GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

Parental Control

Control Parental de Bitdefender

Guía de Usuario

Publication date 04/29/2024

Advertencia legal

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. Primeros pasos 4
1.1. Configurar Parental Control 4
1.2. Instalación de Bitdefender Parental Control en los dispositivos de sus hijos 5
1.2.1. En dispositivos Windows: 5
1.2.2. En dispositivos macOS: 5
1.2.3. En dispositivos Android: 6
1.2.4. En dispositivos iOS: 7
2. Características y funcionalidades 10
2.1. Perfiles 10
2.2. Estadísticas 12
2.3. Código PIN de Control parental 12
2.3.1. ¿Ha olvidado el código PIN? 13
2.3.2. Cambio de su código PIN 13
2.4. Filtro de Contenido 13
2.4.1. Búsqueda segura y restricciones de YouTube 14
2.4.2. Bloquear y permitir categorías de sitios web 14
2.4.3. Excepciones 15
2.5. Tiempo de uso diario de Internet 15
2.5.1. Sistema de recompensas 16
2.6. Desactivación de Internet en el dispositivo de su hijo 17
2.7. Rutinas 18
2.7.1. Configuración de rutinas 19
2.8. Localización de la ubicación de su hijo 20
3. Desinstalación de Parental Control 21
4. Obteniendo ayuda 22
4.1. Solicitando Ayuda 22
4.2. Recursos Online 22
4.2.1. Centro de soporte de Bitdefender 22
4.2.2. La comunidad de expertos de Bitdefender 23
4.2.3. Ciberpedia de Bitdefender 23
4.3. Información de contacto 24

4.3.1. Distribuidores locales 24
Glosario 25

ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía va destinada a cualquier usuario de Bitdefender que haya elegido Bitdefender Parental Control como su solución ideal para la seguridad, la monitorización y la protección continua de la presencia online de sus hijos y de sus dispositivos.

Aprenderá a instalar, configurar y aprovechar al máximo Bitdefender Parental Control para disfrutar de características mejoradas y un mayor control sobre las actividades de sus hijos en Internet.

Le deseamos una lectura útil y agradable.

Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Primeros pasos (página 4)

Empiece por configurar su Bitdefender Parental Control.

Características y funcionalidades (página 10)

Aprenda a usar Bitdefender Parental Control y todas sus características.

Obteniendo ayuda (página 22)

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
sample syntax	Las muestras de sintaxis se imprimen con monospaced 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.
filename	Los archivos y directorios se imprimen usando monospaced 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. PRIMEROS PASOS

Empezaremos con una guía detallada paso a paso de cómo configurar la suscripción a Bitdefender Parental Control en su cuenta de Bitdefender Central. Este es el comienzo de un sencillo proceso necesario para que pueda administrar y monitorizar eficazmente las actividades online de sus hijos.

1.1. Configurar Parental Control

Tras activar su suscripción, para empezar a configurar Bitdefender Parental Control en su cuenta haga lo siguiente:

1. Acceda a su cuenta de Bitdefender Central y vaya a la pestaña **Parental Control** en el lado izquierdo de la pantalla.
2. Haga clic en **Puesta en marcha**.
3. Establecer PIN de la aplicación.

   > **Nota**
   > Este código PIN es para evitar que sus hijos desactiven las características de Parental Control cerrando sesión en su aplicación.
   >
   > No olvide este PIN.

4. Haga clic en **Siguiente**.
5. A continuación, cree un perfil para su hijo. Escriba el nombre del menor y seleccione una imagen para el perfil. Luego, haga clic en **Siguiente**.
6. Seleccione la edad de su hijo. Una vez hecho esto, haga clic en **Siguiente**.
7. Indique si la aplicación de Parental Control se instalará en el dispositivo que está utilizando actualmente o en otro.

Nota

Si selecciona **Otros dispositivos**, se le ofrecerán tres opciones de instalación. Seleccione el método que prefiera:

- Escaneando el código QR.
- Copiando el enlace proporcionado y abriéndolo en el navegador del dispositivo de su hijo.
- Enviando el enlace de instalación por correo electrónico.

8. Espere a que finalice la descarga y, acto seguido, ejecute el instalador en el dispositivo correspondiente.

Ahora, dará comienzo el proceso de instalación. Los pasos que han de seguirse a partir de aquí varían según el tipo de dispositivo y el sistema operativo en el que se realice la instalación.

1.2. Instalación de Bitdefender Parental Control en los dispositivos de sus hijos

1.2.1. En dispositivos Windows:

Tras ejecutar el instalador recién descargado:

1. Haga clic en **Sí** si aparece un cuadro de diálogo del control de cuentas de usuario solicitándole permiso para que el archivo de instalación realice cambios en el dispositivo.
2. Si se le solicita, inicie sesión con las credenciales de su cuenta de Bitdefender Central.

1.2.2. En dispositivos macOS:

Una vez finalizada la descarga del instalador, haga doble clic en el archivo Bitdefender para iniciar el proceso de instalación:

1. Se le guiará por los pasos necesarios para instalar Bitdefender Parental Control for macOS. Si se le solicita, haga clic en **Permitir**.
2. Haga clic en los dos botones **Continuar** que aparecen sucesivamente.
3. Para proseguir con la instalación, tendrá que aceptar los términos del acuerdo de suscripción del software.
4. Haga clic en **Continuar**. A continuación, haga clic en **Instalar**.

5. Cuando se le solicite, introduzca un nombre de administrador y una contraseña y, luego, pulse el botón **Instalar software**.

Espere hasta que aparezca una notificación emergente indicando que *se ha bloqueado una extensión del sistema*. Esto es algo normal durante este procedimiento. Para continuar, debe dar permiso a la extensión del sistema de Parental Control siguiendo las instrucciones que figuran a continuación:

1. Haga clic en el botón **Abrir configuración del sistema**.

> **Nota**
> En versiones anteriores de macOS, este botón se conoce como **Abrir preferencias de seguridad**.

2. Haga clic en el botón **Permitir** en la ventana que aparece en la pantalla y, a continuación, introduzca un nombre de administrador y una contraseña para desbloquear la configuración.

> **Nota**
> En macOS 11 (Big Sur) y macOS 12 (Monterey), para poder hacer clic en el botón **Permitir** deberá hacer clic antes en el icono del candado de la esquina inferior izquierda de la ventana **Seguridad y privacidad** y, luego, introducir un nombre de administrador y una contraseña para realizar cambios.

3. Aparecerá la ventana emergente **Filtrar contenidos de red**. Haga clic en el botón **Permitir** de esta ventana.
4. A continuación, haga clic en el botón **Abrir configuración del sistema**.
5. Haga clic en el botón **Permitir** una vez más.

1.2.3. En dispositivos Android:

Encontrará la página de Bitdefender en Google Play Store correspondiente a la aplicación Parental Control:

1. Toque el botón **Instalar**. La aplicación empezará a descargarse e instalarse.
2. Una vez finalizada la instalación, verá un botón **Abrir**. Tóquelo para lanzar la aplicación Bitdefender Parental Control.

Tras abrir la aplicación, siga los pasos que aparecen en la pantalla para configurar Parental Control en el dispositivo Android de su hijo:

1. Toque **Continuar**.
2. Inicie sesión en la aplicación con las credenciales de su cuenta de Bitdefender Central.
3. Seleccione el perfil de hijo que desea asignar a ese dispositivo Android.
4. Tendrá que otorgar los permisos necesarios para que la aplicación funcione correctamente. Para ello, toque **Siguiente** y, a continuación:
   a. Permita el acceso VPN y, luego, elija **Permitir todo el tiempo** para filtrar los contenidos online en el dispositivo de su hijo.
   b. Para ayudarle a localizar el dispositivo Android de su hijo, toque **Siguiente**, luego, **Permitir**, y elija la opción **Permitir todo el tiempo**.
   c. Tanto el permiso de VPN como el de Ubicación mostrarán una marca de verificación verde. Toque **Finalizar la configuración** y, luego, toque **Siguiente**.
   d. Llegados a este punto, hay tres permisos más para bloquear el acceso a Internet y a las aplicaciones en el dispositivo de su hijo. Toque **Establecer permiso** en el panel **Privilegios de administrador del dispositivo**.
   e. Una vez que haya terminado de configurar la aplicación Bitdefender Parental Control, toque el botón **Finalizar**.

1.2.4. En dispositivos iOS:

Encontrará la página de Bitdefender en la App Store correspondiente a la aplicación Parental Control:

1. Toque el icono de la nube con una flecha hacia abajo. La aplicación empezará a descargarse e instalarse.
2. Una vez finalizada la instalación, verá un botón **Abrir**. Tóquelo para lanzar la aplicación Bitdefender Parental Control.
3. Si se encuentra algún perfil de Mobile Device Management en el dispositivo iOS de su hijo, se le pedirá que lo elimine. Toque **Siguiente** y elija **Eliminar perfiles**.

4. En los **Ajustes** de la aplicación de iOS, acceda a **General** y, a continuación, baje hasta la sección **VPN y gestión de dispositivos** y toque en ella.
5. Toque en todas las entradas de la sección **MOBILE DEVICE MANAGEMENT** y elija **Eliminar administración** en cada una de ellas. Repita este proceso hasta que no queden más entradas de MOBILE DEVICE MANAGEMENT.

Vuelva a abrir la aplicación instalada en el dispositivo de su hijo y siga los pasos que aparecen en la pantalla para configurar Bitdefender Parental Control:

1. Toque **Continuar**.
2. Inicie sesión en la aplicación con las credenciales de su cuenta de Bitdefender Central.
3. Seleccione el perfil de hijo que desea asignar a ese dispositivo iOS.
4. Luego, tendrá que otorgar los permisos necesarios para que la aplicación funcione correctamente. Toque **Siguiente**.
5. Permita el acceso VPN para filtrar los contenidos online en el dispositivo de su hijo. Toque dos veces seguidas **Permitir** para agregar las configuraciones de VPN.
6. Toque **Siguiente** y, a continuación, elija **Permitir** para ayudarle a localizar el dispositivo iOS de su hijo.
7. Luego, siga el proceso de configuración de En familia para bloquear el acceso a Internet y a las aplicaciones en el dispositivo de su hijo.

> **Nota**
> Puede tocar **Averiguar cómo** para acceder a una guía paso a paso sobre cómo hacerlo.

8. Tras configurar En familia en su propio dispositivo y en el de su hijo, seleccione **He configurado En familia** para continuar.
9. Luego, permita el acceso al tiempo de pantalla para filtrar los contenidos online en el dispositivo iOS de su hijo.
10. Toque **Finalizar la configuración**.

.

Una vez realizados estos pasos en los dispositivos de su hijo, habrá completado el proceso de configuración. Como progenitor, ahora puede

monitorizar las actividades online de su hijo y ver las estadísticas de uso en su cuenta de Bitdefender Central, en el panel de Parental Control del que hablaremos en los siguientes capítulos.

2. CARACTERÍSTICAS Y FUNCIONALIDADES

2.1. Perfiles

Un perfil de hijo es un conjunto personalizado de reglas que permiten a la aplicación Bitdefender Parental Control administrar y monitorizar las actividades online de su hijo. Incluye ajustes adaptados a la edad del menor, como filtros de contenido y restricciones de tiempo. Desde su cuenta de Bitdefender Central, los progenitores pueden crear, editar y eliminar estos perfiles, así como asignarles dispositivos o eliminarlos, lo que garantiza un uso seguro y adecuado de Internet por parte de sus hijos.

Para crear un perfil para su hijo:

1. Acceda a Bitdefender Central e inicie sesión en su cuenta.
2. En el menú del lado izquierdo, haga clic en la pestaña **Parental Control**.
3. Haga clic en **Nuevo perfil** para crear un nuevo perfil para su hijo.
4. Introduzca el nombre del menor, la imagen del perfil y la fecha de nacimiento.

> **Nota**
> En función de la edad del niño, Bitdefender bloquea automáticamente ciertas categorías como el chat, las redes sociales, los contenidos explícitos, etc. Más adelante podrá ajustar las categorías bloqueadas.

5. Haga clic en el botón **Guardar**.

Ya se ha creado el nuevo perfil y aparecerá en la página.

Para editar el perfil de su hijo:

1. Haga clic en el botón **Ver detalles** del perfil del menor.
2. Para modificar el perfil de su hijo, acceda a **Editar perfil**.
3. Utilice los campos correspondientes para cambiar el nombre, la fecha de nacimiento o la imagen del perfil del menor.

4. Tras modificar la información necesaria, haga clic en **Guardar cambios**.

Para eliminar el perfil de su hijo:

1. Haga clic en el botón **Ver detalles** del perfil del menor.
2. Acceda a **Editar perfil**.
3. Haga clic en el botón **Eliminar perfil** y confirme la eliminación.

Para asignar dispositivos al perfil de su hijo:

Si su hijo dispone de varios dispositivos (Windows, macOS, Android o iOS), puede asignarlos al mismo perfil.

1. Haga clic en el botón **Ver detalles** del perfil del menor.
2. Haga clic en el número de dispositivos que se indica debajo de su nombre.
3. Haga clic en el botón **Asignar dispositivos**.
4. Seleccione el nombre del dispositivo y, a continuación, haga clic en el botón **Asignar**.

> **Nota**
> Si el dispositivo no aparece en la lista, haga clic en **Instalar un nuevo dispositivo** y, luego, siga las instrucciones que aparecen en la pantalla para instalar y configurar Bitdefender Parental Control en el nuevo dispositivo.

Para eliminar dispositivos del perfil de su hijo:

Si elimina un dispositivo del perfil de su hijo, dejará de poder gestionarlo con Bitdefender Parental Control. Las reglas y ajustes especificados en el perfil de su hijo ya no se aplicarán a ese dispositivo. Aunque la aplicación Parental Control siga instalada en el dispositivo, dejará de funcionar.

1. Haga clic en el botón **Ver detalles** del perfil del menor.
2. Haga clic en el número de dispositivos que se indica debajo de su nombre.
3. Localice el dispositivo del menor y haga clic en la opción **Desasignar dispositivo**.
4. Pulse el botón **Sí, desasignar dispositivo** para confirmar esta acción.

2.2. Estadísticas

Parental Control proporciona valiosa información sobre el uso que hace su hijo de Internet y de sus dispositivos. En esta guía, ahondaremos en las diversas estadísticas disponibles en Bitdefender Central para los progenitores, las cuales les permiten tomar decisiones con la debida información y garantizar un uso seguro y equilibrado de Internet por parte de sus hijos.

Para ver las estadísticas:

1. Acceda a Bitdefender Central e inicie sesión en su cuenta.
2. Tras iniciar sesión, haga clic en la pestaña **Parental Control** en el menú del lado izquierdo.
3. Haga clic en el perfil del menor cuyas estadísticas desea ver.

Tras seleccionar el perfil de su hijo, se le dirigirá a una pantalla que muestra varios paneles de estadísticas,todos ellos referidos a las características que se describen más adelante en esta documentación.

2.3. Código PIN de Control parental

El Código PIN parental es una característica de seguridad incluida en el panel Parental Control de la plataforma Bitdefender Central. Sirve para que los progenitores controlen el acceso de sus hijos a la aplicación Bitdefender Parental Control instalada en sus dispositivos. A continuación se expone detalladamente cómo establecer, encontrar y administrar su PIN parental.

El código PIN parental evita que se cierre sesión sin autorización en la aplicación Bitdefender Parental Control en el dispositivo de su hijo. Cuando su hijo intente cerrar sesión, se le pedirá que introduzca este código PIN. De este modo, se garantiza que solo usted, como progenitor con acceso a la cuenta de Bitdefender Central, pueda controlar los ajustes de la aplicación.

> **Nota**
> Al configurar por primera vez la aplicación de Parental Control, se le pedirá que establezca un PIN parental de cuatro a ocho dígitos de longitud.

2.3.1. ¿Ha olvidado el código PIN?

En caso de que haya olvidado su código PIN parental, puede recuperarlo fácilmente desde su cuenta de Bitdefender Central:

1. Acceda a Bitdefender Central e inicie sesión en su cuenta.
2. Tras iniciar sesión, haga clic en la pestaña **Parental Control** en el menú del lado izquierdo.
3. En la esquina superior derecha de la página, haga clic en **Código PIN**.
4. Haga clic en el icono con forma de ojo para averiguar su código PIN parental.

2.3.2. Cambio de su código PIN

Si sospecha que su código PIN se ha visto comprometido o, simplemente, desea actualizarlo por razones de seguridad, proceda de la siguiente manera:

1. En la sección Parental Control de su cuenta de Bitdefender Central, haga clic en la opción **Código PIN**.
2. Elija **Cambiar PIN** y siga las instrucciones que aparecen en la pantalla para establecer un nuevo código PIN.

2.4. Filtro de Contenido

El Filtrado de contenidos permite a los progenitores restringir el acceso de sus hijos a contenidos en Internet, pudiendo bloquear categorías enteras de sitios web o hacer excepciones en función de la URL o de temas concretos.

> **Nota**
> La característica de Filtrado de contenidos de Bitdefender Parental Control no impide que su hijo use aplicaciones de sitios web sin conexión: solo administra el tráfico de Internet de los dispositivos que utiliza online.

Para acceder al Filtrado de contenidos, haga lo siguiente:

1. Inicie sesión en su cuenta de Bitdefender Central.
2. En el menú del lado izquierdo, haga clic en la pestaña **Parental Control**.

3. Acceda al perfil de su hijo y haga clic en el menú **Más** arriba a la derecha. Luego, seleccione **Filtrado de contenidos**.

2.4.1. Búsqueda segura y restricciones de YouTube

En la sección **Privacidad y seguridad** del lado derecho de la pantalla, puede activar los conmutadores de Búsqueda segura y YouTube restringido.

- **Búsqueda segura:** Al utilizar motores de búsqueda, la Búsqueda segura evita que en los resultados aparezcan contenidos que Google no considere seguros.
- **YouTube restringido:** Muestra en YouTube vídeos apropiados para la edad del menor.

> **Nota**
> La **Búsqueda segura** y **YouTube restringido** redireccionan todas las solicitudes de DNS de **google.com** a **safe.google.com**. Del filtrado de contenidos en sí se encarga Google. Bitdefender Parental Control no filtra los contenidos en la Búsqueda segura o en Google. Asimismo, puede que YouTube no controle eficazmente las etiquetas de los vídeos, lo que podría exponer a los menores a contenidos inapropiados.

2.4.2. Bloquear y permitir categorías de sitios web

> **Nota**
> En la sección **Categorías**, los tipos de sitios web que su hijo puede ver online se permiten o bloquean por defecto, en función de la edad establecida al crear el perfil del menor.

En cualquier momento, puede bloquear o permitir los tipos de sitios web de la siguiente manera:

1. Seleccione una categoría.
2. Para bloquear el acceso a la categoría, elija **Bloqueado** en el menú desplegable. Para permitirlo, elija **Permitido**.

> **Importante**
> Si bloquea la categoría **Intercambio de archivos** en el perfil de su hijo, no funcionará la actualización de macOS. Para actualizar macOS, le recomendamos que permita temporalmente el intercambio de archivos.

2.4.3. Excepciones

En la pestaña **Excepciones**, pueden establecerse exclusiones de sitios web y aplicaciones de la siguiente manera:

- **Añadir excepciones de sitio web:**
  1. Haga clic en el botón **Añadir excepción**.
  2. Seleccione **Solo sitio web** y, a continuación, haga clic en el botón **Siguiente**.
  3. Escriba la dirección del sitio web y seleccione en el menú desplegable si desea permitirlo o bloquearlo.
  4. Luego, haga clic en el botón **Añadir**.

- **Exceptiones de aplicación y plataforma web:**
  1. Haga clic en el botón **Añadir excepción**.
  2. Seleccione **Aplicación y plataforma web** y, a continuación, haga clic en el botón **Siguiente**.
  3. En la lista que se proporciona, elija la plataforma para la que desea establecer una excepción. Como alternativa, puede usar la barra de búsqueda para encontrar la que desea.
  4. Luego, haga clic en el botón **Añadir**.

- **Eliminar excepciones:**
  Todas las excepciones que establezca aparecerán en Filtrado de contenidos en su lista correspondiente de la parte inferior.
  Para eliminar una excepción, basta con que haga clic en el icono de la papelera ubicado a la derecha de la entrada.

2.5. Tiempo de uso diario de Internet

En su cuenta de Bitdefender Central, dentro de la sección Parental Control, se muestra una tarjeta de Tiempo de uso diario de Internet por cada perfil de hijo que haya creado. La tarjeta muestra el tiempo total que el menor ha pasado online en todos los dispositivos que tiene asignados. Para limitar este tiempo, haga lo siguiente:

1. Acceda al perfil de su hijo y haga clic en el botón **Establecer límite de tiempo** en el panel **Tiempo de uso diario de Internet**. Como

alternativa, puede hacer clic en el menú **Más** de la esquina superior derecha y seleccionar **Tiempo de uso diario de Internet**.

2. Haga clic en el botón **Habilitar límite de tiempo** para activar esta característica.

> **Nota**
> Por defecto, al menor se le permite 1 hora y 30 minutos de acceso a Internet al día. En caso de que el progenitor no amplíe este límite de tiempo, el acceso del menor a Internet se detendrá tras alcanzar la hora y media.

Eliminación del límite de tiempo diario:

- Para desactivar la característica de tiempo de uso diario de Internet, acceda al panel del perfil de su hijo, haga clic en el botón **Editar tiempo** del panel **Tiempo de uso diario de Internet** y, a continuación, pulse el botón **Pausa** en el panel **Límite de tiempo**.
- Para quitar la limitación de tiempo solo para un día concreto, haga clic en el botón ⊗ correspondiente a ese día de la semana en el panel **Programación**.

Cambio del límite de tiempo:

- Para establecer un límite de tiempo distinto para un día concreto de la semana, haga clic en el día correspondiente en el panel **Programación**, seleccione el límite deseado en el menú desplegable y, a continuación, haga clic en el botón **Guardar cambios**. Puede seleccionar varios días a la vez.

2.5.1. Sistema de recompensas

La característica de **Recompensa** le permite premiar o ampliar el tiempo que su hijo puede pasar ante la pantalla para incentivar los buenos hábitos online. Puede utilizar el sistema de recompensas de dos maneras:

- **Recompensa manual:**

  1. Desplácese por la sección Parental Control en su cuenta de Bitdefender Central.
  2. Acceda al perfil de su hijo y haga clic en el botón **Recompensa** en el panel **Tiempo de uso diario de Internet**.

3. Elija cuánto tiempo desea añadir y confírmelo haciendo clic en **Recompensa**.

- **Solicitud de su hijo:**
  Cuando su hijo alcance el límite diario, podrá solicitarle más tiempo desde la aplicación de Parental Control instalada en su dispositivo móvil. El progenitor recibirá una notificación en su cuenta de Bitdefender Central.

  1. Una vez que haya iniciado sesión en su cuenta de Bitdefender Central, un punto rojo en la campana de notificaciones de la esquina superior derecha de la pantalla le indicará que tiene una solicitud de su hijo pendiente de atender.
  2. Revise la solicitud y decida cuánto tiempo adicional otorgarle.

  > **Nota**
  > Los menores solo tienen la opción de solicitar ampliaciones de su tiempo de uso diario de Internet en dispositivos iOS y Android.

2.6. Desactivación de Internet en el dispositivo de su hijo

Administrar el uso que su hijo hace de Internet puede ser importante para su bienestar y productividad. Para desactivar temporalmente el acceso a Internet en el dispositivo de su hijo mediante Bitdefender Parental Control, haga lo siguiente:

1. Acceda a Bitdefender Central e inicie sesión en su cuenta.
2. Tras iniciar sesión, haga clic en la pestaña **Parental Control** en el menú del lado izquierdo.
3. Seleccione **Ver detalles** en el perfil del menor cuyo acceso a Internet desea desactivar.
4. Haga clic en el botón **Detener Internet** en la esquina superior derecha del panel de su hijo.

> **Nota**
> Se interrumpirá la conexión a Internet en todos los dispositivos de su hijo. Esta acción prevalece sobre cualquier ajuste existente de Parental Control, como las rutinas, el límite de tiempo diario o las categorías permitidas.

5. Mientras permanezca cortado el acceso a Internet, el botón **Detener Internet** cambiará a **Reanudar Internet**. Para restaurar el acceso a Internet, basta con que haga clic en el botón **Reanudar Internet**.

2.7. Rutinas

En Bitdefender Parental Control, puede configurar hasta tres rutinas distintas para programar cuándo se desconecta el acceso a Internet de su hijo. Las rutinas brindan una manera estructurada de gestionar las actividades online de su hijo para incentivar los buenos hábitos y el tiempo en familia a la vez que se garantiza su seguridad. Como estas rutinas son independientes, puede optar por activar una sola, dos o las tres, según sus necesidades:

- **Tiempo para concentrarse**
  Cree un horario que incluya tiempo para las tareas domésticas, el estudio y otras actividades.
- **Hora de dormir**
  Utilice la rutina para dormir con el fin de reservar un período de descanso para su hijo.
- **Tiempo en familia**
  Emplee la rutina de tiempo en familia para que su hijo esté presente, por ejemplo, durante las comidas familiares.

> **Nota**
> **Rutinas y tiempo de uso diario de Internet:**
>
> Durante las rutinas, el tiempo que su hijo pase online no cuenta para el límite de tiempo de uso diario de Internet. Una vez finalizada la rutina, la característica de tiempo de uso diario de Internet vuelve a computar el tiempo que el menor pasa online.
>
> Para evitar confundir a los progenitores, mientras se esté desarrollando una rutina, dejará de verse la tarjeta de Tiempo de uso diario de Internet en el panel del perfil del menor. En su lugar, se mostrará el nombre de la rutina activa en ese momento.

2.7.1. Configuración de rutinas

Para configurar cualquiera de las rutinas de Parental Control, haga lo siguiente:

1. Acceda a Bitdefender Central e inicie sesión en su cuenta.
2. En el menú del lado izquierdo, haga clic en la pestaña **Parental Control**.
3. Acceda al perfil de su hijo y seleccione la rutina deseada en el menú **Más**.
4. Haga clic en el botón **Activar** para activar la rutina seleccionada.
5. Esto hará que aparezcan los paneles **Programación** y **Acceso a Internet**.

   - **Planificar:**
     Para establecer una rutina para uno o varios días de la semana, haga lo siguiente:

     a. Seleccione los días deseados.

     b. Seleccione las horas de inicio y finalización de la rutina en el menú desplegable.

     c. Por último, haga clic en el botón **Guardar cambios** para confirmar lo que ha seleccionado.

     Para eliminar la rutina en un día concreto, haga clic en el botón ⊗ correspondiente a ese día de la semana.

   - **Acceso a Internet:**
     El panel de Acceso a Internet de una rutina ofrece dos funciones principales para controlar las actividades online de un menor durante determinados períodos de tiempo:

     - **Corte total del acceso a Internet:** Los progenitores tienen la opción de desactivar totalmente el acceso a Internet de sus hijos durante el horario de rutina programado. Al desactivar el conmutador de **Acceso a Internet**, el menor no podrá acceder a Internet desde sus dispositivos dentro del período de tiempo designado.
     - **Ciertas categorías o sitios web:** Como alternativa, los progenitores pueden permitir el acceso a Internet durante las horas de rutina, pero restringir ciertos sitios web

o categorías de contenido. Al activar el conmutador de **Acceso a Internet**, aparecen dos pestañas más: **Categorías** y **Excepciones**, que brindan acceso a más ajustes de Filtrado de contenidos</link>. (página 13)

2.8. Localización de la ubicación de su hijo

Ante la enorme popularización de los smartphones y otros dispositivos móviles, rastrear la ubicación de los menores ha pasado a ser una herramienta esencial para muchas familias. Ya se trate de conocer su paradero al salir del colegio o durante sus salidas con amigos, poder averiguar su ubicación tranquiliza a los padres. A continuación se expone paso a paso cómo rastrear la ubicación de su hijo gracias a la característica de Ubicación de Bitdefender Parental Control.

1. Acceda a Bitdefender Central e inicie sesión en su cuenta.
2. Tras iniciar sesión, haga clic en **Parental Control** en el menú del lado izquierdo.
3. Si tiene varios hijos, seleccione **Ver detalles** en el perfil del menor cuya ubicación desea rastrear.
4. En el panel Ubicación, seleccione el dispositivo Android o iOS que desea rastrear y, luego, haga clic en el botón **Localizar**.

   Nota
   La característica de Ubicación de Bitdefender Parental Control no está disponible para dispositivos Windows y macOS.

5. Tras una breve espera, una marca roja le indicará la ubicación actual de su hijo en el mapa.

   Nota
   Las ubicaciones se actualizan cada veinte minutos. Si intentase rastrear la ubicación de su hijo transcurridos menos de veinte minutos desde la última consulta de ubicación, es posible que la posición mostrada en el mapa no refleje su paradero actual.

3. DESINSTALACIÓN DE PARENTAL CONTROL

Desinstalación de Bitdefender Parental Control en dispositivos Windows:

1. Elimine el dispositivo del perfil de su hijo en Bitdefender Central.
2. Abra el panel de control en el dispositivo en cuestión y busque Bitdefender Parental Control en la lista de **Programas y características**.
3. Desinstale Bitdefender Parental Control.

Desinstalación de Bitdefender Parental Control en dispositivos macOS:

1. Elimine el dispositivo del perfil de su hijo en Bitdefender Central.
2. Abra el **Finder** en el dispositivo macOS.
3. Acceda a sus Aplicaciones y localice la carpeta Bitdefender.
4. Ábrala y ejecute el **Desinstalador de Bitdefender**.
5. En la lista de productos para desinstalar, elija Bitdefender Parental Control.
6. Proporcione las credenciales de administrador y espere a que finalice la desinstalación.

Desinstalación de Bitdefender Parental Control en dispositivos iOS y Android:

1. Elimine el dispositivo del perfil de su hijo en Bitdefender Central.
2. Desinstale Parental Control del dispositivo móvil como cualquier otra aplicación o a través de Google Play Store o App Store, respectivamente.

4. OBTENIENDO AYUDA

4.1. 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.

4.2. 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.

4.2.1. 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/.

4.2.2. 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/

4.2.3. 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/.

4.3. 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 22).

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

4.3.1. 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 determinado. Un código de activación permite la activación de una suscripción válida durante un cierto período de tiempo y para determinado número de dispositivos, y también puede utilizarse para ampliar una suscripción con la condición de que se genere 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 aíslen 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 intercepción 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.