

Bitdefender[®] MOBILE SECURITY



**GUÍA DE
USUARIO**





Bitdefender Mobile Security

Guía de usuario

Fecha de publicación 22/11/2022
Copyright © 2022 Bitdefender

Aviso Legal

Reservados todos los derechos. Ninguna parte de este libro se puede reproducir ni transmitir de ninguna forma ni por ningún medio, electrónico o mecánico, incluidas las fotocopias, las grabaciones o cualquier sistema de recuperación y almacenamiento de información, sin el permiso por escrito de un representante autorizado de Bitdefender. La inclusión de citas breves en las reseñas solo puede ser posible con la mención de la fuente citada. El contenido no puede ser modificado de ninguna manera.

Advertencia y descargo de responsabilidad. Este producto y su documentación están protegidos por derechos de autor. La información en este documento se proporciona "tal cual", sin garantía. Aunque se han tomado todas las precauciones en la preparación de este documento, los autores no tendrán ninguna responsabilidad ante ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en este trabajo.

Este libro contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefender no es responsable del contenido de ningún sitio enlazado. Si accede a un sitio web de terceros enumerado en este documento, lo hará bajo su propio riesgo. Bitdefender proporciona estos enlaces solo para su comodidad, y la inclusión del enlace no implica que Bitdefender respalde o acepte ninguna responsabilidad por el contenido del sitio de terceros.

Marcas registradas. Los nombres de marcas registradas pueden aparecer en este libro. Todas las marcas comerciales registradas y no registradas en este documento son propiedad exclusiva de sus respectivos dueños y se reconocen respetuosamente.

Bitdefender®



Tabla de contenidos

Acerca de esta guía	1
Propósito y público al que se dirige	1
Cómo usar esta guía	1
Convenciones utilizadas en esta guía	1
Convenciones tipográficas	1
Advertencias	2
Solicitud de comentarios	2
1. ¿Qué es Bitdefender Mobile Security?	4
2. Iniciando	5
2.1. Requisitos del Dispositivo	5
2.2. Instalar Bitdefender Mobile Security	5
2.3. Iniciar sesión en su cuenta de Bitdefender	6
2.4. Configurar la protección	7
2.5. Panel de Control	7
3. Características y funcionalidades	11
3.1. Analizador malware	11
3.2. Protección Web	13
3.3. VPN	14
3.3.1. Ajustes de VPN	16
3.3.2. Suscripciones	17
3.4. Alerta de fraude	17
3.4.1. Activación de la Alerta de fraude	19
3.4.2. Protección de chats en tiempo real	19
3.5. Características Antirrobo	20
3.5.1. Activación de Antirrobo	21
3.5.2. Utilización de las características de Antirrobo desde Bitdefender Central	23
3.5.3. Ajustes de Antirrobo	24
3.6. Privacidad de la cuenta	24
3.7. Bloqueo de apps	26
3.7.1. Activación del Bloqueo de apps	26
3.7.2. Modo de bloqueo	27
3.7.3. Opciones de Bloqueo de Apps	28
3.7.4. Hacer foto	28
3.7.5. Desbloqueo inteligente	30
3.8. Informes	30
3.9. Localizador	31
3.9.1. Activación de WearON	32
3.10. Acerca de	32



4. Acerca de Bitdefender Central	33
4.1. Acceso a Bitdefender Central	33
4.2. Autenticación en dos fases	34
4.2.1. Activar la autenticación en dos fases	34
4.3. Añadir dispositivos de confianza	36
4.4. Mis dispositivos	36
4.4.1. Añadir un nuevo dispositivo	37
4.4.2. Personalice su dispositivo	37
4.4.3. Acciones remotas	38
4.5. Actividad	39
4.6. Mis suscripciones	40
4.6.1. Compruebe las suscripciones disponibles	40
4.6.2. Activar la suscripción	41
4.6.3. Renovar suscripción	41
4.7. Notificaciones	42
5. Preguntas frecuentes	43
6. Obteniendo ayuda	49
6.1. Solicitando Ayuda	49
6.2. Recursos Online	49
6.2.1. Centro de soporte de Bitdefender	49
6.2.2. La comunidad de expertos de Bitdefender	50
6.2.3. Ciberpedia de Bitdefender	50
6.3. Información de contacto	51
6.3.1. Distribuidores locales	51
Glosario	52



ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía va dirigida a todos los usuarios de Android que hayan elegido Bitdefender Mobile Security como solución de seguridad para sus dispositivos móviles. La información presentada en esta guía está indicada no sólo para quienes posean conocimientos técnicos, sino para todos aquellos que puedan trabajar con dispositivos Android.

Averiguará cómo configurar y usar Bitdefender Mobile Security para protegerse contra amenazas y otras aplicaciones maliciosas. Aprenderá a sacarle el máximo partido a Bitdefender.

Le deseamos una lectura útil y agradable.

Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

[Iniciando \(página 5\)](#)

Comience con Bitdefender Mobile Security y su interfaz de usuario.

[Características y funcionalidades \(página 11\)](#)

Aprenda a utilizar Bitdefender Mobile Security para protegerse contra amenazas y aplicaciones maliciosas conociendo sus características y funcionalidades.

[Obteniendo ayuda \(página 49\)](#)

Dónde buscar y dónde solicitar ayuda si surge algo inesperado.

Convenciones utilizadas en esta guía

Convenciones tipográficas

En esta guía se utilizan distintos estilos de texto con el fin de mejorar su lectura. En la siguiente tabla se indican su aspecto y significado.



Apariencia	Descripción
<code>sample syntax</code>	Las muestras de sintaxis se imprimen con <code>monospaced</code> caracteres.
https://www.bitdefender.com	La URL del enlace señala a alguna ubicación externa, en servidores http o ftp.
documentation@bitdefender.com	Las direcciones de email se incluyen en el texto como información de contacto.
Acerca de esta guía (página 1)	Este es un enlace interno, hacia algún punto dentro del documento.
<code>filename</code>	Los archivos y directorios se imprimen usando <code>monospaced</code> fuente.
opción	Todas las opciones de productos se imprimen usando atrevido caracteres.
palabra clave	Las palabras clave o frases importantes se resaltan usando atrevido caracteres.

Advertencias

Las advertencias son notas en el texto, marcadas gráficamente, que brindan información adicional respecto al párrafo actual.



Nota

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.



Importante

Este tipo de advertencia requiere su atención y no es recomendable omitirla. Normalmente proporciona información importante, aunque no extremadamente crítica.



Advertencia

Se trata de información crítica que debería tratar con extrema cautela. No ocurrirá nada malo si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente arriesgado.

Solicitud de comentarios

Le invitamos a ayudarnos a mejorar el manual. Hemos comprobado y verificado toda la información como mejor hemos sabido. Por favor, escríbanos para explicarnos cualquier tipo de defecto que encuentre en este manual o cómo podría mejorarse, y así ayudarnos a ofrecerle la mejor documentación posible.

Háganos saber enviando un correo electrónico a documentation@bitdefender.com. Escriba todos sus correos electrónicos



relacionados con la documentación en inglés para que podamos procesarlos de manera eficiente.



1. ¿QUÉ ES BITDEFENDER MOBILE SECURITY?

Las actividades online, como por ejemplo pagar facturas, hacer reservas hoteleras o adquirir bienes y servicios son cómodas y sencillas. No obstante, como muchas otras actividades que han evolucionado en Internet, conllevan altos riesgos y, si no se actúa de forma segura, los datos personales pueden verse comprometidos. ¿Y qué hay más importante que proteger los datos almacenados en sus cuentas online y en su smartphone?

Bitdefender Mobile Security le permite lo siguiente:

- Obtener la mejor protección para su smartphone y tablet Android afectando mínimamente a la duración de la batería.
- Protegerse contra estafas móviles que se basan en enlaces.
- Tener acceso a nuestra VPN protegida para navegar por la web de forma rápida, anónima y segura.
- Localice, bloquee y borre de forma remota su dispositivo Android en caso de pérdida o robo
- Comprobar si su cuenta de correo electrónico se ha visto envuelta en vulneraciones o fugas de datos.



2. INICIANDO

2.1. Requisitos del Dispositivo

Bitdefender Mobile Security funciona en cualquier dispositivo que ejecute Android 5.0 o posterior. Se necesita una conexión a Internet activa para el análisis de amenazas en la nube.

2.2. Instalar Bitdefender Mobile Security

○ Desde Bitdefender Central

○ Para Android

1. Ir a: <https://central.bitdefender.com>.
2. Inicie sesión en su cuenta de Bitdefender.
3. Seleccione el panel **Mis dispositivos**.
4. Toque **INSTALAR PROTECCIÓN** y, a continuación, toque **Proteger este dispositivo**.
5. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
6. Se le redirigirá a la app **Google Play**. En la pantalla de Google Play, toque la opción de instalación.

○ En Windows, iOS y macOS

1. Ir a: <https://central.bitdefender.com>.
2. Inicie sesión en su cuenta de Bitdefender.
3. Selecciona el **Mis dispositivos** panel.
4. Pulse **INSTALAR PROTECCIÓN** y, a continuación, pulse **Proteger otros dispositivos**.
5. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, pulse el botón correspondiente.
6. Pulse **ENVIAR ENLACE DE DESCARGA**.
7. Introduzca una dirección de correo electrónico en el campo correspondiente y pulse **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado solo es



válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.

8. En el dispositivo en que desee instalar Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego pulse el botón de descarga correspondiente.

○ Desde Google Play

Busque Bitdefender Mobile Security para encontrar e instalar la app. Como alternativa, escanee el código QR:



Antes de llevar a cabo los pasos para la validación, debe aceptar el Acuerdo de suscripción. Por favor, dedique un momento a leer el Acuerdo de suscripción, dado que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Mobile Security.

Toque **CONTINUAR** para pasar a la siguiente ventana.

2.3. Iniciar sesión en su cuenta de Bitdefender

Para usar Bitdefender Mobile Security debe vincular su dispositivo a una cuenta de Bitdefender, Facebook, Google, Apple o Microsoft iniciando sesión en la cuenta desde la app. La primera vez que abra la app se le pedirá que registre una cuenta.

Si ha instalado Bitdefender Mobile Security desde su cuenta de Bitdefender, la app intentará iniciar sesión automáticamente en esa cuenta.

Para vincular su dispositivo a una cuenta de Bitdefender:

1. Escriba su dirección de correo electrónico y contraseña de la cuenta de Bitdefender en los campos correspondientes. Si carece de una cuenta de Bitdefender y desea crear una, seleccione el enlace correspondiente.
2. Toque **INICIAR SESIÓN**.



Para iniciar sesión con una cuenta de Facebook, Google o Microsoft, toque el servicio que desee usar en O iniciar sesión con. Se le redirige a la página de inicio de sesión del servicio seleccionado. Siga las instrucciones para vincular su cuenta a Bitdefender Mobile Security.



Nota

Bitdefender no tiene acceso a información confidencial, como la contraseña de la cuenta que utiliza para conectarse, o la información personal de sus amigos y contactos.

2.4. Configurar la protección

Una vez que inicie sesión en la app, aparecerá la ventana Configurar protección. Para proteger su dispositivo, le recomendamos que siga estos pasos:

- **Estado de la suscripción.** Para que Bitdefender Mobile Security le proteja, debe activar su producto con una suscripción, la cual especifica cuánto tiempo puede utilizar el producto. En cuanto caduque, la app dejará de realizar sus funciones y proteger su dispositivo.
Si posee un código de activación, toque **TENGO UN CÓDIGO** y, luego, toque **ACTIVAR**.
Si ha iniciado sesión con una nueva cuenta de Bitdefender y no tiene un código de activación, puede utilizar el producto sin cargo durante catorce días.
- **Protección web.** Si su dispositivo requiere Accesibilidad para activar la Protección web, toque **ACTIVAR**. Se le redirigirá al menú de Accesibilidad. Toque Bitdefender Mobile Security y, a continuación, active el conmutador correspondiente.
- **Analizador de malware.** Ejecute un análisis puntual del sistema para asegurarse de que su dispositivo está libre de amenazas. Para iniciar el proceso de análisis, toque **ANALIZAR AHORA**.
Tan pronto como comienza el proceso de análisis, aparece el panel de control. Aquí puede ver el estado de seguridad de su dispositivo.

2.5. Panel de Control

Toque el icono Bitdefender Mobile Security en la carpeta de aplicaciones del dispositivo para abrir la interfaz de la app.



El panel de control ofrece información sobre el estado de seguridad de su dispositivo y, mediante Autopilot, le permite mejorar la seguridad de su dispositivo proporcionándole recomendaciones de características.

La tarjeta de estado en la parte superior de la ventana le informa sobre el estado de seguridad del dispositivo mediante mensajes explícitos y ciertos colores. Si Bitdefender Mobile Security no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la tarjeta de estado se pone roja.

Para ofrecerle un funcionamiento eficaz y una mayor protección mientras lleva a cabo diferentes actividades, el **Autopilot de Bitdefender** actuará como su asesor de seguridad personal. Dependiendo de la actividad que realice, Autopilot de Bitdefender le ofrecerá recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. Esto le ayudará a descubrir y aprovechar las ventajas que le ofrecen las características incluidas en la app de Bitdefender Mobile Security.

Cada vez que haya un proceso en curso o cuando una función requiera su atención, se mostrará en el panel de control una tarjeta con más información y las posibles acciones.

Puede acceder a las características de Bitdefender Mobile Security y desplazarse fácilmente gracias a la barra de navegación inferior.

Analizador de malware

Le permite iniciar un análisis bajo demanda y habilitar Analizar almacenamiento. Para más información, diríjase a [Analizador malware \(página 11\)](#).

Protección web

Le garantiza una navegación segura por Internet alertándole de posibles páginas web maliciosas. Para más información, diríjase a [Protección Web \(página 13\)](#).

VPN

Cifra la comunicación por Internet y le ayuda a mantener su privacidad sin importar a qué tipo de red se encuentre conectado. Para más información, diríjase a [VPN \(página 14\)](#).

Alerta de fraude

Le mantiene a salvo alertándole de posibles enlaces maliciosos que le lleguen a través de SMS, apps de mensajería y cualquier notificación. Para obtener más información, consulte [Alerta de fraude \(página 17\)](#).



Antirrobo

Le permite activar o desactivar el Antirrobo, así como configurar sus ajustes. Para más información, diríjase a [Características Antirrobo \(página 20\)](#).

Privacidad de cuentas

Comprueba si se ha producido alguna vulneración de datos de sus cuentas en Internet. Para más información, diríjase a [Privacidad de la cuenta \(página 24\)](#).

Bloqueo de apps

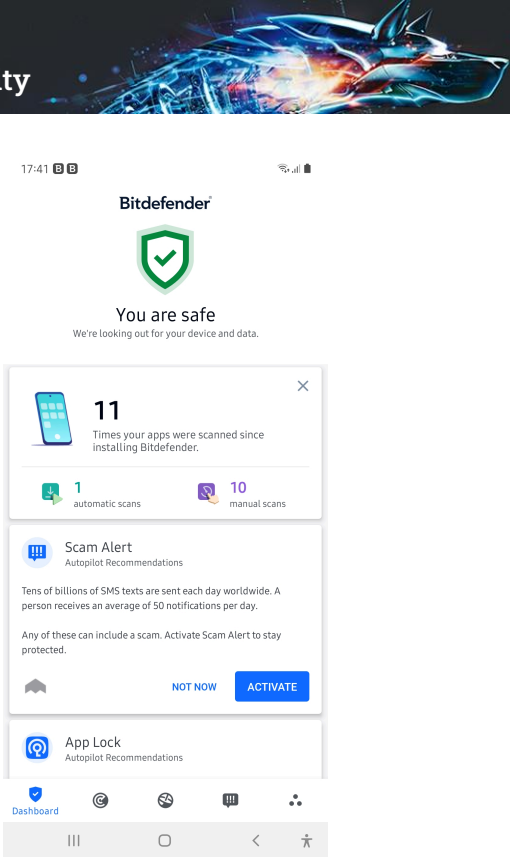
Le permite proteger su aplicaciones instaladas mediante el establecimiento de un código de acceso PIN. Para más información, diríjase a [Bloqueo de apps \(página 26\)](#).

Informes

Mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con la actividad de su dispositivo. Para obtener más información, consulte [Informes \(página 30\)](#).

WearON

Se comunica con su smartwatch para ayudarle a encontrar su teléfono en caso de que lo extravíe u olvide dónde lo dejó. Para más información, diríjase a [Localizador \(página 31\)](#).





3. CARACTERÍSTICAS Y FUNCIONALIDADES

3.1. Analizador malware

Bitdefender protege su dispositivo y sus datos frente a aplicaciones maliciosas utilizando el análisis en la instalación y el análisis bajo demanda.

La interfaz del Analizador de malware proporciona una lista de todos los tipos de amenazas que Bitdefender busca, junto con sus definiciones. Basta con que toque cualquier amenaza para ver su definición.



Nota

Asegúrese de que su dispositivo móvil está conectado a internet. Si su dispositivo no está conectado a internet, no comenzará el proceso de análisis.


○ Análisis al instalar

Siempre que instale una aplicación, Bitdefender Mobile Security la analizará automáticamente mediante la tecnología en la nube. Ese mismo proceso de análisis se lleva a cabo cada vez que se actualizan las apps instaladas.

Si se determina que la aplicación es peligrosa, aparecerá un alerta solicitándole su desinstalación. Toque **Desinstalar** para ir a la pantalla de desinstalación de la aplicación.

○ Análisis bajo demanda

Siempre que quiera asegurarse de que las aplicaciones instaladas en su dispositivo son seguras, puede iniciar un análisis bajo demanda. Para iniciar un análisis bajo demanda:

1. Toque  **Analizador de malware** en la barra de navegación inferior.
2. Toque **INICIAR ANÁLISIS**.



Nota



En Android 6 se requieren permisos adicionales para la característica Analizador de malware. Después de tocar **INICIAR ANÁLISIS**, seleccione **Permitir** para lo siguiente:

- ☐ ¿Permitir que **Antivirus** realice y gestione llamadas telefónicas?
- ☐ ¿Permitir que **Antivirus** acceda a las fotografías, vídeos y archivos en su dispositivo?

Se muestra el progreso del análisis, que podrá detener en cualquier momento.


Por defecto, Bitdefender Mobile Security analizará el almacenamiento interno de su dispositivo, incluyendo cualquier tarjeta SD que tenga montada. De esta forma, podrá detectarse cualquier aplicación peligrosa que pudiera estar en la tarjeta antes de que cause ningún daño.

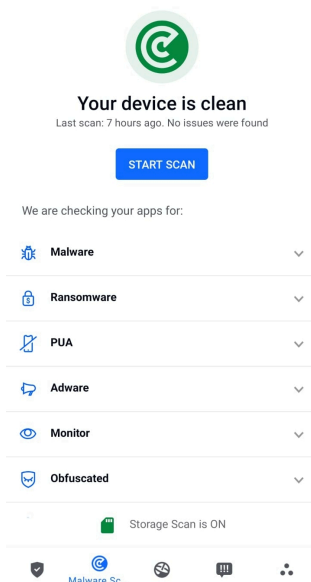
Para deshabilitar el ajuste de Analizar almacenamiento:

1. Toque  **Más** en la barra de navegación inferior.
2. Toque  **Ajustes**.
3. Desactive el conmutador de **Analizar almacenamiento** en el área del Analizador de malware.

Si se detecta cualquier aplicación maliciosa, se mostrará información sobre la misma y la podrá eliminar tocando el botón **DESINSTALAR**.

La tarjeta del Analizador de malware muestra el estado de su dispositivo. Cuando su dispositivo está a salvo, la tarjeta es de color verde. Cuando el dispositivo requiere un análisis, o hay alguna acción que requiera su atención, la tarjeta se vuelve roja.

Si la versión de su Android es 7.1 o posterior, puede tener un acceso directo a Malware Scanner para poder ejecutar análisis más rápidamente, sin abrir la interfaz de Bitdefender Mobile Security. Para ello, mantenga pulsado el icono de Bitdefender en su pantalla de inicio o en el cajón de aplicaciones y, a continuación, seleccione el icono .



3.2. Protección Web

La Protección web comprueba las páginas web de los servicios en la nube de Bitdefender a las que accede con el navegador predeterminado de Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Navegador Yandex, Navegador Huawei y Dolphin.



Nota

En Android 6 se requieren permisos adicionales para la característica Seguridad Web.

Dé permiso para registrarse como servicio de accesibilidad y toque **ACTIVAR** cuando se le solicite. Toque **Antivirus** y active el conmutador. A continuación, confirme que está de acuerdo con el permiso de acceso a su dispositivo.










Web Protection is ON

You are protected against dangerous pages

[TURN OFF](#)

Protected Browsers



Use any of these browsers to be safe

	Chrome Installed	OPEN
	Browser Installed	OPEN
	Puffin Web Browser	
	DuckDuckGo	
	Yandex Browser	
	Dolphin	
	Firefox Focus	



Protección web de Bitdefender está configurado para decirle que use Bitdefender VPN siempre que accede a un sitio de banca online. Dicha notificación aparece en la barra de estado. Le recomendamos que utilice Bitdefender VPN para conectarse a su cuenta bancaria con el fin de que sus datos permanezcan a salvo de posibles vulneraciones de seguridad.

Para deshabilitar la notificación de Protección web:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Desactive el conmutador correspondiente en el área de Protección web.

3.3. VPN

Con Bitdefender VPN puede mantener la privacidad de sus datos personales cada vez que se conecta a redes inalámbricas inseguras de aeropuertos, centros comerciales, cafeterías u hoteles. De esta forma, se pueden evitar situaciones desafortunadas como el robo de datos



personales o que piratas informáticos intenten acceder a la dirección IP de su dispositivo.


La VPN actúa como túnel entre su dispositivo y la red a la que se conecta, para proteger su conexión, cifrar los datos mediante algoritmos de nivel bancario y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente, lo que hace que su dispositivo sea casi imposible de identificar entre la infinidad de dispositivos que utilizan nuestros servicios. Además, mientras está conectado a Internet a través de VPN, puede acceder a contenidos que normalmente están restringidos en determinadas zonas.



Nota

Algunos países practican la censura de Internet y, por lo tanto, el uso de las VPN en su territorio está prohibido por la ley. Para evitar responsabilidades legales, puede que aparezca un mensaje de advertencia cuando trate de utilizar la app Bitdefender VPN por primera vez. Al seguir haciendo uso de esa app, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

Hay dos maneras de activar o desactivar Bitdefender VPN:

- Toque **CONECTAR** en la tarjeta de VPN del panel de control.
Se muestra el estado de Bitdefender VPN.
- Toque  **VPN** en la barra de navegación inferior y, a continuación, toque **CONECTAR**.
Toque **CONECTAR** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras.
Toque **DESCONECTAR** cuando desee desactivar la conexión.



Nota

Cuando activa VPN por primera vez, se le pide que permita que Bitdefender configure una conexión VPN que monitorice el tráfico de red. Toque **OK** para continuar.

Si la versión de su Android es 7.1 o posterior, puede tener un acceso directo a Bitdefender VPN, sin abrir la interfaz de Bitdefender Mobile Security.

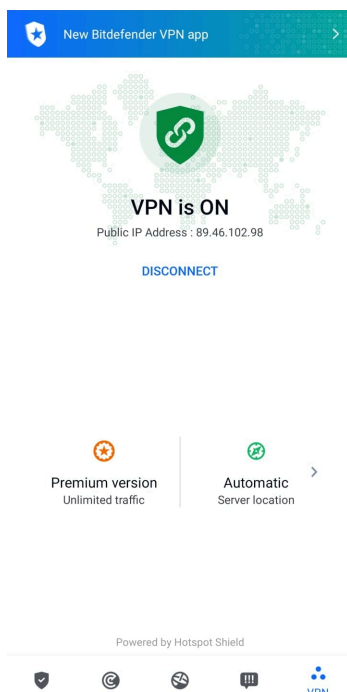
Para ello, mantenga pulsado el icono de Bitdefender en su pantalla de inicio o en el cajón de aplicaciones y, a continuación, seleccione el icono







Para prolongar la duración de la batería, le recomendamos que desactive la característica VPN cuando no la necesite.

Si posee una suscripción Premium y quiere conectarse a determinado servidor, toque en Ubicación del servidor en la característica de VPN y, a continuación, seleccione el lugar que desee. Para más información sobre las suscripciones a VPN, consulte



3.3.1. Ajustes de VPN

Para una configuración avanzada de su VPN:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.

En el área de VPN puede configurar las siguientes opciones:



- Acceso rápido a VPN: Aparecerá una notificación en la barra de estado de su dispositivo para que pueda activar rápidamente la VPN.
- Advertencia de Wi-Fi abierta: cada vez que se conecte a una red Wi-Fi abierta, se le notificará este hecho en la barra de estado de su dispositivo, para que use la VPN.

3.3.2. Suscripciones

Bitdefender VPN ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger su conexión cada vez que lo necesite y le conecta automáticamente a la ubicación del servidor óptimo.

Para disfrutar de tráfico y acceso ilimitado a contenidos en todo el mundo y elegir la ubicación del servidor que desee, actualice a la versión premium.

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento tocando **Activar Premium** en la ventana de VPN.

La suscripción a Bitdefender Premium VPN es independiente de la suscripción a Bitdefender Mobile Security, lo que significa que podrá usarla en toda su extensión independientemente del estado de su suscripción de seguridad. En caso de que caduque la suscripción a Bitdefender Premium VPN, pero la de Bitdefender Mobile Security siga activa, se le revertirá al plan gratuito.

Bitdefender VPN es un producto multiplataforma, disponible en los productos Bitdefender compatibles con Windows, macOS, Android y iOS. Una vez que actualice al plan Premium, podrá usar su suscripción en todos los productos, siempre que inicie sesión con la misma cuenta de Bitdefender.



Nota

Bitdefender VPN también funciona como aplicación independiente en todos los sistemas operativos compatibles: Windows, macOS, iOS y Android.

3.4. Alerta de fraude

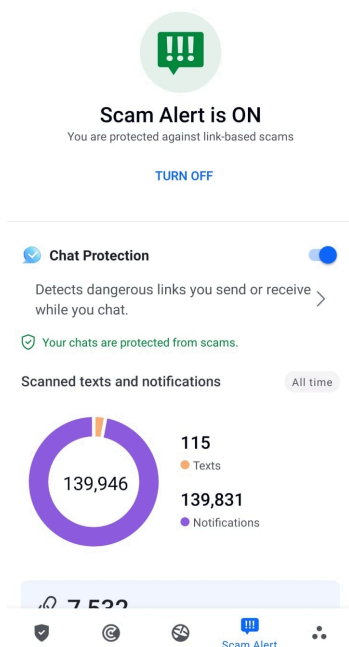
La característica de Alerta de fraude prioriza las medidas preventivas y aborda situaciones potencialmente peligrosas antes de que puedan convertirse en un problema, incluidas las amenazas de malware. La Alerta



de fraude monitoriza en tiempo real todos los mensajes SMS entrantes y notificaciones de Android.

Cuando su teléfono reciba un mensaje con un enlace peligroso, verá una advertencia en la pantalla. Bitdefender le ofrecerá dos opciones. La primera es descartar la información. La segunda opción es **VER DETALLES**. Esto le proporcionará más información sobre el incidente, además de consejos esenciales como los siguientes:

- No abra ni reenvíe el enlace detectado.
- En el caso de los SMS, si es posible, borre el mensaje.
- Bloquee al remitente si no es un contacto de confianza.
- Desinstale la app que envía enlaces peligrosos en sus notificaciones.





Nota

Debido a limitaciones del sistema operativo Android, Bitdefender no puede eliminar mensajes de texto ni adoptar ninguna medida directa en relación con los mensajes SMS ni con ninguna fuente de notificaciones maliciosas. Si ignora la advertencia de la Alerta de fraude e intenta abrir el enlace peligroso, la característica Protección web de Bitdefender lo detectará automáticamente y evitará que su dispositivo se infecte.

3.4.1. Activación de la Alerta de fraude

Para habilitar la Alerta de fraude, debe otorgar a la app Bitdefender Mobile Security acceso a los mensajes SMS y al sistema de notificaciones:

1. Abra la app Bitdefender Mobile Security instalada en su teléfono o tablet Android.
2. En la pantalla principal de la app de Bitdefender, toque la opción **Alerta de fraude** en la barra de navegación inferior y, a continuación, toque **ACTIVAR**.
3. Toque el botón **PERMITIR**.
4. En la lista de Acceso a notificaciones, pase Bitdefender Security a **ACTIVADO**.
5. Confirme la acción tocando **PERMITIR**.
6. Vuelva a la pantalla de Alerta de fraude y toque **PERMITIR** para que Bitdefender pueda analizar los mensajes SMS entrantes.

3.4.2. Protección de chats en tiempo real

Los mensajes de chat son la manera más cómoda de mantenernos en contacto, pero también facilitan que nos lleguen enlaces peligrosos.

Al activar la característica de Protección de chats, el módulo de Alerta de fraude va más allá de la protección de sus mensajes de texto y notificaciones e incluye también la protección de sus chats contra los ataques basados en enlaces, mediante la detección de enlaces peligrosos en los mensajes de chat que usted envíe o reciba.

Para habilitar la Protección de chats:

1. Abra la aplicación Bitdefender Mobile Security instalada en su teléfono o tableta Android.



2. En la pantalla principal de la app de Bitdefender, toque la opción **Alerta de fraude** en la barra de navegación inferior.
3. Encontrará la función característica de Protección de chat en la parte superior de la pestaña Alerta de fraude. Pase el conmutador correspondiente a la posición **ACTIVADO**.



Nota

Actualmente, la Protección de chats es compatible con las siguientes aplicaciones:

- ☐ WhatsApp
- ☐ Facebook Messenger
- ☐ Telegram
- ☐ Discord

3.5. Características Antirrobo

Bitdefender puede ayudarle a encontrar su dispositivo y evitar que sus datos personales caigan en malas manos.

Todo lo que necesita es activar el Antirrobo desde el dispositivo y, cuando sea necesario, acceder a **Bitdefender Central** desde cualquier navegador web en cualquier lugar.



Nota

La interfaz de Antirrobo también incluye un enlace a nuestra app de Bitdefender Central en Google Play Store. Puede usar este enlace para descargar la app, en caso de que aún no lo haya hecho.

Bitdefender Mobile Security ofrece las siguientes características de Antirrobo:

Localización remota

Vea la ubicación actual de su dispositivo en Google Maps. La ubicación se actualiza cada cinco segundos, por lo que puede seguirle la pista si está en movimiento.

La precisión de la ubicación depende de cómo Bitdefender sea capaz de determinarla:



- Si está activado el GPS en el dispositivo, su ubicación puede señalarse con un par de metros de margen siempre que se encuentre en el alcance de los satélites GPS (es decir, no dentro de un edificio).
- Si el dispositivo está en interior, su localización puede determinarse con un margen de decenas de metros si la conexión Wi-Fi está activada y hay redes inalámbricas disponibles a su alcance.
- De lo contrario, la ubicación se determinará utilizando únicamente información de la red móvil, que ofrece una precisión de varios cientos de metros.

Bloqueo remoto

Bloquee la pantalla de su dispositivo y establezca un número PIN para desbloquearla.

Borrado remoto

Borrar todos los datos personales del dispositivo extraviado.

Enviar alerta al dispositivo (Scream)

Enviar de forma remota un mensaje para que se muestre en la pantalla del dispositivo o hacer que reproduzca un sonido fuerte por sus altavoces.



Si pierde su dispositivo, puede indicarle a quien lo encuentre la forma de devolvérselo mostrando un mensaje en la pantalla del dispositivo.

Si ha extraviado su dispositivo y hay probabilidad de que no se encuentre muy lejos (por ejemplo en algún lugar de la casa o la oficina), ¿qué mejor forma de encontrarlo que hacer que reproduzca un sonido a gran volumen? Se reproducirá el sonido incluso aunque el dispositivo se encuentre en modo silencioso.

3.5.1. Activación de Antirrobo

Para habilitar las características antirrobo, simplemente complete el proceso de configuración de la tarjeta Antirrobo disponible en el panel de control.

También puede activar el Antirrobo siguiendo estos pasos:

1. Grifo  **Más** en la barra de navegación inferior.
2. Toque  **Antirrobo**.



3. Toque **ACTIVAR**.
4. Dará comienzo el siguiente procedimiento para ayudarle a activar esta característica:




Nota

En Android 6 se requieren permisos adicionales para la característica Antirrobo.

Para activarlo, siga estos pasos:

- a. Toque **Activar Antirrobo** y, a continuación, toque **ACTIVAR**.
 - b. Dé permiso para que **Antivirus** acceda a la ubicación de este dispositivo
- a. **Conceder privilegios de administrador**
Estos privilegios son esenciales para el funcionamiento del módulo Antirrobo y por tanto debe otorgarlos para poder continuar.
 - b. **Establecer PIN de la aplicación**
Para evitar el acceso no autorizado a su dispositivo, debe establecer un código PIN. Cada vez que desee usar su dispositivo, tendrá que introducir primero el PIN. Como alternativa, en los dispositivos que admiten la autenticación mediante huella dactilar, se puede utilizar una confirmación de este tipo en lugar de usar el código PIN configurado.
El Bloqueo de apps utiliza el mismo código PIN para proteger las aplicaciones que tiene instaladas.
 - c. **Activar Hacer foto**
Si está activada la opción Hacer foto, cada vez que alguien fracase al intentar desbloquear su dispositivo, Bitdefender hará una foto.
Para ser más exactos, cada vez que se introduce mal tres veces seguidas el código PIN o la confirmación de huella dactilar que estableció para proteger su dispositivo, se hace una foto con la cámara frontal. Dicha foto se guarda junto con el motivo de haberla hecho y la hora, y podrá verla cuando abra Bitdefender Mobile Security y seleccione la característica Antirrobo.
Como alternativa, puede ver la foto realizada en su cuenta de Bitdefender.
 - i. Ir a: <https://central.bitdefender.com>.



- ii. Inicie sesión en su cuenta.
- iii. Seleccione el **Mis dispositivos** panel.
- iv. Seleccione su dispositivo Android y, a continuación, la pestaña **Antirrobo**.
- v. Toque  junto a **Consulte sus instantáneas** para ver las últimas fotos que se hicieron.
Solo se guardan las dos últimas fotos.

Una vez activada la función Antirrobo, puede habilitar o deshabilitar los comandos de Control web individualmente desde la ventana de Antirrobo tocando las opciones correspondientes.



3.5.2. Utilización de las características de Antirrobo desde Bitdefender Central



Nota

Todas las características de Antirrobo necesitan que esté activa la opción **Datos en segundo plano** en los ajustes de Uso de datos de su dispositivo.

Para acceder a las características de Antirrobo desde su cuenta de Bitdefender:

1. Acceda a **Bitdefender Central**.
2. Seleccione el **Mis dispositivos** panel.
3. En la ventana **MIS DISPOSITIVOS**, seleccione la tarjeta del dispositivo que desee tocando el botón **Ver detalles** correspondiente.
4. Seleccione la pestaña **Antirrobo**.
5. Toque el botón que corresponda a la característica que desea utilizar:
Localizar - muestra la ubicación de su dispositivo en Google Maps.
Mostrar IP - Muestra la última dirección IP del dispositivo seleccionado.
 **Alerta** - escriba un mensaje para mostrarlo en la pantalla de su dispositivo y/o haga que su dispositivo reproduzca una alarma sonora.
 **Bloquear**: Bloquea su dispositivo y establece un código PIN para desbloquearlo.



 **Borrar:** Elimina toda la información de su dispositivo.





Importante

Después de borrar un dispositivo, todas las características de Anti-Theft dejan de funcionar.

3.5.3. Ajustes de Antirrobo

Si desea habilitar o deshabilitar los comandos remotos:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Anti-rob.**
3. Habilitar o deshabilitar las opciones deseadas.

3.6. Privacidad de la cuenta



Privacidad de cuentas de Bitdefender detecta si se ha producido alguna vulneración de datos en las cuentas que utiliza para realizar pagos y compras online o para iniciar sesión en diferentes apps o sitios web. Una cuenta puede almacenar datos como contraseñas e información de tarjetas de crédito o de cuentas bancarias y, si no están adecuadamente protegidos, es posible que se produzcan robos de identidad o vulneraciones de la privacidad.

El estado de privacidad de la cuenta se indica justo después de la validación.

Se efectúan nuevas comprobaciones automáticas, configuradas para ejecutarse en segundo plano, pero también se pueden ejecutar análisis manuales a diario.

Se mostrarán notificaciones siempre que se detecten nuevas vulneraciones que afecten a cualquiera de las cuentas de correo electrónico validadas.

Para empezar a poner a salvo su información personal:

1. Grifo  **Más** en la barra de navegación inferior.
2. Toque  **Privacidad de cuentas.**
3. Toque **PUESTA EN MARCHA.**



4. Aparece la dirección de correo electrónico que utilizara para crear su cuenta de Bitdefender y se añade automáticamente a la lista de cuentas monitorizadas.
5. Para añadir otra cuenta, toque **AÑADIR CUENTA** en la ventana de Privacidad de cuentas y, a continuación, escriba la dirección de correo electrónico.

Toque **AÑADIR** para continuar.

Bitdefender tiene que validar esta cuenta antes de mostrar información privada. Por ello, se ha enviado un mensaje con un código de validación a la dirección de correo electrónico proporcionada.



Compruebe su bandeja de entrada y, a continuación, escriba el código que ha recibido en la zona **Privacidad de la cuenta** de su app. Si no encuentra el mensaje de validación en su bandeja de entrada, compruebe la carpeta de correo no deseado.

Se muestra el estado de privacidad de la cuenta validada.

En caso de detectarse vulneraciones en cualquiera de sus cuentas, le recomendamos que cambie su contraseña lo antes posible. Para crear una contraseña realmente segura, siga estos consejos:

- Créela de por lo menos ocho caracteres de longitud.
- Utilice una combinación de mayúsculas y minúsculas.
- Incluya al menos un número o un símbolo, como por ejemplo #, @, % o !.



Una vez que haya protegido una cuenta que había sufrido una vulneración de la privacidad, puede confirmar los cambios marcando la vulneración identificada como Solucionada. Para ello:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Privacidad de la cuenta**.
3. Toque la cuenta que acaba de proteger.
4. Toque la vulneración para la que protegió la cuenta.
5. Toque **SOLUCIONADA** para confirmar que la cuenta está protegida.

Cuando todas las vulneraciones detectadas se hayan marcado como **Solucionadas**, la cuenta ya no aparecerá como objeto de vulneraciones, al menos hasta que se vuelva a detectar una nueva vulneración.

Para dejar de recibir notificaciones cada vez que se realicen análisis automáticos:



1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Desactive el conmutador correspondiente en el área de Privacidad de la cuenta.

3.7. Bloqueo de apps

Las aplicaciones instaladas, como las de correo electrónico, fotos o mensajes, pueden contener datos de carácter personal que le gustaría mantener en privado restringiendo selectivamente el acceso a ellos.



El Bloqueo de apps le ayuda a bloquear el acceso no deseado a sus aplicaciones mediante el establecimiento de un código de acceso PIN de seguridad. El código PIN que establezca debe tener un mínimo de cuatro caracteres, pero no más de ocho, y se le requerirá cada vez que quiera acceder a las aplicaciones restringidas seleccionadas.

Se puede recurrir a la autenticación biométrica (como la confirmación mediante huella dactilar o el reconocimiento facial) en lugar de usar el código PIN configurado.

3.7.1. Activación del Bloqueo de apps

Para restringir el acceso a las aplicaciones seleccionadas, configure el Bloqueo de apps en la tarjeta que se muestra en el panel de control después de activar el Antirrobo.

También puede activar el Bloqueo de apps siguiendo estos pasos:

1. Grifo  **Más** en la barra de navegación inferior.
2. Toque  **Bloqueo de apps**.
3. Grifo **ENCENDER**.
4. Permita el acceso a los datos de uso para Bitdefender Security.
5. Permita **mostrar en otras aplicaciones**.
6. Vuelva a la app, configure el código de acceso y, a continuación, toque **ESTABLECER PIN**.



Nota

Este paso solo está disponible si no ha configurado previamente el PIN de Antirrobo.

7. Active la opción Hacer foto para identificar a cualquier persona que intente acceder a sus datos privados.



Nota

En Android 6 se requieren permisos adicionales para la característica Hacer foto. Para activarla, permita que **Antivirus** tome fotos y grabe vídeo.

8. Seleccione las aplicaciones desea proteger.

Si se usa el PIN o la huella dactilar erróneamente cinco veces seguidas, se dejará un tiempo de espera de treinta segundos. Así, se bloqueará cualquier intento de entrada ilegítima en las apps protegidas.



Nota

El Antirrobo utiliza el mismo código PIN para ayudarle a localizar su dispositivo.



Set Application PIN

Set an application PIN to prevent unauthorized access to your device and apps. Also used by Anti-Theft.

Enter PIN (4-8 digits)



NOT NOW

SET PIN

3.7.2. Modo de bloqueo



La primera vez que añada una aplicación al Bloqueo de apps, aparecerá la pantalla del modo de bloqueo de apps. Desde aquí puede elegir cuándo debe el Bloqueo de apps proteger las aplicaciones instaladas en su dispositivo.

Puede escoger una de las siguientes opciones:





- **Requerir el desbloqueo cada vez:** Habrá de utilizar el código PIN o la huella dactilar que ha configurado siempre que acceda a las apps bloqueadas.
- **Mantener desbloqueado hasta que se apague la pantalla:** Podrá acceder libremente a sus aplicaciones hasta que se apague la pantalla.
- **Bloquear después de 30 segundos:** Puede salir y volver a acceder a sus aplicaciones desbloqueadas en un plazo de treinta segundos.

Si desea cambiar el ajuste seleccionado:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Toque **Requerir el desbloqueo cada vez** en el área del Bloqueo de apps.
4. Escoja la opción deseada.

3.7.3. Opciones de Bloqueo de Apps

Para una configuración avanzada del Bloqueo de apps:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.

En el área del Bloqueo de apps puede configurar las siguientes opciones:

- **Sugerencia de aplicación sensible:** Reciba una notificación de bloqueo cada vez que instale una aplicación sensible.
- **Requerir el desbloqueo cada vez:** Elija una de las opciones disponibles de bloqueo y desbloqueo.
- **Desbloqueo inteligente:** Mantenga las aplicaciones desbloqueadas mientras esté conectado a redes Wi-Fi de confianza.
- **Teclado aleatorio:** Evite la lectura del PIN distribuyendo los números al azar.

3.7.4. Hacer foto

Con Hacer foto de Bitdefender puede poner en una situación comprometida a sus amigos o familiares. De esta manera podrá atajar



su curiosidad, para que no traten de ver sus archivos personales o las aplicaciones que utiliza.



El funcionamiento de esta característica es muy sencillo: cada vez que se introduce tres veces seguidas de forma incorrecta el código PIN o la confirmación de huella dactilar que estableció para proteger sus apps, se toma una foto con la cámara frontal. Dicha foto se guarda junto con el motivo de haberla hecho y la hora, y podrá verla cuando abra Bitdefender Mobile Security y acceda a la función de Bloqueo de apps.



Nota


Esta característica solo está disponible en teléfonos que posean una cámara frontal.

Para configurar la característica Hacer foto para el Bloqueo de apps:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Active el conmutador correspondiente en el área de Hacer foto.



Las fotos que se tomen cuando se introduzca un PIN incorrecto se mostrarán en la ventana de Bloqueo de apps y se pueden ver a pantalla completa.

Como alternativa, se pueden ver en su cuenta de Bitdefender:

1. Ir a: <https://central.bitdefender.com>.
2. Iniciar sesión en su cuenta.
3. Seleccione el panel **Mis dispositivos**.
4. Seleccione su dispositivo Android y luego el **Anti-robo** pestaña.
5. Grifo  junto a **Revisa tus instantáneas** para ver las últimas fotos que se tomaron.

Solo se guardan las dos fotos más recientes.

Para detener la carga de fotos en su cuenta de Bitdefender:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Deshabilite **Cargar fotos** en el área de Hacer foto.






3.7.5. Desbloqueo inteligente

Una forma fácil de evitar que el Bloqueo de apps le pida introducir el código PIN o la confirmación de huella dactilar para las apps protegidas cada vez que acceda a ellas es activar el Desbloqueo inteligente.

Con el Desbloqueo inteligente puede determinar que las redes Wi-Fi que utiliza normalmente son de confianza, de forma que cuando se conecte a ellas, se deshabilitarán los ajustes del Bloqueo de apps para las aplicaciones protegidas.

Para configurar el Desbloqueo inteligente:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Bloqueo de aplicación**.
3. Toque el botón .
4. Toque el conmutador junto a **Desbloqueo inteligente** si la característica no estuviera habilitada aún.
Valide con su huella dactilar o su PIN.
La primera vez que active la característica, deberá habilitar el permiso de ubicación. Toque el botón **PERMITIR** y, a continuación, toque nuevamente **PERMITIR**.
5. Toque **AÑADIR** para establecer la conexión Wi-Fi que utiliza actualmente como red de confianza.



Si cambia de opinión, desactive la característica y las redes Wi-Fi que haya establecido como redes de confianza dejarán de ser tratadas como tal.

3.8. Informes

La característica Informes mantiene un registro detallado de los eventos relacionados con las actividades de análisis en su dispositivo.

Siempre que sucede algo relevante para la seguridad de su dispositivo, se añade un nuevo mensaje a los Informes.

Para acceder a la sección Informes:

1. Grifo  **Más** en la barra de navegación inferior.
2. Toque  **Informes**.



Tiene las siguientes pestañas disponibles en la ventana Informes:



- **INFORMES SEMANALES:** Aquí tiene acceso al estado de seguridad y a las tareas realizadas en la semana actual y anterior. Todos los domingos se genera el informe de la semana en curso. Recibirá una notificación informándole al respecto cuando esté disponible.



En esta sección se mostrará un nuevo consejo cada semana, así que asegúrese de revisarla con cierta frecuencia para obtener el máximo partido de la app.

Para dejar de recibir notificaciones cada vez que se genera un informe:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Desactive el conmutador **Notificación de nuevo informe** en el área de Informes.

- **REGISTRO DE ACTIVIDAD:** Aquí puede consultar información detallada sobre la actividad de la app Bitdefender Mobile Security desde que se instaló en su dispositivo Android.

Para borrar el registro de actividad disponible:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Toque **Borrar el registro de actividad** y, a continuación, toque **BORRAR**.

3.9. Localizador

Con Bitdefender WearON podrá encontrar fácilmente su smartphone si se lo dejó en la oficina, en una sala de conferencias o debajo de un cojín en el sofá. Puede encontrar el dispositivo incluso si tiene activado el modo silencioso.

Mantenga esta característica habilitada para asegurarse de que siempre tiene su smartphone a mano.



Nota

Esta característica funciona con Android 4.3 y Android Wear.



3.9.1. Activación de WearON

Para utilizar WearON, solo tiene que conectar su smartwatch a la aplicación Bitdefender Mobile Security y activar la característica con el siguiente comando de voz:

Iniciar:<Dónde está mi teléfono>

Bitdefender WearON tiene dos comandos:

1. **Alerta de teléfono**

Con la característica de Alerta de teléfono puede encontrar rápidamente su smartphone cuando se aleje demasiado de él.

Si lleva puesto su smartwatch, este detectará automáticamente la app en su teléfono y vibrará cuando se aleje mucho y los dispositivos pierdan conectividad Bluetooth.



Para activar esta característica, abra Bitdefender Mobile Security, toque **Ajustes globales** en el menú y seleccione el conmutador correspondiente en la sección WearON.

2. **Scream**

Encontrar su teléfono nunca fue tan fácil. Cuando se olvide de dónde dejó su teléfono, toque el comando Scream de su reloj para hacer que suene su teléfono.

3.10. Acerca de

Para hallar información sobre la versión de Bitdefender Mobile Security que tiene instalada, leer el Acuerdo de suscripción y la Política de privacidad, así como ver las licencias de código abierto:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Toque la opción deseada en el área Acerca de.



4. ACERCA DE BITDEFENDER CENTRAL

Bitdefender Central es la plataforma en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo conectado a Internet accediendo a <https://central.bitdefender.com> o directamente desde la app Bitdefender Central en dispositivos iOS y Android.

Para instalar la app de Bitdefender Central en sus dispositivos:

- **En Android:** Busque Bitdefender Central en Google Play y luego descargue e instale la app. Siga los pasos necesarios para finalizar la instalación.
- **En iOS:** Busque Bitdefender Central en App Store y luego descargue e instale la app. Siga los pasos necesarios para finalizar la instalación.

Una vez que haya iniciado sesión, puede empezar por hacer lo siguiente:

- Descargar e instalar Bitdefender en los sistemas operativos Windows, iOS, macOS y Android. Los productos disponibles para descargar son:
 - Bitdefender Mobile Security for Android
 - Bitdefender Mobile Security for iOS
 - La línea de productos de Windows de Bitdefender
 - Bitdefender Antivirus for Mac
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.
- Proteja los dispositivos de red y sus datos contra robo o pérdida con [Antirrobo](#).

4.1. Acceso a Bitdefender Central

Existen dos formas de acceder a Bitdefender Central

- Desde su navegador Web:



1. Abra un navegador Web en cualquier dispositivo con acceso a internet.
 2. Ir a: <https://central.bitdefender.com>.
 3. Inicie sesión en su cuenta con su dirección de correo electrónico y contraseña.
- Desde su dispositivo Android o iOS:
Abra la app Bitdefender Central que ha instalado.



Nota

En este material, hemos incluido las opciones que puede encontrar en la interfaz web.


4.2. Autenticación en dos fases

El método de autenticación en dos fases aporta una capa adicional de seguridad a su cuenta de Bitdefender, ya que requiere un código de autenticación además de sus credenciales de inicio de sesión. De esta manera, evitará la toma de control de la cuenta y mantendrá alejados ciertos tipos de ataques informáticos, como los de registradores de pulsaciones de teclas, los de fuerza bruta o los de diccionario.

4.2.1. Activar la autenticación en dos fases

Al habilitar la autenticación en dos fases, su cuenta de Bitdefender estará mucho más segura. Su identidad se verificará cada vez que inicie sesión desde diferentes dispositivos, ya sea para instalar uno de los productos de Bitdefender, para verificar el estado de su suscripción o para ejecutar tareas en sus dispositivos de forma remota.

Para habilitar la autenticación en dos fases:

1. Acceso [Centro de Bitdefender](#).
2. Toque el icono  en la parte superior derecha de la pantalla.
3. Toque **Cuenta de Bitdefender** en el menú deslizante.
4. Seleccione la pestaña **Contraseña y seguridad**.
5. Grifo **EMPEZAR**.

Escoja uno de los siguientes métodos:



- **App de autenticación:** Use una app de autenticación para generar un código cada vez que desee iniciar sesión en su cuenta de Bitdefender.
Si desea utilizar una app de autenticación, pero no está seguro de cuál elegir, tiene a su disposición una lista con las que recomendamos.
 - a. Toque **USAR LA APP DE AUTENTICACIÓN** para comenzar.
 - b. Para iniciar sesión en un dispositivo con Android o iOS, use su dispositivo para leer el código QR.
Para iniciar sesión en un equipo de escritorio o portátil, puede añadir manualmente el código mostrado.
Toque **CONTINUAR**.
 - c. Inserte el código proporcionado por la app o el que se muestra en el paso anterior y, a continuación, toque **ACTIVAR**.
- **Correo electrónico:** Cada vez que inicie sesión en su cuenta de Bitdefender, se le enviará un código de verificación a su bandeja de entrada de correo electrónico. Consulte su cuenta de correo electrónico y escriba el código que se le proporciona.
 - a. Toque **USAR CORREO ELECTRÓNICO** para comenzar.
 - b. Lea su correo electrónico y escriba el código que se le proporciona.
Tenga en cuenta que tiene cinco minutos para revisar su cuenta de correo electrónico y escribir el código generado. Si se agotase el tiempo, debería generar uno nuevo siguiendo los mismos pasos.
 - c. Toque **ACTIVAR**.
 - d. Se le proporcionan diez códigos de activación. Puede copiar, descargar o imprimir la lista y utilizarla en caso de que pierda su dirección de correo electrónico o no pueda iniciar sesión. Cada código puede utilizarse una sola vez.
 - e. Toque **HECHO**.

En caso de que desee dejar de usar la autenticación en dos fases:

1. Toque **DESACTIVAR LA AUTENTICACIÓN EN DOS FASES**.



2. Consulte su app o su cuenta de correo electrónico y escriba el código que ha recibido.


En caso de que haya optado por recibir el código de autenticación por correo electrónico, tiene cinco minutos para consultar su cuenta de correo electrónico y escribir el código generado. Si se agotase el tiempo, debería generar uno nuevo siguiendo los mismos pasos.

3. Confirme su elección.

4.3. Añadir dispositivos de confianza

Para asegurarnos de que solo usted pueda acceder a su cuenta de Bitdefender, es posible que le solicitemos antes un código de seguridad. Si desea omitir este paso siempre que se conecte desde el mismo dispositivo, le recomendamos que lo añada como dispositivo de confianza.

Para añadir dispositivos de confianza:

1. Acceso [Centro de Bitdefender](#).
2. Toque en el  icono en la parte superior derecha de la pantalla.
3. Grifo **Cuenta de Bitdefender** en el menú deslizante.
4. Selecciona el **contraseña y seguridad** pestaña.
5. Toque **Dispositivos de confianza**.
6. Aparecerá la lista con los dispositivos en los que está instalado Bitdefender. Toque en el dispositivo deseado.

Puede añadir tantos dispositivos como desee, siempre y cuando tengan Bitdefender instalado y su suscripción sea válida.

4.4. Mis dispositivos

El área **Mis dispositivos** de su cuenta de Bitdefender le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a Internet. Las tarjetas de cada dispositivo muestran el nombre de este, su estado de protección y si existen riesgos para la seguridad que afecten a la protección de sus dispositivos.



4.4.1. Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Mobile Security de la siguiente manera:

1. Acceso [Centro de Bitdefender](#).
2. Selecciona el **Mis dispositivos** panel y, a continuación, toque **INSTALAR PROTECCIÓN**.
3. Elija una de las dos opciones disponibles:

- **Protege este dispositivo**

Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.

- **Proteger otros dispositivos**

Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.


Toque **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y toque **ENVIAR CORREO**. Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.

En el dispositivo en el que desea instalar su producto Bitdefender, verifique la cuenta de correo electrónico que ingresó y luego toque el botón de descarga correspondiente.

4. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

4.4.2. Personalice su dispositivo


Para identificar fácilmente sus dispositivos, puede personalizar el nombre de los mismos:

1. Acceso [Centro de Bitdefender](#).
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, en el icono  de la esquina superior derecha de la pantalla.




4. Seleccione **Ajustes**.
5. Escriba un nuevo nombre en el campo **Nombre del dispositivo** y, a continuación, toque **GUARDAR**.

Puede crear y asignar un propietario a cada uno de los dispositivos para gestionarlos mejor:

1. Acceso [Centro de Bitdefender](#).
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado, y luego el  icono en la esquina superior derecha de la pantalla.
4. Seleccione **Perfil**.
5. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes. Personalice el perfil incluyendo una foto, seleccionando una fecha de nacimiento y añadiendo una dirección de correo electrónico y un número de teléfono.
6. Haga clic en **AÑADIR** para guardar el perfil.
7. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, toque **ASIGNAR**.

4.4.3. Acciones remotas

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceso [Centro de Bitdefender](#).
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado, y luego el  icono en la esquina superior derecha de la pantalla.
4. Seleccione **Actualizar**.

Para tener acceso a más acciones remotas e información acerca de su producto Bitdefender en un dispositivo concreto, haga clic en la tarjeta de dicho dispositivo.

Una vez que haga clic en una tarjeta de dispositivo, tendrá a su disposición las siguientes pestañas:

- **Panel de control.** En esta ventana puede ver información sobre el dispositivo seleccionado, comprobar el estado de su protección, el de Bitdefender VPN y cuántas amenazas se han bloqueado en los



últimos siete días. El estado de la protección puede ser verde, cuando no hay ningún problema que afecte a su producto; amarillo, si el dispositivo requiere su atención; o rojo, cuando el dispositivo está en riesgo. Cuando haya problemas que afecten a su dispositivo, toque la flecha desplegable en el área de estado superior para obtener más información. Desde aquí, puede

- **Protección.** Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Toque el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible.
- **Optimizador.** Aquí puede mejorar el rendimiento de un dispositivo de forma remota mediante un rápido análisis, detección y limpieza de archivos inútiles. Toque el botón **INICIAR** y, a continuación, seleccione las áreas que desea optimizar. Toque nuevamente en el botón **INICIAR** para poner en marcha el proceso de optimización. Toque **Más detalles** para acceder a un informe pormenorizado acerca de los problemas solucionados.
- **Antirrobo.** Si no se acuerda de dónde ha puesto su dispositivo o si se lo han robado o lo ha perdido, con la función Antirrobo puede localizarlo y llevar a cabo acciones remotas. Toque **LOCALIZAR** para conocer la ubicación de su dispositivo. Se mostrará la última posición conocida, junto con la fecha y la hora.
- **Vulnerabilidad.** Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, toque el botón **ANALIZAR** en la pestaña de Vulnerabilidad. Las vulnerabilidades no se pueden solucionar de forma remota. En caso de encontrar cualquier vulnerabilidad, tendrá que ejecutar un nuevo análisis en el dispositivo y adoptar las medidas recomendadas. Toque **Más detalles** para acceder a un informe pormenorizado acerca de los problemas encontrados.

4.5. Actividad

En el área de Actividad, tiene acceso a información sobre los dispositivos que tienen Bitdefender instalado.



Una vez que accede a la ventana **Actividad**, tiene a su disposición las siguientes fichas:

- **Mis dispositivos.** Aquí puede ver el número de dispositivos conectados junto con el estado de su protección. Para solucionar problemas de forma remota en los dispositivos detectados, toque **Solucionar problemas** y, a continuación, toque **ANALIZAR Y SOLUCIONAR LOS PROBLEMAS**.

Para ver más información sobre los problemas detectados, haga clic en **Ver problemas**.

La información sobre las amenazas detectadas no se puede recuperar de los dispositivos basados en iOS.

- **Amenazas bloqueadas.** Aquí puede ver un gráfico que muestra una estadística general con información sobre las amenazas bloqueadas durante las últimas 24 horas y siete días. La información mostrada se recupera dependiendo del comportamiento malicioso detectado en los archivos, aplicaciones y URL a los que se accede.
- **Principales usuarios con amenazas bloqueadas.** Aquí puede ver los usuarios que se han sido objeto de más amenazas.
- **Principales dispositivos con amenazas bloqueadas.** Aquí puede ver los dispositivos donde se han encontrado más amenazas.

4.6. Mis suscripciones

La plataforma Bitdefender Central le da la posibilidad de administrar fácilmente las suscripciones que tiene para todos sus dispositivos.

4.6.1. Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceso [Centro de Bitdefender](#).
2. Seleccione el panel **Mis suscripciones**.

Aquí tiene información sobre la disponibilidad de las suscripciones que posee y el número de dispositivos que utilizan cada una de ellas.

Puede añadir un nuevo dispositivo a una suscripción o renovarlo seleccionando una tarjeta de suscripción.



Nota

Puede tener una o más suscripciones en su cuenta siempre que sean para diferentes plataformas (Windows, macOS, iOS o Android).

4.6.2. Activar la suscripción

Una suscripción se puede activar durante el proceso de instalación mediante su cuenta de Bitdefender. Tras el proceso de activación, da comienzo la cuenta atrás de la validez de la suscripción.

Si ha comprado un código de activación a uno de nuestros resellers o lo ha recibido de regalo, puede añadir su disponibilidad a su suscripción de Bitdefender.

Para activar una suscripción mediante un código de activación, siga estos pasos:

1. Acceso [Centro de Bitdefender](#).
2. Selecciona el **mis Suscripciones** panel.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Toque **ACTIVAR** para continuar.

La suscripción ya está activada.

4.6.3. Renovar suscripción


Si ha inhabilitado la renovación automática de su suscripción de Bitdefender, puede renovarla manualmente siguiendo los pasos que se exponen a continuación:

1. Acceso [Centro de Bitdefender](#).
2. Selecciona el **mis Suscripciones** panel.
3. Seleccione la tarjeta de suscripción deseada.
4. Toque **RENOVAR** para continuar.

Se abrirá una página web en su navegador de Internet, donde puede renovar su suscripción de Bitdefender.



4.7. Notificaciones

Para ayudarle a mantenerse informado de lo que sucede en los dispositivos asociados a su cuenta, tiene fácilmente accesible el icono . Haciendo clic en él dispondrá de una panorámica general con información acerca de la actividad de los productos de Bitdefender instalados en sus dispositivos.



5. PREGUNTAS FRECUENTES

¿Por qué necesita Bitdefender Mobile Security una conexión a Internet?



La aplicación necesita comunicarse con los servidores de Bitdefender para determinar el estado de seguridad de las aplicaciones que analiza y de las páginas Web que visita, y también para recibir comandos de su cuenta Bitdefender cuando utiliza las características de Antirrobo.

¿Para qué necesita Bitdefender Mobile Security cada permiso?

- Acceso a Internet -> Se usa para la comunicación con la nube.
- Leer identidad y estado del teléfono -> Se usa para detectar si el dispositivo está conectado a Internet y extraer determinada información del dispositivo necesaria para crear un ID único cuando se comunica con la nube de Bitdefender.
- Leer y guardar favoritos del navegador -> El módulo de Protección web elimina sitios peligrosos del historial de navegación.
- Leer datos de registro -> Bitdefender Mobile Security detecta signos de amenazas desde los registros de Android.
- Localizar -> Se requiere para la localización remota.
- Cámara -> Necesaria para Hacer foto.
- Almacenamiento -> Se utiliza para permitir que el Analizador de malware compruebe la tarjeta SD.

¿Cómo puedo dejar de enviar información a Bitdefender sobre aplicaciones sospechosas?



Por defecto, Bitdefender Mobile Security envía informes a los servidores de Bitdefender sobre las aplicaciones sospechosas que instala. Esta información es fundamental para mejorar la detección de amenazas y puede ayudarnos a ofrecerle una experiencia de usuario mejor en el futuro. En caso de que desee dejar de enviarnos información sobre aplicaciones sospechosas, haga lo siguiente:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Desactive **Detección en la nube** en el área del Analizador de malware.

¿Dónde puedo ver detalles sobre la actividad de la aplicación?




Bitdefender Mobile Security mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para ver la actividad de la aplicación:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Informes**.



En la ventana INFORMES SEMANALES, puede acceder a los informes que se generan cada semana y en la ventana REGISTRO DE ACTIVIDAD puede ver información sobre la actividad de su aplicación de Bitdefender.

He olvidado el código PIN que establecí para proteger mi aplicación. ¿Qué hago?

1. Acceso [Centro de Bitdefender](#).
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado y, a continuación, toque  en la esquina superior derecha de la pantalla.
4. Seleccionar **Ajustes**.
5. Obtenga el código PIN del campo **PIN de aplicación**.

¿Cómo puedo cambiar el código PIN que establecí para el Bloqueo de apps y Antirrobo?

Si desea cambiar el código PIN que estableció para el Bloqueo de apps y Antirrobo:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Ajustes**.
3. Toque **CÓDIGO PIN** de seguridad en el área de Antirrobo.
4. Escriba el código PIN actual.
5. Escriba el nuevo código PIN que desee establecer.




¿Cómo puedo desactivar el Bloqueo de apps?

No existe forma de eliminar el Bloqueo de apps, pero puede desactivarlo fácilmente dejando sin marcar las casillas de verificación junto a las apps seleccionadas después de validar el PIN o la huella dactilar que ha establecido.




¿Cómo puedo configurar otra red inalámbrica para que se considere de confianza?

Primero, debe conectar su dispositivo a la red inalámbrica que desee establecer como red de confianza. A continuación, siga estos pasos:

1. Grifo  **Más** en la barra de navegación inferior.
2. Grifo  **Bloqueo de aplicación**.
3. Toque  en la esquina superior derecha.
4. Toque **AÑADIR** junto a la red que desee establecer como red de confianza.

¿Cómo puedo dejar de ver las fotos tomadas en mis dispositivos?

Para dejar de visualizar las fotos tomadas en sus dispositivos:

1. Acceso [Centro de Bitdefender](#).
2. Toque  en la parte superior derecha de la pantalla.
3. Toque **Ajustes** en el menú deslizante.
4. Desactive la opción **Mostrar/no mostrar fotos hechas remotamente desde sus dispositivos**.

¿Cómo puedo proteger mis compras online?

Realizar compras online entraña grandes riesgos si se pasan por alto algunos detalles. Para no caer víctima de un fraude, le recomendamos que haga lo siguiente:

- ☐ Mantenga actualizada su app de seguridad.
- ☐ Realice pagos por Internet solo si cuenta con protección de compras.
- ☐ Utilice una VPN cuando se conecte a internet desde lugares públicos o a través de redes inalámbricas que no sean de fiar.
- ☐ Preste atención a las contraseñas que ha asignado a sus cuentas de Internet. Deben ser seguras, combinando letras mayúsculas y minúsculas, números y símbolos (@, !, %, #, etc.).
- ☐ Asegúrese de enviar la información a través de conexiones seguras. La extensión del sitio web ha de ser HTTPS://, y no HTTP://.

¿Cuándo debo usar Bitdefender VPN?



Debe tener cuidado cuando acceda, descargue o cargue contenidos en internet. Para asegurarse de que se mantiene a salvo mientras navega por la web, le recomendamos que use Bitdefender VPN cuando:

- Desee conectarse a redes inalámbricas públicas.
- Desee acceder a contenidos que normalmente están restringidos en zonas concretas, sin importar si está en su hogar o en el extranjero.
- Desee mantener la privacidad de sus datos personales (nombres de usuario, contraseñas, información de tarjetas de crédito, etc.).
- Desee ocultar su dirección IP.

¿Afecta negativamente Bitdefender VPN a la duración de la batería de mi dispositivo?


Bitdefender VPN está diseñado para proteger sus datos personales, ocultar su dirección IP mientras está conectado a redes inalámbricas inseguras y acceder a contenidos restringidos en ciertos países. Para evitar el consumo innecesario de la batería de su dispositivo, le recomendamos que use VPN solo cuando lo necesite, y que prescinda de él cuando no esté conectado.

¿Por qué parece ir más lento Internet cuando me conecto a través de Bitdefender VPN?

Bitdefender VPN está pensado para brindarle agilidad cuando navega por la web; sin embargo, su conectividad a Internet o la distancia al servidor con el que se conecta pueden producir demoras. De ser así, si no es imprescindible que se conecte desde su ubicación a un servidor lejano (por ejemplo, desde Estados Unidos hasta China), le recomendamos que permita que Bitdefender VPN le conecte automáticamente al servidor más cercano o que encuentre un servidor más próximo a su ubicación actual.

¿Puedo cambiar la cuenta de Bitdefender vinculada a mi dispositivo?

Sí, puede cambiar fácilmente la cuenta de Bitdefender vinculada a su dispositivo siguiendo los pasos que se indican a continuación:

1. Grifo  **Más** en la barra de navegación inferior.
2. Toque su dirección de correo electrónico.
3. Toque **Salir de su cuenta**. Si se ha configurado un código PIN, se le pide que lo escriba.



4. Confirme su elección.
5. Escriba la dirección de correo electrónico y la contraseña de su cuenta en los campos correspondientes y, a continuación, toque **INICIAR SESIÓN**.

¿Cómo afecta Bitdefender Mobile Security al rendimiento y a la batería de mi dispositivo?

Conseguimos un impacto mínimo. La aplicación únicamente se ejecuta cuando es imprescindible – lo que incluye la instalación y cuando se utiliza la interfaz de la aplicación – o cuando quiere comprobar la seguridad. Bitdefender Mobile Security no se ejecuta en segundo plano cuando llama a sus amigos, escribe sus mensajes o juega una partida.

¿Qué es el Administrador de dispositivos?

El Administrador de dispositivos es una característica de Android que da a Bitdefender Mobile Security los permisos que necesita para ejecutar determinadas tareas de forma remota. Sin estos privilegios, el bloqueo remoto no funcionaría y el borrado del dispositivo no podría eliminar completamente sus datos. Si desea desinstalar la app, asegúrese de revocar estos privilegios antes de tratar de desinstalarla desde **Ajustes > Seguridad > Seleccionar administradores de dispositivo**.

Cómo arreglar el error "No Google Token" que aparece cuando se inicia sesión en Bitdefender Mobile Security.

Este error ocurre cuando el dispositivo no está asociado con una cuenta de Google, o el dispositivo está asociado con una cuenta pero un problema temporal evita que se conecte a Google. Pruebe una de las siguientes soluciones:

- Acceda en Android a **Ajustes > Aplicaciones > Administrar aplicaciones > Bitdefender Mobile Security** y toque **Borrar datos**. Luego, intente iniciar sesión nuevamente.
- Asegúrese de que su dispositivo está asociado a una cuenta de Google.

Para comprobarlo, acceda a **Ajustes > Cuentas y sincronización** y mire si existe una cuenta de Google en **Administrar cuentas**. Añada su cuenta si no aparece ninguna, reinicie su dispositivo e intente iniciar sesión en Bitdefender Mobile Security.



- ☐ Reinicie su dispositivo y, a continuación, trate de iniciar sesión nuevamente.

¿En qué idiomas está disponible Bitdefender Mobile Security?

Bitdefender Mobile Security está disponible actualmente en los siguientes idiomas:

- ☐ Brasileño
- ☐ Checo
- ☐ Holandés
- ☐ Inglés
- ☐ Francés
- ☐ Alemán
- ☐ Griego
- ☐ Húngaro
- ☐ Italiano
- ☐ Japonés
- ☐ Coreano
- ☐ Polaco
- ☐ Portugués
- ☐ Rumano
- ☐ Ruso
- ☐ Español
- ☐ Sueco
- ☐ Tailandés
- ☐ Turco
- ☐ Vietnamita

Se añadirán otros idiomas en futuras versiones. Para cambiar el idioma de la interfaz de Bitdefender Mobile Security, vaya a los ajustes **Idioma y texto** de su dispositivo y configure el dispositivo con el idioma que desee utilizar.



6. OBTENIENDO AYUDA

6.1. Solicitando Ayuda

Bitdefender proporciona a sus clientes un nivel sin igual de soporte técnico rápido y preciso. Si tiene cualquier problema o alguna pregunta sobre su producto Bitdefender, dispone de varios recursos online para encontrar una solución o una respuesta. Además, puede ponerse en contacto con el equipo de Atención al Cliente de Bitdefender. Nuestros representantes de soporte técnico responderán a sus preguntas con diligencia y le proporcionarán la asistencia que necesite.

6.2. Recursos Online

Hay varios recursos online disponibles para ayudarle a resolver su problemas y preguntas relacionadas con Bitdefender.

- Centro de soporte de Bitdefender:
<https://www.bitdefender.es/consumer/support/>
- La comunidad de expertos de Bitdefender:
<https://community.bitdefender.com/es>
- Ciberpedia de Bitdefender:
<https://www.bitdefender.com/cyberpedia/>

Puede además usar su motor de búsqueda favorito para encontrar más información sobre seguridad de equipo, los productos de Bitdefender y la compañía.

6.2.1. Centro de soporte de Bitdefender

El Centro de soporte Bitdefender es una librería de información online sobre el producto Bitdefender. Alberga, en un formato de fácil acceso, los informes sobre los resultados del soporte técnico en curso y las actividades de solución de errores a cargo de los equipos de soporte y desarrollo de Bitdefender, junto con artículos más generales sobre prevención de amenazas, la administración de las soluciones de Bitdefender con explicaciones detalladas, y muchos otros artículos.

El Centro de soporte de Bitdefender está abierto al público y puede consultarse gratuitamente. La amplia información que contiene es otro



medio de proporcionar a los clientes de Bitdefender los conocimientos técnicos y la información que necesitan. Todas las solicitudes válidas de información o informes de errores procedentes de los clientes acaban finalmente en el Centro de soporte de Bitdefender, como informes de resolución de errores, documentos técnicos o artículos informativos para complementar los archivos de ayuda del producto.

El Centro de soporte de Bitdefender está disponible en cualquier momento en la siguiente dirección: <https://www.bitdefender.es/consumer/support/>.

6.2.2. La comunidad de expertos de Bitdefender

La comunidad de expertos es un entorno en el que los usuarios, entusiastas y fanes de Bitdefender pueden participar, intercambiar ideas, apoyarse mutuamente y compartir sus conocimientos y soluciones. Además, es un lugar de creación de ideas y aporta valiosos comentarios a nuestros equipos de desarrollo. Los miembros de esta comunidad son usuarios experimentados de Bitdefender que se complacen en ayudar a otros en su tiempo libre. Con su inmensa contribución y su genuino esfuerzo de voluntariado, hemos creado una base de conocimientos en la que los usuarios pueden hallar respuestas y orientación, pero con un toque humano.

Aquí encontrará interesantes conversaciones con gente que usa Bitdefender en sus dispositivos. La comunidad establece una auténtica conexión entre sus miembros y hace oír su voz. Es un lugar donde se alienta la participación sabiendo que su opinión y aporte serán respetados y apreciados. Como valioso contribuyente, nos esforzamos por ofrecer un nivel sin igual de soporte técnico rápido y preciso y deseamos aproximarnos a nuestros usuarios. Con este propósito en mente hemos diseñado nuestra comunidad.

Puede encontrar la página web de nuestra comunidad de expertos aquí:

<https://community.bitdefender.com/es>

6.2.3. Ciberpedia de Bitdefender

Bitdefender Cyberpedia contiene toda la información que necesita conocer sobre las últimas amenazas digitales. Aquí es donde los expertos de Bitdefender dan a conocer consejos y trucos para protegerse contra piratas informáticos, vulneraciones de datos, robos de identidad e intentos de suplantación en las redes sociales.



En el siguiente enlace puede encontrar la página web de Bitdefender Cyberpedia:

<https://www.bitdefender.com/cyberpedia/>.

6.3. Información de contacto

La comunicación eficiente es la clave para un negocio exitoso. Desde 2001, BITDEFENDER ha establecido una reputación incuestionable al esforzarse constantemente por mejorar la comunicación para superar las expectativas de nuestros clientes y socios. Si tiene alguna pregunta, no dude en contactarnos directamente a través de nuestro [Centro de soporte de Bitdefender \(página 49\)](#).

<https://www.bitdefender.es/consumer/support/>

6.3.1. Distribuidores locales

Los distribuidores locales de Bitdefender están preparados para responder a cualquier pregunta relacionada con su área de actuación, tanto a nivel comercial como en otros áreas.

Para encontrar un distribuidor de Bitdefender en su país:

1. Ir a <https://www.bitdefender.com/partners/localizador-de-socios.html>.
2. Elija su país y ciudad mediante las opciones correspondientes.



GLOSARIO

Código de activación

Es una clave única que se puede comprar al por menor y se utiliza para activar un producto o servicio específico. Un código de activación permite la activación de una suscripción válida por un cierto período de tiempo y número de dispositivos y también se puede utilizar para extender una suscripción con la condición de generarse para el mismo producto o servicio.

ActiveX

ActiveX es un modelo para escribir programas para que otros programas y el sistema operativo puedan llamarlos. La tecnología ActiveX se usa con Microsoft Internet Explorer para crear páginas web interactivas que se ven y se comportan como programas de computadora, en lugar de páginas estáticas. Con ActiveX, los usuarios pueden hacer o responder preguntas, usar botones e interactuar de otras formas con la página web. Los controles ActiveX a menudo se escriben usando Visual Basic. Active X se destaca por una completa falta de controles de seguridad; los expertos en seguridad informática desaconsejan su uso a través de internet.

Amenaza Persistente Avanzada

La amenaza persistente avanzada (APT) explota las vulnerabilidades de los sistemas para robar información importante y entregarla a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el blanco de esta amenaza. El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo y poder monitorear y recopilar información importante sin dañar las máquinas objetivo. El método utilizado para inyectar la amenaza en la red es a través de un archivo PDF o un documento de Office que parezca inofensivo para que cada usuario pueda ejecutar los archivos.

publicidad

El adware a menudo se combina con una aplicación host que se proporciona sin cargo siempre que el usuario acepte el adware. Debido a que las aplicaciones de adware generalmente se instalan después de que el usuario haya aceptado un acuerdo de licencia que establece el propósito de la aplicación, no se comete ningún delito. Sin embargo, los



anuncios emergentes pueden convertirse en una molestia y, en algunos casos, degradar el rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad para los usuarios que no conocían completamente los términos del acuerdo de licencia.

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

Un archivo que contiene uno o más archivos en un formato comprimido.

Puerta trasera

Un agujero en la seguridad de un sistema dejado deliberadamente por diseñadores o mantenedores. La motivación de tales agujeros no siempre es siniestra; algunos sistemas operativos, por ejemplo, vienen listos para usar con cuentas privilegiadas destinadas a los técnicos de servicio de campo o los programadores de mantenimiento del proveedor.

Sector de arranque

Un sector al comienzo de cada disco que identifica la arquitectura del disco (tamaño del sector, tamaño del clúster, etc.). Para los discos de inicio, el sector de arranque también contiene un programa que carga el sistema operativo.

virus de arranque

Una amenaza que infecta el sector de arranque de un disco fijo o disquete. Un intento de arrancar desde un disquete infectado con un virus del sector de arranque hará que la amenaza se active en la memoria. Cada vez que inicie su sistema a partir de ese momento, tendrá la amenaza activa en la memoria.

red de bots

El término “botnet” se compone de las palabras “robot” y “red”. Los botnets son dispositivos conectados a Internet infectados con amenazas y se pueden usar para enviar correos electrónicos no deseados, robar datos, controlar de forma remota dispositivos vulnerables o propagar spyware, ransomware y otros tipos de amenazas. Su objetivo es infectar el mayor número posible de dispositivos conectados, como PC, servidores, dispositivos móviles o IoT pertenecientes a grandes empresas o industrias.

Navegador



Abreviatura de navegador web, una aplicación de software utilizada para localizar y mostrar páginas web. Los navegadores populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo que significa que pueden mostrar gráficos además de texto. Además, la mayoría de los navegadores modernos pueden presentar información multimedia, incluidos sonido y video, aunque requieren complementos para algunos formatos.

Ataque de fuerza bruta

Ataque de adivinación de contraseñas utilizado para ingresar en un sistema informático ingresando posibles combinaciones de contraseñas, en su mayoría comenzando con la contraseña más fácil de adivinar.

Línea de comando

En una interfaz de línea de comandos, el usuario escribe los comandos en el espacio provisto directamente en la pantalla usando el lenguaje de comandos.

Galletas

Dentro de la industria de Internet, las cookies se describen como pequeños archivos que contienen información sobre computadoras individuales que los anunciantes pueden analizar y usar para rastrear sus intereses y gustos en línea. En este ámbito, la tecnología de cookies aún se está desarrollando y la intención es orientar los anuncios directamente a lo que ha dicho que son sus intereses. Es un arma de doble filo para muchas personas porque, por un lado, es eficiente y pertinente, ya que solo ve anuncios sobre lo que le interesa. Por otro lado, implica realmente "rastrear" y "seguir" a dónde va y lo que haces clic. Comprensiblemente, existe un debate sobre la privacidad y muchas personas se sienten ofendidas por la noción de que se les considera un "número SKU" (ya sabe, el código de barras en la parte posterior de los paquetes que se escanea en la línea de pago del supermercado). Si bien este punto de vista puede ser extremo, en algunos casos es exacto.

Ciberacoso

Cuando compañeros o extraños están cometiendo actos abusivos contra los niños con el propósito de lastimarlos físicamente. Para dañar emocionalmente, los agresores envían mensajes crueles o fotos poco favorecedoras, lo que hace que sus víctimas se aislen de los demás o se sientan frustradas.

Ataque de diccionario



Los ataques de adivinación de contraseñas solían entrar en un sistema informático ingresando una combinación de palabras comunes para generar posibles contraseñas. El mismo método se utiliza para adivinar las claves de descifrado de mensajes o documentos cifrados. Los ataques de diccionario tienen éxito porque muchas personas se inclinan por elegir contraseñas cortas y de una sola palabra que sean fáciles de adivinar.

Disco duro

Es una máquina que lee y escribe datos en un disco. Una unidad de disco duro lee y escribe discos duros. Una unidad de disquete accede a disquetes. Las unidades de disco pueden ser internas (alojadas dentro de una computadora) o externas (alojadas en una caja separada que se conecta a la computadora).

Descargar

Para copiar datos (generalmente un archivo completo) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un archivo de un servicio en línea a la propia computadora. Descargar también puede referirse a copiar un archivo desde un servidor de archivos de red a una computadora en la red.

Correo electrónico

Correo electrónico. Un servicio que envía mensajes en computadoras a través de redes locales o globales.

Eventos

Una acción u ocurrencia detectada por un programa. Los eventos pueden ser acciones del usuario, como hacer clic con el botón del mouse o presionar una tecla, o eventos del sistema, como quedarse sin memoria.

hazañas

Una forma de aprovechar diferentes errores o vulnerabilidades que están presentes en una computadora (software o hardware). Por lo tanto, los piratas informáticos pueden obtener el control de las computadoras o las redes.

Falso positivo

Ocurre cuando un escáner identifica un archivo como infectado cuando en realidad no lo está.



Extensión de nombre de archivo

La parte de un nombre de archivo, después del punto final, que indica el tipo de datos almacenados en el archivo. Muchos sistemas operativos utilizan extensiones de nombre de archivo, por ejemplo, Unix, VMS y MS-DOS. Por lo general, tienen de una a tres letras (algunos sistemas operativos tristes y antiguos no admiten más de tres). Los ejemplos incluyen "c" para código fuente C, "ps" para PostScript, "txt" para texto arbitrario.

Heurístico

Un método basado en reglas para identificar nuevas amenazas. Este método de escaneo no se basa en una base de datos de información de amenazas específica. La ventaja del análisis heurístico es que no se deja engañar por una nueva variante de una amenaza existente. Sin embargo, ocasionalmente puede reportar código sospechoso en programas normales, generando el llamado "falso positivo".

Tarro de miel

Un sistema informático de señuelo configurado para atraer a los piratas informáticos para que estudien la forma en que actúan e identifiquen los métodos heréticos que utilizan para recopilar información del sistema. Las empresas y corporaciones están más interesadas en implementar y utilizar trampas trampa para mejorar su estado general de seguridad.

IP

Protocolo de Internet: un protocolo enrutable en el conjunto de protocolos TCP/IP que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblaje de paquetes IP.

Subprograma de Java

Un programa Java que está diseñado para ejecutarse solo en una página web. Para usar un subprograma en una página web, debe especificar el nombre del subprograma y el tamaño (largo y ancho, en píxeles) que puede utilizar el subprograma. Cuando se accede a la página web, el navegador descarga el applet de un servidor y lo ejecuta en la máquina del usuario (el cliente). Los applets se diferencian de las aplicaciones en que se rigen por un estricto protocolo de seguridad.

Por ejemplo, aunque los subprogramas se ejecutan en el cliente, no pueden leer ni escribir datos en la máquina del cliente. Además, los



subprogramas están más restringidos para que solo puedan leer y escribir datos del mismo dominio desde el que se sirven.

registrador de teclas

Un keylogger es una aplicación que registra todo lo que escribes. Los keyloggers no son de naturaleza maliciosa. Se pueden usar para fines legítimos, como monitorear la actividad de los empleados o los niños. Sin embargo, los ciberdelincuentes los utilizan cada vez más con fines maliciosos (por ejemplo, para recopilar datos privados, como credenciales de inicio de sesión y números de seguridad social).

Virus de macros

Un tipo de amenaza informática que se codifica como una macro incrustada en un documento. Muchas aplicaciones, como Microsoft Word y Excel, admiten potentes lenguajes de macros. Estas aplicaciones le permiten incrustar una macro en un documento y hacer que la macro se ejecute cada vez que se abre el documento.

cliente de correo

Un cliente de correo electrónico es una aplicación que le permite enviar y recibir correo electrónico.

Memoria

Áreas de almacenamiento interno en la computadora. El término memoria identifica el almacenamiento de datos que viene en forma de chips, y la palabra almacenamiento se usa para la memoria que existe en cintas o discos. Cada computadora viene con una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

no heurístico

Este método de escaneo se basa en una base de datos de información de amenazas específicas. La ventaja del análisis no heurístico es que no se deja engañar por lo que podría parecer una amenaza y no genera falsas alarmas.

Depredadores en línea

Individuos que buscan atraer a menores o adolescentes a conversaciones con el propósito de involucrarlos en actividades sexuales ilegales. Las redes sociales son el lugar ideal donde los niños vulnerables pueden ser perseguidos y seducidos fácilmente para que cometan actividades sexuales, en línea o cara a cara.



Programas empaquetados

Un archivo en un formato de compresión. Muchos sistemas operativos y aplicaciones contienen comandos que le permiten empaquetar un archivo para que ocupe menos memoria. Por ejemplo, suponga que tiene un archivo de texto que contiene diez caracteres de espacio consecutivos. Normalmente, esto requeriría diez bytes de almacenamiento.

Sin embargo, un programa que empaqueta archivos reemplazaría los caracteres de espacio por un carácter de serie de espacio especial seguido por la cantidad de espacios que se reemplazan. En este caso, los diez espacios requerirían solo dos bytes. Esta es solo una técnica de empaque, hay muchas más.

Camino

Las direcciones exactas a un archivo en una computadora. Estas direcciones generalmente se describen mediante el sistema de archivo jerárquico de arriba hacia abajo.

La ruta entre dos puntos, como el canal de comunicación entre dos computadoras.

Suplantación de identidad

El acto de enviar un correo electrónico a un usuario que afirma falsamente ser una empresa legítima establecida en un intento de estafar al usuario para que entregue información privada que se utilizará para el robo de identidad. El correo electrónico dirige al usuario a visitar un sitio web donde se le pide que actualice la información personal, como contraseñas y números de tarjetas de crédito, seguridad social y cuentas bancarias, que ya tiene la organización legítima. El sitio web, sin embargo, es falso y está configurado solo para robar la información del usuario.

Fotón

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto en el rendimiento de su solución de seguridad. Al monitorear la actividad de su PC en segundo plano, crea patrones de uso que ayudan a optimizar los procesos de arranque y escaneo.

Virus polimórfico

Una amenaza que cambia de forma con cada archivo que infecta. Como no tienen un patrón binario constante, estas amenazas son difíciles de identificar.



Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el endpoint de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Cryptolocker, CryptoWall y TeslaWall son solo algunas de las variantes que secuestran los sistemas personales de los usuarios.

La infección puede propagarse al acceder a spam, descargar archivos adjuntos, o instalar aplicaciones, evitando que el usuario se percate de lo que está sucediendo en su sistema. Los usuarios habituales y empresas son el objetivo de los hackers de ransomware.

Archivo de informe

Es un fichero que lista las acciones realizadas. BitDefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricos, si éstos incorporan el software apropiado.

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. No obstante, se



usan habitualmente para ocultar amenazas o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con amenazas, los rootkits representan un gran peligro para la integridad y la seguridad de un sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Spam

Correo basura o posts basura en grupos de noticias. Se conoce generalmente como correo no deseado.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información sobre direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

La similitud del spyware con una amenaza de tipo troyano radica en el hecho de que los usuarios instalan involuntariamente el producto al instalar otra cosa. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos de inicio



Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo, una pantalla de inicio, un archivo de sonido para que se reproduzca cuando se inicie el equipo, un calendario de recordatorios o apps pueden ser elementos de inicio. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Suscripción

Acuerdo de compra que otorga al usuario el derecho a utilizar un producto o servicio determinado en un número concreto de dispositivos y durante cierto periodo de tiempo. Una suscripción caducada puede renovarse automáticamente utilizando la información proporcionada por el usuario en su primera compra.

Bandeja del sistema

Elemento introducido con el sistema Windows 95, la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Amenaza

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de las amenazas también pueden autorreplicarse. Todas las amenazas informáticas están creadas por el hombre. Una amenaza sencilla que pueda copiarse una y otra vez es relativamente fácil de producir. Incluso una amenaza tan simple es peligrosa porque consumirá rápidamente toda la memoria disponible y hará que el sistema se detenga. Un tipo de amenaza aún más peligrosa es la capaz de transmitirse a través de las redes y eludir los sistemas de seguridad.



Actualización de información sobre amenazas

El patrón binario de una amenaza, utilizado por la solución de seguridad para detectarla y eliminarla.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los programas de software malicioso y gusanos, los troyanos no se autorreplican, pero pueden ser igualmente destructivos. Uno de los tipos de troyanos más graves es una amenaza que pretende desinfectar su equipo, pero en cambio introduce amenazas en él.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Actualizar

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Bitdefender posee una característica de actualización que le permite comprobar manualmente las actualizaciones o actualizar automáticamente el producto.

Red privada virtual (VPN)

Es una tecnología que permite una conexión directa temporal y cifrada a una determinada red a través de una red menos segura. De esta forma, el envío y recepción de datos está cifrado y es seguro, lo que dificulta su interceptación por parte de los fisgones. Una muestra de seguridad es la autenticación, que solo se puede lograr utilizando un nombre de usuario y contraseña.

Gusano

Un programa que se autopropaga a través de una red, reproduciéndose a medida que avanza. No puede adjuntarse a otros programas.