispositivo móvil está infectado, puede realizar un análisis manual en cualquier momento.

¿Qué partes del dispositivo analiza MMS?

El análisis comprueba el sistema de archivos del dispositivo móvil. Esto incluye mensajes, imágenes, aplicaciones instaladas y archivos comprimidos.

NOTA: Tenga en cuenta que las funciones de protección pueden variar según el dispositivo.

¿Analiza MMS el contenido de los mensajes y los datos adjuntos?

Sí. McAfee analiza los mensajes como, por ejemplo, los SMS, los MMS, el correo electrónico y los datos adjuntos en cuanto llegan al dispositivo.

NOTA: El correo electrónico no se analiza en los dispositivos Android.

¿Detecta MMS los virus en la tarjeta de memoria?

Sí. MMS analiza el contenido de la tarjeta de memoria SD. Es posible configurar MMS para analizar las tarjetas de memoria SD que se inserten en el dispositivo.

¿Puede MMS detener los intentos inalámbricos de hacking?

McAfee impide la descarga de aplicaciones maliciosas e infectadas. MMS también le protege de los sitios web peligrosos a los que podría acceder mediante el navegador móvil, pero no bloquea las comunicaciones

enviadas mediante Wi-Fi, Bluetooth o IrDA.

¿Qué ocurre cuando MMS detecta un virus?

MMS muestra una advertencia a pantalla completa y permite eliminar, poner en cuarentena, reparar o ignorar el archivo infectado. Puede decidir cuándo se le notificarán las amenazas y cómo desea responder a ellas.

NOTA: Si tiene un dispositivo Android, no podrá reparar los archivos infectados. Solo podrá eliminarlos o ignorarlos.

He ignorado una advertencia sobre virus anteriormente. ¿Cómo puedo eliminar el virus?

Puede ejecutar un análisis manual para ver la advertencia de nuevo. Si ignora una aplicación maliciosa, MMS le recordará automáticamente que es necesario solucionar la amenaza la siguiente vez que reinicie, o bien cuando se lleve a cabo un análisis del sistema planificado.

Hace tiempo que no compruebo si hay actualizaciones de MMS. ¿Sigo estando protegido?

Sí. MMS mantiene su protección al día al actualizar de forma automática y periódica los archivos DAT. Puede configurar MMS para que se actualice con la frecuencia que más le convenga. También puede buscar actualizaciones en cualquier momento desde el menú de la aplicación.

¿Cómo puedo ver cuándo se actualizó MMS por última vez?

Puede consultar el archivo de registro desde el menú de la aplicación para ver todos los eventos relacionados con MMS. El archivo de registro incluye eventos como, por ejemplo, el último análisis, la última actualización y las detecciones de virus. También puede restablecer el archivo de registro cuando lo desee.

¿Cuánto espacio necesitan las actualizaciones de la protección?

Las actualizaciones de la protección ocupan menos de 5 KB. Puede cambiar la frecuencia de actualización en la configuración de la aplicación.

Protección/Privacidad de las aplicaciones

IMPORTANTE: La función Protección de aplicaciones solo está disponible en **dispositivos Android** con MMS 2++ instalado. Esta función también se denomina **Privacidad de las aplicaciones**.

¿Qué es Protección/Privacidad de las aplicaciones?

Esta función comprueba las aplicaciones del dispositivo móvil y permite conocer el tipo de datos personales y

funciones del dispositivo a los que pueden acceder y que pueden modificar. Por ejemplo, algunas aplicaciones pueden acceder a su ubicación, contactos, red, calendario y contraseñas; mientras que otras pueden acceder al micrófono, la cámara o la función de GPS.

Con Privacidad de las aplicaciones obtiene información inteligente y actualizada sobre sus aplicaciones, con iconos fáciles de entender que muestran el tipo de información a la que puede acceder cada aplicación en el dispositivo. Esto le permite conservar las aplicaciones de confianza y eliminar las que piense que comparten demasiados datos personales.

¿Qué me puede decir Protección/Privacidad de las aplicaciones sobre una aplicación instalada en mi dispositivo móvil?

Protección de aplicación proporciona descripciones sobre los tipos de datos personales o funciones a los que puede acceder una aplicación en el dispositivo móvil.

¿Por qué algunas aplicaciones son de confianza antes de que las revise?

Protección de aplicaciones califica automáticamente como de confianza las siguientes aplicaciones:

- Aplicaciones de McAfee
- Aplicaciones que no acceden a los datos personales
- Aplicaciones previamente cargadas por el fabricante del dispositivo
- Aplicaciones que forman parte del sistema operativo Android

Una aplicación de confianza, ¿debe revisarse de nuevo cuando se actualiza?

Si actualiza una aplicación de confianza que tiene acceso a sus datos personales, Protección de aplicaciones le pedirá que la revise.

Creo que una de mis aplicaciones está accediendo a demasiados datos. ¿Qué puedo hacer?

Si se da cuenta de que una aplicación puede acceder a más datos personales o funciones de los que pensaba, Protección de aplicaciones permite eliminarla rápidamente del dispositivo móvil.

¿Puede Protección de aplicaciones analizar mi dispositivo móvil en busca de virus y otras amenazas?

Protección de aplicación no analiza el dispositivo en busca de amenazas tales como virus, troyanos o spyware. No obstante, la función Análisis de seguridad analiza el dispositivo en busca de amenazas y mantiene la protección.

Bloqueo

¿Puedo bloquear mi dispositivo de forma remota en caso de pérdida o robo?

Sí. Puede enviar mensajes de texto al dispositivo móvil para controlarlo remotamente. Para bloquear el dispositivo, envíe **Secure lock [Código PIN]**. Por ejemplo,**Secure lock 123456**.

Puede mostrar un mensaje en el dispositivo bloqueado enviando **Secure lock [Código PIN] [MENSAJE]**. Por ejemplo,**Secure lock 123456 Llame al 1-800-555-5555 para devolverlo**.

¿Qué diferencia hay entre el bloqueo incorporado de mi dispositivo móvil y el bloqueo de MMS?

El bloqueo de MMS permite controlar el dispositivo móvil de forma remota. También permite mostrar un mensaje en el dispositivo móvil para solicitar su devolución (tal y como se muestra más arriba).

Además, MMS le indica cuándo se ha bloqueado el dispositivo móvil para que esté tranquilo al saber que está realmente protegido.

¿Puedo enviar una alarma remota a mi dispositivo?

Sí, puede. Inicie sesión en su cuenta de McAfee Mobile Security online. Seleccione la opción **Alarma** o **Bloqueo y alarma.**

Rastreo

Tengo el número de dispositivo del ladrón; ¿qué puedo hacer?

McAfee le recomienda presentar una denuncia ante la policía o el organismo local.

¿Qué rastrea MMS?

MMS permite realizar un rastreo de todas las actividades efectuadas en el dispositivo móvil. En la página de **rastreo** se puede ver cuándo se inserta una tarjeta SIM nueva en el dispositivo. También se puede usar la función de copia de seguridad para realizar un rastreo de todos los mensajes de texto enviados y recibidos, así como ver todas las llamadas entrantes y salientes. Esto le proporciona un registro del uso propio o un rastreo del número de dispositivo de un ladrón.

¿Puedo rastrear la ubicación geográfica de mi dispositivo móvil?

Sí. Puede ver la ubicación del dispositivo móvil en tiempo real desde el sitio web de MMS. Basta con acceder

a https://www.mcafeemobilesecurity.com/, iniciar sesión y hacer clic en **Ubicación**.

Copia de seguridad, carga, restauración y borrado

¿De qué tipos de datos puedo crear copias de seguridad? ¿Cuáles puedo cargar, restaurar y borrar?

- **Copia de seguridad:** contactos, mensajes de texto, registros de llamadas y elementos de calendario.
- **Carga:** fotos y vídeos.
- **Restauración:** contactos, mensajes de texto y elementos de calendario.
- **Borrado:** contactos, mensajes de texto, mensajes de correo electrónico, elementos de calendario, fotos, vídeos y la tarjeta de memoria.

¿Cómo se crean copias de seguridad de los datos?

Es posible crear una copia de seguridad de los datos desde el dispositivo móvil o en el sitio web de MMS. También puede configurar la aplicación MMS para que cree una copia de seguridad de los datos automáticamente. A continuación se explica cómo:

- **Copia de seguridad manual desde el dispositivo móvil:** en la aplicación MMS del dispositivo móvil, seleccione **Copia de seguridad** y elija los datos que desee incluir en la copia.
- **Copia de seguridad manual desde el sitio web de MMS:** inicie sesión en el sitio web de MMS, seleccione **Copia de seguridad** y elija los datos que desee incluir en la copia.
- **Copia de seguridad automática:** en la aplicación MMS del dispositivo móvil, seleccione **Copia de seguridad**. En el menú Configuración, seleccione **Copia de seguridad automática** y elija la frecuencia con la que desea que se cree una copia de seguridad automática. Solo se hará copia de seguridad de los datos nuevos, de modo que no tiene que preocuparse de que esté haciendo un uso excesivo del servicio GPRS.

  NOTA: Si tiene un dispositivo Android, la copia de seguridad automática se realizará una vez al día. Para ahorrar batería, la copia de seguridad automática se realiza únicamente mientras se está cargando el dispositivo.

¿Supone algún coste de tráfico de datos la creación de una copia de seguridad o la restauración de los datos?

No hay ningún cargo adicional por utilizar MMS para crear copias de seguridad de los datos o restaurarlos. No

obstante, en función de su plan de datos, es posible que incurra en cargos de datos adicionales por parte del proveedor de servicios inalámbricos. Asimismo, si se encuentra fuera de Singapur, EE. UU. y el Reino Unido, es posible que el operador le cobre los mensajes de texto internacionales al enviar comandos desde el sitio web al dispositivo móvil.

Filtro de llamadas y SMS

IMPORTANTE: La función de filtrado de llamadas y mensajes está disponible para los teléfonos inteligentes Android y las tabletas Android con capacidad para realizar llamadas.

¿Qué es Filtro de llamadas y SMS?

El filtrado de llamadas y mensajes permite bloquear las llamadas y los mensajes de texto de números no deseados. Se pueden elegir los números de teléfono que se bloquearán o permitir solamente que ciertos números le envíen llamadas o mensajes de texto.

¿Cómo se agregan números nuevos al filtro de llamadas y SMS?

El filtrado de llamadas y mensajes permite importar números de los registros de llamadas, la lista de mensajes o los contactos. También se pueden introducir los números manualmente.

¿Qué son las listas Permitidos y Bloqueados?

- La lista Permitidos es la lista de números de teléfono que pueden llamarle o enviarle mensajes de texto.
- La lista Bloqueados es la lista de números de teléfono que no pueden llamarle ni enviarle mensajes de texto.

¿Cómo bloquea las llamadas el filtro de llamadas y SMS?

Cuando el filtro de llamadas y mensajes identifica que una llamada procede de un número incluido en la lista Bloqueados, la llamada se desvía al buzón de voz o se rechaza. Si la llamada se rechaza, el emisor oirá el tono de ocupado. Puede cambiar las opciones de bloqueo en la configuración del filtro de llamadas y mensajes. También puede ver todas las llamadas bloqueadas en el registro.

¿Cómo bloquea los mensajes de texto el filtro de llamadas y SMS?

Cuando el filtro de llamadas y mensajes identifica que un mensaje de texto procede de un número incluido en la lista Bloqueados, el mensaje se elimina o se mueve a la carpeta que indique. Puede cambiar las opciones de

bloqueo en la configuración del filtro de llamadas y mensajes. También puede ver los mensajes de texto bloqueados en el registro.

NOTA: Aunque el filtro de llamadas y mensajes bloquee el mensaje de texto, seguirá llegando al dispositivo, por lo que es posible que algunos proveedores de servicios inalámbricos le cobren por recibirlo.

Protección web

IMPORTANTE: Las funciones descritas en esta sección solo son aplicables a usuarios con MMS instalado en dispositivos Android.

¿Cómo me protege MMS frente a los sitios web maliciosos y los intentos de phishing?

Cuando se navega por Internet mediante un navegador de Android, MMS bloquea automáticamente los sitios web maliciosos a través de la tecnología de McAfee SiteAdvisor. SiteAdvisor ofrece protección en tiempo real frente al phishing móvil y los exploits del navegador. Además, MMS proporciona calificaciones de seguridad de sitios web para los sitios visitados.

¿Con qué frecuencia actualiza McAfee su protección frente a sitios peligrosos nuevos?

McAfee detecta miles de amenazas nuevas todos los días y actualiza la base de datos de calificaciones de sitios web cada hora. Además, MMS incluye actualizaciones diarias de la protección frente a las amenazas conocidas del navegador.

Miscelánea

¿Hasta qué punto están seguros mis datos?

Nuestros servidores y nuestras comunicaciones emplean tecnología con estándares tan estrictos como los utilizados por bancos o empresas de tarjetas de crédito. Parte de la tecnología de MMS se desarrolló inicialmente para la policía y el ejército, y dispone de toda la seguridad de cifrado y comunicaciones necesarias para garantizar que nadie pueda ver su contenido privado (ni siquiera nuestro personal). No se ha registrado ningún caso de pérdida de privacidad o de integridad de los datos. Dispondrá de un control total, ya que los datos se cargan únicamente si usted decide hacerlo.

Si tiene alguna duda, puede optar por no emplear la función de carga de datos.

Me preocupan los cargos por transferencia de datos. En MMS, ¿se utiliza 3G o GPRS?

Utilizamos una conexión de datos para actualizar la protección, así como para crear copias de seguridad de los

datos y restaurarlos, así que podría incurrir en gastos por tráfico de datos. Sin embargo, puede decidir con qué frecuencia se deben producir las actualizaciones de la protección y cuándo desea crear una copia de seguridad de los datos o restaurarlos a fin de minimizar los cargos por datos. Compruebe las condiciones y las tarifas de uso de datos de su proveedor de servicios inalámbricos. También podría producirse un uso de datos mínimo cuando el dispositivo móvil informa al servidor de su estado, de igual manera que si el dispositivo móvil estuviera bloqueado.

¿Qué significan "3G" y "GPRS"?

General Packet Radio Service (GPRS) y 3G son servicios de datos para el dispositivo móvil que permiten utilizar Internet, enviar mensajes MMS y otras actividades que requieren la transferencia de datos en el dispositivo móvil.

¿Cómo se configuran los servicios 3G y GPRS?

En los dispositivos móviles más recientes, los servicios 3G y GPRS ya están configurados. Si no es el caso en su dispositivo móvil, póngase en contacto con su proveedor de servicios inalámbricos para que le ayude a configurarlos.

¿Existe alguna lista de todos los comandos remotos?

Puede enviar los siguientes comandos remotos a su dispositivo:

Bloqueo del Dispositivo		
Secure lock [Código PIN]	bloquea tu dispositivo	Secure lock (SEGURIDAD BLOQUEAR) 123456
Secure lock [Código PIN] [Mensaje]	Muestra un mensaje personalizado en la pantalla cuando bloqueas el dispositivo	Secure lock (SEGURIDAD BLOQUEAR) 123456 Este teléfono está bloqueado
Secure lock alarm [Código PIN]	bloquea el dispositivo y activa una alarma	Secure lock alarm (SEGURIDAD BLOQUEAR ALARMA) 123456
Secure lock alarm [Código PIN] [Mensaje]	bloquea el dispositivo con una alarma y muestra un mensaje personalizado	Secure lock alarm (SEGURIDAD BLOQUEAR ALARMA) 123456 Este teléfono está bloqueado
Restablecimiento del dispositivo		

Secure reset [Código PIN]	Restablece la configuración de fábrica del dispositivo	Secure reset (SEGURIDAD RESTABLECER) 123456
Desbloqueo del dispositivo		
Secure unlock [Código PIN]	desbloquea el dispositivo	Secure unlock (SEGURIDAD DESBLOQUEAR) 123456
Localización del dispositivo		
Secure locate [Código PIN]	localizar el dispositivo. Tras enviar el mensaje al dispositivo, este te devolverá un mensaje de texto con el vínculo de la ubicación del dispositivo	Secure locate (SEGURIDAD LOCALIZAR) 123456
Borrado de los datos del dispositivo		
Secure wipe [Código PIN]	limpiará todos los datos del dispositivo. Recuerda que se borrarán todos los contactos, mensajes de texto, registros de llamadas, fotos y vídeos del dispositivo, y de la tarjeta SD.	Secure wipe (SEGURIDAD BORRAR) 123456
Activación de la alarma		
Secure alarm [Código PIN]	Sonará la alarma. Recuerda que esta alarma solo durará 60 segundos.	Secure lock (SEGURIDAD ALARMA) 123456
Uso del CaptureCam para ver quién tiene el dispositivo		
Secure message [Código PIN]	Envía un mensaje al dispositivo que se te ha perdido para ver quién lo tiene. Cuando alguien pulse la pantalla o cualquier tecla, CaptureCam hará uma foto y te la enviará por correo electrónico junto con un mapa de la ubicación del dispositivo.	Secure message (SEGURIDAD MENSAJE) 123456

Seguridad de Wi-Fi

La función de seguridad de Wi-Fi de MMS le informa de si la red Wi-Fi a la que está conectado es segura o no. Esto evita que posibles intrusos escuchen su tráfico web mediante la detección periódica de falsificación del protocolo de resolución de direcciones.

La seguridad de Wi-Fi forma parte del componente de seguridad web y puede activarse/desactivarse desde la configuración de seguridad web. De forma predeterminada, esta protección está activada.

Cuando el dispositivo se conecta a una red Wi-Fi, aparece un mensaje que le informa de si la conexión es segura.

Si MMS detecta algún problema de seguridad con la red Wi-Fi, se muestra otro mensaje, y es posible que se cancele la conexión de manera automática para garantizar su protección. Esto le permite comprobar si la conexión es segura. Una vez verificada la conexión, podrá volver a conectarse a su red Wi-Fi preferida cuando quiera.

7. McAfee Mobile Security: Cómo configurar los controles de privacidad sobre las aplicaciones

Entorno

Dispositivos móviles implicados:

Android

Resumen

¿Qué es Perfil de aplicaciones?

Los controles de privacidad sobre las aplicaciones de McAfee Mobile Security (también conocidos como “Perfil de aplicaciones”) le permiten compartir o restringir el acceso a las aplicaciones instaladas cuando otras personas utilicen su dispositivo. En cada perfil que configure, deberá seleccionar las aplicaciones que desea que estén disponibles. Todas las demás aplicaciones estarán ocultas y protegidas mediante un código PIN. Tras configurar un perfil, podrá alternar de uno a otro en función del acceso que desee permitir.

Mobile Security ofrece cuatro perfiles. No puede crear más, pero puede cambiar el nombre de cualquiera de ellos, excepto del perfil Sin restringir:

- **Sin restringir:** no se puede editar y permite acceder a todas las aplicaciones del dispositivo.
- **Oficina:** está vacío hasta que seleccione las aplicaciones que abarcará (protegido con código PIN).
- **Niños:** está vacío hasta que seleccione las aplicaciones que abarcará.
- **Invitado:** está vacío hasta que seleccione las aplicaciones que abarcará (protegido con código PIN).

En algunos casos concretos, las aplicaciones protegidas estarán visibles, pero deberá introducir el código PIN de MMS para abrirlas. Una vez abierta, la aplicación seguirá sin protección mientras permanezca abierta o hasta que se agote el tiempo de espera.

Ejemplos:

- Si configura un perfil de aplicaciones y selecciona MMS para que sea el selector (solo una vez), podrá ver las aplicaciones del perfil. Si pulsa la tecla de inicio y selecciona un selector distinto de MMS, todas las aplicaciones estarán visibles, pero deberá proporcionar el código PIN para acceder a la que no estén seleccionadas dentro del perfil.

- Si configura un perfil de aplicaciones y selecciona el selector de Android (Siempre o Solo una vez), cuando intente acceder a cualquier aplicación que no forme parte del perfil, deberá introducir el código PIN de MMS PIN para continuar. Estas circunstancias también se aplican al acceder a las aplicaciones por medio de notificaciones o manteniendo pulsada la tecla de inicio.

Solución

Para configurar un perfil de aplicaciones

Configurar un perfil de aplicaciones le permite administrar el dispositivo para impedir que nadie lo utilice para acceder a sus aplicaciones personales, de forma que estas permanezcan en privado.

1. Seleccione **Privacidad** en la pantalla de inicio de MMS y seleccione **Establecer perfil** en Control de privacidad.
2. Seleccione el perfil que desee configurar y el símbolo "**>**" (comillas angulares).
3. Introduzca el código PIN de seis dígitos cuando se le solicite.
4. Seleccione las aplicaciones que desea que estén disponibles para ese perfil.
5. Pulse **Guardar**.

Para seleccionar un perfil de aplicaciones

1. Seleccione **Privacidad** en la pantalla de inicio de MMS y seleccione **Establecer perfil**.
2. Seleccione el perfil que desee configurar.
3. Pulse **Establecer**.
4. Introduzca el código PIN de seis dígitos cuando se le solicite.

Para cambiar el perfil de aplicaciones configurado

1. Haga clic en **Cambiar perfil** y seleccione el perfil al que desea pasar.
2. Introduzca el código PIN de seis dígitos cuando se le solicite.

Para cambiar el nombre de un perfil

1. Seleccione **Privacidad** en la pantalla de inicio de MMS y seleccione **Establecer perfil**.
2. Seleccione **Cambiar nombre** junto al nombre del perfil que aparece en la parte superior y escriba el nuevo nombre.

   NOTA: Los nombres de perfil deben contener como máximo 10 caracteres. **Se pueden** utilizar números, símbolos y caracteres especiales en los nombres de perfil.

De forma predeterminada, la función **Requerir código PIN para acceder a este perfil** está activada. Esto impide que los usuarios puedan cambiar de perfil sin su permiso. Puede desactivar el parámetro **Requerir código PIN para acceder a este perfil** si no desea obligar a los usuarios a introducir el código PIN de MMS antes de que cambien de perfil.

8. Cómo utilizar su suscripción existente de Mobile Security con un dispositivo nuevo

Resumen

Este artículo le ayudará a mover una suscripción de producto móvil existente a un teléfono inteligente o una tableta nuevos.

Solución

Para actualizar su cuenta de Mobile Security con la información del teléfono nuevo, siga estos pasos:

NOTA: En cuanto transfiera su suscripción de Mobile Security al dispositivo nuevo, el anterior dejará de estar protegido.

1. Descargue e instale Mobile Security en el dispositivo. Para obtener las instrucciones de descarga, consulte el artículo TS101406.
2. Abra Mobile Security y utilice la opción **Iniciar sesión** para activarlo.
3. Seleccione el país adecuado.
4. Escriba su dirección de correo electrónico y contraseña de McAfee.

   NOTA: Seleccione **Mostrar contraseña** para ver los caracteres reales.

5. Haga clic en **Continuar**.
6. Seleccione la suscripción disponible que desee usar.
7. Haga clic en **Continuar**.

8. Escriba su número de teléfono (opcional).
9. Escriba y verifique el código PIN de la cuenta de Mobile Security existente.
10. Haga clic en **Continuar**.
11. Seleccione **Activar** o **Cancelar** en la pantalla Establecimiento del administrador del dispositivo.

Para actualizar su cuenta de Mobile Security con la información de la nueva tableta, descargue e instale Mobile Security con su cuenta actual.

Información relacionada

Si ha adquirido un teléfono usado, puede que reciba el siguiente mensaje de error:

Este dispositivo se ha registrado anteriormente con una tarjeta SIM diferente.
Para continuar McAfee Mobile Security, use esa tarjeta SIM.
Si ya no dispone de esa tarjeta SIM, póngase en contacto con el soporte técnico.

Si ha adquirido una tableta usada, puede que reciba el siguiente mensaje de error:

Este dispositivo se ha registrado anteriormente con una dirección de correo electrónico diferente.
Utilice esa cuenta de McAfee Security para registrar este dispositivo.

Esto quiere decir que el anterior propietario instaló y activó Mobile Security en el dispositivo.

Póngase en contacto con el propietario anterior y obtenga la siguiente información:

- Nombre de usuario original (número de teléfono para teléfonos inteligentes y dirección de correo electrónico para tabletas)
- El nombre de uno de los contactos del propietario anterior

Si no puede ponerse en contacto con el propietario anterior para desbloquear el teléfono, póngase en contacto con el Soporte técnico de McAfee en http://service.mcafee.com y asegúrese de tener disponible la información siguiente:

En el caso de teléfonos inteligentes:

- El número IMEI del dispositivo anterior
- El número IMEI del dispositivo nuevo
- El número de teléfono registrado

En el caso de tabletas:

- El número IMEI e ID de Android del dispositivo anterior
- El número IMEI e ID de Android del dispositivo nuevo
- La dirección de correo electrónico registrada

NOTA: Informe al agente de soporte técnico de si ha instalado el producto independiente Mobile Security. No se permiten cambios de dispositivo en cuentas de tipo **Completa e ilimitada**.

9. La instalación de software de McAfee falla con el error: Instalación incompleta

Resumen

Cuando intenta descargar e instalar McAfee LiveSafe, Total Protection o uno de nuestros productos de seguridad para Windows, la instalación falla y se muestra el mensaje de error:

Instalación incompleta

Siga los pasos de la **solución 1** para resolver el problema. Si eso no da resultado, siga los pasos de la **solución 2**.

También debería hacer lo siguiente:

- Guarde y cierre todas las aplicaciones y los archivos abiertos.
- Reinicie el equipo.
- Asegúrese de tener una conexión de red. Es preferible una conexión por cable.
- Utilice una fuente de alimentación si utiliza un portátil.

Requisitos previos:

- ¿Cumple su PC con los **requisitos mínimos del sistema**?
    - TS102471: Requisitos mínimos del sistema para las suites de seguridad de McAfee en Windows y Mac
- ¿Hay algún **firewall o software de seguridad de terceros no compatible** instalado?
    - Encontrará una lista de aplicaciones, así como instrucciones para eliminarlas, en TS102253
- ¿Está Windows actualizado en el PC?
    - Para buscar e instalar actualizaciones, consulte Windows Update: preguntas frecuentes en el sitio web de Microsoft.

Solución 1

Siga los pasos en el orden indicado. Cuando haya completado cada paso, vuelva a intentar instalar el producto de McAfee. Si la instalación vuelve a fallar, continúe con el siguiente paso.

Paso 1: Ejecutar Pre-Install ToolLa herramienta Pre-Install Tool prepara el PC para la instalación.

1. Descargue Pre-Install Tool.
   NOTA: Guarde el archivo en una ubicación temporal, como por ejemplo el escritorio.

Vuelva a intentar instalar el producto. Si la instalación falla, continúe con el **paso 2**.

Paso 2: Activar temporalmente la cuenta de administradorLa instalación podría fallar porque la cuenta de Windows con la que inicia sesión carece de permisos. Siga estos pasos para activar temporalmente la cuenta de administrador integrada, y luego inicie sesión e intente realizar la instalación con esa cuenta:

1. Abra el símbolo del sistema como **administrador**:
   a. Haga clic en **Inicio** y escriba **cmd.exe** en el cuadro de búsqueda.
   b. En los resultados de búsqueda, haga clic con el botón derecho en **Símbolo del sistema** y seleccione **Ejecutar como administrador**.
2. Escriba el siguiente comando en el símbolo del sistema y pulse INTRO:

   net user administrator /active:yes
3. Cierre el símbolo del sistema.
4. Pulse simultáneamente las teclas **CTRL+ALT+SUPR**.
5. Haga clic en **Cerrar sesión** para cerrar la sesión en Windows.
6. En la pantalla de inicio de sesión, haga clic en la cuenta de **administrador** e inicie sesión. El proceso de inicio de sesión puede tardar más de lo normal en completarse.

Intente realizar la instalación de nuevo, siguiendo los pasos indicados en TS100342. Si la instalación falla, continúe con el **paso 3**.

IMPORTANTE: Si la instalación se realiza correctamente, siga los pasos a continuación para desactivar la cuenta de administrador integrada.

Paso 3: Descargar y ejecutar la herramienta de desinstalación McAfee Consumer Product Removal

(MCPR)0MCPR elimina el producto de McAfee existente y archivos "residuales" de instalaciones anteriores que podrían dar lugar a problemas de instalación.

Intente realizar la instalación de nuevo, siguiendo los pasos indicados en TS100342. Si la instalación falla, continúe con la**solución 2**.

IMPORTANTE: Si la instalación se realiza correctamente, siga los pasos a continuación para desactivar la cuenta de administrador integrada. Si había activado la cuenta de administrador integrada durante el procedimiento anterior, **acuérdese de desactivarla** una vez instalado el software de McAfee:

Cómo desactivar la cuenta de administrador

1. Pulse simultáneamente las teclas **CTRL+ALT+SUPR**.
2. Haga clic en **Cerrar sesión** para cerrar la sesión en la cuenta de administrador.
3. Inicie sesión con su cuenta habitual.
4. Abra el símbolo del sistema como **administrador**:
    a. Haga clic en **Inicio** y escriba **cmd.exe** en el cuadro de búsqueda.
    b. En los resultados de búsqueda, haga clic con el botón derecho en **Símbolo del sistema** y seleccione **Ejecutar como administrador**.
5. Escriba el siguiente comando en el símbolo del sistema y pulse INTRO:

    net user administrator /active:no
6. Cierre el símbolo del sistema.

La cuenta de administrador quedará desactivada.

Solución 2

Si sigue sin poder instalar el producto a pesar de haber realizado los procedimientos indicados, utilice una de estas herramientas o servicios de McAfee para comprobar si su PC está infectado por malware:

- **GetSusp:**
  Utilice McAfee GetSusp si sospecha de la existencia de malware en el equipo. GetSusp también ayuda a aislar malware no detectado. Haga clic para descargar GetSusp.

- **McAfee Stinger:**
  Stinger es una utilidad independiente de McAfee Labs que sirve para detectar y eliminar virus concretos. Para obtener más información sobre Stinger, consulte: TS100815.

10. Cómo eliminar productos de McAfee de un PC con Windows

Resumen

Este artículo describe cómo eliminar o desinstalar un producto de McAfee para particulares de un PC con Windows mediante los pasos de eliminación estándar de Windows y la herramienta MCPR de McAfee.

- Para eliminar de un Mac, consulte TS101226.
- Para eliminar de un PC que ejecuta Linux, consulte TS101168.
- Para eliminar de iOS o Android, consulte TS101407.

Solución

IMPORTANTE: Si su producto de McAfee vino **preinstalado** en el equipo:

- Active la suscripción de McAfee **antes** de intentar eliminar el producto.
  Esto es para que conserve su derecho a usar el producto (la licencia) sin tener que adquirir una nueva suscripción.
- Para activar el software de McAfee que vino preinstalado, consulte TS102477.

Paso 1: Eliminar con Windows

El método de eliminación estándar de Windows es la mejor manera de desinstalar los productos de McAfee.

Haga clic en el vínculo correspondiente a su versión de Windows. Se le dirigirá a Microsoft.com.
Siga los pasos de eliminación de Microsoft:

- Windows 10
- Windows 8, 8.1
- Windows 7 o Vista

Si la **eliminación se realiza correctamente**, los productos de McAfee ya están eliminados de su PC.

IMPORTANTE: Su PC dejará de estar protegido contra virus y malware. Asegúrese de volver a instalar el software de seguridad lo antes posible para restaurar la protección.

Si la **eliminación falla** con el método de eliminación estándar de Windows, vaya al Paso 2.

Paso 2: Descargar y ejecutar la herramienta de desinstalación McAfee Consumer Product Removal (MCPR)

Solo debe utilizar la herramienta MCPR si los métodos de eliminación de Windows especificados anteriormente no funcionan.

Asistente virtual

Si desea obtener asistencia al ejecutar MCPR, utilice el Asistente virtual.

NOTA: Al hacer clic en el vínculo anterior, se abrirá una ventana nueva. Siga las indicaciones. Cuando haya completado todos los pasos, cierre la ventana.

11. Cómo activar o desactivar el firewall

Resumen

Siga los pasos indicados en la Solución para activar y/o desactivar el firewall en su producto de seguridad de McAfee.

Solución

Para desactivar el firewall:

1. Abra el producto.
2. Haga clic en **Navegación** (o haga clic en la rueda dentada de la esquina superior derecha).
3. Haga clic en **Firewall**.
4. Haga clic en **Desactivar**.

El icono se volverá gris y mostrará un símbolo de exclamación rojo y blanco. Además, la barra de color de SecurityCenter se volverá roja y le informará de que su equipo está en peligro. Ambos problemas se resolverán al volver a activar el firewall.

Para activar el firewall:

1. Abra el producto.
2. Haga clic en **Navegación** (o haga clic en la rueda dentada de la esquina superior derecha).
3. Haga clic en **Firewall**.
4. Haga clic en **Activar**.

ID de documento anterior: 101068

12. Cómo desinstalar McAfee WebAdvisor o SiteAdvisor

Resumen

Siga estos pasos para eliminar (desinstalar) McAfee WebAdvisor o SiteAdvisor.

NOTA: WebAdvisor es compatible con Windows 7, 8 y 10. Si su PC ejecuta Windows XP o Vista, se instalará SiteAdvisor en vez de WebAdvisor.

WebAdvisor y SiteAdvisor pueden instalarse como:

- Una aplicación independiente
- Una parte integrada de una suite de seguridad de McAfee

Siga los pasos para su tipo de instalación.

Si solo desea desactivar su protección **temporalmente**, utilice la primera opción. Esto desactivará el complemento del navegador sin desinstalar el programa.

¿Qué desea hacer?

Apagar temporalmente (desactivar) el complemento del navegador WebAdvisor o SiteAdvisor

IMPORTANTE: Después de seguir estos pasos, recuerde encender (activar) la extensión nuevamente para permanecer protegido.

Uso Google Chrome

1. Abra **Chrome**.
2. Haga clic en el icono de menú en la esquina superior derecha (tres puntos apilados verticalmente).

3. Haga clic en **Más herramientas**, **Extensiones**.
4. Elimine la **marca** junto a **McAfee WebAdvisor** o **SiteAdvisor**.

Uso Internet Explorer

1. Abra **Internet Explorer**.
2. Haga clic en el menú **Herramientas**.
3. Seleccione **Administrar complementos**.
4. Seleccione el complemento **McAfee WebAdvisor** o **SiteAdvisor** y haga clic en **Desactivar**.

Uso Firefox

1. Abra Firefox.
2. Haga clic en el icono de menú apilado en la esquina superior derecha.
3. Seleccione **Complementos**.
4. Haga clic en **Desactivar** junto a **McAfee WebAdvisor** o **SiteAdvisor**.

Eliminar SiteAdvisor o WebAdvisor (versión independiente)**IMPORTANTE**: Después de seguir estos pasos, asegúrese de volver a instalar el producto lo antes posible para permanecer protegido (consulte Información relacionada, a continuación).

Eliminar de Windows

1. Cierre todos los navegadores web.
2. Haga clic en el botón **Inicio** en la esquina inferior izquierda del escritorio de Windows.
3. En el cuadro de búsqueda:
    a. Escriba **Panel de control**.
    b. Pulse INTRO
4. En el **Panel de control**:
    a. Haga doble clic en **Programas y características** (o **Agregar o quitar programas**).
    b. Seleccione **McAfee WebAdvisor** (o **McAfee SiteAdvisor**) en la lista de programas.

c. Haga clic en **Desinstalar/Modificar** (o **Eliminar**).

5. Reinicie el equipo.

Eliminar de Mac

NOTA: Estos pasos se aplican únicamente a SiteAdvisor. WebAdvisor no está disponible para macOS.

1. Haga clic en **Ir**, **Aplicaciones**.
2. Navegue a la carpeta **/Aplicación/SiteAdvisor**.
3. Haga doble clic en **desinstalar .tgz** para descomprimirlo.
4. Haga doble clic en el archivo de **desinstalación**.
5. Siga las instrucciones para completar la desinstalación.

Eliminar de AndroidSiteAdvisor ya no está disponible como producto independiente para Android; se ha integrado en la suite de McAfee Mobile Security (MMS).

Para desinstalar SiteAdvisor de Android, debe desinstalar MMS. Para obtener instrucciones, consulte el artículo TS101407.

NOTA: SiteAdvisor no está disponible para iOS.

Desinstale SiteAdvisor o WebAdvisor (integrados con la suite de seguridad)

IMPORTANTE: Después de seguir estos pasos, asegúrese de volver a instalar el producto lo antes posible para permanecer protegido (consulte Información relacionada, a continuación).

Eliminar de Windows

1. Cierre todos los navegadores web.
2. Haga clic en el botón **Inicio** en la esquina inferior izquierda del escritorio de Windows.
3. En el cuadro de búsqueda:
   a. Escriba **Panel de control**.
   b. Pulse INTRO.

4. En el **Panel de control**:

a. Haga doble clic en **Programas y características** (o **Agregar o quitar programas**).
b. Seleccione **McAfee SiteAdvisor** (o **McAfee WebAdvisor**) de la lista.
c. Haga clic en **Desinstalar/Modificar** o **Eliminar**.
d. Cuando se le solicite, seleccione **solo** la casilla de verificación situada junto a **SiteAdvisor** (o **McAfee WebAdvisor**).
e. Haga clic en **Desinstalar** (o **Eliminar**).

5. Reinicie el equipo.

Eliminar de MacSiteAdvisor es una parte integrada de Internet Security for Mac.

Para desinstalar SiteAdvisor también debe desinstalar Internet Security for Mac. Para obtener instrucciones, consulte el artículo TS101226.

Eliminar de AndroidSiteAdvisor es una parte integrada de la suite McAfee Mobile Security.

Para desinstalar SiteAdvisor de Android, debe desinstalar toda la suite. Para obtener instrucciones, consulte el artículo TS101407.

NOTA: SiteAdvisor no está disponible para iOS.

13. Cómo gestionar y restaurar archivos y programas en cuarentena

Resumen

Las suites de seguridad de McAfee para Windows y macOS contienen un programa llamado VirusScan que analiza y protege su equipo. Cuando se analiza un archivo o programa, VirusScan lo compara con amenazas conocidas y puede borrarlo o ponerlo en cuarentena si encuentra un virus u otro tipo de amenaza. Cuando un archivo se pone en cuarentena, se almacena en una ubicación especial de su equipo y se bloquea su uso. VirusScan también usa un análisis **heurístico** para detectar comportamientos inusuales que también puede poner elementos en cuarentena.

SUGERENCIA: El **análisis heurístico** es una técnica de análisis que usa VirusScan para identificar amenazas potenciales. Cuando VirusScan usa la heurística (también conocida como protección activa), analiza el código interno de un archivo o una aplicación para determinar si tiene un

comportamiento similar al de un virus. Por ejemplo, el análisis heurístico puede avisar si el archivo analizado puede:

- **Replicarse** (crear muchas copias de sí mismo)
- **Sobrescribir otros archivos** (algo que también hacen muchos virus)
- **Ocultarse** (los virus hacen esto para evitar ser detectados por programas antivirus)

Si VirusScan determina que el archivo analizado hace alguna de estas de estas cosas, indicará que podría contener un virus o algún tipo de malware y, por lo tanto, lo pondrá en cuarentena.

En la mayoría de casos, Active Protection acierta al poner en cuarentena elementos que ha evaluado y considera que no son seguros.Sin embargo, puede que en algunos casos los archivos se pongan en cuarentena cuando no deberían. Para ayudarle a gestionar elementos en cuarentena, puede llevar a cabo estas tres acciones:

- **Eliminar**: borra el elemento en cuarentena de forma permanente

- **Restaurar**: libera el elemento de la cuarentena y lo restaura a la ubicación donde fue detectado. **IMPORTANTE:** no restaure un elemento en cuarentena a menos que se **haya asegurado** de que se trata de un elemento seguro.Consulte la sección **Información relacionada** para obtener más detalles sobre cómo restaurar archivos y programas de la cuarentena.

- **Enviar a McAfee**: envía automáticamente el elemento en cuarentena a McAfee Labs para realizar más análisis (solo para equipos Windows)

Solución

Siga estos pasos para gestionar elementos en cuarentena:

Equipos Windows:

1. Abra su producto de McAfee Security.
2. Haga clic en **Navegación**.
3. Haga clic en **Elementos en cuarentena y de confianza**.
4. Abra **Elementos en cuarentena** (para seleccionar archivos individuales) o **Programas potencialmente no deseados en cuarentena** (para programas).
5. Seleccione elementos específicos individualmente o haga clic en **Seleccionar todos**.

6. Seleccione la acción que desee llevar a cabo (**Eliminar**, **Restaurar** o **Enviar a McAfee**).

   NOTA: Si previamente había elegido confiar en los archivos o programas identificados como potencialmente peligrosos durante un análisis previo, puede quitar estos elementos de la lista de confianza, abriendo **Elementos de confianza**, seleccionando el elemento y haciendo clic en **Quitar de la lista de confianza**.

Equipos Mac:

1. Haga clic en el icono McAfee y seleccione **Consola de McAfee Internet Security...**
2. Seleccione **Cuarentena**.
3. Haga clic en el candado para realizar cambios.
4. Escriba la contraseña de administrador y haga clic en **Aceptar**.
5. Seleccione la ubicación o mantenga pulsada la tecla Mayúsculas y seleccione múltiples ubicaciones.
6. Seleccione **Restaurar** para restaurar el elemento de Cuarentena o **Eliminar** para borrar el elemento de la lista.
7. Haga clic en el candado para evitar cambios.

14. Cómo configurar McAfee Personal Firewall para permitir las conexiones entrantes en puertos específicos

Entorno

Suites afectadas:

Todas las suites de seguridad de McAfee para Windows

Productos afectados:

Firewall

Sistemas operativos afectados:

Microsoft Windows 8

Microsoft Windows 7

Microsoft Windows Vista

Microsoft Windows XP

Resumen

Este artículo le ayudará a configurar el software de McAfee para permitir las conexiones remotas con el sistema.

Problema

McAfee Personal Firewall tiene los niveles de seguridad predeterminados definidos para bloquear las conexiones iniciadas de forma remota. Esta configuración contribuye a proteger el equipo de actividades malintencionadas.

Aunque la configuración predeterminada permite al equipo acceder a equipos remotos, bloquea el acceso de otros equipos al suyo. Si desea que ciertos equipos remotos puedan conectar con el suyo, deberá configurar Personal Firewall para permitir las conexiones entrantes específicas.

Cuando se comparten recursos, hay diversas formas de restringir el acceso a los datos:

- Por puerto (software de seguridad como Personal Firewall)
- Por la configuración del enrutador (incluye un firewall integrado)
- Por el proveedor de servicios de Internet

NOTA: Los problemas de conexión pueden estar relacionados con las reglas de acceso predeterminadas del enrutador o con el número máximo de conexiones permitidas por el propio enrutador. Si el enrutador alcanza su número máximo de conexiones, puede rechazar los intentos de conexión subsiguientes. Los problemas de conexión del enrutador pueden parecer debidos al software de McAfee o a otras aplicaciones; sin embargo, la solución normalmente pasa por restablecer el enrutador o configurarlo para que permita más conexiones simultáneas. Consulte la documentación del enrutador para obtener instrucciones específicas antes de intentar restablecer el enrutador.
Para abrir los puertos necesarios en McAfee Firewall, realice los pasos siguientes.

Solución

Apertura de un puerto

1. Abra el software de seguridad de McAfee para Windows.
2. Haga clic en **Protección del correo electrónico y la Web**.

3. Haga clic en **Firewall**.
4. Haga clic en **Puertos y servicios del sistema**.
5. Haga clic en **Agregar**.
6. Introduzca el **Nombre de programa** de la aplicación mediante el campo Nombre del servicio del sistema.
7. Introduzca una descripción de la aplicación o el servicio para contribuir a identificar la regla nueva.
8. Introduzca los **puertos TCP** o **UDP** necesarios para la aplicación.
9. Cambie la opción de la lista desplegable correspondiente al campo **Abrir puertos en** a **Todos los equipos**.
10. Haga clic en **Guardar**.
11. Compruebe que la aplicación funciona correctamente.

IMPORTANTE:

- Si tiene un enrutador local con un firewall integrado, deberá configurar la misma regla entrante para activar los puertos requeridos por la aplicación a fin de dirigir el tráfico a su equipo.
- La apertura de puertos tanto en el enrutador como en el equipo puede permitir conexiones no deseadas, de modo que será necesaria una vigilancia adicional para asegurarse de que el sistema siga siendo seguro.

Puertos comunes:

- **80/TCP**: HTTP (HyperText Transfer Protocol), puerto predeterminado de servidor web.
- **3389/TCP**: Escritorio remoto de Microsoft, registrado oficialmente como WBT (terminal basado en Windows).
- **3724/TCP, UDP**: World of Warcraft (juego multijugador en línea).
- **6881-6999/TCP**: P2P (uso compartido de archivos entre componentes del mismo nivel)

  NOTA: Las aplicaciones P2P pueden usar cualquier puerto. Consulte la documentación del fabricante para conocer la información específica de puertos necesaria.

Glosario de términos técnicos

Activación

El proceso por el que se activa la licencia del software de un cliente.

Administración remota

La capacidad de administrar un sistema desde una ubicación remota.

ADSL

Línea de abonado digital asimétrica. Una tecnología que permite la transferencia de datos a alta velocidad sobre las líneas de teléfono existentes. Admite las tasas de datos entre 1,5 y 9 Mbits/s al recibir datos, y entre 16 y 640 Kbit/s al enviar datos.

AES

Estándar de cifrado avanzado. Un estándar cifrado de bloques desarrollado por NIST (el Instituto de estándares y tecnología de Estados Unidos) que reemplaza al estándar de cifrado de datos (DES). Los cifrados AES utilizan un bloque de 128 bits y claves de 128, 192 o 256 bits. El tamaño de bloque más grande ayuda a resistir los ataques de cumpleaños mientras que el tamaño de clave grande evita los ataques de fuerza bruta.

Alerta

Una reacción automática del sistema que informa de un evento sospechoso.

Antimalware

Permite configurar la detección exhaustiva de malware y el bloqueo en el gateway corporativo, lo que protege su red frente a ataques procedentes del tráfico de la Web y de los correos electrónicos.

Antispam

La protección antispam que le ayuda a mantener a su familia, su negocio y a usted mismo protegido frente a falsos sitios web peligrosos que pueden conducir a su PC, comprometer su identidad y poner en peligro la seguridad de aquello que valora.

Antivirus

Software que trata de identificar, frustrar y eliminar virus informáticos, así como otros software maliciosos.

API

Interfaz de programación de aplicaciones. Una interfaz de software publicada y estable para un sistema operativo o programa de software específico mediante la cual un programador que crea una aplicación personalizada puede realizar solicitudes del sistema operativo o programa de software concreto. Una API proporciona una conexión sencilla y estándar a un componente de software particular.

Archivo de registro

Un archivo que contiene los datos recopilados por un origen de registro.

Autenticación

Un proceso que verifica la autenticidad de una persona o un sistema antes de permitir el acceso a un sistema o servicio de red. La autenticación confirma que los datos se envían a los destinatarios deseados y les garantiza que los datos proceden del remitente esperado, así como que no se han alterado por el camino.

Autenticador

Un dispositivo o mecanismo utilizados para verificar la identidad de una persona que inicia sesión en una red, una aplicación o un equipo.

Caballo de Troya

Un programa malicioso que se muestra como una aplicación benigna. Un programa troyano realiza de forma deliberada algo que el usuario no espera. Los troyanos no son virus porque no se reproducen, pero pueden ser igual de destructivos.

Caché

Un área de ensayo temporal o permanente en el almacenamiento en memoria o en disco de un equipo que contiene los datos más frecuentes o a los últimos a los que se ha accedido. Una caché se utiliza para acelerar la transferencia de datos, la ejecución de instrucciones y la recuperación de datos, así como la actualización.

Categorías

Las URL que se agrupan según el tipo de sitio web que identifica la base de datos de Internet.

Certificado

Conocido también como certificado digital. Una declaración firmada digitalmente que contiene información acerca de una entidad y la clave pública de esta, y que enlaza estos dos datos. Como parte del protocolo X.509 (estructura de autenticación ISO), una autoridad de certificación emite un certificado después de haber comprobado que la entidad es quien dice ser.

Cifrado

La técnica que permite convertir un mensaje legible (texto sin formato) en material aparentemente aleatorio (texto cifrado), de modo que pueda leerse solo en equipos que utilizan el mismo código o tecnología de cifrado. El cifrado reduce el riesgo de un acceso no autorizado, pero no crea un entorno de red totalmente seguro por su cuenta.

Clave privada

Utilizada para descifrar mensajes que se cifraron con la clave pública correspondiente. Una clave privada también sirve para firmar digitalmente los mensajes. El destinatario puede utilizar la clave pública correspondiente para verificar la autenticidad del mensaje.

Clave pública

Una clave pública se utiliza para cifrar mensajes que solo el propietario de la correspondiente clave privada puede descifrar. Las claves públicas también pueden utilizarse para verificar la autenticidad de los documentos firmados digitalmente.

Complemento

(1) Un módulo complementario de software que depende de una interfaz bien definida para añadir funcionalidades a un producto de software conocido. Los proveedores que crean productos de software multiusos como navegadores de Internet, con frecuencia, introducen puntos bien definidos en su flujo lógico donde la ejecución comprueba la existencia de un módulo externo y, si está presente, lo ejecuta, pasando la información relacionada de un lado a otro según los patrones establecidos. Esto permite a los clientes o a otros proveedores personalizar áreas concretas del producto. El concepto se ha conocido por otros muchos nombres, incluidos exits o user exits.

(2) Un módulo de hardware o software que añade una función o servicio específico a un sistema más grande. Los complementos también pueden mostrar o interpretar un protocolo o formato de archivo concreto, por ejemplo, Shockwave o RealAudio.

Consola

Un terminal físico o virtual conectado a un appliance que se utiliza para supervisar y controlar un appliance.

Consola de administración

Una interfaz gráfica de usuario (GUI) utilizada para configurar y administrar software.

Correo web

También conocido como correo electrónico basado en la Web. Una cuenta de correo electrónico a la que se accede a través de un navegador web. Algunas versiones conocidas entre los usuarios de esta tecnología incluyen Gmail, Hotmail y Yahoo Mail. Muchas empresas también aprueban el uso del correo electrónico web como forma de permitir a los empleados acceder a sus cuentas de correo de forma remota.

Código PIN

Número de identificación personal. Un número conocido únicamente por un usuario con el fin de ayudar a identificar a una persona durante el proceso de autenticación informática. Los usuarios deben memorizar sus números PIN.

DHCP

Protocolo de configuración dinámica de host. Un protocolo de comunicación que simplifica la distribución de direcciones IP de una red. El protocolo dinámico permite a los administradores asignar y administrar direcciones IP de forma centralizada en lugar de tener que hacer dichas tareas localmente.

Dirección de red

El octeto más a la izquierda de una dirección cuadrada de puntos. Las direcciones de red de clase A se componen de un octeto, las de clase B de dos y las de clase C de tres. Normalmente escritos en formato decimal, cada octeto puede encontrarse en formato hexadecimal u octal. Los octetos omitidos se interpretan como 0.

Dirección IP

Una dirección de 32 bits que utiliza formato estándar de cuatro números separados por puntos asignado a dispositivos de red TCP/IP. Cada máquina tiene una dirección IP única en Internet, y contiene un campo host y uno de red.

Directiva

Un conjunto de reglas que rigen las comunicaciones.

DNS

Sistema de nombres de dominio. Un servicio TCP/IP que asigna nombres de dominio y host a direcciones IP (y viceversa), y que proporciona información sobre los servicios y puntos de contacto en una red o en Internet. Un conjunto de solucionadores y servidores de nombres conectados que permite a los usuarios utilizar un nombre de host en lugar de una dirección de Internet de 32 bits.

Dominio

(1) En relación con la red, es la parte de una dirección de Internet que indica el nombre de una red de equipo. De hecho, en la dirección IP jones@bizco.sales.com, el dominio es bizco.sales.com.

(2) En relación con Type Enforcement, un atributo aplicado a un proceso que se ejecuta en SecureOS que determina qué operación del sistema debe realizar el proceso.

Encabezado

La parte de un mensaje de correo electrónico que, normalmente, no se muestra en el cliente de correo electrónico. El encabezado de correo electrónico contiene metadatos e información de enrutamiento, como las identidades y las direcciones IP del remitente y el destinatario, todas las entradas de correo electrónico entre el remitente y el destinatario, y la prioridad y el asunto del correo electrónico. Algunos remitentes de spam manipulan de manera deliberada la información del encabezado en un intento de engañar (o falsificar) a los filtros de spam como la fuente real del mensaje de correo electrónico.

Enrutador

Un dispositivo de red que reenvía datos entre dos o más redes, entregándolos en su destino final o a otro enrutador. Un enrutador se diferencia de los concentradores y conmutadores en que se considera "inteligente" y en que puede enrutar paquetes a su destino final.

Ethernet

Un protocolo de capa física basado en los estándares IEEE.

Exploit

Software, fragmento de datos o secuencia de comandos que aprovecha un error, una interrupción o una vulnerabilidad para provocar comportamientos inesperados o imprevistos. Los exploits se identifican mejor a través de búsquedas basadas en firmas, las cuales resultan más costosas de llevar a cabo desde un punto de vista informático.

Falsificación

(1) La creación de un sitio web fraudulento que se asemeja a uno real y bien conocido ejecutado por un tercero.

(2) Alteración de una dirección de envío de correo electrónico, de modo que parezca que es de un remitente diferente.

Falso negativo

Un correo electrónico marcado como legítimo, incluso aunque es spam.

Falso positivo

Un correo electrónico marcado como spam, incluso aunque es legítimo.

Firma

Una firma describe un exploit para una vulnerabilidad conocida que puede encontrarse al evaluar el tráfico a un objeto de red de destino.

FTP

Protocolo de transferencia de archivos. Un protocolo utilizado en Internet para la transferencia de archivos.

Gravedad

El grado al que una vulnerabilidad puede afectar a un sistema de destino.

Gusano

Un programa informático independiente que se reproduce copiándose a sí mismo de un sistema a otro a través de una red. A diferencia de los virus informáticos, los gusanos no precisan de intervención humana para propagarse. Los gusanos se crean para infiltrar programas de procesamiento de datos legítimos, con el fin de alterar o destruir dichos datos. Lo que con frecuencia parece una infección de un virus es, en realidad, un gusano.

Hash

Una cadena criptográfica basada en el contenido de un mensaje. El algoritmo utilizado para crear el hash debe permitir la creación de un mensaje, de modo que su hash se convierta en un valor específico. Los hashes pueden adjuntarse a un mensaje para demostrar que no se ha modificado. Si se modifica un mensaje, su nuevo hash dejará de coincidir con el valor de hash original.

HTML

Lenguaje de marcado de hipertexto. Un lenguaje de programación simple utilizado para crear documentos web. El hipertexto utiliza vínculos especiales en los que puede hacer clic para saltar de un tema relacionado a otro.

HTTP

Protocolo de transferencia de hipertexto. Un formato acordado (protocolo) que solicita y transfiere documentos HTML en la World Wide Web.

HTTPS

Protocolo seguro de transferencia de hipertexto. Un formato acordado (protocolo) que solicita y transfiere documentos HTML en la Web de una manera segura.

IMAP

Protocolo de acceso a mensajes de Internet. El método utilizado para acceder al correo electrónico de forma remota, normalmente, a través del correo web u otro protocolo que no descarga los mensajes al cliente. Permite mantener los mensajes en varias carpetas, admite el uso compartido de carpetas y permite la

administración online del correo. IMAP es un método más avanzado de almacenaje de correo que POP, que se basa en la descarga de mensajes a una unidad local del usuario.

Independiente

Hace referencia a un dispositivo o software autónomo, es decir, uno que no requiere que ningún otro dispositivo o software funcione.

Interfaz

Un límite compartido a través del cual puede intercambiarse información. Una interfaz puede ser una parte compartida de un software informático accesible para dos o más programas, un componente de hardware que conecta dos dispositivos, o un dispositivo o programa que permite a un usuario comunicar y utilizar el equipo o el programa.

Interfaz web

Una recopilación de páginas web que se proporcionan para acceder a un sistema informático a través de un navegador web.

IPv6

IPv6 (Protocolo de Internet, versión 6) es el sustituto del anticuado IPv4, que se lanzó a principios de los años 80. IPv6 aumentará el número de direcciones de Internet disponibles (de 32 bits a 128 bits), lo que resuelve un problema relacionado con el crecimiento del número de equipos conectados a Internet.

LAN

Red de área local. Una red de equipos que cubre un área geográfica pequeña, por ejemplo, una casa, una oficina o un grupo de edificios.

Lista blanca

Una lista de entidades de confianza que tienen permiso para enviar mensajes. El concepto es totalmente opuesto al de lista negra. Utilice la inclusión en lista blanca con moderación para impedir que entre mucho spam.

Lista negra

Relacionada con el spam, las listas negras son registros de remitentes de spam conocidos, sus direcciones IP y sus proveedores de servicios de Internet (ISP). Con esta información, los filtros de spam pueden bloquear todos los mensajes procedentes de dichos remitentes o de sus respectivos ISP. Los ISP que no sancionen a sus remitentes de spam, podrían encontrarse con que todos los correos electrónicos de sus clientes legítimos quedarían bloqueados por un gran número de destinatarios. Esta táctica obliga a los ISP a actuar contra los remitentes de spam que utilizan sus sistemas, ya que los usuarios legítimos no quieren verse perjudicados al bloqueárseles todos sus correos electrónicos. El concepto es totalmente opuesto al de lista blanca.

Malware

Software malicioso diseñado para llevar a cabo acciones molestas o dañinas. Con frecuencia, el malware se enmascara en forma de programas útiles o se incrusta en ellos, de modo que los usuarios se vean inducidos a activarlos. El malware puede incluir virus, gusanos y spyware.

NIC

Tarjeta de interfaz de red. Hardware, como una placa de circuito eléctrico, que contiene un puerto o un conector jack que permite a un equipo conectarse al cableado de red (cable Ethernet, línea de teléfono, etc.).

Nombre de host

El nombre o alias asignado a un sistema.

Nombre de sitio

El primer nombre de dominio (con su extensión) o el único en una cadena URL. Cuando un sitio web alberga otro sitio web, el primer nombre de dominio (con su extensión) es el del sitio y el último el del host. Por ejemplo, en la cadena URL "www.SecureWeb.com/aaa/www.example.com/home.htm", el nombre del sitio es "www.SecureWeb.com" y el del host es "www.example.com".

Paquete

Una unidad de datos como se envía en una red.

Par de claves

La referencia a una clave privada y a una clave pública relacionada matemáticamente. Solo el propietario conoce y protege su clave privada. La clave pública puede distribuirse a cualquier persona. Esto permite que una clave pueda utilizarse para el cifrado y la otra para el descifrado.

Phishing

Una técnica de fraude de alta tecnología que utiliza los mensajes emergente o el spam para engañar a las personas y lograr que revelen el número de la tarjeta de crédito, información de la cuenta bancaria, el número de la Seguridad Social, contraseñas u otra información de carácter confidencial. Los estafadores por Internet utilizan el correo electrónico como señuelo para "cazar" contraseñas y datos financieros de los usuarios de Internet.

ping

Un comando que envía un mensaje de ICMP de un host a otro en una red para probar la conectividad y la pérdida de paquetes.

POP3

Protocolo de oficina de correos. El protocolo que lee los mensajes de otro host.

PPP

Protocolo punto a punto. Un protocolo de red para establecer enlaces simples entre dos componentes del mismo nivel.

Protocolo

Un conjunto de reglas mediante el cual una entidad se comunica con otra, especialmente, en una red. Este es importante al definir las reglas mediante las cuales los clientes y servidores se comunican entre ellos en una red. Los protocolos importantes se publican, estandarizan y difunden.

Protocolo de Internet

También conocido como IP. La capa de red para la suite de protocolos TCP/IP. IP es un protocolo de intercambio de paquetes de mejor solución sin conexión diseñado para ofrecer la entrega de paquetes más eficiente de Internet. La dirección IP sirve como base para un variado número de protocolos, define la unidad básica de transmisión por Internet, establece el plan de direcciones de Internet y mucho más.

Proxy

Un agente de software que actúa en nombre de un usuario que solicita una conexión de red a través del firewall. Los proxies aceptan una conexión de un usuario, toman una decisión sobre si el usuario o la dirección IP del cliente puede utilizar el proxy o no, realizan otra autenticación de manera opcional y, por último, completan una conexión con un destino remoto en nombre del usuario.

Puerto

El número que identifica el proceso de aplicación de destino para los datos transmitidos. Los números de puerto van del 1 al 65535. Por ejemplo, Telnet utiliza habitualmente el puerto 23 y DNS el puerto 53.

Regla

La unidad operativa básica de la directiva de comunicaciones electrónicas. Se encarga de especificar las condiciones del acceso web y se encuentra en una posición de prioridad en la directiva. Cualquier acceso que coincide con las condiciones de una regla la activa si esta tiene la máxima prioridad de todas las reglas coincidentes.

Remitente de spam

Una persona que envía spam.

Retraso

Una función de SmartFilter que configura el sistema para ralentizar el acceso a un sitio en lugar de bloquearlo. Esta función también puede ralentizar el acceso a los tipos de archivos especificados.

Robos de identidad

El acto de robar la información personal de una víctima. Con frecuencia, los ladrones de identidad abren cuentas de crédito en nombre de la víctima. El robo de identidad tiene el riesgo de que puede caerse víctima de un intento de suplantación de identidad (phishing).

RSA

Un algoritmo de clave pública muy utilizado que puede utilizarse para un cifrado o una firma digital. RSA utiliza claves públicas y privadas que son funciones de un par de números primos grandes.

Las siglas RSA responden a Ron Rivest, Adi Shamir y Leonard Adleman, que fueron los primeros en describir el algoritmo en el año 1977.

Servidor de nombres

Un equipo de red que mantiene una relación entre las direcciones IP y los nombres de dominio correspondientes.

Servidor proxy

Un servidor que actúa en nombre de otro y que puede realizar tareas como, por ejemplo, almacenamiento en caché, control de acceso, o proporcionar una ruta a un servidor de destino. Los administradores pueden elegir configurar los servidores proxy de una de las siguientes formas:

Transparente: El usuario final no es consciente de la presencia del servidor proxy.

No transparente: El usuario final debe autenticarse en el servidor o interactuar con él.

Servidor web

Un dispositivo de red que almacena y sirve cualquier tipo de archivo de datos incluidos texto, imágenes gráficas, vídeo o audio. Es posible acceder a la información almacenada a través de Internet utilizando protocolos estándar, con frecuencia HTTP/HTTPS.

Sesión

(1) El período de tiempo durante el que un usuario de terminales registra en el sistema hasta que se cierra la sesión.

(2) Las sesiones definen un conjunto de parámetros de seguridad criptográficos que pueden compartirse entre varias conexiones. Las sesiones se utilizan para evitar la costosa negociación de nuevos parámetros de seguridad para cada conexión. Las sesiones se crean mediante el protocolo de enlace.

Skype

Una red de telefonía por Internet de componente a componente del mismo nivel (VoIP). El conjunto de usuarios de la aplicación de software de escritorio gratuita suministra la red. Los usuarios de Skype pueden hablar con otros usuarios de Skype de forma gratuita, llamar a números de teléfono tradicionales gratis (SkypeOut), recibir llamadas de números tradicionales (SkypeIn) y recibir mensajes de voz.

SMTP

Protocolo simple de transferencia de correo. El protocolo TCP/IP que transfiere correo electrónico mientras se mueve por el sistema.

Spam

Correos electrónicos comerciales no solicitados, enviados a través de un programa de correo electrónico automatizado, que anuncian productos, servicios y sitios web. El spam también se puede utilizar como mecanismo de entrega de malware y otras amenazas cibernéticas.

Spyware

Malware instalado sin el conocimiento del usuario para rastrear o transmitir datos a un tercero no autorizado.

SSL

Protocolo de capa de sockets seguros. Proporciona un método de encapsulación de datos para permitir la privacidad entre dos aplicaciones que se comunican por Internet. El protocolo de seguridad de la capa de transporte (TLS) se basa en la versión 3.0 de SSL.

Subred

Un plan de direcciones de red que separa una sola red en varias redes físicas más pequeñas para simplificar el enrutamiento.

TCP

Proxy de control de transmisión. Un protocolo de capa de transporte estándar de Internet orientado a la conexión y a la transmisión.

TCP/IP

Protocolo de control de transmisión/Protocolo de Internet. La suite de protocolos de red básica para la comunicación con Internet.

TLS

Seguridad de la capa de transporte. La última versión de SSL. Una mejora de la versión 3.0 de SSL.

Transmisión

Un archivo multimedia que se transmite mediante un flujo continuo en la red. Las transmisiones son de dos tipos: en vivo y bajo demanda.

Transmisión multimedia en tiempo real

Archivos multimedia que empiezan a reproducirse mientras se están transmitiendo por la red al reproductor multimedia del equipo cliente.

TrustedSource

Un motor de correlación de amenazas globales y base de inteligencia que sigue las tendencias de correo electrónico, tráfico web y malware, y que asigna calificaciones de reputación web. TrustedSource también cuenta con una herramienta para verificar si un sitio está incluido en la versión más actual de la base de datos web TrustedSource.

UDP

Protocolo de datagrama de usuario. Un protocolo sin conexión que transfiere datos en una red sin comprobaciones de errores ni de fiabilidad.

URL

Localizador uniforme de recursos. Proporciona la dirección de documentos específicos en la Web. Cada archivo de Internet cuenta con una URL única, que indica el nombre del servidor, el directorio y el documento específico. La forma de una URL es el protocolo://pathname. Por ejemplo: ftp://www.website.com y http://www.website.com.

Virus

Un programa (normalmente, ejecutable) que infecta un archivo del equipo, introduciendo una copia propia en el archivo. Estas copias suelen ejecutarse cuando el archivo infectado se carga en la memoria, dejando que el virus infecte otros archivos. Un virus requiere intervención humana (normalmente de forma inadvertida) para propagarse. Cuando un virus está activo en un equipo host, la infección puede propagarse rápidamente a otros sistemas a través de una red.

Algunos virus pueden ser benignos y provocar únicamente distracciones o algo de molestias. Otros pueden ser maliciosos y destruir o alterar los datos.

VPN

Red privada virtual. Un método de autenticación y cifrado de transmisiones de datos entre las máquinas (de firewall a firewall, de firewall a cliente) a través de Internet. La VPN hace que parezca como si las redes en el lado interno de los firewalls estuvieran conectadas entre ellas a través de un par de enrutadores con una línea arrendada entre ellas.

WINS

Servicio de nombres Internet de Windows. Administra la asociación de nombres de estaciones de trabajo y ubicaciones con las direcciones IP.