Bitdefender®
SMALL OFFICE SECURITY

GUÍA DE USUARIO

Bitdefender Small Office Security
Guía de Usuario

fecha de publicación 12/21/2018

Copyright© 2018 Bitdefender

Advertencia legal

Todos los derechos reservados. Ninguna parte de este libro puede ser reproducida o transmitida de forma alguna, ni por ningún medio, electrónico o mecánico, incluyendo fotocopia, grabación o mediante un sistema de almacenamiento y recuperación, sin la autorización previa por escrito de un representante de Bitdefender. La inclusión de breves citas de reseñas se puede hacer sólo con la mención de la fuente citada. El contenido no puede ser modificado en forma alguna.

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

Este documento contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefenderno se hace responsable por el contenido de ningún sitio enlazado. Si usted accede a sitios web de terceros listados en este documento, lo hará bajo su responsabilidad. Bitdefender proporciona estos vínculos solamente para su conveniencia, y la inclusión del enlace no implica la aprobación por parte de Bitdefender o aceptar responsabilidad alguna sobre el contenido del sitio de terceros.

Marcas Registradas. En este documento pueden aparecer nombres de marcas registradas. Todas las marcas registradas y no registradas, en este documento, son propiedad exclusiva de sus respectivos propietarios, y respectivamente reconocidas.

Bitdefender

Tabla de contenidos

Introducción a Bitdefender Small Office Security ix

Total Security para PC 1

1. Pasos de la Instalación 2
1.1. Preparándose para la instalación 2
1.2. Requisitos del sistema 2
1.3. Instalando su producto Bitdefender 4

2. Primeros Pasos 7
2.1. Fundamentos 7
2.1.1. Notificaciones 9
2.1.2. Perfiles 10
2.1.3. Informes de productos 11
2.1.4. Notificaciones de ofertas especiales 12
2.1.5. Interfaz de análisis antimalware 12
2.2. Interfaz de Bitdefender 12
2.2.1. Icono del área de notificación 13
2.2.2. Menú de navegación 15
2.2.3. Panel de Control 16
2.2.4. Las secciones de Bitdefender 19
2.2.5. Widget de seguridad 24
2.3. Bitdefender Central 26
2.3.1. Mis suscripciones 27
2.3.2. Mis dispositivos 28
2.3.3. Configuración de protección por contraseña de Bitdefender 31
2.3.4. Actividad 32
2.3.5. Mi cuenta 32
2.3.6. Notificaciones 33
2.4. Mantenimiento de Bitdefender al día 33
2.4.1. Comprobar si Bitdefender está actualizado 33
2.4.2. Realizar una actualización 34
2.4.3. Activar o desactivar la actualización automática 35
2.4.4. Ajustar las opciones de actualización 35
2.4.5. Actualizaciones continuas 36

3. Cómo 37
3.1. Pasos de la Instalación 37
3.1.1. ¿Cómo puedo reinstalar Bitdefender? 37
3.1.2. ¿Desde dónde puedo descargar mi producto Bitdefender? 38
3.2. Bitdefender Central 39
3.2.1. ¿Cómo inicio sesión en Bitdefender Central usando otra cuenta online? 39
3.2.2. ¿Cómo puedo desactivar los mensajes de ayuda de Bitdefender Central? 39
3.2.3. He olvidado la contraseña que establecí para cuenta Bitdefender. ¿Cómo la restablezco? 40

3.2.4. ¿Cómo puedo gestionar las sesiones asociadas a mi cuenta de Bitdefender? . . . 41
3.3. Analizando con Bitdefender . . . 41
3.3.1. ¿Cómo analizo un archivo o una carpeta? . . . 41
3.3.2. ¿Cómo analizo mi sistema? . . . 42
3.3.3. ¿Cómo puedo programar un análisis? . . . 42
3.3.4. ¿Cómo creo una tarea de análisis personalizada? . . . 43
3.3.5. ¿Cómo puedo evitar que se analice una carpeta? . . . 44
3.3.6. ¿Qué hacer cuando Bitdefender detecta un archivo limpio como infectado? . . . 44
3.3.7. ¿Cómo compruebo qué amenazas ha detectado Bitdefender? . . . 45
3.4. Protección de Privacidad . . . 46
3.4.1. ¿Cómo me aseguro de que mis transacciones online son seguras? . . . 46
3.4.2. ¿Qué puedo hacer si han robado mi dispositivo? . . . 46
3.4.3. ¿Cómo puedo utilizar los blindajes de archivos? . . . 47
3.4.4. ¿Cómo elimino permanentemente un archivo con Bitdefender? . . . 49
3.4.5. ¿Cómo puedo proteger mi cámara web frente a los piratas informáticos? . . . 49
3.4.6. ¿Cómo puedo restaurar manualmente los archivos cifrados cuando falla el proceso de restauración? . . . 50
3.5. Herramientas de optimización . . . 51
3.5.1. ¿Cómo puedo mejorar el rendimiento de mi sistema? . . . 51
3.5.2. ¿Cómo puedo mejorar el tiempo de inicio de mi sistema? . . . 52
3.6. Información de Utilidad . . . 52
3.6.1. ¿Cómo pruebo mi solución de seguridad? . . . 52
3.6.2. ¿Cómo puedo eliminar Bitdefender? . . . 53
3.6.3. ¿Cómo puedo eliminar Bitdefender VPN? . . . 54
3.6.4. ¿Cómo apago el equipo automáticamente después de que finalice el análisis? . . . 55
3.6.5. ¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy? . . . 56
3.6.6. ¿Estoy utilizando una versión de Windows de 32 o 64 bit? . . . 57
3.6.7. ¿Cómo puedo mostrar los objetos ocultos en Windows? . . . 58
3.6.8. ¿Cómo desinstalo otras soluciones de seguridad? . . . 58
3.6.9. ¿Cómo puedo reiniciar en Modo Seguro? . . . 60

4. Gestión de su seguridad . . . 62
4.1. Protección Antivirus . . . 62
4.1.1. Análisis on-access (protección en tiempo real) . . . 63
4.1.2. Análisis solicitado . . . 68
4.1.3. Análisis automático de los medios extraíbles . . . 77
4.1.4. Analizar archivo del host . . . 79
4.1.5. Configurar excepciones de análisis . . . 79
4.1.6. Administración de los archivos en cuarentena . . . 82
4.2. Advanced Threat Defense . . . 83
4.3. Prevención de amenazas online . . . 85
4.4. Antispam . . . 87
4.4.1. Conocimientos antispam . . . 88
4.4.2. Activar o desactivar la protección antispam . . . 90

4.4.3. Utilizar la barra de herramientas antispam en su ventana de cliente de correo ... 90
4.4.4. Configurando la Lista de Amigos ... 92
4.4.5. Configurando la Lista de Spammers ... 94
4.4.6. Configuración de los filtros antispam locales ... 95
4.4.7. Configurando la configuración de la nube ... 96
4.5. Cortafuego ... 96
4.5.1. Administración de las reglas de apps ... 97
4.5.2. Administración de ajustes de conexión ... 100
4.5.3. Configuración de opciones avanzadas ... 101
4.6. Vulnerabilidad ... 102
4.6.1. Analizar su sistema en busca de vulnerabilidades ... 103
4.6.2. Usar el control automático de la vulnerabilidad ... 104
4.6.3. Asesor de seguridad Wi-Fi ... 106
4.7. Protección de cámaras web ... 110
4.8. Archivos seguros ... 112
4.8.1. Activar o desactivar Archivos seguros ... 113
4.8.2. Proteger los archivos personales de los ataques de ransomware ... 113
4.8.3. Configuración del acceso de las apps ... 114
4.8.4. Protección en el arranque ... 114
4.9. Reparación de ransomware ... 115
4.10. Cifrado de archivo ... 117
4.11. Protección del Gestor de contraseñas para sus credenciales ... 122
4.12. VPN ... 129
4.13. Seguridad Safepay para las transacciones online ... 132
4.14. Protección de datos ... 137
4.15. Antirrobo de Dispositivos ... 138
4.16. Bitdefender USB Immunizer ... 141

5. Optimización del sistema ... 143
5.1. Utilidades ... 143
5.1.1. Optimizar la velocidad de su sistema con un solo clic ... 143
5.1.2. Optimización del tiempo de arranque de su PC ... 144
5.1.3. Optimizar su disco ... 145
5.2. Perfiles ... 147
5.2.1. Perfil de Trabajo ... 148
5.2.2. Perfil de Películas ... 150
5.2.3. Perfil de Juego ... 151
5.2.4. Perfil de redes Wi-Fi públicas ... 152
5.2.5. Perfil del modo Batería ... 153
5.2.6. Optimización en tiempo real ... 154

6. Resolución de Problemas ... 155
6.1. Resolución de incidencias comunes ... 155
6.1.1. Mi sistema parece que se ejecuta lento ... 155
6.1.2. El análisis no se inicia ... 157
6.1.3. Ya no puedo usar una app ... 159
6.1.4. Qué hacer cuando Bitdefender bloquea un sitio Web seguro o una aplicación online ... 160

6.1.5. Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware . . . 161
6.1.6. No me puedo conectar a Internet . . . 161
6.1.7. No puedo acceder a un dispositivo en mi red . . . 162
6.1.8. Mi conexión a Internet es lenta . . . 164
6.1.9. Cómo actualizo Bitdefender en una conexión de internet lenta . . . 165
6.1.10. Los servicios de Bitdefender no responden . . . 165
6.1.11. El Filtro antispam no funciona correctamente . . . 166
6.1.12. El Autorrellenado de mi Wallet no funciona . . . 171
6.1.13. La desinstalación de Bitdefender ha fallado . . . 172
6.1.14. Mi sistema no se inicia tras la instalación de Bitdefender . . . 173
6.2. Eliminación de amenazas de su sistema . . . 176
6.2.1. Bitdefender Modo de Rescate (Entorno de rescate en Windows 10) . . . 177
6.2.2. ¿Qué hacer cuando Bitdefender encuentra amenazas en su equipo? . . . 181
6.2.3. ¿Cómo limpio una amenaza de un archivo? . . . 182
6.2.4. ¿Cómo limpio una amenaza de un archivo de correo electrónico? . . . 183
6.2.5. ¿Qué hacer si sospecho que un archivo es peligroso? . . . 184
6.2.6. ¿Qué son los archivos protegidos con contraseña del registro de análisis? . . . 185
6.2.7. ¿Qué son los elementos omitidos en el registro de análisis? . . . 185
6.2.8. ¿Qué son los archivos sobre-comprimidos en el registro de análisis? . . . 185
6.2.9. ¿Por qué eliminó Bitdefender automáticamente un archivo infectado? . . . 186

Antivirus para Mac . . . 187

7. Instalación y Desinstalación . . . 188
7.1. Requisitos del Sistema . . . 188
7.2. Instalando Bitdefender Antivirus for Mac . . . 189
7.2.1. Proceso de instalación . . . 189
7.3. Eliminando Bitdefender Antivirus for Mac . . . 193

8. Iniciando . . . 194
8.1. Acerca de Bitdefender Antivirus for Mac . . . 194
8.2. Abrir Bitdefender Antivirus for Mac . . . 194
8.3. Ventana principal de la app . . . 195
8.4. Icono de app del Dock . . . 196
8.5. Menú de navegación . . . 197

9. Protección contra Software Malicioso . . . 198
9.1. Buenas Prácticas . . . 198
9.2. Analizando Su Mac . . . 199
9.3. Asistente del Análisis . . . 200
9.4. Cuarentena . . . 201
9.5. Escudo de Bitdefender (protección en tiempo real) . . . 202
9.6. Excepciones de Análisis . . . 202
9.7. Protección Web . . . 203
9.8. Archivos seguros . . . 205
9.8.1. Aplicaciones administradas . . . 206
9.9. Protección de Time Machine . . . 207
9.10. Reparar Incidencias . . . 208

9.11. Notificaciones ... 209
9.12. Actualizaciones ... 210
9.12.1. Solicitando una Actualización ... 211
9.12.2. Obteniendo Actualizaciones a través de un Servidor Proxy ... 211
9.12.3. Actualice a una nueva versión ... 211
9.12.4. Encontrar información sobre Bitdefender Antivirus for Mac ... 212
10. Preferencias de Configuración ... 213
10.1. Preferencias de Acceso ... 213
10.2. Preferencias de protección ... 213
10.3. Preferencias avanzadas ... 214
10.4. Ofertas especiales ... 214
11. VPN ... 215
11.1. Acerca de VPN ... 215
11.2. Abrir VPN ... 215
11.3. Interfaz ... 216
11.4. Suscripciones ... 218
12. Bitdefender Central ... 219
12.1. Acerca de Bitdefender Central ... 219
12.2. Acceso a Bitdefender Central ... 220
12.3. Mis suscripciones ... 220
12.3.1. Activar la suscripción ... 220
12.3.2. Comprar suscripción ... 221
12.4. Mis dispositivos ... 221
12.4.1. Personalice su dispositivo ... 221
12.4.2. Acciones remotas ... 222
13. Preguntas frecuentes ... 224
Mobile Security para iOS ... 229
14. Qué es Bitdefender Mobile Security for iOS ... 230
15. Iniciando ... 231
16. VPN ... 235
16.1. Suscripciones ... 236
17. Privacidad de la cuenta ... 238
18. Características Antirrobo ... 240
19. Cuenta Bitdefender ... 244
Mobile Security para Android ... 246
20. Funciones de protección ... 247
21. Iniciando ... 248
22. Analizador malware ... 253

23. Protección Web 256
24. VPN 258
25. Características Antirrobo 261
26. Privacidad de la cuenta 265
27. Bloqueo de apps 267
28. Informes 272
29. Localizador 273
30. Acerca de 274
31. Bitdefender Central 275
32. Preguntas frecuentes 279

Contacto 285

33. Pedir ayuda 286
34. Recursos online 289
34.1. Centro de soporte de Bitdefender 289
34.2. Foro de Soporte de Bitdefender 290
34.3. Portal HOTforSecurity 290
35. Información de Contacto 291
35.1. Direcciones Web 291
35.2. Distribuidores locales 291
35.3. Oficinas de Bitdefender 291

Glosario 294

Introducción a Bitdefender Small Office Security

La suscripción a Bitdefender Small Office Security se dirige a pequeñas empresas que utilizan de cinco a veinte dispositivos basados en Windows, macOS, iOS y Android y desean mejorar la seguridad, evitar la pérdida de datos o impedir que los hackers y el software malicioso aprovechen vulnerabilidades en sus redes.

Se puede realizar la administración de todos los dispositivos conectados desde la plataforma Bitdefender Central siempre que el administrador haya iniciado sesión con las credenciales utilizadas para adquirir la suscripción. Para acceder a Bitdefender Central en Windows y macOS, vaya a https://central.bitdefender.com, y en iOS y Android instale la aplicación dedicada que se puede descargar en la aplicación de tienda de cada plataforma.

Para evitar que los usuarios realicen cambios de características y ajustes que puedan afectar a la seguridad de la red, el administrador puede configurar una contraseña desde la cuenta de Bitdefender. Esta opción está disponible para el producto Bitdefender Total Security, que puede instalarse en dispositivos Windows.

El área de Actividad en Bitdefender Central brinda una descripción general de los dispositivos conectados y de su estado de protección. Si se identifican amenazas, el administrador puede ejecutar un análisis en todos los dispositivos afectados al mismo tiempo.

Esta guía se basa en los cuatro productos incluidos en Bitdefender Small Office Security:

- “Total Security para PC” (p. 1)

  Aprenda a usar el producto en sus PCs y portátiles Windows.

- “Antivirus para Mac” (p. 187)

  Aprenda a usar el producto en sus Macs.

- “Mobile Security para iOS” (p. 229)

  Aprenda a usar el producto en sus tablets y smartphones iOS.

- “Mobile Security para Android” (p. 246)

  Aprenda a usar el producto en sus tablets y smartphones Android.

- “Contacto” (p. 285)

Sepa dónde buscar ayuda si surge algún problema.

TOTAL SECURITY PARA PC

1. PASOS DE LA INSTALACIÓN

1.1. Preparándose para la instalación

Antes de instalar Bitdefender Total Security, complete estos preparativos para garantizar la instalación sin problemas:

- Asegúrese que el equipo donde va a instalar Bitdefender cumple los requisitos mínimos de sistema. Si el equipo no cumple todos los requisitos mínimos del sistema, Bitdefender no se instalará o, si es instalado, no funcionará correctamente y provocará que el sistema se ralentice y sea inestable. Para ver una lista completa de los requisitos del sistema, consulte "*Requisitos del Sistema*" (p. 188).
- Inicie sesión en el equipo utilizando una cuenta de Administrador.
- Desinstale cualquier otro software similar del equipo. Si se detectase alguno durante el proceso de instalación de Bitdefender, se le notificará para que lo desinstale. La ejecución de dos programas de seguridad simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Defender se desactivará durante la instalación.
- Desactive o elimine cualquier programa cortafuego que puede estar ejecutándose en el equipo. La ejecución de dos programas de cortafuego simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Firewall se desactivará durante la instalación.
- Durante la instalación, se recomienda que su equipo esté conectado a internet. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

1.2. Requisitos del sistema

Sólo podrá instalar Bitdefender Total Security en aquellos equipos que dispongan de los siguientes sistemas operativos:

- Windows 7 con Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

Antes de instalar el producto, compruebe que el equipo reúne los siguientes requisitos del sistema:

Nota
Para saber qué sistema operativo Windows está ejecutando su equipo y obtener información del hardware:

- En **Windows 7**, haga clic con el botón derecho sobre el icono **Mi PC** del Escritorio y seleccione la opción **Propiedades** del menú.
- En **Windows 8**, desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono. En **Windows 8.1**, acceda a **Este equipo**.

  Seleccione **Propiedades** en el menú inferior. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.
- En **Windows 10**, escriba **Sistema** en el cuadro de búsqueda de la barra de tareas y haga clic en su icono. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.

Requisitos mínimos del sistema

- 2 GB de espacio disponible en disco duro
- Procesador de doble núcleo a 1,6 GHz
- 1 GB de memoria (RAM)

Requisitos de sistema recomendados

- 2,5 GB de espacio disponible en disco duro (al menos 800 MB en la unidad de sistema)
- Intel CORE Duo (2 GHz) o procesador equivalente
- 2 GB de memoria (RAM)

Requisitos de software

Para poder usar Bitdefender y todas sus funciones, su equipo necesita cumplir los siguientes requisitos software:

- Microsoft Edge 40 y superior
- Internet Explorer 10 y superior
- Mozilla Firefox 51 y superior

- Google Chrome 34 y superior

1.3. Instalando su producto Bitdefender

Puede instalar Bitdefender mediante el instalador web descargado en su equipo desde Bitdefender Central.

Si su compra cubre más de un equipo, repita el proceso de instalación y active su producto con la misma cuenta en cada equipo. La cuenta que tiene que utilizar es la que contiene la suscripción activa a su Bitdefender.

Instalar desde Bitdefender Central

Desde Bitdefender Central puede descargar el kit de instalación correspondiente a la suscripción adquirida. Una vez que el proceso de instalación se haya completado, se activa Bitdefender Total Security.

Para descargar Bitdefender Total Security desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
3. Escoja una de las dos opciones disponibles:

   - **Proteger este dispositivo**

     Seleccione esta opción y guarde el archivo de instalación.

   - **Proteger otros dispositivos**

     Seleccione esta opción y, a continuación, haga clic en **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **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.

     En el dispositivo en que desee instalar su producto Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.

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

Validación de la instalación

Bitdefender comprobará primero su equipo para validar la instalación.

Si su sistema no cumple con los requisitos mínimos para la instalación de Bitdefender, se le informará de las zonas qu desea mejorar antes de proceder.

Si se detecta una solución de seguridad incompatible o una versión anterior de Bitdefender, se le solicitará que la desinstale de su sistema. Por favor, siga las instrucciones para desinstalar el software de su sistema, evitando así posibles problemas que ocurran en un futuro. Es posible que deba reiniciar su equipo para completar la eliminación de las soluciones de seguridad detectadas.

El paquete de instalación de Bitdefender Total Security está constantemente actualizado.

Nota
Descargar los archivos de instalación puede llevar un buen rato, especialmente con conexiones a internet lentas.

Una vez que se haya validado la instalación, aparecerá el asistente de configuración. Siga los pasos para instalar Bitdefender Total Security.

Paso 1 - Instalación de Bitdefender

Antes de proceder a la instalación, 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 Total Security.

Si no acepta estos términos, cierre la ventana. Se abandonará el proceso de instalación y saldrá del programa instalador.

Pueden realizarse dos tareas adicionales en este paso:

- Mantenga habilitada la opción **Enviar informes del producto**. Permitiendo esta opción se envían informes con datos sobre cómo utiliza el producto a los servidores de Bitdefender. Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro. Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y que no se utilizarán con fines comerciales.

- Seleccione el idioma en el que desea que se instale el producto.

Haga clic en el botón **INSTALAR** para iniciar el proceso de instalación de su producto Bitdefender.

Paso 2 - Instalación en curso

Espere a que la instalación se complete. Se muestra información detallada sobre el progreso.

Se analizan las áreas más críticas de su sistema en busca de amenazas, se descargan e instalan las últimas versiones de los archivos de aplicación, y se inician los servicios de Bitdefender. Este paso puede tardar un par de minutos. Haga clic en **OMITIR ANÁLISIS** si desea analizar su sistema más adelante. Para más información sobre la ejecución de un análisis del sistema, consulte "*Ejecución de un análisis del sistema*" (p. 69).

Paso 3 - Instalación completada

Su producto Bitdefender se ha instalado correctamente.

Se muestra un resumen de la instalación. Si durante la instalación se detecta y elimina cualquier tipo de amenaza activa, puede que necesite reiniciar su equipo. Haga clic en **EMPEZAR A USAR Bitdefender** para continuar.

Paso 4 - Primeros pasos

En la ventana de **Primeros pasos** puede ver la información relativa a su suscripción activa.

Haga clic en **FINALIZAR** para acceder a la interfaz de Bitdefender Total Security.

2. PRIMEROS PASOS

2.1. Fundamentos

Una vez que haya instalado Bitdefender Total Security, su equipo estará protegido contra todo tipo de amenazas (como malware, spyware, ransomware, exploits, botnets y troyanos) y amenazas de Internet (como piratas informáticos, phishing y spam).

La aplicación utiliza la tecnología Photon para aumentar la velocidad y el rendimiento del proceso de análisis contra amenazas. Funciona gracias al aprendizaje de los patrones de uso de las aplicaciones de su sistema para saber qué y cuándo analizar, minimizando así el impacto en el rendimiento del sistema.

La conexión a redes inalámbricas públicas pertenecientes a aeropuertos, centros comerciales, cafeterías u hoteles sin protección puede ser peligrosa para su dispositivo y sus datos. Ello se debe principalmente a que podría haber delincuentes vigilando sus actividades y esperando el mejor momento para robar sus datos personales, pero también a que cualquiera puede ver su dirección IP, lo que convierte a su máquina en víctima de futuros ataques informáticos. Para evitar situaciones tan comprometidas, instale y use la app "*VPN*" (p. 129).

Puede realizar un seguimiento de sus contraseñas y cuentas en Internet almacenándolas "*Protección del Gestor de contraseñas para sus credenciales*" (p. 122)en un wallet. Con una sola contraseña maestra, podrá proteger su privacidad frente a los intrusos que traten de arrebatarle su dinero.

"*Protección de cámaras web*" (p. 110)mantiene a raya las apps que no son de fiar para que no accedan a su cámara de vídeo, con lo que evita cualquier intento de ataque por parte de piratas informáticos. El acceso de las apps populares a su cámara web se permitirá o no según las opciones escogidas por los usuarios de Bitdefender.

Para protegerle ante posibles fisgones y espías cuando su dispositivo esté conectado a una red inalámbrica que no sea segura, Bitdefender analiza su nivel de seguridad y, si es necesario, le hace recomendaciones para aumentar la seguridad de sus actividades en Internet. Para obtener instrucciones sobre cómo mantener sus datos personales a salvo, consulte el apartado "*Asesor de seguridad Wi-Fi*" (p. 106).

Sus archivos personales almacenados localmente, como documentos, fotos o películas, y también los almacenados en la nube, pueden mantenerse a salvo de la amenaza más peligrosa a día de hoy: el ransomware. Para obtener información sobre cómo poner a buen recaudo sus archivos, consulte "*Archivos seguros*" (p. 112).

Los archivos cifrados por el ransomware se pueden recuperar ahora sin tener que pagar el dinero del rescate solicitado. Para obtener información sobre cómo recuperar los archivos cifrados, consulte "*Reparación de ransomware*" (p. 115).

Mientras trabaja, juega o ve películas, Bitdefender puede ofrecerle una experiencia de usuario constante posponiendo las tareas de mantenimiento, eliminando las interrupciones y ajustando los efectos visuales del sistema. Puede beneficiarse de todo esto activando y configurando los "*Perfiles*" (p. 147).

Bitdefender tomará por usted la mayoría de las decisiones relacionadas con la seguridad y rara vez se mostrarán alertas emergentes. Los detalles sobre las medidas adoptadas y la información acerca de la operativa del programa están disponibles en la ventana de Notificaciones. Para más información, diríjase a "*Notificaciones*" (p. 9).

De vez en cuando, debe abrir Bitdefender y reparar las incidencias existentes. Puede que tenga que configurar componentes específicos de Bitdefender o tomar medidas de prevención para proteger su sistema y sus datos.

Para usar las opciones online de Bitdefender Total Security y administrar sus dispositivos, acceda a su cuenta de Bitdefender. Para más información, diríjase a "*Bitdefender Central*" (p. 26).

La sección "*Cómo*" (p. 37) es donde encontrará paso a paso instrucciones de cómo realizar tareas comunes. Si tiene algún problema mientras utiliza Bitdefender, revise la sección "*Resolución de incidencias comunes*" (p. 155) con soluciones para la mayoría de los problemas comunes.

Apertura de la ventana de Bitdefender

Para acceder a la interfaz principal de Bitdefender Total Security, siga estos pasos:

- En **Windows 7**:

  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.

2. Haga clic en **Bitdefender**.
3. Haga en clic en **Bitdefender Total Security**, o más rápido, haga doble clic en el icono de Bitdefender en el área de notificación.

- En **Windows 8 y Windows 8.1**:

  Localice Bitdefender desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender" en la pantalla de inicio) y luego haga clic en su icono. Opcionalmente, abra la app de escritorio y haga doble clic en el icono de Bitdefender en el área de notificación.

- En **Windows 10**:

  Escriba "Bitdefender" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono. Opcionalmente, haga doble clic en el icono de Bitdefender en el área de notificación.

Para obtener más información sobre la ventana de Bitdefender y el icono del área de notificación, consulte "*Interfaz de Bitdefender*" (p. 12).

2.1.1. Notificaciones

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su PC. Siempre que ocurra algo relevante respecto a la seguridad de su sistema o información, se añadirá un nuevo mensaje a las Notificaciones de Bitdefender, de forma parecida a un nuevo e-mail apareciendo en su bandeja de entrada.

Las notificaciones son una herramienta importante en la supervisión y la gestión de la protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontraron vulnerabilidades o amenazas en su equipo, etc. Además, si es necesario puede realizar acciones adicionales o cambiar las acciones que Bitdefender ha llevado a cabo.

Para acceder al registro de notificaciones, haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender. Cada vez que se produce un evento crítico, se puede ver un contador en el icono .

Dependiendo del tipo y la gravedad, las notificaciones se agrupan en:

- Los eventos **críticos** indican problemas críticos. Debe verificarlos inmediatamente.

- Los eventos de **Advertencia** indican incidencias no críticas. Cuando tenga tiempo debería comprobarlas y repararlas.
- Los eventos de **Información** indican operaciones que se han completado con éxito.

Haga clic en cada pestaña para obtener más información sobre los eventos generados. Con un simple clic en el título de cada evento se muestran algunos detalles: una breve descripción, la medida que Bitdefender adoptó cuando este se produjo, y la fecha y hora en que ocurrió. Si fuera necesario pueden proporcionarse opciones con el fin de tomar nuevas medidas.

Para ayudar a administrar fácilmente los eventos registrados, la ventana de Notificaciones proporciona opciones para eliminar o marcar como leídos todos los eventos en esta sección.

2.1.2. Perfiles

Algunas actividades informáticas, como los juegos online o las presentaciones en vídeo, requieren mayor capacidad de respuesta del sistema, alto rendimiento y ausencia de interrupciones. Cuando el portátil está funcionando con la batería, es mejor que las operaciones innecesarias, que consumen más energía, se aplacen hasta que el portátil está conectado de nuevo a la corriente.

Los Perfiles de Bitdefender asignan más recursos del sistema a las apps en ejecución, modificando temporalmente los ajustes de protección y adaptando la configuración del sistema. En consecuencia, se minimiza el impacto del sistema en sus actividades.

Para adaptarse a las diferentes actividades, Bitdefender viene con los siguientes perfiles:

Perfil de Trabajo
: Optimiza la eficiencia en su trabajo identificando y adaptando los ajustes del producto y del sistema.

Perfil de Películas
: Mejora los efectos visuales y elimina las interrupciones cuando se ven películas.

Perfil de Juego
: Mejora los efectos visuales y elimina las interrupciones cuando se juega.

Perfil de redes Wi-Fi públicas
: Aplica los ajustes del producto para beneficiarse de una protección completa mientras está conectado a una red inalámbrica no segura.

Perfil del modo Batería
: Aplica los ajustes del producto y reduce la actividad en segundo plano para ahorrar batería.

Configurar la activación automática de perfiles

Para una experiencia de usuario sencilla, puede configurar Bitdefender para que gestione su perfil de trabajo. En tal caso, Bitdefender detecta automáticamente la actividad que usted lleva a cabo y aplica los ajustes de optimización del producto y del sistema.

Para permitir que Bitdefender active los perfiles:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Utilice el conmutador correspondiente para habilitar **Activar perfiles automáticamente**.

Si no desea que los perfiles se activen automáticamente, deshabilite el conmutador.

Para activar manualmente un perfil, active el conmutador correspondiente. Solo se puede activar manualmente un perfil a la vez.

Para obtener más información sobre los Perfiles, consulte"*Perfiles*" (p. 147)

2.1.3. Informes de productos

Los informes del producto contienen información sobre cómo usa el producto Bitdefender que ha instalado. Esta información es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro.

Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y que no se utilizan con fines comerciales.

Si durante el proceso de instalación ha elegido enviar dichos informes a los servidores de Bitdefender y ahora desea detener dicho proceso:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Desactive los **Informes del producto**.

2.1.4. Notificaciones de ofertas especiales

Cuando haya ofertas promocionales disponibles, el producto Bitdefender está configurado para que se lo notifique mediante una ventana emergente. Esto le da la oportunidad de beneficiarse de precios ventajosos y mantener sus dispositivos protegidos durante un mayor período de tiempo.

Para activar o desactivar las notificaciones de ofertas especiales:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, active o desactive el conmutador correspondiente.

La opción de ofertas especiales y notificaciones del producto está activada por defecto.

2.1.5. Interfaz de análisis antimalware

Bitdefender se integra con la Antimalware Scan Interface (AMSI) de Microsoft: una forma de ayudarle a mantenerse protegido del malware dinámico basado en secuencias de comandos y oleadas no tradicionales de ataques informáticos. AMSI es un estándar de interfaz genérico que permite que las aplicaciones y los servicios se integren con los productos de Bitdefender.

Para activar o desactivar la integración con la Antimalware Scan Interface:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, active o desactive el conmutador correspondiente.

La integración con la opción Antimalware Scan Interface está habilitada por defecto y solo está disponible en Windows 10.

2.2. Interfaz de Bitdefender

Bitdefender Total Security satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. Esta interfaz de usuario

gráfica esta diseñada para satisfacer todas y cada una de las categorías de usuario.

Para que conozca la interfaz de Bitdefender, se muestra en la parte superior izquierda un asistente introductorio con información detallada sobre cómo configurar y manejar el producto. Seleccione Seleccione el soporte de ángulo recto para continuar, u **Omitir recorrido** para cerrar el asistente.

El icono de la bandeja del sistema de Bitdefender está disponible en cualquier momento, ya sea para abrir la ventana principal, ejecutar una actualización del producto o ver información sobre la versión instalada.

La ventana principal le brinda información sobre el estado de su seguridad. Según el uso y las necesidades de su dispositivo, Autopilot muestra aquí diferentes tipos de recomendaciones para ayudarle a mejorar la seguridad y el rendimiento de su dispositivo. Además, puede añadir las acciones rápidas que más use, para tenerlas a mano cuando las necesite.

Desde el menú de navegación de la izquierda, puede acceder a su cuenta de Bitdefender, al área de ajustes, a las notificaciones y a las secciones de Bitdefender para realizar una configuración detallada y tareas administrativas avanzadas. Además, puede ponerse en contacto con nosotros para obtener ayuda en caso de tener alguna pregunta o si sucede algo inesperado.

Si desea vigilar constantemente la información de seguridad esencial y tener un acceso rápido a los ajustes clave, añada el Widget de seguridad en su escritorio.

2.2.1. Icono del área de notificación

Para administrar todo el producto más fácilmente, puede usar el icono Bitdefender en la barra de tareas.

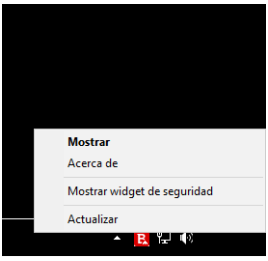
Nota

El icono de Bitdefender puede que no esté visible en todo momento. Para que el icono se muestre de forma permanente:

- En **Windows 7, Windows 8 y Windows 8.1**:
  1. Haga clic en la flecha en la esquina inferior derecha de la pantalla.
  2. Haga clic en **Personalizar...** para abrir la ventana de Iconos del área de notificación.
  3. Seleccione la opción **Mostrar icono y notificaciones** en el icono del **agente de Bitdefender**.

- En **Windows 10**:
  1. Haga clic derecho en la barra de tareas y seleccione **Propiedades**.
  2. Haga clic en **Personalizar** en la ventana de la barra de tareas.
  3. Haga clic en el enlace **Seleccionar qué iconos aparecen en la barra de tareas** en la ventana **Notificaciones y acciones**.
  4. Active el conmutador junto al **agente de Bitdefender**.

Si hace doble clic en este icono se abrirá la interfaz de Bitdefender. Además, al hacer clic derecho sobre el icono, un menú contextual le permitirá administrar rápidamente el producto Bitdefender.



Icono Bandeja

- **Mostrar** - abre la ventana principal de Bitdefender.
- **Acerca de**: Abre una ventana donde puede ver información sobre Bitdefender, buscar ayuda en caso de que suceda algo inesperado, acceder al Acuerdo de suscripción y ver los componentes de terceros y la política de privacidad.
- **Ocultar / Mostrar el Widget de seguridad** - habilita / deshabilita el Widget de seguridad.
- **Actualizar** - realiza una actualización inmediata. Puede seguir el estado de la actualización en el panel de Actualización de la ventana principal de Bitdefender.

El icono de Bitdefender en la barra de herramientas le informa cuando una incidencia afecta a su equipo o como funciona el producto, mostrando un símbolo especial, como el siguiente:

No hay ninguna incidencia que afecte a la seguridad de su sistema.
Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.

Si Bitdefender no funciona, el icono del área de notificación aparecerá en un fondo gris: . Normalmente sucede cuando una suscripción caduca. Esto puede ocurrir cuando los servicios de Bitdefender no están respondiendo o cuando otros errores afectan al funcionamiento normal de Bitdefender.

2.2.2. Menú de navegación

En el lado izquierdo de la interfaz de Bitdefender está el menú de navegación, que le permite acceder rápidamente a las características y las herramientas de Bitdefender que necesita para gestionar su producto. Las pestañas disponibles en esta área son las siguientes:

- **Panel de control**. Desde aquí puede solucionar rápidamente los problemas de seguridad, ver recomendaciones según las necesidades de su sistema y sus patrones de uso, realizar acciones rápidas e instalar Bitdefender en otros dispositivos.
- **Protección**. Desde aquí puede lanzar y configurar análisis antivirus, acceder a los ajustes del cortafuego, proteger archivos y apps de ataques de ransomware, recuperar datos en caso de que resulten cifrados por algún ransomware y configurar su protección mientras navega por Internet.
- **Privacidad**. Desde aquí puede crear gestores de contraseñas para sus cuentas online, proteger el acceso a su cámara web de miradas indiscretas, realizar pagos por Internet en un entorno seguro, abrir la app de VPN y proteger a sus hijos monitorizando y restringiendo su actividad online.
- **Utilidades**. Desde aquí, puede mejorar la velocidad del sistema y configurar la característica Antirrobo para sus dispositivos.
- **Notificaciones**. Desde aquí tiene acceso a las notificaciones generadas.
- **Mi cuenta**. Desde aquí puede acceder a su cuenta de Bitdefender para comprobar su suscripción y realizar tareas de seguridad en los dispositivos que administra. También dispone de información acerca de la cuenta de Bitdefender y de la suscripción en uso.
- **Ajustes**. Desde aquí tiene acceso a los ajustes generales.
- **Soporte**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su Bitdefender Total Security, puede ponerse en contacto con el servicio de soporte técnico de Bitdefender.

2.2.3. Panel de Control

La ventana del panel de control le permite realizar tareas comunes, solucionar rápidamente problemas de seguridad, ver la información sobre el uso del producto y acceder a los paneles desde los cuales se configuran los ajustes.

Todo se encuentra a tan sólo unos clics.

La ventana está organizada en tres áreas principales:

Área de estado de seguridad
: Aquí es donde puede comprobar el estado de la seguridad de su equipo.

Autopilot
: Aquí es donde puede comprobar las recomendaciones de Autopilot para garantizar el adecuado funcionamiento del sistema.

Acciones rápidas
: Aquí es donde puede ejecutar diferentes tareas para mantener su sistema protegido y funcionando a la velocidad óptima. También puede instalar Bitdefender en otros dispositivos, siempre y cuando su suscripción tenga suficientes puestos disponibles.

Área de estado de seguridad

Bitdefender utiliza un sistema de seguimiento de incidencias para detectar e informarle sobre las incidencias que puedan afectar a la seguridad de su equipo e información. Las incidencias detectadas incluyen la desactivación de ajustes importantes de protección y otras condiciones que pueden representar un riesgo de seguridad.

Cuando existan problemas que afecten a la seguridad de su equipo, el estado que aparece en la parte superior de la interfaz de Bitdefender pasa a color rojo. El estado mostrado indica la naturaleza de los problemas que afectan a su sistema. Además, el icono de la bandeja del sistema cambia a y, si desplaza el cursor del ratón sobre el icono, una ventana emergente confirmará la existencia de problemas pendientes.

Dado que los problemas detectados pueden impedir que Bitdefender le proteja contra amenazas o suponga un gran riesgo para la seguridad, le recomendamos que preste atención y los solucione lo antes posible. Para solucionar un problema, haga clic en el botón junto al problema detectado.

Autopilot

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 (trabajo, pagos por Internet, ver películas o jugar) el Autopilot de Bitdefender le ofrecerá recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. Las recomendaciones propuestas también pueden estar relacionadas con las acciones que debe realizar para mantener su producto funcionando a la máxima capacidad.

Para comenzar a utilizar una característica sugerida o realizar mejoras en su producto, haga clic en el botón correspondiente.

Desactivar las notificaciones de Autopilot

Para llamar su atención respecto a las recomendaciones de Autopilot, el producto Bitdefender está configurado para realizar notificaciones mediante una ventana emergente.

Para desactivar las notificaciones de Autopilot:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, desactive **Notificaciones de recomendación**.

Acciones rápidas

Mediante acciones rápidas, puede iniciar rápidamente tareas que considere importantes para mantener su sistema protegido y funcionando a una velocidad óptima.

Por defecto, Bitdefender ya incorpora algunas acciones rápidas que puede sustituir por las que usted use más frecuentemente. Para reemplazar una acción rápida:

1. Haga clic en el icono + de la esquina superior derecha de la tarjeta que desee eliminar.
2. Escoja la tarea que desee añadir a la interfaz principal y, a continuación, haga clic en **AÑADIR**.

Las tareas que puede añadir a la interfaz principal son las siguientes:

- **Análisis rápido**. Ejecute un análisis rápido para detectar de inmediato las posibles amenazas que puedan existir en su equipo.
- **Análisis de sistema**. Ejecute un análisis del sistema para asegurarse de que su equipo está libre de amenazas.
- **Análisis de vulnerabilidades**. Analice su equipo en busca de vulnerabilidades para asegurarse de que todas las aplicaciones instaladas, además del sistema operativo, están actualizadas y funcionan correctamente.
- **Comprobar la seguridad de la conexión Wi-Fi**. Abra el Asesor de seguridad Wi-Fi para comprobar si la red doméstica inalámbrica a la que se conecta es segura y si tiene vulnerabilidades.
- **Wallets**. Ver y administrar sus wallets.
- **Abrir Safepay**. Abra Bitdefender Safepay™ para proteger sus datos confidenciales mientras efectúa transacciones online.
- **Abrir VPN**. Abra Bitdefender VPN para añadir una capa más de protección mientras permanece conectado a Internet.
- **Destructor de archivos**. Inicie la herramienta Destructor de archivos para eliminar todo rastro de datos confidenciales de su equipo.
- **Blindajes de archivos**. Cree blindajes donde almacenar sus documentos confidenciales y sensibles.
- **Abra el Optimizador en un clic**. Libere espacio en disco, corrija errores del registro y proteja su privacidad eliminando archivos que ya no le hacen falta con solo hacer clic en un botón.
- **Abrir el Optimizador de inicio**. Disminuya el tiempo de arranque del sistema evitando que las apps innecesarias se ejecuten en el arranque.
- **Limpiar mi dispositivo**. Haga espacio para nuevos datos borrando archivos innecesarios.

Para empezar a proteger dispositivos adicionales con Bitdefender:

1. Haga clic en **Instalar en otro dispositivo**.

   Se le redirigirá a la página web de cuenta Bitdefender. Asegúrese de que ha iniciado sesión con sus credenciales.

2. Haga clic en **ENVIAR ENLACE DE DESCARGA** en la ventana que aparece.

3. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **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.

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

Dependiendo de su elección, se instalarán los siguientes productos de Bitdefender:

- Bitdefender Total Security en dispositivos basados ??en Windows.
- Bitdefender Antivirus for Mac en dispositivos basados ??en macOS.
- Bitdefender Mobile Security en dispositivos basados en Android.
- Bitdefender Mobile Security en dispositivos basados ??en iOS.

2.2.4. Las secciones de Bitdefender

El producto Bitdefender cuenta con tres secciones divididas en útiles características que le ayudarán a mantenerse protegido mientras trabaja, navega por la web o efectúa pagos online, a mejorar la velocidad de su sistema, y mucho más.

Para acceder a las características de una determinada sección o para empezar a configurar su producto, acceda a los siguientes iconos situados en el menú de navegación de la interfaz de Bitdefender:

- Protección
- Privacidad
- Utilidades

Protección

En la sección de Protección puede configurar sus ajustes de seguridad avanzados, gestionar los amigos y los emisores de spam, ver y editar los ajustes de conexión de red, configurar las características de Archivos seguros y Prevención de amenazas online, buscar y corregir posibles vulnerabilidades del sistema y evaluar la seguridad de las redes inalámbricas a las que se conecta.

Las características que puede administrar en la sección de Protección son:

ANTIVIRUS

La protección antivirus es la base de su seguridad. Bitdefender le protege en tiempo real y bajo demanda contra todo tipo de amenazas, como malware, troyanos, spyware, adware, etc.

En la característica Antivirus puede acceder fácilmente a las siguientes tareas de análisis:

- Análisis rápido
- Análisis de sistema
- Administrar análisis
- Modo de Rescate (Entorno de rescate en Windows 10)

Si desea obtener más información sobre las tareas de análisis y sobre cómo configurar la protección antivirus, consulte "*Protección Antivirus*" (p. 62).

PREVENCIÓN DE AMENAZAS ONLINE

La Prevención de amenazas online le ayuda a mantenerse protegido contra ataques de phishing, intentos de fraude y filtraciones de datos privados mientras navega por Internet.

Para obtener más información sobre cómo configurar Bitdefender para proteger sus actividades en la Web, consulte "*Prevención de amenazas online*" (p. 85).

CORTAFUEGOS

El cortafuego le protege mientras está conectado a redes y a Internet mediante el filtrado de todos los intentos de conexión.

Para obtener más información sobre la configuración del cortafuego, consulte "*Cortafuego*" (p. 96).

DEFENSA CONTRA AMENAZAS AVANZADAS

Advanced Threat Defense protege activamente su sistema contra amenazas como ransomware, spyware y troyanos, analizando el comportamiento de todas las apps instaladas. Se identifican los procesos sospechosos y, cuando es necesario, se bloquean.

Para obtener más información sobre cómo proteger su sistema contra amenazas, consulte "*Advanced Threat Defense*" (p. 83).

ANTISPAM

La característica antispam de Bitdefender garantiza que su bandeja de entrada esté libre de correo electrónico no deseado mediante el filtrado del tráfico de correo POP3.

Para obtener más información sobre la protección antispam, consulte "*Antispam*" (p. 87).

VULNERABILIDAD

La característica Vulnerabilidades le ayuda a mantener al día el sistema operativo y las aplicaciones que usa con regularidad, así como identificar las redes inalámbricas inseguras a las que se conecta.

Haga clic en **Análisis de vulnerabilidades** en la característica Vulnerabilidades para empezar a identificar las actualizaciones críticas de Windows, actualizaciones de aplicaciones, contraseñas débiles pertenecientes a cuentas de Windows, y redes inalámbricas que no sean seguras.

Haga clic en **Seguridad Wi-Fi** para ver la lista de redes inalámbricas a las que se conecta, junto con nuestra evaluación de reputación de cada una de ellas y las medidas que puede adoptar para mantenerse a salvo de potenciales fisgones.

Para obtener más información sobre la configuración de la protección contra vulnerabilidades, consulte "*Vulnerabilidad*" (p. 102).

ARCHIVOS SEGUROS

La característica de Archivos seguros le garantiza que sus archivos personales permanecerán protegidos contra los ataques de ransomware.

Para obtener más información sobre cómo configurar Archivos seguros para proteger sus archivos personales frente a los ataques de ransomware, consulte "*Archivos seguros*" (p. 112).

REPARACIÓN DE RANSOMWARE

La característica de Reparación de ransomware le ayuda a recuperar sus archivos en caso de que los cifre un ransomware.

Para obtener más información sobre cómo recuperar los archivos cifrados, consulte "*Reparación de ransomware*" (p. 115).

Privacidad

En la sección de Privacidad puede abrir la app Bitdefender VPN, cifrar sus datos privados, proteger sus transacciones online, mantener a salvo su cámara web y su experiencia de navegación, así como proteger a sus hijos monitorizando y restringiendo sus actividades en Internet.

Las características que puede administrar en la sección de Privacidad son:

VPN

Bitdefender VPN protege sus actividades online y oculta su dirección IP cada vez que se conecta a redes inalámbricas inseguras de aeropuertos, centros comerciales, cafeterías u hoteles. Además, puede acceder a contenidos que normalmente le estarían vedados en ciertas zonas.

Para obtener más información sobre esta característica, consulte "*VPN*" (p. 129).

CIFRAR ARCHIVOS

Cree unidades lógicas encriptadas y protegidas por contraseña (o blindajes) en su equipo donde podrá almacenar con seguridad todos sus documentos confidenciales y sensibles.

Para obtener más información acerca de cómo crear unidades lógicas protegidas por contraseña cifradas (o blindajes) en su equipo, consulte "*Cifrado de archivo*" (p. 117).

PROTECCIÓN DE CÁMARAS WEB

La Protección de cámaras web de Bitdefender mantiene su cámara web a salvo bloqueando el acceso a las apps que no sean de fiar.

Para obtener más información sobre cómo proteger su cámara web contra accesos no autorizados, consulte "*Protección de cámaras web*" (p. 110).

GESTOR DE CONTRASEÑAS

El Gestor de contraseñas de Bitdefender le ayuda a controlar sus contraseñas, protege su privacidad y le proporciona una experiencia de navegación segura.

Para obtener más información sobre la configuración del Gestor de contraseñas, consulte "*Protección del Gestor de contraseñas para sus credenciales*" (p. 122).

SAFEPAY

El navegador Bitdefender Safepay™ le ayuda a mantener a salvo y en privado su banca electrónica, sus compras por Internet y cualquier otro tipo de transacción online.

Para obtener más información sobre Bitdefender Safepay™, consulte "*Seguridad Safepay para las transacciones online*" (p. 132).

PROTECCIÓN DE DATOS

La característica de Protección de datos le permite borrar archivos de forma permanente.

Haga clic en el **Destructor de archivos** en el panel de Protección de datos para iniciar un asistente que le permitirá eliminar completamente archivos de su sistema.

Para obtener más información sobre la configuración de la Protección de datos, consulte "*Protección de datos*" (p. 137).

Utilidades

En la sección Utilidades puede mejorar la velocidad del sistema y administrar sus dispositivos.

Herramientas de optimización

Bitdefender Total Security no sólo ofrece seguridad, sino que también le ayuda a mantener en forma el funcionamiento de su equipo.

Las herramientas de optimización disponibles son las siguientes:

- Optimizador en un clic
- Optimizador de inicio
- Limpieza de disco

Para obtener más información acerca de las herramientas de optimización del rendimiento, consulte "*Utilidades*" (p. 143).

Antirrobo

Bitdefender Antirrobo protege su equipo e información contra robo o pérdida. En caso de un evento de este tipo, le permite localizar de forma remota o bloquear su equipo. También puede borrar todos los datos presentes en su sistema.

Bitdefender Antirrobo ofrece las siguientes características:

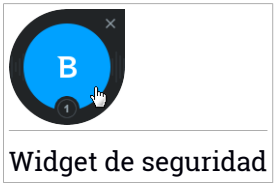
- Localizar remotamente
- Bloqueo remoto
- Borrado remoto
- Alerta remota

Para obtener más información sobre cómo puede evitar que su sistema caiga en malas manos, consulte "*Antirrobo de Dispositivos*" (p. 138).

2.2.5. Widget de seguridad

El **Widget de seguridad** es la forma rápida y fácil de monitorizar y controlar Bitdefender Total Security. Añadir este pequeño y no intrusivo widget a su escritorio le permite ver la información crítica y realizar tareas clave en todo momento:

- abra la ventana principal de Bitdefender.
- monitorice la actividad del análisis en tiempo real.
- monitorice el estado de seguridad de su sistema y solucione cualquier incidencia existente.
- vea cuándo una actualización está en curso.
- vea las notificaciones y tenga acceso a los últimos eventos de los que haya informado Bitdefender.
- analice archivos o carpetas arrastrando y soltando uno o varios elementos sobre el widget.



Widget de seguridad

El estado global de seguridad de su equipo se muestra **en el centro** del widget. El estado está indicado por el color y la forma del icono que se muestra en esta área.

Las incidencias críticas afectan a la seguridad de su sistema.

Requieren su atención inmediata y deben ser reparadas lo antes posible. Haga clic en el icono de estado para comenzar a solucionar las incidencias de las que se ha informado.

Las incidencias no críticas afectan a la seguridad de su sistema. Cuando tenga tiempo debería comprobarlas y repararlas. Haga clic en el icono de estado para comenzar a solucionar las incidencias de las que se ha informado.

Su sistema está protegido.

Cuando hay un análisis bajo demanda en curso, se muestra este icono animado.

Cuando se informe sobre las incidencias, haga clic en el icono de estado para ejecutar el asistente de Solución de incidencias.

En la **parte inferior** del widget se muestra el contador de eventos no leídos (el número de eventos destacados de los que ha informado Bitdefender, si los hay). Haga clic en el contador de eventos, por ejemplo para un evento no leído, para abrir la ventana de Notificaciones. Para más información, diríjase a "*Notificaciones*" (p. 9).

Análisis de archivos y carpetas

Puede usar el Widget de seguridad para analizar rápidamente archivos y carpetas. Arrastre cualquier archivo o carpeta que desee analizar y suéltelo sobre el **Widget de seguridad**.

El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis. Las opciones de análisis están preconfiguradas para obtener los mejores resultados de detección y no se pueden cambiar. Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminar el código malicioso). Si la desinfección falla, el Asistente de Análisis Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados.

Ocultar / mostrar el Widget de seguridad

Cuando no desee ver más el widget, haga clic en .

Para restaurar el Widget de seguridad, utilice uno de los métodos siguientes:

- Desde el área de notificación:
  1. Haga clic derecho en el icono de Bitdefender en el área de notificación.
  2. Haga clic en **Mostrar widget de seguridad** en el menú contextual que aparece.
- Desde la interfaz de Bitdefender:
  1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
  2. En la ventana **General**, active el **Widget de seguridad**.

El widget de seguridad de Bitdefender está desactivado por defecto.

2.3. 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 Android e iOS.

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:

- Descargue e instale Bitdefender en los sistemas operativos Windows, iOS, macOS y Android. Los productos disponibles para su descarga son:
  - Bitdefender Total Security
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
- Renueve su suscripción a 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.

Acceso a Bitdefender Central

Existen varias formas de acceder Bitdefender Central:

- Desde la interfaz principal de Bitdefender:
  1. Haga clic en **Mi cuenta** en el menú de navegación de la interfaz de Bitdefender.

2. Haga clic en **Acceder a Bitdefender Central**.
3. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.

- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a internet.
  2. Diríjase a: https://central.bitdefender.com.
  3. Inicie sesión en su cuenta de Bitdefender 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, se le proporcionan las opciones e instrucciones disponibles en la plataforma web.

2.3.1. Mis suscripciones

Una cuenta de Bitdefender que ha incluido una suscripción a Bitdefender Small Office Security no puede llevar asociada otra suscripción de Bitdefender, excepto la de Premium VPN de Bitdefender. El propietario de la cuenta es el que puede administrar la red, renovar la suscripción y actualizar a la versión Premium de Bitdefender VPN.

Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceda a Bitdefender Central.
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.

Añadir un nuevo dispositivo

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

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
3. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**

     Seleccione esta opción y guarde el archivo de instalación.
   - **Proteger otros dispositivos**

     Seleccione esta opción y, a continuación, haga clic en **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **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.

     En el dispositivo en que desee instalar su producto Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.
4. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

Renovar la suscripción

Si no opta por la renovación automática de su suscripción de Bitdefender, puede renovarla manualmente siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis suscripciones**.
3. Seleccione la tarjeta de suscripción deseada.
4. Haga clic en **RENOVAR** para continuar.

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

2.3.2. Mis dispositivos

El área **Mis dispositivos** en Bitdefender Central 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.

Para ver una lista de sus dispositivos ordenados según su estado o usuarios, haga clic en la flecha desplegable de la esquina superior derecha de la pantalla.

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

1. Acceda a Bitdefender Central.
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, haga clic en **GUARDAR**.

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

1. Acceda a Bitdefender Central.
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 **Perfil**.
5. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes. Personalice el perfil añadiendo una foto y seleccionando una fecha de nacimiento.
6. Haga clic en **AÑADIR** para guardar el perfil.
7. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, haga clic en **ASIGNAR**.

Para actualizar Bitdefender en un dispositivo Windows:

1. Acceda a Bitdefender Central.
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 **Actualización**.

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, haga clic en la flecha desplegable en el área de estado superior para obtener más información. Desde aquí puede solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Haga clic en 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.Para más información sobre estos dos procesos de análisis, consulte "*Ejecución de un análisis del sistema*" (p. 69) y "*Ejecución de un análisis Quick Scan*" (p. 69).
- **Optimizador**. Aquí puede mejorar el rendimiento de un dispositivo de forma remota mediante un rápido análisis, detección y limpieza de archivos inútiles. Haga clic en el botón **INICIAR** y, a continuación, seleccione las áreas que desea optimizar. Haga clic nuevamente en el botón **INICIAR** para poner en marcha el proceso de optimización. Haga clic en **Más detalles** para acceder a un informe pormenorizado acerca de los problemas solucionados.

  Además, puede mejorar el arranque de su dispositivo identificando qué aplicaciones tienen un alto consumo de recursos del sistema. Haga clic en **MÁS DETALLES** y, a continuación, elija lo que quiere hacer con las apps

detectadas. Para más información sobre estas características, consulte "*Optimizar la velocidad de su sistema con un solo clic*" (p. 143) y "*Optimización del tiempo de arranque de su PC*" (p. 144).

- **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. Haga clic en **LOCALIZAR** para conocer la ubicación de su dispositivo. Se mostrará la última posición conocida, junto con la fecha y la hora. Para más información sobre esta característica, consulte "*Antirrobo de Dispositivos*" (p. 138).
- **Vulnerabilidad**. Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, haga clic en 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. Haga clic en **Más detalles** para acceder a un informe detallado acerca de los problemas encontrados. Para más información sobre esta característica, consulte "*Vulnerabilidad*" (p. 102).

2.3.3. Configuración de protección por contraseña de Bitdefender

Si es el administrador de la suscripción a Bitdefender Small Office Security, puede establecer una contraseña para evitar que los miembros de su equipo realicen cambios en el producto.

Para configurar la protección por contraseña para los ajustes de Bitdefender Total Security:

- Acceda a Bitdefender Central.
- Haga clic en el icono de la parte superior derecha de la pantalla.
- Haga clic en **Cuenta de administrador** en el menú deslizante.
- Active el conmutador correspondiente.
- Escriba la contraseña en el campo correspondiente y, a continuación, haga clic en **ESTABLECER CONTRASEÑA DE ADMINISTRADOR**.

Una vez que haya establecido una contraseña, cualquiera que desee cambiar la configuración de Bitdefender tendrá primero que proporcionar la contraseña.

2.3.4. Actividad

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, haga clic en **Solucionar problemas** y, a continuación, haga clic en **ANALIZAR Y REPARAR LOS DISPOSITIVOS**.

  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 dispositivos donde se han encontrado más amenazas.

2.3.5. Mi cuenta

En la sección **Mi Cuenta** tiene la posibilidad de personalizar su perfil, cambiar la contraseña asociada a su cuenta, gestionar las sesiones y los mensajes de ayuda de Bitdefender Central.

Tras hacer clic en el icono de la parte superior derecha de la pantalla y escoger **Mi cuenta**, tendrá a su disposición las siguientes pestañas:

- **Perfil** - aquí puede añadir y modificar la información de la cuenta.

- **Cambiar contraseña** - aquí puede cambiar la contraseña asociada a su cuenta.

- **Gestión de sesiones** - aquí puede ver y gestionar las últimas sesiones inactivas y activas iniciadas en los dispositivos asociados a su cuenta.

- **Ajustes**: Aquí puede activar y desactivar los mensajes de ayuda de Bitdefender Central y decidir si desea recibir notificaciones o no cuando se tomen fotos de forma remota con sus dispositivos Android.

2.3.6. 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.

2.4. Mantenimiento de Bitdefender al día

Todos los días se encuentran e identifican nuevas amenazas. Por este motivo es muy importante mantener Bitdefender actualizado con la última base de datos de información de amenazas.

Si está conectado a internet a través de una conexión de banda ancha o ADSL, Bitdefender se actualizará sólo. Por omisión, busca actualizaciones cuando enciende su equipo y cada **hora** a partir de ese momento. Si se detecta una actualización, esta es automáticamente descargada e instalada en su equipo.

El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afectará al rendimiento del producto, a la vez que se evita cualquier riesgo.

> **Importante**
> Para estar protegido contra las últimas amenazas mantenga activo Actualización automática.

En algunas situaciones particulares, se precisa su intervención para mantener la protección de su Bitdefender actualizada:

- Si su equipo se conecta a internet a través de un servidor proxy, puede configurar las opciones del proxy según se describe en "*¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?*" (p. 56).
- Si está conectado a internet a través de una conexión por módem analógico, es recomendable actualizar Bitdefender manualmente. Para más información, diríjase a "*Realizar una actualización*" (p. 34).

2.4.1. Comprobar si Bitdefender está actualizado

Para comprobar la hora a la que se actualizó su Bitdefender por última vez:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente a la última actualización.

Puede saber cuándo se iniciaron las actualizaciones y obtener información sobre ellas (si se realizaron con éxito o no, si requieren reiniciar para completar la instalación). Si es necesario, reinicie el sistema en cuanto pueda.

2.4.2. Realizar una actualización

Para poder hacer actualizaciones es necesaria una conexión a internet.

Para comenzar una actualización, haga clic con el botón derecho en el icono de Bitdefender en la bandeja del sistema y, a continuación, seleccione **Actualizar ahora**.

La característica Actualizar se conectará al Servidor de actualizaciones de Bitdefender y buscará actualizaciones. Al detectar una actualización se le solicitará su confirmación para instalarla, o bien podrá realizarse de forma automática dependiendo de lo haya definido en la Configuración de actualización.

Importante
Podría ser necesario reiniciar el equipo cuando haya completado la actualización. Le recomendamos que lo haga lo antes posible.

También puede realizar actualizaciones en sus dispositivos de forma remota, siempre y cuando estén encendidos y conectados a Internet.

Para actualizar Bitdefender en un dispositivo Windows:

1. Acceda a Bitdefender Central.
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 **Actualización**.

2.4.3. Activar o desactivar la actualización automática

Para activar o desactivar la actualización automática:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar**.
3. Active o desactive el conmutador correspondiente.
4. Aparecerá una ventana de advertencia. Debe confirmar esta elección seleccionando del menú cuánto tiempo desea que esté deshabilitada la actualización automática. Puede desactivar la actualización automática durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.

Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Si Bitdefender no se actualiza regularmente, no podrá protegerle contra las amenazas más recientes.

2.4.4. Ajustar las opciones de actualización

Las actualizaciones se pueden realizar desde la red local, por internet, directamente o mediante un servidor proxy. Por defecto, Bitdefender comprobará si existen actualizaciones cada hora, a través de Internet, e instalará las actualizaciones disponibles sin alertarle.

La configuración de actualizaciones predeterminada se ajusta a la mayoría de usuarios y normalmente no tiene que cambiarla.

Para modificar los ajustes de actualización:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar** y ajuste la configuración de acuerdo a sus preferencias.

Frecuencia de actualización

Bitdefender está configurado para buscar actualizaciones cada hora. Para cambiar la frecuencia de actualización, arrastre el control deslizante sobre

la escala para establecer el período de tiempo deseado en que deben producirse las actualizaciones.

Reglas de proceso de actualización

Siempre que haya una actualización disponible, Bitdefender descargará e implementará automáticamente la actualización sin mostrar notificaciones. Desactive la opción **Actualización silenciosa** si desea que se le notifique cada vez que haya una nueva actualización disponible.

Algunas actualizaciones necesitan reiniciar el sistema para completar la instalación.

Si una actualización necesita reiniciar el sistema, de forma predeterminada Bitdefender seguirá utilizando los archivos antiguos hasta que el usuario reinicie voluntariamente el equipo. Esto es así para evitar que el proceso de actualización de Bitdefender interfiera con el trabajo del usuario.

Si desea que se le pregunte cuando una actualización requiera reiniciar, active **Notificación de reinicio**.

2.4.5. Actualizaciones continuas

Para asegurarse de que está utilizando la última versión, su Bitdefender comprueba automáticamente si existen actualizaciones del producto. Estas actualizaciones pueden aportar nuevas características y mejoras, solucionar problemas del producto o actualizarlo automáticamente a una nueva versión. Cuando se produce una actualización a una nueva versión de Bitdefender, se guardan los ajustes personalizados y se omite el proceso de desinstalación y reinstalación.

Estas actualizaciones requieren un reinicio del sistema para dar paso a la instalación de nuevos archivos. Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si pasa por alto esta notificación, puede hacer clic en **REINICIAR AHORA** en la ventana Notificaciones donde se indica la actualización más reciente, o reiniciar manualmente el sistema.

3. CÓMO

3.1. Pasos de la Instalación

3.1.1. ¿Cómo puedo reinstalar Bitdefender?

Las situaciones típicas en las cuales necesitaría reinstalar Bitdefender incluyen las siguientes:

- ha reinstalado el sistema operativo.
- desea reparar los problemas que puedan haber causado demoras o cierres inesperados.
- su producto Bitdefender no se inicia o no funciona correctamente.

Si experimenta alguna de las situaciones mencionadas, siga estos pasos:

- En **Windows 7**:
  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
  2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. Haga clic en **REINSTALAR** en la ventana que aparece.
  4. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Haga clic en **REINSTALAR** en la ventana que aparece.
  5. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Apps y características**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

4. Haga clic en **Desinstalar** para confirmar su elección.
5. Haga clic en **REINSTALAR**.
6. Necesita reiniciar el equipo para completar el proceso.

Nota
Siguiendo este procedimiento de reinstalación, se guardan los ajustes personalizados para que estén disponibles en el nuevo producto instalado. Puede que otros ajustes vuelvan a su valor por defecto.

3.1.2. ¿Desde dónde puedo descargar mi producto Bitdefender?

Puede instalar Bitdefender mediante el instalador web descargable en su equipo desde la plataforma Bitdefender Central.

Nota
Antes de ejecutar el kit, se recomienda desinstalar cualquier solución de seguridad instalada en su sistema. Cuando utiliza más de una solución de seguridad en el mismo equipo, el sistema se vuelve inestable.

Para instalar Bitdefender desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
3. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**

     Seleccione esta opción y guarde el archivo de instalación.
   - **Proteger otros dispositivos**

     Seleccione esta opción y, a continuación, haga clic en **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **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.

En el dispositivo en que desee instalar su producto Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.

4. Ejecute el producto Bitdefender que ha descargado.

3.2. Bitdefender Central

3.2.1. ¿Cómo inicio sesión en Bitdefender Central usando otra cuenta online?

Ha creado una nueva cuenta Bitdefender y desea utilizarla a partir de ahora.

Para utilizar otra cuenta:

1. Haga clic en **Mi cuenta** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **Cambiar cuenta** en la esquina superior derecha de la pantalla para cambiar la cuenta vinculada al equipo.
3. Escriba la dirección de correo electrónico y la contraseña de su cuenta en los campos correspondientes y, a continuación, haga clic en **INICIAR SESIÓN**.

Nota
El producto Bitdefender de su dispositivo cambia automáticamente de acuerdo con la suscripción asociada a la nueva cuenta de Bitdefender.
Si no hay ninguna suscripción disponible asociada a la nueva cuenta de Bitdefender, o si desea transferirla desde la cuenta anterior, puede ponerse en contacto con el soporte técnico de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

3.2.2. ¿Cómo puedo desactivar los mensajes de ayuda de Bitdefender Central?

Para ayudarle a entender para qué vale cada opción de Bitdefender Central, el panel de control muestra mensajes de ayuda.

Si no desea ver este tipo de mensajes:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.

3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Configuración**.
5. Desactive la opción **Activar o desactivar los mensajes de ayuda**.

3.2.3. He olvidado la contraseña que establecí para cuenta Bitdefender. ¿Cómo la restablezco?

Hay dos posibilidades para establecer una nueva contraseña para su cuenta de Bitdefender:

- Desde la interfaz de Bitdefender:
  1. Haga clic en **Mi cuenta** en el menú de navegación de la interfaz de Bitdefender.
  2. Haga clic en **Cambiar cuenta** en la esquina superior derecha de la pantalla.

     Aparecerá una nueva ventana.
  3. Haga clic en **Olvidé la contraseña**.
  4. Escriba la dirección de correo electrónico utilizada para crear su cuenta de Bitdefender y, a continuación, haga clic en **OLVIDÉ LA CONTRASEÑA**.
  5. Compruebe su correo y haga clic en el botón proporcionado.

     Se abre la ventana RESTABLECER CONTRASEÑA de Bitdefender.
  6. Escriba su dirección de correo electrónico y la nueva contraseña en los campos correspondientes. La contraseña debe tener al menos ocho caracteres e incluir números.
  7. Haga clic en **RESTABLECER CONTRASEÑA**.
- Desde su navegador Web:
  1. Diríjase a: https://central.bitdefender.com.
  2. Haga clic en **Olvidé la contraseña**.
  3. Escriba su dirección de correo electrónico y, a continuación, haga clic en **OLVIDÉ LA CONTRASEÑA**.
  4. Revise su cuenta de correo electrónico y siga las instrucciones que se le proporcionan para establecer una nueva contraseña para su cuenta Bitdefender.

De ahora en adelante, para acceder a su cuenta Bitdefender, escriba su dirección de correo electrónico y la nueva contraseña que acaba de establecer.

3.2.4. ¿Cómo puedo gestionar las sesiones asociadas a mi cuenta de Bitdefender?

En su cuenta de Bitdefender tiene la posibilidad de ver las últimas sesiones inactivas y activas iniciadas en los dispositivos asociados a su cuenta. También puede cerrar sesión de forma remota siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Gestión de sesiones**.
5. En la sección **Sesiones activas**, seleccione la opción **CERRAR SESIÓN** junto al dispositivo en el que desee cerrar la sesión.

3.3. Analizando con Bitdefender

3.3.1. ¿Cómo analizo un archivo o una carpeta?

La manera más fácil para analizar un archivo o carpeta es hacer clic con el botón derecho en el objeto que desee analizar, escoger Bitdefender y seleccionar **Analizar con Bitdefender** en el menú.

Para completar el análisis, siga las indicaciones del asistente de Análisis antivirus. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Las situaciones típicas en las cuales debería utilizar este método de análisis incluyen las siguientes:

- Sospecha que un fichero o carpeta concreta está infectada.
- Siempre que descargue archivos de internet que crea que pueden ser peligrosos.

- Analizar una carpeta compartida en red antes de copiar ficheros a su ordenador.

3.3.2. ¿Cómo analizo mi sistema?

Para llevar a cabo un análisis completo del sistema:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
3. Siga el Asistente de análisis del sistema para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.

   Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, diríjase a "*Asistente del análisis Antivirus*" (p. 73).

3.3.3. ¿Cómo puedo programar un análisis?

Puede configurar su producto Bitdefender para que empiece a analizar las ubicaciones importantes del sistema cuando no esté frente a su equipo.

Para programar un análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. Seleccione el tipo de análisis que desea programar: análisis completo del sistema o Quick Scan y, a continuación, haga clic en **OPCIONES DE ANÁLISIS**.

   Como alternativa, puede crear un tipo de análisis que se adapte a sus necesidades haciendo clic en **NUEVA TAREA PERSONALIZADA**.
4. Active la opción **Programar**.

   Seleccione una de las opciones correspondientes para establecer una programación:

   - Al iniciar el sistema
   - Una sola vez
   - Periódicamente

En la ventana de **Objetivos de análisis** puede seleccionar las ubicaciones que desea que se analicen. Esta opción solo está disponible si elige crear un nuevo análisis personalizado.

3.3.4. ¿Cómo creo una tarea de análisis personalizada?

Si desea analizar ubicaciones concretas en su equipo o configurar las opciones de análisis, configure y ejecute una tarea de análisis personalizada.

Para crear una tarea de análisis personalizada, proceda como se indica a continuación:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. Haga clic en **NUEVO ANÁLISIS PERSONALIZADO**. Haga clic en la ventana **Básico** para introducir un nombre para el análisis y seleccione las ubicaciones que desea analizar.
4. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**.

   Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Arrastre la barra de desplazamiento por la escala para asignar el nivel de análisis deseado.

   También puede elegir apagar el equipo cuando haya terminado el análisis si no se encuentran amenazas. Recuerde que este será el comportamiento por omisión cada vez que ejecute esta tarea.
5. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
6. Utilice el conmutador correspondiente si desea establecer una programación para su tarea de análisis.
7. Haga clic en **INICIAR ANÁLISIS** y siga el Asistente de análisis para llevarlo a cabo. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.
8. Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

3.3.5. ¿Cómo puedo evitar que se analice una carpeta?

Bitdefender permite exceptuar del análisis determinados archivos, carpetas o extensiones de archivo.

Las excepciones son para que las utilicen usuarios con conocimientos avanzados en informática y solo en las siguientes situaciones:

- Tiene una carpeta de gran tamaño en su sistema donde guarda películas y música.
- Tiene un archivo grande en su sistema donde guarda distintos tipos de datos.
- Mantenga una carpeta donde instalar diferentes tipos de software y aplicaciones para la realización de pruebas. Analizar la carpeta puede provocar la pérdida de algunos de los datos.

Para añadir carpetas a la lista de excepciones:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Haga clic en la pestaña **Excepciones**.
4. Haga clic en el menú de acordeón **Lista de archivos y carpetas exceptuados del análisis** y, a continuación, en el botón **Añadir**.
5. Haga clic en **EXAMINAR**, seleccione la carpeta que desea exceptuar del análisis y, a continuación, elija el tipo de análisis del que se debe exceptuar.
6. Haga clic en **AÑADIR** para aplicar los cambios y cierre la ventana.

3.3.6. ¿Qué hacer cuando Bitdefender detecta un archivo limpio como infectado?

Puede haber casos en los que Bitdefender marque erróneamente como amenaza un archivo legítimo (un falso positivo). Para corregir este error, añada el archivo al área de excepciones de Bitdefender:

1. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.

b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.

c. En la ventana **Escudo**, desactive **Escudo de Bitdefender**.

Aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.

2. Muestra los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 58).
3. Restaurar el archivo desde el área de Cuarentena:

a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.

b. En el panel **ANTIVIRUS**, haga clic en **Cuarentena**.

c. Seleccione el archivo y haga clic en **RESTAURAR**.

4. Añada el archivo a la lista de excepciones. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo evitar que se analice una carpeta?*" (p. 44).
5. Active la protección antivirus en tiempo real de Bitdefender.
6. Póngase en contacto con nuestros agentes de soporte técnico para que podamos eliminar la detección de la actualización de información sobre amenazas. Para averiguar cómo hacerlo, consulte "*Pedir ayuda*" (p. 286).

3.3.7. ¿Cómo compruebo qué amenazas ha detectado Bitdefender?

Cada vez que se realiza un análisis, se crea un registro y Bitdefender anota los problemas detectados.

El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde el asistente de análisis, una vez finalizado este, haciendo clic en **MOSTRAR REGISTRO**.

Para revisar más tarde un informe de análisis o cualquier infección detectada:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.

2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

   Aquí es donde puede encontrar todos los eventos de análisis de amenazas, incluyendo las detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.

3. En la lista de notificaciones puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificacione para ver más detalles sobre él.

4. Para abrir un registro de análisis, haga clic en **Ver log**.

3.4. Protección de Privacidad

3.4.1. ¿Cómo me aseguro de que mis transacciones online son seguras?

Para asegurarse de que sus operaciones online se mantienen en privado, puede usar el navegador que le proporciona Bitdefender para proteger sus transacciones y aplicaciones de banca electrónica.

Bitdefender Safepay™ es un navegador seguro diseñado para proteger la información de su tarjeta de crédito, número de cuenta o cualquier otra información confidencial que pueda introducir al acceder a diferentes sitios online.

Para mantener sus actividades online protegidas y en privado:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **Safepay**, haga clic en **Abrir Safepay**.
3. Haga clic en el botón para acceder al **Teclado virtual**.

   Utilice el **Teclado virtual** cuando teclee información sensible como sus contraseñas.

3.4.2. ¿Qué puedo hacer si han robado mi dispositivo?

El robo de dispositivos móviles, ya sean smartphones, tablets o portátiles es uno de los principales problemas que afectan hoy en día a personas y organizaciones de todo el mundo.

El Antirrobo Bitdefender le permite no solo localizar y bloquear el dispositivo robado, sino también borrar toda la información del mismo para asegurarse de que el ladrón no podrá utilizarla.

Para acceder a las características de Antirrobo desde su cuenta:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, seleccione **Antirrobo**.
4. Seleccione la característica que desea usar:
   - **LOCALIZAR** - muestra la ubicación de su dispositivo en Google Maps.
   - **Alerta**: envía una alerta al dispositivo.
   - **Bloquear** - bloquee su equipo y establezca un código numérico PIN para desbloquearlo. Como alternativa, active la opción correspondiente para permitir que Bitdefender tome instantáneas de la persona que esté tratando de acceder a su dispositivo.
   - **Borrar** - borra todos los datos de su equipo.

     Importante
     Después de borrar un dispositivo, todas las características de Antirrobo dejan de funcionar.

   - **Mostrar IP** - Muestra la última dirección IP del dispositivo seleccionado.

3.4.3. ¿Cómo puedo utilizar los blindajes de archivos?

El Blindaje de Archivo de Bitdefender le permite crear cifrados, unidades lógicas protegidas con contraseña (o blindajes) en su equipo donde puede almacenar de forma segura sus documentos sensibles y confidenciales. Físicamente, el blindaje es un archivo guardado en el disco duro local que tiene la extensión .bvd.

Cuando crear un blindaje de archivo, dos aspectos son importantes: el tamaño y la contraseña. El tamaño de 100 MB predeterminado debería ser suficiente para sus documentos privados, archivos de Excel y otros datos

similares. Sin embargo, para vídeo y otras archivos más grandes puede necesitar más espacio.

Para almacenar de forma segura los archivos o carpetas que contengan información confidencial o sensible en los blindajes de archivos de Bitdefender:

- **Crear un blindaje de archivo y establecer una contraseña fuerte para este.**

  Para crear un blindaje, haga clic con el botón derecho en un área vacía del escritorio o en una carpeta de su equipo, escoja **Bitdefender** > **Blindaje de archivo Bitdefender** y seleccione **Crear blindaje de archivo**.

  Aparecerá una nueva ventana. Siga estos pasos:

  1. Haga clic en **Explorar**, seleccione la ubicación del blindaje y guarde el archivo de blindaje con el nombre deseado.
  2. Seleccione la letra de la unidad en el menú. Cuando abre el blindaje, aparece una unidad de disco virtual etiquetada con la letra seleccionada en **Mi PC**.
  3. Introduzca la contraseña del blindaje en los campos **Contraseña** y **Confirme**.
  4. Si desea cambiar el tamaño por defecto del blindaje (100 MB), use las teclas de flecha arriba y abajo en **Tamaño del blindaje (MB)**.
  5. Haga clic en **Crear**.

  > **Nota**
  > Cuando abre el blindaje, aparece una unidad de disco virtual en **Mi PC**. Esta unidad estará etiquetada con la letra de unidad asignada al Blindaje.

- **Añada los archivos o carpetas que desee mantener a salvo al blindaje.**

  Para añadir un archivo a un blindaje, primero debe abrir el blindaje.

  1. Explorar hasta el archivo de blindaje .bvd.
  2. Haga clic derecho en el archivo de blindaje, apunte a Bitdefender Blindaje de Archivo y seleccione **Abrir**.
  3. En la ventana que aparece, introduzca la contraseña, seleccione una letra de unidad para el blindaje y haga clic en **Aceptar**.

  Puede realizar ahora operaciones en la unidad que corresponde al blindaje de archivo deseado utilizando Windows Explorer, igual que lo haría con

una unidad normal. Para añadir un archivo a un blindaje abierto, puede también hacer clic derecho en el archivo, hacer clic en Blindaje de Archivos de Bitdefender y seleccionar **Añadir a Blindaje**.

- **Mantenga el blindaje bloqueado en todo momento.**

  Solo abra los blindajes cuando necesite acceder a ellos o administrar su contenido. Para bloquear un blindaje, haga clic derecho en la unidad de disco virtual correspondiente desde **Mi PC**, apunte a **Blindaje de Archivo Bitdefender** y seleccione **Bloquear**.

- **Asegurar no eliminar el archivo de blindaje .bvd.**

  Borrando el archivo también se borrará el contenido del blindaje.

Para más información sobre la operación con los blindajes de archivo, por favor diríjase a "*Cifrado de archivo*" (p. 117).

3.4.4. ¿Cómo elimino permanentemente un archivo con Bitdefender?

Si desea eliminar un archivo de su sistema permanentemente, necesita eliminar físicamente la información de su disco duro.

El Destructor de archivos de Bitdefender le ayudará a eliminar rápidamente archivos o capetas de su ordenador usando el menú contextual de Windows siguiendo estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente, escoja Bitdefender y seleccione **Destructor de archivos**.
2. Haga clic en **ELIMINAR PERMANENTEMENTE** y, a continuación, confirme que desea continuar con el proceso.

   Espere a que Bitdefender finalice la destrucción de archivos.
3. Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

3.4.5. ¿Cómo puedo proteger mi cámara web frente a los piratas informáticos?

Puede configurar su producto Bitdefender para que permita o deniegue el acceso de las apps instaladas a su cámara web siguiendo estos pasos:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PROTECCIÓN DE CÁMARAS WEB**, haga clic en **Acceso a la cámara web**.

   Se muestra la lista con las apps que han solicitado acceso a su cámara.
3. Señale la aplicación a la que desea permitir o prohibir el acceso y, a continuación, haga clic en el conmutador correspondiente.

   Para ver lo que los otros usuarios de Bitdefender han decidido hacer con la app seleccionada, haga clic en el icono . Se le notificará cada vez que una de las apps de la lista resulte bloqueada por los usuarios de Bitdefender.

Para añadir apps a esta lista manualmente, haga clic en el enlace **Añadir una nueva aplicación a la lista**.

3.4.6. ¿Cómo puedo restaurar manualmente los archivos cifrados cuando falla el proceso de restauración?

En caso de que los archivos cifrados no se puedan restaurar automáticamente, puede hacerlo manualmente siguiendo estos pasos:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación referente al último comportamiento de ransomware detectado y luego haga clic en **Archivos cifrados**.
3. Se muestra la lista con los archivos cifrados.

   Haga clic en **RECUPERAR ARCHIVOS** para continuar.
4. En caso de que la totalidad o una parte del proceso de restauración falle, debe elegir la ubicación donde se guardarán los archivos descifrados. Haga clic en **RESTAURAR UBICACIÓN** y luego elija una en su PC.
5. Aparecerá una ventana de confirmación.

   Haga clic en **FINALIZAR** para terminar el proceso de restauración.

En caso de cifrado, se pueden restaurar los archivos con las siguientes extensiones:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.5. Herramientas de optimización

3.5.1. ¿Cómo puedo mejorar el rendimiento de mi sistema?

El rendimiento del sistema depende no sólo de la configuración del hardware, sino también de la carga de la CPU, el uso de la memoria y el espacio del disco duro. También está conectado directamente a su configuración de software y a la administración de sus datos.

Estas son las principales acciones que puede tomar con Bitdefender para mejorar la velocidad y rendimiento de su sistema:

- "*Optimice el rendimiento de su sistema con un solo clic*" (p. 51)
- "*Analice su sistema periódicamente*" (p. 52)

Optimice el rendimiento de su sistema con un solo clic

La opción Optimizador en un clic le ahorra un tiempo valioso cuando desea una forma rápida de mejorar el rendimiento de su sistema mediante un rápido análisis, detección y limpieza de archivos inútiles.

Para iniciar el proceso del Optimizador en un clic:

1. Haga clic en **Utilidades** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **OPTIMIZAR MI DISPOSITIVO**.
3. Deje que Bitdefender busque los archivos que se pueden borrar y, a continuación, haga clic en el botón **OPTIMIZAR** para finalizar el proceso.

Para obtener más información sobre cómo puede aumentar la velocidad de su equipo con un solo clic, consulte "*Optimizar la velocidad de su sistema con un solo clic*" (p. 143).

Analice su sistema periódicamente

La velocidad de su sistema y su comportamiento general también pueden verse afectados por las amenazas.

Asegúrese de que puede analizar su sistema periódicamente, al menos una vez a la semana.

Se recomienda utilizar el análisis de sistema porque analiza todos los tipos de amenazas que ponen en peligro la seguridad de su sistema y también analiza el contenido de los archivos comprimidos.

Para iniciar el análisis del sistema:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
3. Siga los pasos del asistente.

3.5.2. ¿Cómo puedo mejorar el tiempo de inicio de mi sistema?

Las aplicaciones innecesarias que prolongan irritantemente el tiempo que tarda su PC en arrancar pueden deshabilitarse o posponerse su apertura con el Optimizador de inicio, ahorrándose así un tiempo valioso.

Para utilizar el Optimizador de inicio:

1. Haga clic en **Utilidades** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **OPTIMIZAR EL ARRANQUE DEL DISPOSITIVO**.
3. Seleccione las aplicaciones que desee posponer en el arranque del sistema.

Para obtener más información sobre cómo optimizar el tiempo de arranque de su equipo, consulte "*Optimización del tiempo de arranque de su PC*" (p. 144).

3.6. Información de Utilidad

3.6.1. ¿Cómo pruebo mi solución de seguridad?

Para asegurarse de que su producto Bitdefender se ejecutara correctamente, le recomendamos que utilice la prueba Eicar.

La prueba Eicar le permite comprobar la protección de su solución de seguridad utilizando un archivo seguro desarrollado a tal fin.

Para probar su solución de seguridad:

1. Descargue la prueba desde la página web oficial de la organización EICAR http://www.eicar.org/.
2. Haga clic en la pestaña **Anti-Malware Testfile**.
3. Haga clic en **Descargar** en el menú de la izquierda.
4. En **Download area using the standard protocol http** haga clic en el archivo de prueba **eicar.com**.
5. Se le informará de que la página a la que está intentando acceder contiene el EICAR-Test-File (no una amenaza).

   Si hace clic en **Comprendo los riesgos, ir ahí de todas formas**, se iniciará la descarga de la prueba y una ventana emergente de Bitdefender le informará de que se ha detectado una amenaza.

   Haga clic en **Más detalles** para obtener más información sobre esta acción.

Si no recibe ninguna alerta de Bitdefender, le recomendamos que contacte con Bitdefender para obtener soporte técnico como se describe en la sección "*Pedir ayuda*" (p. 286).

3.6.2. ¿Cómo puedo eliminar Bitdefender?

Si desea eliminar su Bitdefender Total Security:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. Haga clic en **ELIMINAR** en la ventana que aparece.
  4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.

2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
4. Haga clic en **ELIMINAR** en la ventana que aparece.
5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Haga clic en **ELIMINAR** en la ventana que aparece.
  6. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

Nota
Este procedimiento de reinstalación eliminará permanentemente los ajustes personalizados.

3.6.3. ¿Cómo puedo eliminar Bitdefender VPN?

El procedimiento para eliminar Bitdefender VPN es similar al empleado para desinstalar otros programas de su equipo:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender VPN** y seleccione **Desinstalar**.

     Espere a que el proceso de desinstalación se complete.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.

3. Encuentre **Bitdefender VPN** y seleccione **Desinstalar**.

   Espere a que el proceso de desinstalación se complete.

- En **Windows 10**:

  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre **Bitdefender VPN** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.

     Espere a que el proceso de desinstalación se complete.

3.6.4. ¿Cómo apago el equipo automáticamente después de que finalice el análisis?

Bitdefender ofrece múltiples tareas de análisis que puede utilizar para asegurarse de que su sistema no está infectado con amenazas. Analizar todo el equipo puede que tarde más tiempo en completarse dependiendo de la configuración de hardware y software de su sistema.

Por esta razón, Bitdefender le permite configurar su producto para que apague su sistema cuando el análisis haya acabado.

Piense en este ejemplo: ha acabado su trabajo con el equipo y quiere irse a dormir. Desearía que Bitdefender comprobase todo su sistema en busca de amenazas.

Así es como puede configurar Bitdefender para apagar su sistema al finalizar el análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. En la ventana **Administrar tareas de análisis**, haga clic en **NUEVA TAREA PERSONALIZADA** para introducir un nombre para el análisis y seleccione las ubicaciones que desea analizar.
4. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**.

5. Elija apagar el equipo cuando el análisis finalice si no se encuentra ninguna amenaza.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.
7. Haga clic en **INICIAR ANÁLISIS** para analizar su sistema.

Si no se encuentran amenazas, su equipo se apagará.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, diríjase a "*Asistente del análisis Antivirus*" (p. 73).

3.6.5. ¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?

Si su equipo está conectado a Internet a través de un servidor proxy, debe configurar Bitdefender utilizando la configuración del proxy. Normalmente, Bitdefender automáticamente detecta e importa la configuración del proxy desde su sistema.

> **Importante**
> Las conexiones a internet desde el propio domicilio no suelen utilizar un servidor proxy. Como regla de oro, compruebe y configure las opciones de la conexión proxy de su programa Bitdefender mientras no se estén aplicando actualizaciones. Si Bitdefender se puede actualizar, entonces está configurado correctamente para conectarse a internet.

Para administrar las opciones del proxy:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Active el **Servidor Proxy**.
4. Haga clic en **Cambio de proxy**.
5. Hay dos opciones para establecer la configuración del proxy:
   - **Importar configuración proxy desde el navegador predeterminado** - la configuración del proxy del usuario actual, extraída del navegador predeterminado. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.

Nota
Bitdefender puede importar la configuración proxy desde los navegadores más populares, incluyendo las últimas versiones de Microsoft Edge, Internet Explorer, Mozilla Firefox y Google Chrome.

- **Configuración personalizada del proxy** - la configuración del proxy que puede modificar. Deben indicarse las siguientes opciones:
  - **Dirección** - introduzca la IP del servidor proxy.
  - **Puerto** - introduzca el puerto que Bitdefender debe utilizar para conectarse con el servidor proxy.
  - **Nombre** - escriba un nombre de usuario que el proxy reconozca.
  - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Bitdefender usará las opciones disponibles de proxy hasta que consiga conectarse a internet.

3.6.6. ¿Estoy utilizando una versión de Windows de 32 o 64 bit?

Para averiguar si tiene un sistema operativo de 32 o de 64 bits:

- En **Windows 7**:
  1. Haga clic en **Inicio**.
  2. Localice **Equipo** en el menú **Inicio**.
  3. Haga clic derecho en **Equipo** y seleccione **Propiedades**.
  4. Mire en **Sistema** para comprobar la información de su sistema.
- En **Windows 7**:
  1. Desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono.

     En **Windows 8.1**, acceda a **Este equipo**.
  2. Seleccione **Propiedades** en el menú inferior.
  3. Consulte el área del sistema para ver su tipo de sistema.
- En **Windows 10**:

1. Escriba "Sistema" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
2. Consulte el área del sistema para obtener información sobre el tipo de sistema.

3.6.7. ¿Cómo puedo mostrar los objetos ocultos en Windows?

Estos pasos son útiles cuando se enfrenta a una amenaza y necesita encontrar y eliminar los archivos infectados, que podrían estar ocultos.

Siga estos pasos para ver los elementos ocultos de Windows:

1. Haga clic en **Inicio**, y vaya al **Panel de control**.

   En **Windows 8 y Windows 8.1**: Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Seleccione **Opciones de carpeta**.
3. Vaya a la pestaña **Ver**.
4. Seleccione **Mostrar archivo y carpetas ocultos**.
5. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
6. Desmarque **Ocultar archivos protegidos del sistema operativo**.
7. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

En **Windows 10**:

1. Escriba "Mostrar todos los archivos y carpetas ocultos" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
2. Seleccione **Mostrar archivos, carpetas y unidades ocultos**.
3. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
4. Desmarque **Ocultar archivos protegidos del sistema operativo**.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

3.6.8. ¿Cómo desinstalo otras soluciones de seguridad?

La principal razón para utilizar una solución de seguridad es para proporcionar protección y seguridad para sus datos. ¿Pero que pasa cuando tengo más de un producto de seguridad en el mismo sistema?

Cuando utiliza más de una solución de seguridad en el mismo equipo, el sistema se vuelve inestable. El instalador de Bitdefender Total Security automáticamente detecta otros programas de seguridad y le ofrece la opción de desinstalarlos.

Si no desea eliminar las otras soluciones de seguridad durante la instalación inicial:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Espere un momento a que el software instalado se muestre.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Espere un momento a que el software instalado se muestre.
  4. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.

5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

Si falla la eliminación de otra solución de seguridad de su sistema, obtenga la herramienta de desinstalación de la página del proveedor o contacte con el directamente con el fin que le proporcionen las lineas de desinstalación.

3.6.9. ¿Cómo puedo reiniciar en Modo Seguro?

El Modo Seguro es un modo de diagnóstico operativo, utilizado principalmente para resolver problemas que afectan a la operación normal de Windows. Dichos problemas van desde controladores en conflicto hasta amenazas que impiden que Windows se inicie normalmente. En Modo Seguro solo una cuantas aplicaciones trabajan y Windows carga solo los controladores básicos y un mínimo de componentes del sistema operativo. Por esta razón la mayoría de las amenazas están inactivas cuando se usa Windows en modo seguro y se pueden eliminar fácilmente.

Para iniciar Windows en Modo Seguro:

- En **Windows 7**:
  1. Reinicie el equipo.
  2. Presione la tecla **F8** varias veces antes de iniciar Windows para tener acceso al menú de inicio.
  3. Seleccione **Modo seguro** en el menú de arranque o **Modo seguro con red** si quiere disponer de acceso a internet.
  4. Presione la tecla **Intro** y espere mientras Windows se carga en Modo seguro.
  5. Este proceso finaliza con un mensaje de confirmación. Haga clic en **OK** para reconocer.
  6. Para iniciar Windows normal, simplemente reinicie el sistema.
- En **Windows 8, Windows 8.1 y Windows 10**:
  1. Acceda a la **Configuración del sistema** en Windows pulsando al mismo tiempo las teclas **Windows + R**.
  2. Escriba **msconfig** en el campo **Abrir** del cuadro de diálogo y, a continuación, haga clic en **Aceptar**.
  3. Seleccione la pestaña **Arranque**.

4. En la sección de **Opciones de arranque**, marque la casilla de verificación **Arranque a prueba de errores**.
5. Haga clic en **Red** y, a continuación, en **Aceptar**.
6. Haga clic en **Aceptar** en la ventana de **Configuración del sistema** que le informa de que el sistema debe reiniciarse para realizar los cambios que acaba de establecer.

   Su sistema se reiniciará en modo seguro con funciones de red.

Para reiniciarlo en modo normal, vuelva a cambiar los ajustes ejecutando nuevamente la **operación del sistema** y dejando sin marcar la casilla de verificación **Arranque a prueba de errores**. Haga clic en **Aceptar** y, a continuación, seleccione **Reiniciar**. Espere a que se apliquen los nuevos ajustes.

4. GESTIÓN DE SU SEGURIDAD

4.1. Protección Antivirus

Bitdefender protege su equipo contra todo tipo de amenazas (malware, troyanos, spyware, rootkits, etc.). La protección que ofrece Bitdefender está dividida en dos apartados:

- Análisis on-access - impide que las nuevas amenazas entren en su sistema. Por ejemplo, Bitdefender analizará un documento de Word cuando lo abra, o los mensajes de correo a medida que los vaya recibiendo.

  El análisis on-access garantiza la protección en tiempo real contra amenazas, siendo un componente esencial de cualquier programa de seguridad informática.

  > **Importante**
  > Para evitar que las amenazas infecten su equipo, mantenga activado **Análisis on-access**.

- Análisis bajo demanda - permite detectar y eliminar la amenaza que ya reside en el sistema. Se trata del clásico análisis antivirus iniciado por el usuario - usted selecciona la unidad, carpeta o archivo que Bitdefender debe analizar, y Bitdefender lo analizará cuando se lo indique.

Bitdefender analiza automáticamente cualquier dispositivo extraíble que se conecte a su equipo para así asegurarse de que se puede acceder al mismo de forma segura. Para más información, diríjase a "*Análisis automático de los medios extraíbles*" (p. 77).

Los usuarios avanzados pueden configurar excepciones de análisis si no desean que se analicen ciertos archivos o tipos de archivo. Para más información, diríjase a "*Configurar excepciones de análisis*" (p. 79).

Cuando detecte una amenaza, Bitdefender intentará eliminar automáticamente el código malicioso del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección. Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Para más información, diríjase a "*Administración de los archivos en cuarentena*" (p. 82).

Si su equipo se ha visto infectado con amenazas, consulte "*Eliminación de amenazas de su sistema*" (p. 176). Para ayudarle a limpiar su equipo de amenazas que no pueden eliminarse desde el propio sistema operativo Windows, Bitdefender le ofrece"*Bitdefender Modo de Rescate (Entorno de rescate en Windows 10)*" (p. 177). Este es un entorno de confianza, especialmente diseñado para la eliminación de amenazas, lo que le permite arrancar el equipo independientemente de Windows. Cuando el equipo se ejecuta en modo Rescate (Entorno de rescate en Windows 10), las amenazas de Windows están inactivas, por lo que es fácil eliminarlas.

4.1.1. Análisis on-access (protección en tiempo real)

Bitdefender proporciona protección en tiempo real contra un amplio abanico de amenazas, analizando todos los archivos a los que se accede y los mensajes de correo electrónico.

Activar o desactivar la protección en tiempo real

Para activar o desactivar la protección en tiempo real contra amenazas:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, active o desactive **Escudo de Bitdefender**.
4. Si desea desactivar la protección en tiempo real, aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema. La protección en tiempo real se activará automáticamente cuando finalice el tiempo seleccionado.

Aviso

Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Si desactiva la protección en tiempo real, no estará protegido contra las amenazas.

Configuración de los ajustes avanzados de la protección en tiempo real

Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender. Puede configurar los ajustes de la protección en tiempo real en detalle creando un nivel de protección personalizado.

Para configurar los ajustes avanzados de la protección en tiempo real:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, haga clic en el menú de acordeón **Mostrar ajustes avanzados**.

   Se muestra una ventana con paneles.
4. Desplácese hacia abajo por la ventana para configurar los ajustes de análisis según sea preciso.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- **Analizar únicamente aplicaciones.** Puede configurar Bitdefender para analizar solo las apps a las que accede.
- **Analizar en busca de aplicaciones potencialmente no deseadas.** Seleccione esta opción para analizar en busca de aplicaciones no deseadas. Una aplicación potencialmente no deseada (APND) o programa potencialmente no deseado (PPND) es un software que viene incluido generalmente con el freeware y mostrará ventanas emergentes o una barra de herramientas en el navegador por defecto. Algunos cambiarán la página de inicio o el motor de búsqueda, mientras que otros ejecutarán varios procesos en segundo plano, ralentizando el PC, o mostrarán numerosos anuncios. Estos programas pueden instalarse sin su consentimiento (también llamados adware) o incluirse por defecto en el kit de instalación (que tiene publicidad).
- **Analizar recursos compartidos.** Para acceder de forma segura a una red remota desde su equipo, le recomendamos que mantenga habilitada la opción Analizar recursos compartidos.

- **Analizar el interior de los comprimidos.** Analizar dentro de archivos es una proceso lento, requiere muchos recursos, por esta razón no lo recomendamos para la protección en tiempo real. Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema. Las amenazas pueden afectar a su sistema solo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada.

  Si decide utilizar esta opción, actívela y, a continuación, arrastre el control deslizante por la escala para establecer un límite de tamaño máximo aceptado (en MB) de los archivos que se van a analizar on-access.

- **Analizar emails.** Para evitar que se descarguen amenazas en su equipo, Bitdefender analiza automáticamente los mensajes de correo electrónico entrantes y salientes.

  Aunque no es recomendable, puede desactivar el análisis de amenazas del correo electrónico para mejorar el rendimiento de su sistema. Si desactiva las opciones de análisis correspondientes, no se analizarán los mensajes de correo electrónico y sus posibles adjuntos, lo que permitirá que los archivos infectados se guarden en su equipo. Esta no es una amenaza importante porque la protección en tiempo real bloqueará la amenaza cuando se acceda a los archivos infectados (se abran, muevan, copien o ejecuten).

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar sus sistema y acceder a sus datos.

- **Analizar solo los archivos nuevos o modificados.** Al analizar únicamente los archivos nuevos o modificados, puede mejorar en gran medida la capacidad de respuesta general del sistema comprometiendo mínimamente la seguridad.

- **Analizar en busca de keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger. Los Keyloggers registran lo que escribe en el teclado y envían informes por internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.

- **Analizar al arrancar el sistema.** Seleccione la opción de **Análisis de arranque** para analizar su sistema al iniciarse, tan pronto como se hayan cargado todos los servicios críticos. La finalidad de esta característica es mejorar la detección de amenazas en el inicio del sistema, así como el tiempo de arranque del mismo.

Medidas adoptadas sobre las amenazas detectadas

Puede configurar las acciones llevadas a cabo por la protección en tiempo real siguiendo los pasos que se indican a continuación:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, haga clic en el menú de acordeón **Mostrar ajustes avanzados**.

   Se muestra una ventana con paneles.
4. Desplácese hacia abajo por la ventana hasta que aparezca la opción **Acciones de amenazas**.
5. Configure los ajustes del análisis como necesite.

La protección en tiempo real de Bitdefender puede llevar a cabo las siguientes acciones:

Adoptar medidas

Bitdefender tomará las medidas recomendadas dependiendo del tipo de archivo detectado:

- **Archivos infectados.** Los archivos detectados como infectados coinciden con una información sobre amenazas encontrada en la base de datos de información de amenazas de Bitdefender. Bitdefender intentará automáticamente eliminar el código malicioso del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

  Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, diríjase a "*Administración de los archivos en cuarentena*" (p. 82).

Importante
En ciertos tipos de amenazas, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible. Estos serán trasladados a la cuarentena para evitar una infección potencial.

  Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de amenazas de Bitdefender. Si se confirma la presencia de amenazas, se publica una actualización de información de amenazas para permitirle eliminarla.

- **Archivos empaquetados que contienen archivos infectados.**
  - Los archivos empaquetados que contengan únicamente archivos infectados son eliminados automáticamente.
  - Si un archivo empaquetado contiene tanto archivos infectados como limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el paquete con los archivos limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Mover a Cuarentena
Traslada los archivos detectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, diríjase a "*Administración de los archivos en cuarentena*" (p. 82).

Bloquear acceso
Si se detecta un archivo infectado, se bloqueará el acceso al mismo.

Restaurar la configuración predeterminada

Los ajustes por defecto de protección en tiempo real garantizan una buena defensa contra las amenazas con escaso impacto en el rendimiento del sistema.

Para restaurar la configuración predeterminada de la protección en tiempo real:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, haga clic en el menú de acordeón **Mostrar ajustes avanzados**.

   Se muestra una ventana con paneles.
4. Desplácese hacia abajo por la ventana hasta que aparezca la opción **Reiniciar ajustes**. Seleccione esta opción para reiniciar los ajustes del antivirus y que adopten los valores por defecto.

4.1.2. Análisis solicitado

El objetivo principal de Bitdefender es mantener su equipo limpio de amenazas. Esto se consigue manteniendo las nuevas amenazas fuera de su equipo y analizando los mensajes de correo y cualquier archivo nuevo descargado o copiado a su sistema.

Existe el riesgo de que ya exista una amenaza en su sistema, antes siquiera de instalar Bitdefender. Por eso es buena idea analizar su equipo en busca de amenazas preexistentes nada más instalar Bitdefender. Y, desde luego, es buena idea analizar frecuentemente su equipo en busca de amenazas.

El análisis bajo demanda está basado en tareas de análisis. Las tareas de análisis especifican las opciones de análisis y los objetos a analizar. Puede analizar el equipo siempre que quiera ejecutando las tareas predeterminadas o sus propias tareas de análisis (tareas definidas por el usuario). Si desea analizar ubicaciones específicas en el equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

Analizar un archivo o una carpeta en busca de amenazas

Debe analizar archivos y carpetas que sospeche que puedan estar infectados. Haga clic con el botón derecho en el archivo o carpeta que desee analizar, escoja **Bitdefender** y seleccione **Analizar con Bitdefender**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.

Ejecución de un análisis Quick Scan

QuickScan utiliza el análisis en la nube para detectar amenazas que se estén ejecutando en su sistema. La ejecución de QuickScan tarda por lo general menos de un minuto y utiliza una fracción de los recursos del sistema necesarios para un análisis antivirus normal.

Para ejecutar un análisis Quick Scan:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **QuickScan**.
3. Siga el Asistente de análisis antivirus para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Ejecución de un análisis del sistema

La tarea de análisis del sistema analiza todo el equipo en busca de todo tipo de amenazas que pongan en peligro su seguridad, como malware, spyware, adware, rootkits y otros.

> **Nota**
> Ya que el **Análisis del sistema** realiza un análisis exhaustivo de todo el sistema, el análisis puede tomar cierto tiempo. Por lo tanto, se recomienda ejecutar esta tarea cuando no está utilizando su equipo.

Antes de realizar un análisis del sistema, se recomienda lo siguiente:

- Asegúrese de que Bitdefender está actualizado con su base de datos de información de amenazas. Analizar su equipo con una base de datos de información de amenazas obsoleta puede impedir que Bitdefender detecte nuevas amenazas encontradas desde la última actualización. Para más información, diríjase a "*Mantenimiento de Bitdefender al día*" (p. 33).
- Cierre todos los programas abiertos.

Si desea analizar ubicaciones específicas en su equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado. Para más información, diríjase a "*Configuración de un análisis personalizado*" (p. 70).

Para ejecutar un Análisis del sistema:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
3. La primera vez que ejecuta un Análisis del sistema, se le presenta esta característica. Haga clic en **BIEN, ENTENDIDO** para continuar.
4. Siga el Asistente de análisis antivirus para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Configuración de un análisis personalizado

Para configurar detalladamente un análisis personalizado y luego ejecutarlo:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. Haga clic en **NUEVO ANÁLISIS PERSONALIZADO**. Haga clic en la ventana **Básico** para introducir un nombre para el análisis y seleccione las ubicaciones que desea analizar.
4. Si desea configurar detalladamente las opciones de análisis, seleccione la pestaña **Avanzado**. Aparecerá una nueva ventana. Siga estos pasos:
   a. Puede fácilmente configurar las opciones de análisis ajustando el nivel de análisis. Arrastre la barra de desplazamiento por la escala para asignar el nivel de análisis deseado. Utilice la descripción en la parte derecha de la escala para identificar el nivel de análisis que mejor se ajuste a sus necesidades.

      Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender. Para configurar las opciones de análisis en detalle, haga clic en **Personalizado**. Puede encontrar información sobre ellas al final de esta sección.

   b. Puede además configurar estas opciones generales:

      - **Ejecutar la tarea con baja prioridad .** Disminuye la prioridad de los procesos de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.

- **Minimizar Asistente de Análisis a la barra de tareas .** Minimiza la ventana de análisis al área de notificación. Haga doble clic en el icono de Bitdefender para abrirlo.
- Especifica la acción a realizar si no se encuentran amenazas.

c. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

5. Si desea establecer una programación para su tarea de análisis, utilice el conmutador **Planificar** en la ventana **Básico**. Seleccione una de las opciones correspondientes para establecer una programación:
   - Al iniciar el sistema
   - Una sola vez
   - Periódicamente
6. Haga clic en **INICIAR ANÁLISIS** y siga el Asistente de análisis antivirus para llevarlo a cabo. Dependiendo de las ubicaciones a analizar, el análisis puede llevar más tiempo. Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.
7. Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- Si no se familiariza con algunos términos, compruebe estos en el glosario. También puede encontrar información de utilidad buscando en internet.
- **Analizar ficheros.** Puede configurar Bitdefender para analizar todos los tipos de archivos o aplicaciones (archivos de programa) únicamente. Analizando todos los archivos se proporciona una mejor protección, mientras que analizar solo aplicaciones puede ser utilizado solamente para realizar un análisis más rápido.

  Las aplicaciones (o archivos de programa) son mucho más vulnerables a los ataques de amenazas que otro tipo de archivos. Esta categoría incluye las siguientes extensiones de archivo: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde;

mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

- **Opciones de análisis para archivos.** Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema. Las amenazas pueden afectar a su sistema solo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es una amenaza inmediata.

  > **Nota**
  > El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema.

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar sus sistema y acceder a sus datos.
- **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
- **Analizar registro.** Seleccione esta opción para analizar las claves de registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.
- **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su equipo.
- **Analizar archivos nuevos y modificados.** Al analizar únicamente los archivos nuevos o modificados, puede mejorar en gran medida la capacidad

de respuesta general del sistema comprometiendo mínimamente la seguridad.

- **Ignorar keyloggers comerciales.** Seleccione esta opción si ha instalado y utilizado un software comercial keylogger en su equipo. Los keyloggers comerciales son programas legítimos de monitorización de equipos cuya función básica es grabar todo lo que se escribe en el teclado.
- **Analizar en busca de Rootkits.** Seleccione esta opción para analizar en busca de rootkits y objetos ocultos que utilicen este tipo de software.
- **Analizar en busca de aplicaciones potencialmente no deseadas.** Seleccione esta opción para analizar en busca de aplicaciones no deseadas. Una aplicación potencialmente no deseada (APND) o programa potencialmente no deseado (PPND) es un software que viene incluido generalmente con el freeware y mostrará ventanas emergentes o una barra de herramientas en el navegador por defecto. Algunos cambiarán la página de inicio o el motor de búsqueda, mientras que otros ejecutarán varios procesos en segundo plano, ralentizando el PC, o mostrarán numerosos anuncios. Estos programas pueden instalarse sin su consentimiento (también llamados adware) o incluirse por defecto en el kit de instalación (que tiene publicidad).

Asistente del análisis Antivirus

Cuando inicie un análisis bajo demanda (por ejemplo, haga clic con el botón derecho en una carpeta, escoja Bitdefender y seleccione **Analizar con Bitdefender**) aparecerá el asistente de Bitdefender Antivirus Scan. Siga el asistente para completar el proceso de análisis.

Nota

Si el asistente de análisis no aparece, puede que el análisis esté configurado para ejecutarse en modo silencioso, en segundo plano. Busque el icono de progreso del análisis en la barra de tareas. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Paso 1 - Ejecutar análisis

Bitdefender analizará los objetos seleccionados. Puede ver la información en tiempo real sobre el estado del análisis y las estadísticas (incluyendo el tiempo transcurrido, una estimación del tiempo restante y el número de amenazas detectadas).

Espere a que Bitdefender finalice el análisis. El análisis puede llevar un tiempo, dependiendo de la complejidad del análisis.

Detener o pausar el análisis. Puede detener el análisis en cualquier momento que desee haciendo clic en **DETENER**. Irá directamente al último paso del asistente. Para detener temporalmente el proceso de análisis, haga clic en **PAUSA**. Tendrá que hacer clic en **REANUDAR** para retomar el análisis.

Archivos protegidos por contraseña. Cuando se detecta un archivo protegido por contraseña, dependiendo de las opciones de análisis, puede ser preguntado para que proporcione la contraseña. Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña. Tiene las siguientes opciones a su disposición:

- **Contraseña.** Si desea que Bitdefender analice el archivo, seleccione esta opción e introduzca la contraseña. Si no conoce la contraseña, elija una de las otras opciones.
- **No preguntar por una contraseña y omitir este objeto del análisis.** Marque esta opción para omitir el análisis de este archivo.
- **Omitir todos los elementos protegidos con contraseña sin analizarlos.** Seleccione esta opción si no desea que se le pregunte acerca de archivos protegidos por contraseña. Bitdefender no podrá analizarlos, pero se guardará información acerca de ellos en el informe de análisis.

Elija la acción deseada y haga clic en **Aceptar** para continuar el análisis.

Paso 2 - Elegir acciones

Al final del análisis, se le pedirá que elija las acciones a aplicar sobre los archivos detectados, si existe alguno.

Nota

Cuando ejecute un Quick Scan o un análisis del sistema, Bitdefender llevará automáticamente a cabo las acciones recomendadas sobre los archivos detectados durante el análisis. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Los objetos infectados se muestran en grupos, según las amenazas con las que estén infectados. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

Puede elegir una opción global que se aplicará a todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias. Una o varias de las siguientes opciones pueden aparecer en el menú:

Adoptar medidas

Bitdefender tomará las medidas recomendadas dependiendo del tipo de archivo detectado:

- **Archivos infectados.** Los archivos detectados como infectados coinciden con una información sobre amenazas encontrada en la base de datos de información de amenazas de Bitdefender. Bitdefender intentará automáticamente eliminar el código malicioso del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

  Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, diríjase a "*Administración de los archivos en cuarentena*" (p. 82).

  Importante

  En ciertos tipos de amenazas, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** Los archivos detectados como sospechosos por el análisis heurístico. Los archivos sospechosos no pueden ser desinfectados, porque no hay una rutina de desinfección disponible. Estos serán trasladados a la cuarentena para evitar una infección potencial.

  Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de amenazas de Bitdefender. Si se confirma la presencia de una amenaza, se publica una actualización de información para permitirle eliminarla.

- **Archivos empaquetados que contienen archivos infectados.**
  - Los archivos empaquetados que contengan únicamente archivos infectados son eliminados automáticamente.

- Si un archivo empaquetado contiene tanto archivos infectados como limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el paquete con los archivos limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Eliminar

Elimina los archivos detectados del disco.

Si se almacenan archivos infectados junto con archivos limpios en un mismo paquete, Bitdefender intentará limpiar los archivos infectados y reconstruir el paquete con los limpios. Si es imposible la reconstrucción del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

Ninguna acción

No se realizará ninguna acción sobre los archivos detectados. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.

Haga clic en **Continuar** para aplicar las acciones indicadas.

Paso 3 – Resumen

Una vez Bitdefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana. Si desea información completa sobre el proceso de análisis, haga clic en **MOSTRAR REGISTRO** para ver el registro de análisis. El registro se proporciona en formato .xml y se puede guardar localmente haciendo clic en el botón **Guardar registro** y, a continuación, eligiendo una ubicación.

Importante

En la mayoría de casos, Bitdefender desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, hay incidencias que no pueden resolverse automáticamente. En caso necesario, reinicie su equipo para completar el proceso de desinfección. Para obtener más información e instrucciones sobre cómo eliminar manualmente una amenaza, consulte "*Eliminación de amenazas de su sistema*" (p. 176).

Comprobación de los resultados del análisis

Cada vez que se realiza un análisis, se crea un registro del mismo y Bitdefender graba los problemas detectados en la ventana del antivirus. El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde el asistente de análisis, una vez finalizado este, haciendo clic en **MOSTRAR REGISTRO**.

Para revisar más tarde un informe de análisis o cualquier infección detectada:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

   Aquí es donde puede encontrar todos los eventos de análisis de amenazas, incluyendo las detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.
3. En la lista de notificaciones puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificacione para ver más detalles sobre él.
4. Para abrir el registro de análisis, haga clic en **Ver registro**.

4.1.3. Análisis automático de los medios extraíbles

Bitdefender detecta automáticamente si conecta un dispositivo de almacenamiento extraíble a su equipo, y lo analiza en segundo plano cuando está activada la opción de Autoanálisis. Esto se recomienda con el fin de evitar que su equipo se infecte con amenazas.

La detección de dispositivos se dividen en una de estas categorías:

- Cds/DVDs
- Unidades flash, como lápices flash y discos duros externos
- Unidades de red (remotas) mapeadas.

Puede configurar el análisis automático de manera independiente para cada categoría de dispositivos de almacenamiento. Por defecto, el análisis automático de las unidades de red mapeadas está desactivado.

¿Cómo funciona?

Cuando se detecta un dispositivo de almacenamiento extraíble, Bitdefender inicia el análisis en busca de amenazas (siempre y cuando se haya habilitado el análisis automático para este tipo). Mediante una ventana emergente se le notificará que se ha detectado un nuevo dispositivo y se está analizando.

Aparece un icono de análisis de Bitdefender en el área de notificación. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Cuando el análisis se ha completado, la ventana de los resultados del análisis se mostrará para informarle si es seguro acceder a los archivos en el medio extraíble.

En la mayoría de los casos, Bitdefender elimina automáticamente las amenazas detectadas o mantiene aislados en cuarentena los archivos infectados. Si quedan amenazas sin resolver tras el análisis, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Nota
Tenga en cuenta que no se pueden tomar medidas en archivos infectados o sospechosos detectado en CDs/DVDs. Del mismo modo, no se puede tomar ninguna acción en los archivos detectados como infectados o sospechosos en unidades de red si no tiene los privilegios apropiados.

Esta información le puede ser útil:

- Tenga cuidado al usar un CD/DVD infectado con una amenaza, porque esta no puede eliminarse del disco (el soporte es de solo lectura). Asegúrese de que la protección en tiempo real está activada para evitar que las amenazas se propaguen por su sistema. Es una buena práctica copiar los datos importantes desde el disco a su sistema y luego deshacerse de los discos.
- En algunos casos, Bitdefender puede no ser capaz de eliminar amenazas de determinados archivos debido a restricciones legales o técnicas. Un ejemplo son los archivos comprimidos con una tecnología propia (esto es porque el archivo no se puede recrear correctamente).

  Para averiguar cómo enfrentarse a las amenazas, consulte "*Eliminación de amenazas de su sistema*" (p. 176).

Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de medios extraíbles:

Para una mejor protección, se recomienda dejar seleccionada la opción de **Autoanálisis** para todos los tipos de dispositivos de almacenamiento extraíbles.

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Discos y dispositivos**.

Las opciones de análisis están preconfiguradas para mejores resultados de detección. Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso). Si ambas medidas fallan, el asistente de Análisis del Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados. Las opciones de análisis son estándar y no las puede modificar.

4.1.4. Analizar archivo del host

El archivo hosts viene por defecto con la instalación de su sistema operativo y se utiliza para asignar direcciones IP a nombres de hosts cada vez que accede a una nueva página web, se conecta a un FTP o a otros servidores de Internet. Es un archivo de texto sin formato y los programas maliciosos pueden modificarlo. Los usuarios avanzados saben cómo usarlo para bloquear molestos anuncios, banners, cookies de terceros o programas de secuestro.

Para configurar el análisis del archivo hosts:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Active o desactive el **análisis del archivo hosts**.

4.1.5. Configurar excepciones de análisis

Bitdefender permite exceptuar del análisis determinados archivos, carpetas o extensiones de archivo. Esta característica está diseñada para evitar interferencias con su trabajo y también para ayudarle a mejorar el rendimiento

de su sistema. Las excepciones las deben utilizar usuarios con conocimientos avanzados de informática o bien hacerlo siguiendo las recomendaciones de un representante de Bitdefender.

Puede configurar excepciones para aplicar solamente al análisis en tiempo real o bajo demanda, o a ambos. No se analizarán los objetos exceptuados del análisis on-access, ya sean accedidos por usted o por una app.

Nota

NO se aplicarán las excepciones al análisis contextual y del sistema. El análisis del sistema y bajo demanda le da la posibilidad de analizar todo el sistema en busca de amenazas que puedan poner en peligro la seguridad de sus datos. El análisis contextual es un tipo de análisis bajo demanda: haga clic derecha sobre un fichero o carpeta que desee analizar y seleccione **Analizar con Bitdefender**.

Exceptuar del análisis los archivos o carpetas

Para exceptuar determinados archivos y carpetas del análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Excepciones**.
4. Haga clic en el menú de acordeón **Lista de archivos y carpetas exceptuados del análisis**. En la ventana que aparece puede administrar los archivos y carpetas exceptuados del análisis.
5. Añada excepciones siguiendo estos pasos:
   a. Haga clic en **Añadir**.
   b. Haga clic en **EXAMINAR**, seleccione el archivo o carpeta que desea exceptuar del análisis y, a continuación, haga clic en **AÑADIR**. Como alternativa, puede escribir (o copiar y pegar) en el campo de edición la ruta del archivo o carpeta.
   c. Por defecto, el archivo o carpeta seleccionado se exceptúa tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la excepción, seleccione una de las otras opciones.
   d. Haga clic en **Añadir**.

Exceptuar del análisis las extensiones de archivo

Al exceptuar una extensión de archivo del análisis, Bitdefender ya no analizará archivos con esa extensión, independientemente de la ubicación en su equipo. La excepción también se aplica a los archivos en medios extraíbles, como CD, DVD, dispositivos de almacenamiento USB o unidades de red.

> **Importante**
> Tenga cuidado al exceptuar las extensiones del análisis ya que tales excepciones pueden hacer que su equipo sea vulnerable a las amenazas.

Para exceptuar extensiones de archivo del análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Excepciones**.
4. Haga clic en el menú de acordeón **Lista de extensiones exceptuadas del análisis**. En la ventana que aparece puede administrar las extensiones de archivo exceptuadas del análisis.
5. Añada excepciones siguiendo estos pasos:
   a. Haga clic en **Añadir**.
   b. Escriba las extensiones que desea exceptuar del análisis, separándolas con punto y coma (;). Aquí tiene un ejemplo:

      txt;avi;jpg

   c. Por defecto, todos los archivos con las extensiones mencionadas son exceptuados tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la excepción, seleccione una de las otras opciones.
   d. Haga clic en **AÑADIR**.

Administrar excepciones de análisis

Si las excepciones de análisis configuradas dejan de ser necesarias, se recomienda que las elimine o desactive las excepciones de análisis.

Para administrar las excepciones del análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Excepciones**.
4. Utilice las opciones del menú de acordeón **Lista de archivos y carpetas exceptuados del análisis** para administrar las excepciones del análisis.
5. Para eliminar o editar excepciones del análisis, haga clic en uno de los enlaces disponibles. Siga estos pasos:
   - Para eliminar una entrada de la lista, selecciónela y haga clic en **Eliminar**.
   - Para editar un elemento de la tabla, haga doble clic en él (o selecciónelo y haga clic en **Editar**). Aparece una nueva ventana donde podrá cambiar la extensión o la ruta que desee exceptuar, así como el tipo de análisis del que desea exceptuarla. Realice los cambios necesarios y haga clic en **MODIFICAR**.

4.1.6. Administración de los archivos en cuarentena

Bitdefender aísla los archivos infectados con amenazas que no puede desinfectar y los archivos sospechosos en un área segura denominada cuarentena. Cuando una amenaza está aislada en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de amenazas de Bitdefender. Si se confirma la presencia de una amenaza, se publica una actualización de información para permitirle eliminarla.

Además, Bitdefender analiza los archivos en cuarentena cada vez que se actualiza la base de datos de información de amenazas. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Para comprobar y administrar los archivos en cuarentena:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Cuarentena**.

   Aquí puede ver el nombre de los archivos en cuarentena, su ubicación original y el nombre de las amenazas detectadas.

3. Bitdefender gestiona automáticamente los archivos en cuarentena, según la configuración de cuarentena predeterminada.

   Aunque no es recomendable, puede ajustar la configuración de la cuarentena según sus preferencias haciendo clic en **Ver ajustes**.

   Haga clic en los conmutadores para activar o desactivar:

   Volver a analizar la cuarentena tras actualizar la información de amenazas
   Mantenga activada esta opción para analizar automáticamente los archivos en cuarentena después de cada actualización de la base de datos de información de amenazas. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

   Eliminar contenido con una antigüedad superior a 30 días
   Los archivos con antigüedad superior a 30 días se eliminan automáticamente.

   Crear excepciones para los archivos restaurados
   Los archivos que restaura desde la cuarentena vuelven a su ubicación original sin ser reparados y se exceptúan automáticamente de futuros análisis.

4. Para eliminar un archivo en cuarentena, selecciónelo y haga clic en el botón **ELIMINAR**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **RESTAURAR**.

4.2. Advanced Threat Defense

Defensa Contra Amenazas Avanzadas de Bitdefender es una tecnología de detección proactiva innovadora que utiliza avanzados métodos heurísticos para detectar ransomware y otras nuevas amenazas potenciales en tiempo real.

Advanced Threat Defense monitoriza continuamente las aplicaciones que se están ejecutando en su equipo, buscando acciones propias de amenazas. Cada una de estas acciones se puntúa y se calcula una puntuación global para cada proceso.

Como medida de seguridad, se le notificará cada vez que se detecten y bloqueen procesos potencialmente maliciosos.

Activar o desactivar Defensa Contra Amenazas Avanzadas

Para activar o desactivar Defensa Contra Amenazas Avanzadas:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ADVANCED THREAT DEFENSE**, active o desactive el conmutador.

> **Nota**
> Para mantener su sistema a salvo de ransomware y de otras amenazas, le recomendamos que desactive Advanced Threat Defense durante el menor tiempo posible.

Comprobación de los ataques maliciosos detectados

Siempre que se detecten amenazas o procesos potencialmente maliciosos, Bitdefender los bloqueará para evitar que su equipo resulte infectado por ransomware u otro malware. Puede consultar en cualquier momento la lista de ataques maliciosos detectados siguiendo los pasos que se exponen a continuación:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **DEFENSA CONTRA AMENAZAS AVANZADAS**, haga clic en **Defensa contra amenazas**.
3. La primera vez que accede a la Protección contra ransomware, se le presenta esta característica. Haga clic en **BIEN, ENTENDIDO** para continuar.

   Se muestran los ataques detectados durante los últimos noventa días. Para obtener detalles acerca del tipo de ransomware detectado, la ruta del proceso malicioso, o si la desinfección tuvo éxito, simplemente haga clic en el elemento.

Añadir procesos a las excepciones

Puede configurar reglas de excepción para las apps de confianza, de modo que Advanced Threat Defense no las bloquee si realizan acciones típicas de amenazas.

Para empezar a añadir procesos a la lista de excepciones de Advanced Threat Defense:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.

2. En el panel **ADVANCED THREAT DEFENSE**, haga clic en **Ajustes**.
3. En la ventana **Excepciones**, haga clic en **Añadir aplicaciones a la lista blanca**.
4. Busque y seleccione la app que desea exceptuar y, a continuación, haga clic en **ACEPTAR**.

   Para eliminar un elemento de la lista, haga clic en la opción **Eliminar** junto a él.

4.3. Prevención de amenazas online

La Prevención de amenazas online de Bitdefender le garantiza una navegación segura por Internet alertándole sobre posibles páginas web maliciosas.

Bitdefender proporciona prevención de amenazas online en tiempo real para:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Para configurar los ajustes de la Prevención de amenazas online:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Ajustes**.

En la ventana **Protección web**, haga clic en los conmutadores para activar o desactivar:

- La prevención de ataques web bloquea las amenazas procedentes de Internet, incluyendo las descargas ocultas.
- Asesor de búsqueda, un componente que califica los resultados de las consultas en su motor de búsqueda y los enlaces publicados en sitios Web de redes sociales añadiendo un icono junto a cada resultado:

  No debería visitar esta página web.

Esta página web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.

Esta página es segura.

El Asesor de búsqueda califica los resultados de los siguientes motores de búsqueda:

- Google
- Yahoo!
- Bing
- Baidu

El Asesor de búsqueda califica los enlaces publicados en los siguientes servicios de redes sociales:

- Facebook
- Twitter

- Análisis de sitios web cifrados.

  Los ataques más sofisticados pueden utilizar el tráfico de Internet seguro para engañar a sus víctimas. Por lo tanto, le recomendamos que mantenga habilitada la opción de Análisis de sitios web cifrados.

- Protección contra el fraude.
- Protección contra phishing.

En la ventana **Prevención de amenazas de red**, tiene la opción de **Prevención de amenazas de red**. Para mantener su equipo a salvo de los ataques de malware complejo (como el ransomware) a través del aprovechamiento de vulnerabilidades, mantenga esta opción habilitada.

Puede crear una lista de los sitios web que no serán analizados por los motores antiphishing, antifraude y contra amenazas de Bitdefender. La lista debería contener únicamente sitios Web en los que confíe plenamente. Por ejemplo, añada las páginas web en las que realice compras online.

Para configurar y administrar sitios web utilizando la característica de Prevención de amenazas online ofrecida por Bitdefender:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Excepciones**.

3. Escriba el nombre del sitio web que desea añadir a la lista blanca en el campo correspondiente y luego haga clic en **AÑADIR**.

   Para eliminar un sitio web de la lista, selecciónelo y, a continuación, haga clic en el enlace **Eliminar** correspondiente.

   Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Alertas de Bitdefender en el navegador

Cada vez que intenta visitar un sitio Web clasificado como peligroso, éste queda bloqueado y aparecerá una página de advertencia en su navegador.

La página contiene información tal como la URL del sitio Web y la amenaza detectada.

Tiene que decidir que hacer a continuación. Tiene las siguientes opciones a su disposición:

- Abandone la página haciendo clic en **LLÉVAME A UN SITIO SEGURO**.
- Diríjase a la página web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos**.
- Si sabe a ciencia cierta que la página web detectada es segura, haga clic en **ENVIAR** para añadirla a la lista blanca. Le recomendamos que solo añada páginas web en las que confíe plenamente.

4.4. Antispam

Spam es un termino utilizado para describir correo no solicitado. El correo no solicitado se ha convertido en un problema cada vez más agobiante, tanto para los usuarios individuales como para las empresas. No es agradable, no le gustaría que sus hijos lo viesen, puede dejarlo sin trabajo (al perder mucho tiempo con el spam o al recibir contenido pornográfico en su cuenta de correo de la empresa) y no puede hacer nada para detenerlo. Lo mejor del correo no solicitado es, obviamente, dejar de recibirlo. Desgraciadamente, el correo no solicitado llega en una gran variedad de formas y tamaños y siempre en una cantidad increíble.

Bitdefender Antispam emplea sorprendentes innovaciones tecnológicas y filtros antispam estándares en la industria para impedir que el spam llegue a su bandeja de entrada. Para más información, diríjase a "*Conocimientos antispam*" (p. 88).

La protección Antispam de Bitdefender está disponible solo para clientes de correo configurados para recibir mensajes de correo mediante el protocolo POP3. POP3 es uno de los protocolos más extensos utilizados para descargar mensajes de correo de un servidor de correo.

Nota
Bitdefender no proporciona la protección antispam para cuentas de correo que accedes a través de un servicio de correo basado en web.

Los mensajes spam detectados por Bitdefender están marcados con el prefijo [spam] en linea del asunto. Bitdefender mueve automáticamente los mensajes de spam a una carpeta específica de la siguiente manera:

- En Microsoft Outlook, los mensajes de spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Elementos eliminados**. La carpeta de **Spam** se crea cuando se etiqueta un correo electrónico como spam.
- En Mozilla Thunderbird, los mensajes spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Papelera**. La carpeta de **Spam** se crea cuando se etiqueta un correo electrónico como spam.

Si utiliza otro cliente de correo, debe crear una regla para mover los mensajes de correo marcados como [spam] por Bitdefendera una carpeta de cuarentena personalizada. Si se suprimen las carpetas de papelera o de elementos eliminados, también se eliminará la carpeta de Spam. No obstante, se creará una nueva carpeta de Spam en cuanto se etiquete un correo electrónico como tal.

4.4.1. Conocimientos antispam

Los Filtros Antispam

El Motor Antispam de Bitdefender incorpora protección cloud y otros filtros diversos que aseguran que su buzón esté libre de SPAM, como Lista de amigos, Lista de Spammers y Filtro de juego de caracteres.

Lista de amigos / Lista de Spammers

La mayoría de la gente se suele comunicar con el mismo grupo de personas, o recibe mensajes de empresas y organizaciones de la misma área laboral. Mediante el uso de listas de **amigos o spammers**, podrá distinguir fácilmente la gente de la que desea recibir correo electrónico (amigos), sin importar lo

que el mensaje contenga, o la gente de la que no quiere saber nada (spammers).

> **Nota**
> Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Bitdefenderno bloquea los mensajes provenientes de este listado; de esta manera, al agregar amigos se asegura que los mensajes legítimos llegarán a su bandeja de entrada.

Filtro de carácteres

Gran parte del Spam está redactado con caracteres asiáticos o cirílicos. El Filtro de Caracteres detecta este tipo de mensajes y los marca como SPAM.

Manejo de Antispam

El motor de Bitdefender Antispam utiliza todos los filtros combinados para determinar si un correo puede entrar en su **Bandeja de Entrada** o no.

Cualquier mensaje que provenga de Internet pasará primero por los filtros Lista de Amigos/Lista de Spammers. Si el remitente se encuentra en la Lista de Amigos el mensaje será trasladado directamente a su **Bandeja de Entrada**.

Por otra parte, el filtro de la Lista de spammers se hará cargo del e-mail para verificar si la dirección del remitente está en su lista. Si hay una coincidencia, el e-mail se catalogará como SPAM y se moverá a la carpeta de **Spam**.

Si el remitente no se encuentra en ninguno de los dos listados el Filtro de caracteres verificará si el mensaje está escrito con caracteres cirílicos o asiáticos. En tal caso, el mensaje será marcado como SPAM y trasladado a la carpeta **Spam**.

> **Nota**
> Si el correo está marcado como SEXUALMENTE EXPLÍCITO en la línea del asunto, Bitdefender lo considerará SPAM.

Clientes de correo electrónico y protocolos soportados

Protección Antispam disponible para todos los clientes de correo POP3/SMTP. Sin embargo, la barra de herramientas de Bitdefender Antispam sólo se integra con los siguientes clientes:

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 y superior

4.4.2. Activar o desactivar la protección antispam

La protección antispam está habilitada por omisión.

Para activar o desactivar la característica Antispam:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTISPAM**, active o desactive el conmutador.

4.4.3. Utilizar la barra de herramientas antispam en su ventana de cliente de correo

En el área superior de la ventana de su cliente de correo puede ver la barra Antispam. La barra Antispam le ayuda a administrar la protección antispam directamente desde su cliente de correo. Puede corregir a Bitdefender fácilmente si ha marcado un mensaje legítimo como SPAM.

Importante

Bitdefender se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, diríjase a "*Clientes de correo electrónico y protocolos soportados*" (p. 89).

A continuación se explican las funciones de los botones de la Barra de Herramientas de Bitdefender:

Configuración - abre una ventana donde puede configurar los filtros antispam y las opciones de la barra de herramientas.
Es spam - indica que el correo electrónico seleccionado es spam. El correo electrónico se trasladará de inmediato a la carpeta **Spam**. Si los servicios antispam en la nube están activados, se envía el mensaje a la nube de Bitdefender para su posterior análisis.
No es spam - indica que el e-mail seleccionado no es spam y Bitdefender no debería haberlo etiquetado. El correo será movido a la carpeta **Spam** de la **Bandeja de Entrada**. Si los servicios antispam en la nube están activados, se envía el mensaje a la nube de Bitdefender para su posterior análisis.

Importante

El botón **No Spam** se activa al seleccionar un mensaje marcado como spam por Bitdefender (normalmente, estos mensajes se almacenan en la carpeta **Spam**).

Añadir a Spammer - añade el remitente del correo seleccionado a la lista de Spammers. Puede que necesite hacer clic en **Aceptar** para admitirlo. Los mensajes de correo recibidos de las direcciones que están en la lista de Spammer son marcados automáticamente como [spam].

Añadir Amigo - añade el remitente del correo seleccionado a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.

Spammers - abre la **Lista de Spammers** que contiene todas las direcciones de correo electrónico de las cuales no quiere recibir mensajes, independientemente de su contenido. Para más información, diríjase a "*Configurando la Lista de Spammers*" (p. 94).

Amigos - abre la **Lista de Amigos** que contiene todas las direcciones desde las que siempre quiere recibir mensajes, independientemente de su contenido. Para más información, diríjase a "*Configurando la Lista de Amigos*" (p. 92).

Indicar los errores de detección

Si está utilizando un cliente de correo compatible, puede corregir fácilmente el filtro antispam (indicando qué mensajes de correo no deben ser marcados como [spam]). Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccione el mensaje legítimos incorrecto marcado como [spam] por Bitdefender.
4. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Bitdefender para añadir los remitentes a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.
5. Haga clic en el botón **No es spam** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo). El mensaje de correo electrónico se moverá a la carpeta Bandeja de entrada.

Indicando mensajes spam no detectados

Si esta utilizando un cliente de correo compatible, puede indicar fácilmente que mensajes de correo deben ser detectados como spam. Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta Bandeja de Entrada.
3. Seleccione los mensajes spam no detectados.
4. Haga clic en el botón **Es spam** en la barra antispam de Bitdefender (localizada normalmente en la parte superior de la ventana del cliente de correo). Inmediatamente serán marcados como [spam] y trasladados a la carpeta de correo no deseado.

Configurar las opciones de la barra de herramientas

Para configurar los ajustes de la barra de herramientas antispam para su cliente de correo electrónico, haga clic en el botón **Configuración** de la barra de herramientas y, a continuación, en la pestaña **Opciones de barra de herramientas**.

Aquí tiene las siguientes opciones:

- **Marcar mensajes de spam como 'leídos'** - marca automáticamente los mensajes de spam como leídos de forma que no causen ninguna molestia cuando se reciben.
- Puede elegir si desea o no mostrar las ventanas de confirmación cuando hace clic en los botones **Añadir spammer** y **Añadir amigo** en la barra de herramientas de antispam.

  Las ventanas de confirmación pueden evitar que se añadan accidentalmente remitentes de correo electrónico a la lista de Amigos / Correo no deseado.

4.4.4. Configurando la Lista de Amigos

La **Lista de amigos** es una lista con todas las direcciones de e-mail de las que siempre quiera recibir mensajes, cualquiera que sea su contenido. Los mensajes de sus amigos no serán marcados como spam, aunque su contenido tenga múltiples características del correo no solicitado.

Nota
Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Bitdefender no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al agregar a sus conocidos en el Listado de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de entrada.

Para configurar y administrar la lista de Amigos:

- Si está utilizando Microsoft Outlook o Thunderbird, haga clic en el botón **Amigos** en la barra de herramientas antispam de Bitdefender.
- Como alternativa:
  1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
  2. En el panel **ANTISPAM**, haga clic en **Gestionar amigos**.

Para añadir una dirección de correo electrónico, seleccione la opción **Dirección de correo electrónico**, introduzca la dirección y, a continuación, haga clic en **AÑADIR**. Sintaxis: nombre@dominio.com.

Para añadir todas las direcciones de correo electrónico de un dominio específico, seleccione la opción **Nombre de dominio**, introduzca el nombre de dominio y luego haga clic en el botón **AÑADIR**. Sintaxis:

- @dominio.com y dominio.com - todos los mensajes provenientes de dominio.com llegarán a su **Bandeja de entrada** independientemente de su contenido;
- dominio - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) serán marcados como SPAM;
- com - todos mensajes con tales sufijos de dominios com serán marcados como SPAM;

Recomendamos evitar añadir dominios enteros, pero esto puede ser útil en algunas situaciones. Por ejemplo, puede añadir el dominio de correo de la compañía con la que trabaja, o sus distribuidores de confianza.

Para eliminar un elemento de la lista, haga clic en el enlace **Eliminar** correspondiente. Para eliminar todas las entradas de la lista, haga clic en **BORRAR LISTA**.

Puede guardar la lista de Amigos a un archivo la cual puede utilizarse en otro equipo o después de reinstalar el producto. Para guardar la lista de

Amigos, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión .bwl.

Para cargar una lista de amigos guardada previamente, haga clic en **CARGAR** y abra el archivo .bwl correspondiente. Para reiniciar el contenido de la lista existente al cargar una lista previamente guardada, seleccione **Sobrescribir la lista actual**.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

4.4.5. Configurando la Lista de Spammers

El **Listado de Spammers** es un listado que reúne todas las personas cuyos mensajes no desea recibir más, independientemente de sus formatos o contenidos. Cualquier mensaje proveniente de una dirección incluida en su **listado de spammers** será automáticamente marcada como spam, sin procesamientos ulteriores.

Para configurar y administrar la lista de Spammers:

- Si está utilizando Microsoft Outlook o Thunderbird, haga clic en el botón **Spammers** en la barra de herramientas antispam Bitdefender integrada dentro de su cliente de correo.
- Como alternativa:
  1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
  2. En el panel **ANTISPAM**, haga clic en **Gestionar emisores de spam**.

Para añadir una dirección de correo electrónico, seleccione la opción **Dirección de correo electrónico**, introduzca la dirección y, a continuación, haga clic en **AÑADIR**. Sintaxis: nombre@dominio.com.

Para añadir todas las direcciones de correo electrónico de un dominio específico, seleccione la opción **Nombre de dominio**, introduzca el nombre de dominio y luego haga clic en el botón **AÑADIR**. Sintaxis:

- @dominio.com y dominio.com - todos los mensajes provenientes de dominio.com llegarán a su **correo no deseado** independientemente de su contenido;
- dominio - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) serán marcados como SPAM;
- com - todos mensajes con tales sufijos de dominios com serán marcados como SPAM.

Recomendamos evitar añadir dominios enteros, pero esto puede ser útil en algunas situaciones.

Aviso

No agregar dominio legítimos de correo basados en servicios web (como un Yahoo, Gmail, Hotmail u otros) a la lista de Spammers. De lo contrario, los mensajes recibidos de cualquier usuario registrados en estos servicios serán detectados como spam. Si, por ejemplo, añade yahoo.com a la lista de Spammers, todas las direcciones de correo que vengan de yahoo.com serán marcados como [spam].

Para eliminar un elemento de la lista, haga clic en el enlace **Eliminar** correspondiente. Para eliminar todas las entradas de la lista, haga clic en **BORRAR LISTA**.

Puede guardar la lista de Spammers en un archivo la cual puede utilizarla en otro equipo o después de reinstalar el producto. Para guardar la lista Spammers, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión .bwl.

Para cargar una lista de emisores de spam guardada previamente, haga clic en **CARGAR** y abra el archivo .bwl correspondiente. Para reiniciar el contenido de la lista existente al cargar una lista previamente guardada, seleccione **Sobrescribir la lista actual**.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

4.4.6. Configuración de los filtros antispam locales

Cómo se describe en "*Conocimientos antispam*" (p. 88), Bitdefender utiliza una combinación de diferentes filtros antispam para identificar el spam. Los filtros antispam están preconfigurados para una protección eficiente.

Importante

Dependiendo en que si recibe o no correo legítimos escrito con caracteres Asiáticos o Cirílicos, desactive o active la configuración que bloquea automáticamente dichos correos. La correspondiente configuración está desactivada en las versiones del programa que utilizan conjunto de caracteres tales como (por ejemplo, en las versiones Rusas o Chinas).

Para configurar los filtros antispam locales:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTISPAM**, haga clic en **Ajustes**.
3. Haga clic en los conmutadores para activar o desactivar correspondientes.

Si está utilizando Microsoft Outlook o Thunderbird, puede configurar los filtros antispam directamente desde su cliente de correo. Haga clic en el botón ⚙ **Configuración** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo) y luego en la pestaña **Filtros antispam**.

4.4.7. Configurando la configuración de la nube

La detección en la nube hace uso de los servicios Cloud de Bitdefender para ofrecerle protección antispam siempre actualizada.

La protección cloud funciona mientras tenga activado Bitdefender Antispam.

Las muestras de correos electrónicos legítimos o spam pueden enviarse a la nube Bitdefender si indica errores de detección o correos electrónicos spam no detectados. Esto ayuda a mejorar la detección antispam de Bitdefender.

Configure el envío de muestras por correo electrónico a Bitdefender Cloud seleccionando las opciones deseadas siguiendo estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTISPAM**, haga clic en **Ajustes**.
3. Haga clic en los conmutadores para activar o desactivar correspondientes.

Si está utilizando Microsoft Outlook o Thunderbird, puede configurar la detección cloud directamente desde su cliente de correo. Haga clic en el botón ⚙ **Configuración** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo) y luego en la pestaña **Configuración en la nube**.

4.5. Cortafuego

El cortafuegos protege su equipo frente a intentos de conexión no autorizados internos y externos, tanto en la red local como en Internet. Es

muy similar a un guardia en su puerta, ya que mantiene un registro de intentos de conexión y decide cuál permitir y cuál bloquear.

El cortafuego de Bitdefender usa un conjunto de reglas para filtrar los datos transmitidos desde y hacia su sistema.

En condiciones normales, Bitdefender crea automáticamente una regla cada vez que una aplicación intenta acceder a Internet. También puede añadir o editar manualmente las reglas para las aplicaciones.

Como medida de seguridad, se le notificará cada vez que se bloquee el acceso a Internet de una app potencialmente maliciosa.

Bitdefender asigna automáticamente un tipo de red a cada conexión de red que detecta. Dependiendo del tipo de red, la protección del cortafuegos se ajusta al nivel apropiado para cada conexión.

Para saber más sobre las opciones del cortafuego para cada tipo de red y cómo editar la configuración de la red, vea "*Administración de ajustes de conexión*" (p. 100).

Activar o desactivar la protección del cortafuego

Para activar o desactivar la protección del cortafuego:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, active o desactive el conmutador.

Aviso

Apagar el cortafuego sólo debe hacerse como medida temporal, ya que expondría el equipo a conexiones no autorizadas. Vuelva a activar el cortafuego tan pronto como sea posible.

4.5.1. Administración de las reglas de apps

Para ver y administrar las reglas del cortafuego que controlan el acceso de las aplicaciones a los recursos de red y a Internet:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, haga clic en **Acceso de las aplicaciones**.

3. La primera vez que accede al Cortafuego, se le presenta esta característica. Haga clic en **BIEN, ENTENDIDO** para continuar.

Puede ver los quince últimos programas (procesos) que han pasado por el cortafuego de Bitdefender y la red de Internet a la que está conectado. Para ver las reglas creadas para una aplicación concreta, simplemente haga clic en ella y, a continuación, haga clic en el enlace **Ver reglas de aplicaciones**. Se abre la ventana **Reglas**.

Para cada regla se mostrará la siguiente información:

- **RED**: El proceso y tipos de adaptadores de red (Hogar/Oficina, Público o Todos) a los que se aplica la regla. Las reglas se crean automáticamente para filtrar el tráfico de la red / Internet a través de cualquier adaptador. De forma predeterminada, las reglas se aplican a cualquier red. Puede crear reglas manualmente o editar reglas existentes y así filtrar el acceso a la red/Internet de una aplicación en un adaptador de red específico (por ejemplo, un adaptador de red Wi-Fi).
- **PROTOCOLO**: El protocolo IP al que se aplica la regla. De forma predeterminada, las reglas se aplican a todos los protocolos.
- **TRÁFICO**: La regla se aplica en ambas direcciones (entrante y saliente).
- **PORTS**: El protocolo de puerto al que se aplica la regla. Por defecto, las reglas se aplican a todos los puertos.
- **IP**: El protocolo de Internet (IP) al que se aplica la regla. Por defecto, las reglas se aplican a todas las direcciones IP.
- **ACCESO**: Indica si la aplicación tiene acceso o no a la red o a Internet bajo las circunstancias especificadas.

Para editar o eliminar las reglas para la aplicación seleccionada, haga clic en el icono ⋯.

- **Editar regla**: Abre una ventana donde puede modificar la regla actual.
- **Eliminar regla**: Abre una ventana donde puede optar por eliminar el conjunto actual de reglas para la app seleccionada.

Añadir reglas de apps

Para añadir una regla de app:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.

2. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.
3. En la ventana de **Reglas**, haga clic en **Añadir regla**.

En la ventana **Ajustes** puede aplicar los siguientes cambios:

- **Aplicar esta regla a todas las aplicaciones.** Active este conmutador para aplicar la regla creada a todas las aplicaciones.
- **Ruta del Programa.** Haga clic en **EXAMINAR** y seleccione la app a la que se aplica la regla.
- **Permisos.** Seleccione uno de los permisos disponibles:

Permisos	Descripción
Permitir	Se permitirá el acceso de la aplicación especificada a la red / internet bajo las condiciones indicadas.
Bloquear	Se bloqueará el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.

- **Tipo de red.** Seleccione el tipo de red al que se aplica la regla. Puede cambiar el tipo accediendo al menú desplegable **Tipo de red** y seleccionar uno de los tipos disponibles de la lista.

Tipo de red	Descripción
Ninguna Red	Permitir todo el tráfico entre su equipo y otros equipos sin importar el tipo de red.
Casa/Oficina	Permite todo el tráfico entre su equipo y los equipos de la red local.
Público	Se filtrará todo el tráfico.

- **Protocolo.** En el menú, seleccione el protocolo IP sobre el que desea aplicar la regla.
  - Si desea aplicar la regla a todos los protocolos, seleccione la casilla **Cualquiera**.
  - Si desea aplicar la regla para TCP, seleccione **TCP**.
  - Se desea aplicar la regla para UDP, seleccione **UDP**.
  - Si desea que la regla se aplique a ICMP, seleccione **ICMP**.

- Si desea que la regla se aplique a IGMP, seleccione **IGMP**.
- Si desea que la regla se aplique a un protocolo concreto, escriba el número asignado al protocolo que desea filtrar en el campo editable en blanco.

> **Nota**
>
> Los números de los protocolos IP están asignados por la Internet Assigned Numbers Authority (IANA). Puede encontrar una lista completa de los números asignados a los protocolos IP en http://www.iana.org/assignments/protocol-numbers.

- **Dirección.** En el menú, seleccione la dirección del tráfico a la que se aplicará la regla.

Dirección	Descripción
Saliente	La regla se aplicará sólo para el tráfico saliente.
Entrante	La regla se aplicará sólo para el tráfico entrante.
Ambos	La regla se aplicará en ambas direcciones.

En la ventana **Avanzado** puede personalizar los siguientes ajustes:

- **Dirección local personalizada.** Indique la dirección IP local y el puerto a los que se aplicará la regla.
- **Dirección remota personalizada.** Indique la dirección IP remota y el puerto a los que aplicará la regla.

Para eliminar el conjunto actual de reglas y restaurar las predeterminadas, haga clic en **Reiniciar reglas** en la ventana **Reglas**.

4.5.2. Administración de ajustes de conexión

Ya se conecte a Internet por Wi-Fi o mediante un adaptador Ethernet, puede configurar qué ajustes deben aplicarse para una navegación segura. Las opciones entre las que puede elegir son:

- **Dinámico**: El tipo de red se establecerá automáticamente en función del perfil de la red conectada, Hogar/Oficina o Público. Cuando esto sucede, solo se aplican las reglas de cortafuego para el tipo de red concreto o las definidas para aplicar a todos los tipos de red.

- **Hogar/Oficina**: El tipo de red siempre será Hogar/Oficina, sin tener en cuenta el perfil de la red conectada. Cuando esto sucede, solo se aplican las reglas de cortafuego para Hogar/Oficina o las definidas para aplicar a todos los tipos de red.
- **Público**: El tipo de red siempre será Público, sin tener en cuenta el perfil de la red conectada. Cuando esto sucede, solo se aplican las reglas de cortafuego para Público o las definidas para su aplicación a todos los tipos de red.

Para configurar sus adaptadores de red:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Adaptadores de red**.
4. Seleccione los ajustes que desee aplicar al conectarse con los siguientes adaptadores:
   - Wi-Fi
   - Ethernet

4.5.3. Configuración de opciones avanzadas

Para configurar los ajustes avanzados del cortafuego:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Configuración**.

Pueden configurarse las siguientes características:

- **Protección del análisis de puertos**: Detecta y bloquea los intentos de averiguar qué puertos están abiertos.

  Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers para averiguar los puertos abiertos en su equipo. Si encuentran un puerto vulnerable o inseguro, pueden intentar entrar en su equipo sin su autorización.
- **Modo alertas**: Se muestran alertas cada vez que una app intenta conectarse a Internet. Seleccione **Permitir** o **Bloquear**. Cuando el modo

Alertas está activo, la característica Perfiles se desactiva automáticamente. El modo Alertas se puede utilizar junto con el **modo Batería**.

- **Modo Oculto** - indica si quiere que otros ordenadores detecten a su equipo o no. Haga clic en **Editar los ajustes de invisibilidad** para elegir cuándo su dispositivo debe o no estar visible para otros equipos.
- **Comportamiento por defecto de la aplicación**: Permite que Bitdefender aplique ajustes automáticos a las aplicaciones sin reglas definidas. Haga clic en **Editar reglas por defecto** para elegir si se deben aplicar o no los ajustes automáticos.
  - Automático: Se permitirá o denegará el acceso a las aplicaciones en función de las reglas automáticas de cortafuego y de usuario.
  - Permitir: Se permitirán automáticamente las aplicaciones que carezcan de una regla de cortafuego definida.
  - Bloquear: Se bloquearán automáticamente las aplicaciones que carezcan de una regla de cortafuego definida.

4.6. Vulnerabilidad

Un paso importante para la protección de su equipo frente a acciones o aplicaciones malintencionadas es mantener actualizado el sistema operativo y las aplicaciones que utiliza habitualmente. Es más, para evitar el acceso físico no autorizado a su equipo, deberán configurarse contraseñas seguras (contraseñas que no puedan adivinarse fácilmente) para cada cuenta de usuario de Windows y también para las redes Wi-Fi a las que se conecte.

Bitdefender comprueba automáticamente las vulnerabilidades de su sistema y le avisa sobre ellas. Se analiza en busca de lo siguiente:

- apps obsoletas en su equipo.
- Actualizaciones de Windows que faltan.
- contraseñas inseguras de cuentas de usuario de Windows.
- routers y redes inalámbricas que no sean seguras.

Bitdefender ofrece dos formas fáciles de solucionar las vulnerabilidades de su sistema:

- Puede analizar su sistema en busca de vulnerabilidades y repararlas paso a paso utilizando la opción **Análisis de vulnerabilidades**.

- Mediante la monitorización de vulnerabilidades, puede averiguar y corregir las vulnerabilidades detectadas en la ventana Notificaciones.

Debería revisar y corregir las vulnerabilidades del sistema cada una o dos semanas.

4.6.1. Analizar su sistema en busca de vulnerabilidades

Para reparar vulnerabilidades del sistema usando la opción Análisis de vulnerabilidades:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Análisis de vulnerabilidades**.
3. Espere a que Bitdefender compruebe su sistema en busca de vulnerabilidades. Para detener el proceso de análisis, haga clic en el botón **Omitir** en la parte superior de la ventana.
   - **Actualizaciones críticas de Windows**

     Haga clic en **Ver detalles** para ver la lista de actualizaciones críticas de Windows que no están instaladas en su equipo.

     Para iniciar la instalación de las actualizaciones seleccionadas, haga clic en **Instalar actualizaciones**. Tenga en cuenta que puede llevar bastante tiempo instalar las actualizaciones, y alguna de ellas puede requerir que reinicie el sistema para completar la instalación. Si es necesario, reinicie el sistema en cuanto pueda.

   - **Actualizaciones de aplicaciones**

     Si una aplicación no está actualizada, haga clic en el enlace **Descargar una nueva versión** para descargar la última versión.

     Haga clic en **Ver detalles** para ver la información sobre la aplicación que necesita actualizarse.

   - **Contraseñas débiles de cuentas de Windows**

     Puede ver la lista de las cuentas de usuario de Windows configuraras en su equipo y el nivel de protección de sus contraseñas.

     Haga clic en **Cambiar contraseña al iniciar sesión** para establecer una nueva contraseña para su sistema.

Haga clic en **Ver detalles** para modificar las contraseñas débiles. Puede elegir entre pedir al usuario que cambie la contraseña en el siguiente inicio de sesión o cambiarla usted mismo inmediatamente. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

- **Redes Wi-Fi**

  Haga clic en **Ver detalles** para averiguar más sobre la red inalámbrica a la que está conectado. Si se le recomienda establecer una contraseña más segura para su red doméstica, haga clic en el enlace correspondiente.

  Cuando haya otras recomendaciones, siga las instrucciones que se le proporcionan para asegurarse de que su red doméstica se mantiene a salvo de las miradas indiscretas de los piratas informáticos.

En la esquina superior derecha de la ventana puede filtrar los resultados según sus preferencias.

4.6.2. Usar el control automático de la vulnerabilidad

Bitdefender analiza frecuentemente el sistema en segundo plano en busca de vulnerabilidades y registra las incidencias detectadas en la ventana Notificaciones.

Para revisar y reparar las incidencias detectadas:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al Análisis de vulnerabilidades.
3. Puede ver información detallada sobre las vulnerabilidades del sistema detectadas. Dependiendo de la incidencia, para reparar una vulnerabilidad específica haga lo siguiente:
   - Si hay actualizaciones de Windows disponibles, haga clic en **Instalar**.
   - Si la actualización automática de Windows está desactivada, haga clic en **Activar**.

- Si una app está obsoleta, haga clic en **Actualizar ahora** para encontrar un enlace a la página web del proveedor desde donde pueda instalar su última versión.
- Si una cuenta de usuario de Windows tiene una contraseña débil, haga clic en **Cambiar contraseña** para forzar al usuario a cambiar la contraseña en el próximo inicio de sesión o cámbiela usted mismo. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).
- Si la función Ejecución automática de Windows está activada, haga clic en **Reparar** para desactivarla.
- Si el router que ha configurado tiene establecida una contraseña vulnerable, haga clic en **Cambiar contraseña** para acceder a su interfaz, desde donde podrá establecer una contraseña segura.
- Si la red a la que está conectado presenta vulnerabilidades que podrían poner en riesgo su sistema, haga clic en **Cambiar ajustes de Wi-Fi**.

Para configurar los ajustes de la monitorización de vulnerabilidades:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Ajustes**.

   ! **Importante**
   Para recibir notificaciones automáticas sobre las vulnerabilidades del sistema o de aplicaciones, mantenga activada la opción **Vulnerabilidades**.

3. Elija las vulnerabilidades del sistema que quiere comprobar regularmente usando los conmutadores correspondientes.

   Actualización de Windows
   Compruebe si su sistema operativo Windows tiene las últimas actualizaciones críticas de seguridad de Microsoft.

   Actualizaciones de aplicaciones
   Compruebe si las aplicaciones instaladas en su sistema están actualizadas. Las aplicaciones obsoletas pueden ser explotadas por software malicioso, haciendo vulnerable su PC a los ataques externos.

Contraseñas de usuario

Compruebe si las contraseñas de los routers y cuentas de Windows configuradas en el sistema son fáciles de adivinar o no. Establecer contraseñas que sean difíciles de averiguar (contraseñas fuertes) hace que sea muy difícil para los hackers entrar en el sistema. Una contraseña segura necesita letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

Reproducción automática

Comprobar el estado de la función Ejecución automática de Windows. Esta función permite a las aplicaciones iniciarse automáticamente desde CDs, DVDs, unidades USB y otros dispositivos externos.

Algunos tipos de amenazas utilizan la ejecución automática para propagarse desde unidades extraíbles al PC. Esta es la razón por la que se recomienda deshabilitar esta opción de Windows.

Seguridad de Wi-Fi

Compruebe si la red inalámbrica doméstica a la que está conectado es segura o no, y si tiene vulnerabilidades. Además, compruebe si la contraseña de su router es lo suficientemente segura, y cómo puede hacer que lo sea aún más.

La mayoría de las redes inalámbricas desprotegidas no son seguras, lo que permite que las miradas indiscretas de los piratas informáticos se posen sobre sus actividades privadas.

Nota

Si desactiva la monitorización de una vulnerabilidad específica, los problemas derivados de ella no se registrarán en la ventana Notificaciones.

4.6.3. Asesor de seguridad Wi-Fi

Mientras viaja, trabaja en un café o espera en el aeropuerto, conectarse a una red inalámbrica pública para hacer pagos o revisar sus mensajes de correo electrónico o cuentas de redes sociales puede ser la solución más rápida. Pero puede haber miradas indiscretas tratando de acceder a sus datos personales, observando cómo se filtra su información a través de la red.

Por datos personales se entienden las contraseñas y nombres de usuario que utiliza para acceder a sus cuentas online, como por ejemplo las de correo electrónico, bancos, o redes sociales, además de los mensajes que envíe.

Por lo general, es más habitual que las redes inalámbricas públicas sean poco fiables, ya que no requieren una contraseña al iniciar la sesión y, si lo hacen, esa contraseña se habrá puesto a disposición de cualquier persona que quisiera conectarse. Por otra parte, pueden constituir redes maliciosas o honeypots que suponen un objetivo para los delincuentes informáticos.

Para protegerle contra los peligros de los puntos de acceso inalámbricos públicos desprotegidos o sin cifrar, el Asesor de seguridad Wi-Fi de Bitdefender analiza el grado de seguridad de una red inalámbrica y, de ser necesario, le recomienda utilizar Bitdefender VPN.

El Asesor de seguridad Wi-Fi de Bitdefender le brinda información sobre:

- Redes Wi-Fi domésticas
- Redes Wi-Fi públicas

Activar o desactivar las notificaciones del Asesor de seguridad Wi-Fi

Para activar o desactivar las notificaciones del Asesor de seguridad Wi-Fi:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Ajustes**.
3. En la ventana **Ajustes**, active o desactive la opción de **Seguridad Wi-Fi**.

Configurar una red Wi-Fi doméstica

Para empezar a configurar su red doméstica:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Seguridad Wi-Fi**.
3. En la pestaña **WI-FI DOMÉSTICA**, haga clic en el botón **SELECCIONAR WI-FI DOMÉSTICA**.

   Se muestra una lista con las redes inalámbricas a las que se haya conectado hasta ese momento.

4. Elija su red doméstica y, a continuación, haga clic en **SELECCIONAR**.

Si una red doméstica se considera poco fiable o insegura, se muestran recomendaciones de configuración para mejorar su seguridad.

Para eliminar la red inalámbrica que ha establecido como red doméstica, haga clic en el botón **ELIMINAR**.

Wi-Fi Pública

Mientras esté conectado a una red inalámbrica poco fiable o insegura, se activará el perfil de Wi-Fi pública. Al trabajar bajo este perfil, Bitdefender Total Security se configura automáticamente para reflejar los siguientes ajustes del programa:

- Se activa Defensa Contra Amenazas Avanzadas
- El cortafuego de Bitdefender está activado y se aplican los siguientes ajustes a su adaptador inalámbrico:
  - Modo oculto - ACTIVADO
  - Tipo de red: Pública
- Se activan los siguientes ajustes de la Prevención de amenazas online:
  - Análisis de sitios web cifrados
  - Protección contra fraude
  - Protección contra phishing
- Hay disponible un botón que abre Bitdefender Safepay™. En este caso, se activa por defecto la protección de puntos de acceso para redes no seguras.

Revisar la información relativa a las redes Wi-Fi

Para revisar la información relativa a las redes inalámbricas a las que se conecte habitualmente:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Seguridad Wi-Fi**.
3. En función de la información que necesite, seleccione una de las pestañas: **WI-FI DOMÉSTICA** o **WI-FI PÚBLICA**.

4. Haga clic en **Ver detalles** junto a la red de la que desea obtener más información.

Hay tres tipos de redes inalámbricas filtradas según su importancia, cada uno de los cuales se identifica mediante un icono:

La red Wi-Fi es poco fiable - Indica que el nivel de seguridad de la red es bajo. Esto significa que existe un alto riesgo al usarla y no se recomienda realizar pagos o revisar cuentas bancarias sin una protección adicional. En tales situaciones, se recomienda utilizar Bitdefender Safepay™ con protección de punto de acceso para las redes poco fiables habilitadas.

La red Wi-Fi es poco fiable - Indica que el nivel de seguridad de la red es moderado. Esto significa que puede presentar vulnerabilidades y no se recomienda realizar pagos o revisar cuentas bancarias sin una protección adicional. En tales situaciones, se recomienda utilizar Bitdefender Safepay™ con protección de punto de acceso para las redes poco fiables habilitadas.

La red Wi-Fi es segura - Indica que la red que utiliza es segura. En este caso, puede intercambiar datos confidenciales en sus operaciones online.

Al hacer clic en el enlace **Ver detalles** del apartado de cada red, se mostrará la siguiente información:

- **Protegida** - aquí puede ver si la red seleccionada está protegida o no. Las redes sin cifrar pueden dejar expuestos los datos que utilice.
- **Tipo de cifrado** - Aquí puede ver el tipo de cifrado utilizado por la red seleccionada. Algunos tipos de cifrado pueden ser poco fiables. Por lo tanto, le recomendamos encarecidamente que revise la información relativa al tipo de cifrado que se muestra para asegurarse de que está protegido mientras navega por Internet.
- **Canal/Frecuencia** - Aquí puede ver la frecuencia del canal utilizado por la red seleccionada.
- **Seguridad de la contraseña** - Aquí puede ver el grado de seguridad de la contraseña. Tenga en cuenta que las redes que tienen contraseñas vulnerables constituyen un objetivo para los delincuentes informáticos.
- **Tipo de registro** - Aquí puede ver si la red seleccionada está protegida por contraseña o no. Es muy recomendable conectarse únicamente a redes que tengan establecidas contraseñas seguras.
- **Tipo de autenticación** - Aquí puede ver el tipo de autenticación utilizado por la red seleccionada.

Mantenga activada la opción **Notificar** para recibir notificaciones cada vez que su sistema se conecte a esta red.

4.7. Protección de cámaras web

Que los piratas informáticos pueden apoderarse de su cámara web para espiarle no es una novedad, y las soluciones para protegerle, como la revocación de los privilegios de las aplicaciones, la desactivación de la cámara integrada del dispositivo, o sencillamente taparla, no son muy prácticas. Para evitar los intentos de vulneración de su privacidad, la Protección de cámaras web de Bitdefender monitoriza permanentemente las apps que intentan acceder a su cámara, y bloquea aquellas que no sean de fiar.

Como medida de seguridad, se le notificará cada vez que una app que no sea de fiar intente acceder a su cámara.

Activación y desactivación de la Protección de cámaras web

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PROTECCIÓN DE CÁMARAS WEB**, active o desactive el conmutador.

Configuración de la Protección de cámaras web

Puede configurar qué reglas deben aplicarse cuando una app intente acceder a su cámara siguiendo estos pasos:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PROTECCIÓN DE CÁMARAS WEB**, haga clic en **Ajustes**.

Reglas de bloqueo de aplicaciones

- **Bloquear todos los accesos a la cámara web** - No se permitirá a ninguna aplicación acceder a su cámara web.
- **Bloquear el acceso del navegador a la cámara web** - No se permitirá el acceso a su cámara web a ningún navegador web, excepto Internet Explorer y Microsoft Edge. Como las apps de la Tienda Windows se ejecutan en un único proceso, Bitdefender no puede identificar a Internet Explorer y

Microsoft Edge como navegadores web y, por lo tanto, quedan exceptuados de este ajuste.

- **Establecer el acceso de las aplicaciones a la cámara web según la elección de los usuarios de Bitdefender** - Si la mayoría de los usuarios de Bitdefender considera que una app popular es inofensiva, entonces su acceso a la cámara web se fijará automáticamente en Permitir. Si muchos usuarios consideran peligrosa una app popular, entonces su acceso se fijará automáticamente en Bloqueado.

  Se le informará siempre que una de las apps que tiene instaladas resulte bloqueada por la mayoría de los usuarios de Bitdefender.

Notificaciones

- **Notificar cuando las aplicaciones permitidas se conecten a la cámara web**: Se le notificará siempre que una app permitida acceda a su cámara web.

Añadir apps a la lista de Protección de cámaras web

Las apps que intentan conectarse a su cámara web se detectan automáticamente y, dependiendo de su comportamiento y de la elección de la comunidad, se les permite o no su acceso. No obstante, puede determinar manualmente por su cuenta la acción que debe adoptarse siguiendo estos pasos:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PROTECCIÓN DE CÁMARAS WEB**, haga clic en **Acceso a la cámara web**.
3. La primera vez que accede a la Protección de cámaras web, se le presenta esta característica.
4. Haga clic en el enlace que desee:
   - **Seleccionar apps de la Tienda Windows para añadir a la lista de permisos**: Muestra una lista con las apps de la Tienda de Windows detectadas. Active los conmutadores junto a las apps que desee añadir a la lista.
   - **Empezar a añadir aplicaciones a la lista de acceso a la cámara web**: Vaya al archivo .exe que desea añadir a la lista y, a continuación, haga clic en **Aceptar**.

Para añadir más apps, haga clic en el enlace **Añadir una nueva aplicación a la lista**.

Haga clic en el conmutador de **Acceso permitido/Acceso bloqueado**.

Para ver lo que los usuarios de Bitdefender han decidido hacer con la app seleccionada, haga clic en el icono .

En esta ventana aparecerán las apps que soliciten acceso a su cámara, junto con la hora de su última actividad.

Se le notificará cada vez que una de las apps permitidas resulte bloqueada por los usuarios de Bitdefender.

4.8. Archivos seguros

El ransomware es un software malicioso que ataca a los sistemas vulnerables y los bloquea, con el fin de solicitar dinero al usuario a cambio de permitirle recuperar el control de su sistema. Este software malicioso actúa astutamente, mostrando mensajes falsos para que el usuario entre en pánico, instándole a efectuar el pago solicitado.

Dicha infección puede propagarse mediante spam, al descargar archivos adjuntos, o por visitar sitios web infectados e instalar apps maliciosas sin que el usuario se percate de lo que está sucediendo en su sistema.

El ransomware puede presentar cualquiera de los siguientes comportamientos que impiden que el usuario acceda a su sistema:

- Cifrar archivos confidenciales y personales sin dar la posibilidad de descifrarlos hasta que la víctima pague un rescate.
- Bloquear la pantalla del equipo y mostrar un mensaje pidiendo dinero. En este caso, no se cifra ningún archivo y simplemente se fuerza al usuario a que efectúe el pago.
- Bloquear la ejecución de apps.

Con Archivos seguros de Bitdefender puede proteger sus archivos personales contra los ataques de ransomware, como por ejemplo sus documentos, fotos o películas.

Nota

Defensa Contra Amenazas Avanzadas y Archivos seguros son dos capas de protección contra ransomware. Defensa Contra Amenazas Avanzadas es la característica que bloquea los ataques de ransomware que tratan de acceder

a las áreas críticas de su sistema, mientras que Archivos seguros se cerciora de que no se cifre ningún archivo importante de su equipo.

4.8.1. Activar o desactivar Archivos seguros

Para activar o desactivar la característica Archivos seguros:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, active o desactive el conmutador.

Cada vez que una aplicación intente acceder a uno de los archivos protegidos, aparecerá una ventana emergente de Bitdefender. Puede permitir o bloquear el acceso.

Nota
La característica Archivos seguros no está activada por defecto.

4.8.2. Proteger los archivos personales de los ataques de ransomware

Si desea poner a buen recaudo sus archivos personales:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Carpetas protegidas**.
3. La primera vez que accede a Carpetas protegidas, se le presenta esta característica. Haga clic en **PROTEGER MÁS CARPETAS** para continuar.
4. Seleccione la carpeta que desea proteger y, a continuación, haga clic en **Aceptar**.

   Para añadir más carpetas, haga clic en el enlace **Proteger más carpetas**. Como alternativa, arrastre las carpetas a esta ventana.

Las carpetas Imágenes, Vídeos, Música y Escritorio están protegidas por defecto contra los ataques. Los datos personales almacenados en servicios de alojamiento de archivos online, como Box, Dropbox, Google Drive y OneDrive también están incluidos en el entorno de protección, siempre que sus aplicaciones estén instaladas en el sistema.

Para evitar que el sistema se ralentice, le recomendamos que añada un máximo de treinta carpetas, o que guarde varios archivos en una sola carpeta.

Nota
Se pueden proteger carpetas personalizadas solo para los usuarios actuales. Los archivos del sistema y de aplicaciones no se pueden añadir a las excepciones.

4.8.3. Configuración del acceso de las apps

Puede que las aplicaciones que intenten cambiar o borrar archivos protegidos se identifiquen como potencialmente poco fiables y se añadan a la lista de aplicaciones bloqueadas. Si se bloquease una aplicación y estuviese seguro de que su comportamiento es el adecuado, puede permitirla siguiendo estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Acceso de las aplicaciones**.
3. Aparecen las apps que hayan solicitado cambiar archivos de sus carpetas protegidas. Active el conmutador junto a la app que considera segura.

En la misma ventana, puede desactivar la protección contra ransomware para determinadas apps desactivando el conmutador correspondiente.

Si desea añadir nuevas aplicaciones a la lista, haga clic en el enlace **Añadir una nueva aplicación a la lista**.

4.8.4. Protección en el arranque

Se sabe que muchas apps maliciosas se ponen en funcionamiento al arrancar el sistema, lo que puede dañar seriamente una máquina. La Protección en el arranque de Bitdefender analiza todas las áreas críticas del sistema antes de que se carguen todos los archivos, con un impacto nulo en el sistema.

Para desactivar la protección en el arranque:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Ajustes**.
3. Desactive la **Protección en el arranque**.

Nota
Las apps añadidas a las excepciones también se analizarán y se tratarán en consecuencia.

4.9. Reparación de ransomware

La Reparación de ransomware de Bitdefender realiza una copia de seguridad de sus archivos, como documentos, imágenes, vídeos o música, para asegurarse de que estén protegidos contra daños o pérdida en caso de que un ransomware los cifre. Si se detecta un ataque de ransomware, Bitdefender bloqueará todos los procesos implicados en el ataque y comenzará el proceso de reparación. De esta forma, podrá recuperar todo el contenido de sus archivos sin pagar ningún rescate.

Activación y desactivación de la Reparación de ransomware

Para activar y desactivar la Reparación de ransomware:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **REPARACIÓN DE RANSOMWARE**, active o desactive el conmutador.

> **Nota**
> Para asegurarse de que sus archivos estén protegidos contra el ransomware, le recomendamos que mantenga habilitada la Reparación de ransomware.

Activar o desactivar la restauración automática

La restauración automática se asegura de que sus archivos se restauren automáticamente en caso de que un ransomware los cifre.

Para activar o desactivar la restauración automática:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **REPARACIÓN DE RANSOMWARE**, haga clic en **Ajustes**.
3. Activar o desactivar el conmutador **Restauración automática**.

Visualización de archivos que se restauraron automáticamente

Cuando se habilita la opción **Restauración automática**, Bitdefender restaura automáticamente los archivos que un ransomware pudiera cifrar. De esta

forma, puede usar su equipo sin preocupaciones, sabiendo que sus archivos están a salvo.

Para ver archivos que se restauraron automáticamente:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación referente al último comportamiento de ransomware reparado y luego haga clic en **Archivos restaurados**.

   Se muestra la lista con los archivos restaurados. Aquí también puede ver la ubicación donde se restauraron sus archivos.

Restaurar manualmente archivos cifrados

En caso de tener que restaurar manualmente los archivos que resultaron cifrados, siga los pasos que se exponen a continuación:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación referente al último comportamiento de ransomware detectado y luego haga clic en **Archivos cifrados**.
3. Se muestra la lista con los archivos cifrados.

   Haga clic en **RECUPERAR ARCHIVOS** para continuar.
4. En caso de que la totalidad o una parte del proceso de restauración falle, debe elegir la ubicación donde se guardarán los archivos descifrados. Haga clic en **RESTAURAR UBICACIÓN** y luego elija una en su PC.
5. Aparecerá una ventana de confirmación.

   Haga clic en **FINALIZAR** para terminar el proceso de restauración.

En caso de cifrado, se pueden restaurar los archivos con las siguientes extensiones:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar;

.tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

Añadir aplicaciones a excepciones

Puede configurar reglas de excepción para las apps de confianza, de modo que la característica de Reparación de ransomware no las bloquee si realizan acciones típicas del ransomware.

Para añadir apps a la lista de excepciones de la Reparación de ransomware:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **REPARACIÓN DE RANSOMWARE**, haga clic en **Ajustes**.
3. Para añadir nuevas aplicaciones a la lista, haga clic en **Añadir una nueva aplicación a la lista**.

4.10. Cifrado de archivo

El Blindaje de Archivo de Bitdefender le permite crear unidades logicas cifradas y protegidos por contraseña en su equipo, en los que puede almacenar sus documentos confidenciales y sensibles. Sólo la persona que conozca la contraseña podrá acceder a los datos almacenados en los blindajes.

La contraseña le permite abrir el blindaje, almacenar datos en éste y cerrarlo, a la vez que asegura su protección. Cuando un blindaje está abierto, puede añadir nuevos archivos, abrir los archivos que contiene y modificarlos.

Físicamente, el blindaje es un archivo cifrado almacenado en su equipo cuya extensión es bvd. Aunque es posible acceder a los archivos físicos de las unidades blindadas desde diferentes sistemas operativos (como Linux), la información almacenada en los mismos no puede leerse al estar cifrada.

Pueden administrase cinco blindajes desde la ventana Bitdefender o utilizando el menú contexto de Windows y la unidad lógica asociada con el blindaje.

Administración de blindajes de archivos

Para administrar sus blindajes de archivos de Bitdefender:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Ajustes**.

   Los blindajes de archivos existentes aparecen en esta ventana.

Crear blindajes de archivo

Para crear un nuevo blindaje:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Crear Nuevo Archivo Blindado**.
3. Especifique el nombre y ubicación del blindaje de archivos.
   - Escriba el nombre del blindaje de archivos en el campo correspondiente.
   - Haga clic en **EXAMINAR**, seleccione la ubicación del blindaje y guarde el archivo del blindaje con el nombre deseado.
4. Seleccione una letra de unidad en el menú correspondiente. Al abrir un blindaje, en Mi PC aparecerá un nuevo disco virtual con la letra de unidad seleccionada.
5. Si desea cambiar el tamaño por defecto del blindaje (100 MB), use las teclas de flecha arriba y abajo en **Tamaño del blindaje (MB)**.
6. Escriba la contraseña deseada para el blindaje en los campos **Contraseña** y **Confirmar contraseña**. La contraseña debe tener como mínimo 8 caracteres. Cada vez que alguien que intente abrir el blindaje y acceder a sus archivos, deberá introducir la contraseña.
7. Haga clic en **CREAR**.

Bitdefender le informará de inmediato sobre el resultado de la operación. Si se ha producido un error, utilice el mensaje de error para solucionar el problema.

Para crear un blindaje más rápidamente, haga clic con el botón derecho en una carpeta de su equipo, escoja **Bitdefender** > **Blindaje de archivos de Bitdefender** y seleccione **Crear blindaje de archivos**.

Nota
Podría ser conveniente guardar todos los blindajes de archivos en la misma ubicación. De esta manera, puede localizarlos fácilmente.

Importación de un blindaje de archivos

Para importar un blindaje de archivos almacenado localmente:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Importar blindaje**.
3. Busque la ubicación de su blindaje y selecciónelo (archivo .bvd).
4. Haga clic en **Abrir**.

Abrir blindajes de archivo

Para poder acceder y trabajar con los archivos almacenados en el Blindaje, antes debería abrirlo. Al abrir un Blindaje, aparecerá una unidad de disco virtual en Mi PC. Esta unidad estará etiquetada con la letra de unidad asignada al Blindaje.

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Ajustes**.
3. Seleccione el blindaje que desea abrir y, a continuación, haga clic en **DESBLOQUEAR**.
4. Escriba la contraseña requerida y, a continuación, haga clic en **ACEPTAR**.
5. Haga clic en **ABRIR** para abrir su blindaje.

Bitdefender le informará de inmediato sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia.

Para abrir rápidamente un blindaje, busque en su equipo el archivo .bvd correspondiente al blindaje que desee abrir. Haga clic con el botón derecho en el archivo, escoja **Bitdefender** > **Blindaje de archivos de Bitdefender** y seleccione **Desbloquear**. Escriba la contraseña exigida y, a continuación, haga clic en **Aceptar**.

Añadir archivos a los blindajes

Antes de añadir ficheros o carpetas a un blindaje, deberá abrir el blindaje.

Para añadir nuevos archivos a su blindaje:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Ajustes**.
3. Seleccione el blindaje al que desea añadir archivos y, a continuación, haga clic en **DESBLOQUEAR**.
4. Escriba la contraseña requerida y, a continuación, haga clic en **ACEPTAR**.
5. Haga clic en **ABRIR** para abrir su blindaje.
6. Añada archivos o carpetas como hace normalmente en Windows (por ejemplo, puede utilizar el método de copiar y pegar).

Para añadir archivos más rápidamente a su blindaje, haga clic con el botón derecho en el archivo o carpeta que desee copiar a un blindaje, escoja **Bitdefender** > **Blindaje de archivos de Bitdefender** y seleccione **Añadir a blindaje de archivos**.

- Si sólo hay un blindaje abierto, el fichero o carpeta será copiado directamente a ese blindaje.
- Si hay varios blindajes abiertos, se le pedirá elegir a qué blindaje copiar el elemento. Seleccione desde el menú la letra correspondiente al blindaje deseado y haga clic en **Aceptar** para copiar el elemento.

Bloquear blindajes

Cuando acabe de trabajar con el blindaje de archivos, debería bloquearlo para proteger sus datos. Al bloquear el blindaje, la unidad de disco virual desaparecerá de Mi PC. En consecuencia, el acceso a los datos guardados en el blindaje será completamente bloqueado.

Para bloquear un blindaje:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Ajustes**.

3. Seleccione el blindaje que desea bloquear y, a continuación, haga clic en **BLOQUEAR**.

Bitdefender le informará de inmediato sobre el resultado de la operación. Si se ha producido un error, utilice el mensaje de error para solucionar el problema.

Para bloquear más rápidamente un blindaje, haga clic con el botón derecho en el archivo .bvd correspondiente al blindaje, escoja **Bitdefender** > **Blindaje de archivos de Bitdefender** y seleccione **Bloquear**.

Borrar archivos del blindaje

Para eliminar archivos o carpetas de un blindaje, el blindaje debe estar abierto. Para eliminar archivos o carpetas de un blindaje:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Ajustes**.
3. Seleccione el blindaje del que desea eliminar archivos y, a continuación, haga clic en **DESBLOQUEAR** en caso de que esté bloqueado.
4. Haga clic en **ABRIR**.

   Elimina archivos o carpetas como lo hace en Windows (por ejemplo, clic derecho en un archivo que quiere eliminar y seleccione **Eliminar**).

Cambiar la contraseña del blindaje

La contraseña protege el contenido de un blindaje de accesos sin autorización. Sólo los usuarios que conocen la contraseña pueden abrir el blindaje y tener acceso a los documentos y datos guardados dentro de él.

El blindaje debe bloquearse antes de cambiar la contraseña. Para cambiar la contraseña de un blindaje:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CIFRADO DE ARCHIVOS**, haga clic en **Ajustes**.
3. Seleccione el blindaje al que desea cambiar la contraseña y, a continuación, haga clic en **AJUSTES**.

4. Introduzca la contraseña actual para el blindaje en el campo **Contraseña Antigua**.
5. Introduzca la nueva contraseña para el blindaje en los campos **Nueva Contraseña** y **Confirmar Nueva Contraseña**.

> **Nota**
> La contraseña debe tener como mínimo 8 caracteres. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

Bitdefender le informará de inmediato sobre el resultado de la operación. Si se ha producido un error, utilice el mensaje de error para solucionar el problema.

Para cambiar rápidamente la contraseña de un blindaje, busque en su equipo el archivo .bvd correspondiente al blindaje. Haga clic con el botón derecho en el archivo, escoja **Bitdefender** > **Blindaje de archivos de Bitdefender** y seleccione **Cambiar contraseña del blindaje**.

4.11. Protección del Gestor de contraseñas para sus credenciales

Usamos nuestros equipos para comprar online o pagar nuestras facturas, para conectarnos a plataformas de redes sociales o iniciar sesión con aplicaciones de mensajería instantánea.

¡Pero como todo el mundo sabe, no siempre es fácil recordar una contraseña!

Y si no tenemos cuidado mientras navegamos online, nuestra información privada, como nuestra dirección de correo, nuestro ID de mensajería instantánea o los datos de nuestra tarjeta de crédito pueden verse comprometidos.

Guardar sus contraseñas o sus datos personales en una hoja de papel o en el equipo puede ser peligroso porque pueden acceder a ellos personas que quieran robar y usar esa información. Y recordar todas las claves que haya establecido para sus cuentas online o para sus sitios Web favoritos no es una tarea fácil.

Por consiguiente, ¿hay alguna manera de asegurar que podamos encontrar nuestras contraseñas siempre que las necesitemos? ¿Y podamos descansar

tranquilos sabiendo que nuestras contraseñas secretas están siempre a salvo?

El Gestor de contraseñas le ayuda a controlar sus contraseñas, protege su privacidad y le proporciona una experiencia de navegación segura.

Utilizando una única contraseña maestra para acceder a sus credenciales, el Gestor de contraseñas le facilita mantener sus contraseñas a salvo en un Wallet.

Para ofrecer la mejor protección para sus actividades online, el Gestor de contraseñas se integra con Bitdefender Safepay™ y proporciona una solución única para las distintas formas en las que puede comprometerse su información privada.

El Gestor de contraseñas protege la siguiente información privada:

- Información personal, tal como la dirección de e-mail o el número de teléfono
- Credenciales de inicio de sesión en sitios Web
- Información de cuentas bancarias o números de tarjetas de crédito
- Datos de acceso a cuentas de correo
- Contraseñas para apps
- Contraseñas para las redes Wi-Fi

Crear una nueva base de datos de Wallet

El Wallet de Bitdefender es el lugar donde puede guardar sus datos personales. Para facilitar su experiencia de navegación, debe crear una base de datos de Wallet de la siguiente manera:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Crear nuevo wallet**.
3. Haga clic en **Crear nuevo**.
4. Introduzca la información requerida en los campos correspondientes.
   - Etiqueta de Wallet: escriba un nombre único para su base de datos de Wallet.
   - Contraseña maestra: introduzca una contraseña para su Wallet.

- Repetir contraseña: vuelva a escribir la contraseña que estableció.
- Pista: escriba una pista para recordar la contraseña.

5. Haga clic en **CONTINUAR**.
6. En este paso puede optar por almacenar su información en la nube. Si selecciona Sí, la información bancaria permanecerá almacenada localmente en su dispositivo. Elija la opción deseada y, a continuación, haga clic en **CONTINUAR**.
7. Seleccione el navegador Web desde el que desea importar las credenciales.
8. Haga clic en **FINALIZAR**.

Importar una base de datos existente

Para importar una base de datos de Wallet almacenada localmente:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Crear nuevo wallet**.
3. Haga clic en **DESDE OBJETIVO**.
4. Diríjase a la ubicación de su dispositivo donde desee guardar la base de datos de Wallet y, a continuación, elija un nombre para ella.
5. Haga clic en **Abrir**.
6. Otorgue un nombre a su Wallet y escriba la contraseña que se le asignó durante su creación inicial.
7. Haga clic en **IMPORTAR**.
8. Seleccione los programas desde los que desea que Wallet importe las credenciales y, a continuación, pulse el botón **FINALIZAR**.

Exportar la base de datos de Wallet

Para exportar la base de datos de su Wallet:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Mis wallets**.

3. Haga clic en el icono ⋮ del Wallet deseado y, a continuación, seleccione **Exportar**.
4. Busque la ubicación de su base de datos de Wallet y selecciónela (el archivo .db).
5. Haga clic en **Guardar**.

> **Nota**
> Para que la opción **Exportar** esté disponible, ha de estar abierto el Wallet. Si el Wallet que necesita exportar está bloqueado, haga clic en **ACTIVAR WALLET** y, a continuación, escriba la contraseña que se le asignó durante su creación inicial.

Sincronización de sus Wallets en la nube

Para activar o desactivar la sincronización de Wallets en la nube:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Mis wallets**.
3. Haga clic en el icono ⋮ del Wallet deseado y, a continuación, seleccione **Ajustes**.
4. Elija la opción que desee en la ventana que aparece y, a continuación, haga clic en **Guardar**.

> **Nota**
> Para que la opción **Exportar** esté disponible, ha de estar abierto el Wallet. Si el Wallet que necesita sincronizar está bloqueado, haga clic en **ACTIVAR WALLET** y, a continuación, escriba la contraseña que se le asignó durante su creación inicial.

Administrar sus credenciales de Wallet

Para administrar sus contraseñas:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Mis wallets**.

3. Seleccione la base de datos de Wallet deseada y, a continuación, haga clic en **ACTIVAR WALLET**.
4. Escriba la contraseña maestra y, a continuación, haga clic en **Aceptar**.

Aparecerá una nueva ventana. Seleccione la categoría deseada desde la parte superior de la ventana:

- Identidad
- Sitios Web
- Banca online
- Direcciones
- Apps
- Redes Wi-Fi

Añadir/Modificar las credenciales

- Para añadir una contraseña nueva, escoja arriba la categoría deseada, haga clic en **+ Añadir elemento**, inserte la información en los campos correspondientes y haga clic en el botón Guardar.
- Para editar un elemento de la tabla, selecciónelo y haga clic en el botón **Editar**.
- Para eliminar una entrada, selecciónela y haga clic en el botón **Eliminar**.

Activar o desactivar la protección del Gestor de contraseñas

Para activar o desactivar la protección del Gestor de contraseñas:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, active o desactive el conmutador.

Administración de los ajustes del Gestor de contraseñas

Para configurar en detalle la contraseña maestra:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Ajustes**.

3. Seleccione la pestaña **Ajustes de seguridad**.

Tiene las siguientes opciones a su disposición:

- **Pedir mi contraseña maestra cuando inicie sesión en mi dispositivo** - se le pedirá que escriba su contraseña maestra cuando acceda al dispositivo.
- **Pedir mi contraseña maestra cuando abra mi navegador y apps** - se le pedirá que escriba su contraseña maestra cuando acceda a un navegador o a una aplicación.
- **No pedir mi contraseña maestra**: No se le pedirá que escriba su contraseña maestra cuando acceda al equipo, a un navegador o a una app.
- **Bloquear automáticamente Wallet cuando deje mi dispositivo desatendido** - se le pedirá que escriba su contraseña maestra cuando vuelva a su dispositivo tras 15 minutos.

Importante
Asegúrese de recordar su contraseña maestra o guardar registro de ella en un lugar seguro. Si olvidó la contraseña, deberá reinstalar el programa o ponerse en contacto con Bitdefender para recibir ayuda.

Mejore su experiencia

Para seleccionar los navegadores o las aplicaciones donde quiera integrar el Gestor de contraseñas:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Plugins**.

   Marque una aplicación para usar el Gestor de contraseñas y mejorar su experiencia:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurar Autocompletar

La característica Autocompletar facilita conectar con sus sitios Web favoritos o iniciar sesión en sus cuentas online. La primera vez que introduzca sus credenciales de acceso e información personal en su navegador Web, se protegerán automáticamente en Wallet.

Para configurar las opciones de **Autocompletar**:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Configuración de autocompletar**.
4. Configure de las opciones siguientes:
   - **Configurar la forma en que el Gestor de contraseñas protege sus credenciales**:
     - **Guardar las credenciales automáticamente en Wallet** - las credenciales de inicio de sesión y otra información de identificación, como sus datos personales y de tarjetas de crédito, se guardan y actualizan automáticamente en Wallet.
     - **Preguntarme siempre** - se le preguntará cada vez que quiera añadir sus credenciales a Wallet.
     - **No guardar, actualizaré la información manualmente** - las credenciales pueden añadirse únicamente de forma manual en Wallet.
   - **Autocompletar credenciales de inicio de sesión**:
     - **Autocompletar credenciales de inicio de sesión siempre** - las credenciales se introducen automáticamente en el navegador.
   - **Autocompletar formularios**:
     - **Preguntar mis opciones de completado cuando visito una página con formularios** - aparecerá una ventana emergente con las opciones de completado cada vez que Bitdefender detecte que desea realizar un pago online o un registro.

Administrar la información del Gestor de contraseñas desde su navegador

Puede administrar fácilmente la información del Gestor de contraseñas directamente desde su navegador, para que tenga a mano todos sus datos importantes. El complemento Wallet de Bitdefender es compatible con los siguientes navegadores: Google Chrome, Internet Explorer y Mozilla Firefox, y también va integrado en Safepay.

Para acceder a la extensión Wallet de Bitdefender, abra su navegador Web, permita que se instale el complemento y haga clic en el icono de la barra de herramientas.

La extensión Wallet de Bitdefender contiene las siguientes opciones:

- Abrir Wallet - abre Wallet.
- Bloquear Wallet - bloquea Wallet.
- Páginas Web - abre un submenú con todos los inicios de sesión en sitios Web almacenados en Wallet. Haga clic en **Añadir página Web** para añadir nuevos sitios Web a la lista.
- Rellenar formularios - abre un submenú que contiene la información añadida por usted para una categoría determinada. Desde aquí puede añadir nuevos datos a su Wallet.
- Generador de contraseñas: le permite generar contraseñas aleatorias que puede utilizar para cuentas nuevas o existentes. Haga clic en **Mostrar ajustes avanzados** para personalizar la complejidad de la contraseña.
- Ajustes: abre la ventana de ajustes del Gestor de contraseñas.
- Informar de un problema: informe de cualquier problema que encuentre con el Gestor de contraseñas de Bitdefender.

4.12. VPN

Puede instalar la aplicación VPN desde su producto Bitdefender y usarla cada vez que desee añadir una capa más de protección a su conexión. 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 Bitdefender 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.

Instalación de VPN

Puede instalar la app VPN desde la interfaz de Bitdefender de la siguiente manera:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VPN**, haga clic en **Instalar VPN**.
3. En la ventana con la descripción de la app VPN, lea el **Acuerdo de suscripción** y, a continuación, haga clic en **INSTALAR BITDEFENDER VPN**.

   Espere unos momentos a que se descarguen e instalen los archivos.
4. Haga clic en **ABRIR BITDEFENDER VPN** para finalizar el proceso de instalación.

Nota
Bitdefender VPN requiere la instalación de .Net Framework 4.5.2 o superior. En caso de que no tenga instalado este paquete, aparecerá una ventana de notificación. Haga clic en **instalar .Net Framework** para que se le redirija a una página desde donde puede descargar la versión más reciente de este software.

Abrir VPN

Para acceder a la interfaz principal de Bitdefender VPN, utilice uno de los siguientes métodos:

- Desde el área de notificación

1. Haga clic con el botón derecho en el icono del área de notificación y, a continuación, haga clic en **Mostrar**.

- Desde la interfaz de Bitdefender:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VPN**, haga clic en **Abrir VPN**.

Interfaz de VPN

La interfaz de VPN muestra el estado de la app: conectada o desconectada. Para los usuarios con la versión gratuita, Bitdefender configura automáticamente la ubicación del servidor a la más apropiada, mientras que los usuarios premium tienen la posibilidad de cambiar la ubicación del servidor al que deseen conectarse. Para obtener más información sobre las suscripciones a VPN, consulte “Suscripciones” (p. 132).

Para conectarse o desconectarse, basta con hacer clic en el estado que se muestra en la parte superior de la pantalla o hacer clic con el botón derecho en el icono del área de notificación. El icono del área de notificación muestra una marca de verificación verde cuando la VPN está conectada y una roja cuando no lo está.

Mientras está conectado, el tiempo transcurrido y la dirección IP asignada automáticamente a su dispositivo se muestran en la parte inferior de la interfaz.

Para disponer de más opciones, acceda al **Menú** haciendo clic en el icono de la zona superior derecha. Aquí tiene las siguientes opciones:

- **Mi cuenta**: se muestran los detalles sobre su cuenta de Bitdefender y su suscripción a VPN. Haga clic en **Cambiar cuenta** si desea iniciar sesión con otra distinta.
- **Ajustes**: puede personalizar el comportamiento de su producto según sus necesidades:
  - Recibir notificaciones cuando la VPN se conecta o desconecta automáticamente.
  - ejecutar automáticamente la app VPN al inicio de Windows
  - iniciar automáticamente la app VPN cuando su dispositivo se conecte a redes inalámbricas inseguras

- **Actualizar a Premium**: si utiliza la versión gratuita, puede actualizar al plan premium desde aquí.
- **Soporte**: se le redirige a la plataforma de nuestro Centro de soporte, donde puede leer un artículo sobre cómo usar Bitdefender VPN.
- **Acerca de** : Muestra información acerca de la versión instalada.

Suscripciones

Bitdefender VPN ofrece gratuitamente una cuota de tráfico diaria de 200 MB por dispositivo para que proteja la conexión cuando su equipo lo necesite.

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

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento desde el panel Mis suscripciones disponible en su cuenta de Bitdefender.

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

Bitdefender VPN es un producto multiplataforma, disponible en 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.

4.13. Seguridad Safepay para las transacciones online

El PC se está convirtiendo rápidamente en la herramienta para compras y banca electrónica. Pagar facturas, transferir dinero, comprar prácticamente todo lo que pueda imaginar nunca ha sido más fácil y rápido.

Esto supone enviar información personal, de cuenta y datos de la tarjeta de crédito, contraseñas y otro tipo de información privada a través de Internet, en otras palabras, exactamente el tipo de información en la que los cibercriminales están interesados. Los hackers son implacables en sus

esfuerzos para robar esta información, por lo que nunca se es demasiado cuidadoso a la hora de proteger las transacciones en línea.

Bitdefender Safepay™ es sobre todo un navegador protegido, un entorno sellado que está diseñado para mantener privadas y seguras sus operaciones de banca online, compras online y cualquier otro tipo de transacción online.

Para la mejor protección de la privacidad, se ha integrado el Gestor de contraseñas de Bitdefender en Bitdefender Safepay™, con el fin de proteger sus credenciales siempre que desee acceder a ubicaciones privadas online. Para más información, diríjase a "*Protección del Gestor de contraseñas para sus credenciales*" (p. 122).

Bitdefender Safepay™ ofrece las siguientes opciones:

- Bloquea el acceso a su escritorio y cualquier intento de tomar capturas de su pantalla.
- Protege sus contraseñas secretas mientras navega por Internet con el Gestor de contraseñas.
- Viene con un teclado virtual que, cuando se utiliza, hace imposible a los hackers leer sus pulsaciones en el teclado.
- Es completamente independiente de sus otros navegadores.
- Viene con una función de protección de punto de acceso para cuando su equipo esté conectado a redes Wi-Fi no seguras.
- Acepta marcadores y le permite navegar entre sus sitios favoritos de banca y compras.
- No está limitado a banca electrónica y compras por Internet. Puede abrirse cualquier sitio Web en Bitdefender Safepay™.

Utilizar Bitdefender Safepay™

Por omisión, Bitdefender detecta cuando navega hacia una página de un banco online o a una tienda online en cualquier navegador de su equipo y le pide que la lance en Bitdefender Safepay™.

Para acceder a la interfaz principal de Bitdefender Safepay™, utilice uno de los siguientes métodos:

- Desde la interfaz de Bitdefender:
  1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.

2. En el panel **Safepay**, haga clic en **Abrir Safepay**.

- En Windows:
  - En **Windows 7**:
    1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
    2. Haga clic en **Bitdefender**.
    3. Haga clic en **Bitdefender Safepay™**.
  - En **Windows 8 y Windows 8.1**:

    Localice Bitdefender Safepay™ desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender Safepay" en la pantalla Inicio) y luego haga clic en el icono.
  - En **Windows 10**:

    Escriba "Bitdefender Safepay™" en el cuadro de búsqueda de la barra de tareas y haga clic en su icono.

Nota

Si el plugin Adobe Flash Player no está instalado o está obsoleto, se mostrará un mensaje de Bitdefender. Haga clic en el botón correspondiente para continuar

Una vez completado el proceso de instalación, tendrá que reabrir manualmente el navegador Bitdefender Safepay™ para continuar su trabajo.

Si está acostumbrado a los navegadores Web, no tendrá ningún problema utilizando Bitdefender Safepay™ - se parece y se comporta igual que cualquier navegador:

- introduzca las URLs a las que desea ir en la barra de direcciones.
- añada pestañas para visitar múltiples sitios Web en la ventana de Bitdefender Safepay™ haciendo clic en .
- navegue atrás y hacia delante y refresque las páginas usando respectivamente.
- acceda a los ajustes de Bitdefender Safepay™ haciendo clic en y seleccionando **Ajustes**.
- Proteja sus contraseña con el Gestor de contraseñas haciendo clic en .

- administre sus marcadores haciendo clic junto a la barra de dirección.
- abra el teclado virtual haciendo clic en .
- aumente o disminuya el tamaño del navegador pulsando simultáneamente **Ctrl** y las teclas **+/-** del teclado numérico.
- vea información sobre su producto Bitdefender haciendo clic en y eligiendo **Acerca de**.
- imprima la información importante haciendo clic .

Nota
Para cambiar entre el Escritorio de Windows y el de Bitdefender Safepay™, pulse las teclas **Alt+Tab** o haga clic en la opción **Cambiar a escritorio** de la esquina superior izquierda de la ventana.

Configuración de ajustes

Haga clic en y seleccione **Ajustes** para configurar Bitdefender Safepay™:

Lista de dominios

Elija cómo se comportará Bitdefender Safepay™ cuando visite sitios Web de dominios específicos en su navegador habitual añadiéndolos a la lista de dominios y seleccionando un comportamiento para cada uno:

- Abrir automáticamente en Bitdefender Safepay™.
- Hacer que Bitdefender le pregunte qué hacer cada vez.
- Nunca utilizar Bitdefender Safepay™ al visitar una página del dominio en un navegador habitual.

Bloqueo de ventanas emergentes

Puede decidir bloquear las ventanas emergentes haciendo clic en el conmutador.

También puede crear una lista de sitios Web en los que permitir las ventanas emergentes. La lista debería contener únicamente sitios Web en los que confíe plenamente.

Para añadir un sitio a la lista, escriba su dirección en el campo correspondiente y haga clic en **Añadir dominio**.

Para eliminar un sitio Web de la lista, seleccione la X correspondiente a la entrada deseada.

Administrar plugins
Puede elegir si desea habilitar o deshabilitar determinados plugins en Bitdefender Safepay™.

Administrar certificados
Puede importar certificados desde su sistema a un almacén de certificados.

Seleccione **Importar certificados** y siga el asistente para utilizar los certificados en Bitdefender Safepay™.

Iniciar automáticamente el Teclado virtual en los campos de contraseñas
Cuando seleccione un campo de contraseña, aparecerá automáticamente el teclado virtual.

Utilice el conmutador correspondiente para activar o desactivar la función.

Pedir confirmación antes de imprimir
Active esta opción si desea dar su confirmación antes de que comience el proceso de impresión.

Administración de marcadores

Si ha deshabilitado la detección automática para algunos o todos los sitios Web, o Bitdefender simplemente no detecta ciertas sitios Web, puede añadir marcadores a Bitdefender Safepay™ para poder abrir con facilidad sus sitios Web favoritos en el futuro.

Siga estos pasos para añadir una URL a los marcadores de Bitdefender Safepay™:

1. Haga clic en el icono junto a la barra de direcciones para abrir la página de marcadores.

   Nota
   La página de marcadores aparece abierta por omisión cuando inicia Bitdefender Safepay™.

2. Haga clic en el botón **+** para añadir un nuevo marcador.
3. Escriba la URL y el título del marcador y haga clic en **Crear**. Marque la opción **Abrir automáticamente los sitios Web en Safepay** si desea que la página marcada se abra con Bitdefender Safepay™ cada vez que acceda a ella. La URL también se añade a la lista de dominios en la página Ajustes.

Desactivar las notificaciones de Safepay

El producto Bitdefender está configurado para que le notifique, mediante una ventana emergente, cuando detecte un sitio de banca.

Para desactivar las notificaciones de Safepay:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **Safepay**, haga clic en **Ajustes**.
3. Desactivar las **notificaciones de Safepay**.

Uso de VPN con Safepay

Para realizar pagos online en un entorno seguro mientras está conectado a redes inseguras, el producto de Bitdefender puede configurarse para iniciar automáticamente la app VPN al mismo tiempo que Safepay.

Para usar la app VPN junto con Safepay:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **Safepay**, haga clic en **Ajustes**.
3. Active **Usar VPN con Safepay**.

4.14. Protección de datos

Eliminar archivos de forma permanente

Cuando elimina un archivo, no se podrá acceder a él como lo hace habitualmente. Sin embargo, el archivo continúa estando almacenado en su disco hasta que no se sobrescriba al copiar archivos nuevos.

El Destructor de archivos de Bitdefender le ayuda a borrar datos permanentemente mediante su eliminación física del disco duro.

Puede destruir rápidamente archivos y carpetas desde su equipo usando el menú contextual de Windows siguiendo estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente.

2. Seleccione **Bitdefender** > **Destructor de archivos** en el menú contextual que aparece.
3. Haga clic en **ELIMINAR PERMANENTEMENTE** y, a continuación, confirme que desea continuar con el proceso.

   Espere a que Bitdefender finalice la destrucción de archivos.
4. Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

Como alternativa, puede destruir los archivos desde la interfaz de Bitdefender de la siguiente manera:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PROTECCIÓN DE DATOS**, haga clic en **Destructor de archivos**.
3. Siga el asistente del Destructor de archivos:
   a. Haga clic en el botón **AÑADIR CARPETAS** para añadir los archivos o carpetas que desee eliminar de forma permanente.

      Como alternativa, arrastre los archivos o carpetas a esta ventana.
   b. Haga clic en **ELIMINAR PERMANENTEMENTE** y, a continuación, confirme que desea continuar con el proceso.

      Espere a que Bitdefender finalice la destrucción de archivos.
   c. **Resumen de resultados**

      Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

4.15. Antirrobo de Dispositivos

El robo de portátiles es un gran problema que afecta a particulares y empresas por igual. Más que perder el hardware en sí, la información que se pierde con él puede causar daños significativos, tanto financieros como emocionales.

Aún sólo unas pocas personas siguen los pasos adecuados para proteger su importante información personal, financiera y empresarial en caso de robo o pérdida.

Antirrobo de Bitdefender le ayuda a estar mejor preparado para un problema como este, permitiéndole localizar o bloquear remotamente su portátil e

incluso borrar toda la información que haya él si tuviera que desprenderse de su portátil contra su voluntad.

Para utilizar las características de Antirrobo, se deben cumplir los siguientes requisitos:

- Los comandos solo pueden enviarse desde la cuenta de Bitdefender.
- El portátil debe estar conectado a Internet para recibir los comandos.

Las características de Antirrobo funcionan de la siguiente manera:

Localizar

Vea la ubicación de su dispositivo en Google Maps.

La precisión de la ubicación depende de cómo Bitdefender sea capaz de determinarla. La ubicación se determina con una precisión de decenas de metros si el Wi-Fi está habilitado en su portátil y hay redes inalámbricas a su alcance.

Si el portátil está conectado a una red de cable LAN sin un punto Wi-Fi disponible, la ubicación se determinará basándose en la dirección IP, que es considerablemente menos precisa.

Alerta

Envíe una alerta remota al dispositivo.

Esta característica solo está disponible en dispositivos móviles.

Bloquear

Bloquee su portátil y establezca un PIN de cuatro dígitos para desbloquearlo. Cuando envía el comando **Bloquear**, se reinicia el sistema y solo es posible volver a iniciar sesión en Windows tras introducir el PIN que ha establecido.

Si desea que Bitdefender tome fotos de la persona que intenta acceder a su portátil, marque la casilla de verificación correspondiente. Las instantáneas se realizan mediante la cámara frontal y se muestran junto a su fecha y hora en el panel de control de Antirrobo. Solo se guardarán las dos últimas fotos.

Esta acción solo está disponible en portátiles que posean una cámara frontal.

Borrar
Elimine toda la información de su sistema. Cuando envía el comando **Borrar**, se reinicia el portátil y se borra la información de todas las particiones del disco duro.

Mostrar IP
Muestra la última dirección IP del dispositivo seleccionado. Haga clic en **MOSTRAR IP** para que se vea.

Antirrobo se activa después de la instalación y puede accederse a él exclusivamente a través de su cuenta en Bitdefender desde cualquier dispositivo conectado a Internet, en cualquier parte.

Usar las características Antirrobo

Para acceder a las características Antirrobo, haga uso de una de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender:
  1. Haga clic en **Utilidades** en el menú de navegación de la interfaz de Bitdefender.
  2. Haga clic en **EXPLORAR ANTIRROBO**.
  3. En la ventana de Bitdefender Central que se abre, haga clic en la tarjeta del dispositivo deseado y, a continuación, seleccione **Antirrobo**.
- En cualquier dispositivo con acceso a internet:
  1. Abra un navegador Web y acceda a: https://central.bitdefender.com.
  2. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.
  3. Seleccione el panel **Mis dispositivos**.
  4. Haga clic en la tarjeta del dispositivo deseado y, a continuación, seleccione **Antirrobo**.
  5. Seleccione la característica que desea usar:

     Mostrar IP - Muestra la última dirección IP de su dispositivo.
     Localizar - muestra la ubicación de su dispositivo en Google Maps.
     Alerta: envía una alerta al dispositivo.

Bloquear - Bloquea su portátil y establece un código PIN para desbloquearlo.

Borrar - Borra todos los datos de su portátil.

Importante
Después de borrar un dispositivo, todas las características de Antirrobo dejan de funcionar.

4.16. Bitdefender USB Immunizer

La opción de Autorun integrada en el sistema operativo Windows es una herramienta muy útil que permite a los equipos ejecutar automáticamente un archivo de un medio conectado a él. Por ejemplo, las instalaciones de software pueden comenzar automáticamente cuando se inserta un CD en la unidad óptica.

Desgraciadamente, esta opción pueden también utilizarla las amenazas para ejecutarse automáticamente e infiltrarse en su equipo desde un medio reescribible como una unidad flash USB y tarjetas conectadas mediante lectores de tarjetas. En los últimos años se han producido numerosos ataques basados en la autoejecución.

Con el inmunizador USB puede evitar que ninguna unidad flash formateada con NTFS, FAT32 o FAT vuelva a ejecutar amenazas nunca más. Una vez que el dispositivo USB está inmunizado, las amenazas no pueden volver a configurarlo para ejecutar cierta aplicación cuando el dispositivo se conecte a un equipo con Windows.

Para inmunizar un dispositivo USB:

1. Conecte la unidad flash a su equipo.
2. Examine su equipo para localizar el dispositivo de almacenamiento extraíble y haga clic con el botón derecho en su icono.
3. En el menú contextual, escoja **Bitdefender** y seleccione **Inmunizar esta unidad**.

Nota
Si la unidad ya se inmunizó, aparecerá el mensaje **El dispositivo USB está protegido contra amenazas de?ejecución automática** en vez de la opción Inmunizar.

Para evitar que su equipo ejecute amenazas desde dispositivos USB no inmunizados, desactive la opción de autoarranque del dispositivo. Para más información, diríjase a "*Usar el control automático de la vulnerabilidad*" (p. 104).

5. OPTIMIZACIÓN DEL SISTEMA

5.1. Utilidades

Bitdefender incluye una sección de Utilidades que le ayuda a mantener la integridad de su sistema. Las herramientas de mantenimiento que se ofrecen son muy importantes para mejorar el rendimiento de su sistema y administrar eficientemente el espacio de los discos duros.

Bitdefender proporciona las siguientes herramientas de optimización para el PC:

- Optimizador en un clic analiza y mejora la velocidad de su sistema ejecutando múltiples tareas con solo hacer clic en un botón.
- El Optimizador de inicio reduce el tiempo de inicio del sistema al evitar la carga de las aplicaciones innecesarias cuando arranca el equipo.
- La Limpieza de disco identifica los archivos que pueden ser los principales culpables de la escasez de espacio en el disco, lo que le brinda la posibilidad de decidir si conservarlos o no.

5.1.1. Optimizar la velocidad de su sistema con un solo clic

Problemas como los fallos de disco duro, archivos inútiles en el registro y el historial del navegador, pueden ralentizar el trabajo de su equipo, hasta el punto de resultarle molesto. Todo esto se puede solucionar ahora con solo hacer clic en un botón.

El Optimizador en un clic le permite identificar y eliminar archivos inútiles mediante la ejecución de múltiples tareas de limpieza simultáneas.

Para iniciar el proceso del Optimizador en un clic:

1. Haga clic en **Utilidades** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **OPTIMIZAR MI DISPOSITIVO**.
   a. **Analizando**

      Espere a que Bitdefender termine la búsqueda de problemas en el sistema.

      - Limpieza de disco: Identifica las carpetas y archivos innecesarios.

- Limpieza del registro - identifica entradas obsoletas o no válidas en el registro de Windows.
- Limpieza de datos privados - identifica los archivos temporales de Internet y cookies, caché del navegador e historial.

Se muestra el número de problemas encontrados. Haga clic en el enlace **Ver detalles** para revisarlos antes de continuar con el proceso de limpieza. Haga clic en **OPTIMIZAR** para continuar.

b. **Optimización**

Espere a que Bitdefender termine de optimizar su sistema.

c. **Incidencias**

Aquí es donde puede ver el resultado de la operación.

Si desea información completa sobre el proceso de optimización, haga clic en el botón **VER INFORME DETALLADO**.

5.1.2. Optimización del tiempo de arranque de su PC

La prolongación del tiempo de arranque del sistema es un problema real debido a que hay aplicaciones configuradas para ejecutarse sin que sean necesarias. Esperar varios minutos a que arranque su sistema puede costarle un tiempo y productividad valiosos.

La ventana del Optimizador de inicio muestra qué aplicaciones se ejecutan durante el inicio del sistema y le permite administrar su comportamiento en este punto.

Para ejecutar el proceso del Optimizador de inicio:

1. Haga clic en **Utilidades** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **OPTIMIZAR EL ARRANQUE DEL DISPOSITIVO**.

a. **Seleccione las aplicaciones**

Puede ver una lista de las aplicaciones que se ejecutan al arrancar el sistema. Seleccione las que desea bloquear o retrasar en el inicio.

b. **Elección de la comunidad**

Vea lo que otros usuarios de Bitdefender han decidido hacer con la aplicación que ha seleccionado.

c. **Hora de arranque del sistema**

Fíjese en el control deslizante de la parte superior de la ventana para ver el tiempo de ejecución en el arranque requerido tanto por su sistema como por las aplicaciones seleccionadas.

Es necesario reiniciar el sistema para poder recopilar la información sobre el tiempo de arranque del sistema y de las aplicaciones.

d. **Estado de arranque**

- **Activar.** Seleccione esta opción cuando desee que una aplicación empiece a ejecutarse en el arranque del sistema. Esta opción está activada por omisión.
- **Posponer.** Seleccione esta opción para posponer la ejecución de un programa en el arranque del sistema. Esto significa que las aplicaciones seleccionadas se ejecutarán con un retraso de cinco minutos después de que el usuario inicie sesión en el sistema. La funcionalidad **Posponer** está predefinida y no la puede configurar el usuario.
- **Desactivar.** Seleccione esta opción para desactivar un programa que se ejecute en el arranque del sistema.

e. **Resultados**

Se muestra información como el tiempo estimado de arranque del sistema después de posponer o desactivar los programas.

Puede que sea necesario reiniciar el sistema para poder ver toda esta información.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Nota
En caso de que su suscripción haya caducado o decida desinstalar Bitdefender, los programas cuyo arranque decidiera posponer en el inicio se restaurarán a sus valores de arranque por defecto.

5.1.3. Optimizar su disco

Las carpetas y archivos innecesarios que consumen espacio en su disco pueden conducir a la ralentización del sistema. Por lo tanto, es recomendable que realice limpiezas periódicamente para mejorar la velocidad de su sistema.

Limpieza de disco de Bitdefender le ayuda a optimizar fácilmente su espacio en el disco identificando los archivos que pueden ser los principales culpables de la escasez de espacio en el disco. Además, tiene la posibilidad de decidir qué hacer con los archivos identificados.

Para empezar a limpiar su sistema:

1. Haga clic en **Utilidades** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **LIMPIAR MI DISPOSITIVO**.
3. La primera vez que accede a la Limpieza de disco, se le presenta esta característica. Haga clic en **BIEN, ENTENDIDO** para continuar.
   a. **Unidades y dispositivos**

      Puede ver una lista de los discos disponibles. Además de los discos de Windows, se analizan y se muestran en la lista los discos duros externos y los dispositivos USB. Haga clic en **ANALIZAR UNIDAD** en el apartado del disco que desee limpiar.

   b. **Analizando la unidad**

      Se analiza la unidad seleccionada. Espere a que Bitdefender termine la búsqueda de carpetas y archivos grandes.

   c. **Incidencias**

      Aquí es donde puede ver los resultados de la operación. Para seleccionar en qué orden deben mostrarse los resultados, use la flecha desplegable **ORDENAR POR** ubicada en el lado izquierdo de la ventana. Puede ordenar los resultados por tamaño (de 10 MB a más de 5 GB) o por tipo (los archivos se ordenan en carpetas separadas por sus extensiones).

      Seleccione los archivos que desea eliminar y luego haga clic en **CONFIRMAR SELECCIÓN** para comenzar el proceso de borrado.

      Se identifican también los archivos importantes y protegidos responsables del funcionamiento de su sistema, pero no se pueden seleccionar ni eliminar.

      Haga clic en el icono para tener acceso a las carpetas correspondientes a los archivos seleccionados.

   d. **Confirme su selección**

Se muestra la lista con los archivos seleccionados. Mire la lista y asegúrese de que realmente ya no necesita esos archivos, dado que una vez que continúe no se podrán recuperar de la papelera de reciclaje. Confirme su elección haciendo clic en **ELIMINAR**.

e. **Resumen de resultados**

El estado del proceso se muestra de la siguiente manera:

Se eliminaron todos los archivos seleccionados.
No fue posible eliminar uno o varios de los archivos seleccionados **o** no fue posible eliminar ninguno de los archivos seleccionados.

Haga clic en **Finalizar** para cerrar la ventana.

5.2. Perfiles

Las actividades de trabajo diarias, ver películas o utilizar juegos pueden provocar que el sistema se ralentice, especialmente si se están ejecutando de manera simultánea con los procesos de actualización de Windows y las tareas de mantenimiento. Con Bitdefender, ahora puede elegir y aplicar su perfil preferido, lo que lleva a cabo los ajustes del sistema adecuados para aumentar el rendimiento de las aplicaciones específicas instaladas.

Bitdefender ofrece los siguientes perfiles:

- Perfil de Trabajo
- Perfil de Películas
- Perfil de Juego
- Perfil de redes Wi-Fi públicas
- Perfil del modo Batería

Si decide no utilizar los **Perfiles**, se activa un perfil por defecto denominado **Estándar** que no aporta optimización a su sistema.

Según su actividad, se aplican los siguientes ajustes del producto cuando se activa el perfil de trabajo, juego o ver películas:

- Todas las alertas y ventanas emergentes de Bitdefender quedan desactivadas.
- Se pospone la actualización automática.
- Se posponen los análisis programados.

- Se deshabilita el Asesor de búsquedas.
- Las notificaciones de ofertas especiales están desactivadas.

Según su actividad, se aplican los siguientes ajustes del sistema cuando se activa el perfil de trabajo, juego o ver películas:

- Se posponen las actualizaciones automáticas de Windows.
- Se deshabilitan las ventanas emergentes y alertas de Windows.
- Se suspenden los programas innecesarios en segundo plano.
- Se ajustan los efectos visuales para un mejor rendimiento.
- Se posponen las tareas de mantenimiento.
- Se ajusta la configuración del plan de energía.

Al trabajar bajo el perfil de redes Wi-Fi públicas, Bitdefender Total Security se configura automáticamente para reflejar los siguientes ajustes del programa:

- Se activa Defensa Contra Amenazas Avanzadas
- El cortafuego de Bitdefender está activado y se aplican los siguientes ajustes a su adaptador inalámbrico:
  - Modo oculto - ACTIVADO
  - Tipo de red: Pública
- Se activan los siguientes ajustes de la Prevención de amenazas online:
  - Análisis de sitios web cifrados
  - Protección contra fraude
  - Protección contra phishing

5.2.1. Perfil de Trabajo

La ejecución de varias tareas en el trabajo, como el envío de mensajes de correo electrónico, mantener una videoconferencia con sus compañeros o trabajar con aplicaciones de diseño puede afectar al rendimiento del sistema. El Perfil de trabajo se ha diseñado para ayudarle a mejorar su eficiencia en el trabajo, desactivando algunos de sus servicios en segundo plano y tareas de mantenimiento.

Configuración del Perfil de trabajo

Para configurar las acciones a llevar a cabo en el Perfil de trabajo:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.
4. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en aplicaciones de trabajo
   - Optimizar los ajustes del producto para el perfil de Trabajo
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
5. Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Añadir aplicaciones manualmente a la lista del Perfil de trabajo

Si Bitdefender no entra automáticamente en el Perfil de trabajo cuando ejecute cierta app de trabajo, puede añadirla manualmente a la **Lista de aplicaciones de trabajo**.

Para añadir apps manualmente a la Lista de aplicaciones de trabajo en el Perfil de trabajo:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.
4. En la ventana **Ajustes del perfil de trabajo**, haga clic en **Lista de aplicaciones**.
5. Haga clic en **AÑADIR**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

5.2.2. Perfil de Películas

Mostrar vídeo de alta calidad, como por ejemplo películas de alta definición, requiere unos recursos del sistema significativos. El Perfil de películas ajusta la configuración del sistema y del producto para que pueda disfrutar de una experiencia cinematográfica óptima y sin interrupciones.

Configuración del Perfil de películas

Para configurar las acciones a llevar a cabo en el Perfil de películas:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
4. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en reproductores de vídeo
   - Optimizar los ajustes del producto para el perfil de Películas
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para películas
5. Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Añadir reproductores de vídeo manualmente a la lista del Perfil de películas

Si Bitdefender no entra automáticamente en el Perfil de películas cuando ejecute cierta app de reproducción de vídeo, puede añadirla manualmente a la **Lista de aplicaciones de películas**.

Para añadir reproductores de vídeo manualmente a la Lista de aplicaciones de películas en el Perfil de películas:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.

3. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
4. En la ventana **Ajustes del perfil de películas**, haga clic en **Lista de reproductores**.
5. Haga clic en **AÑADIR**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

5.2.3. Perfil de Juego

Disfrutar de una experiencia de juego ininterrumpido supone reducir la carga del sistema y disminuir cualquier posible retraso. Recurriendo a la heurística de comportamientos y a una lista de juegos conocidos, Bitdefender puede detectar automáticamente los juegos que se ejecuten y optimizar los recursos del sistema para que pueda disfrutar de su pausa para jugar.

Configuración del Perfil de juego

Para configurar las acciones que desea llevar a cabo en el Perfil de juego:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
4. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en los juegos
   - Optimizar los ajustes del producto para el perfil de Juego
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para juegos
5. Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Añadir juegos manualmente a la Lista de Juegos

Si Bitdefender no entra automáticamente en el Perfil de juego cuando ejecute cierto juego o app, puede añadirlo manualmente a la **Lista de aplicaciones de juego**.

Para añadir juegos manualmente a la Lista de aplicaciones de juego en el Perfil de juego:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
4. En la ventana **Ajustes del perfil de juego**, haga clic en **Lista de juegos**.
5. Haga clic en **AÑADIR**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable del juego, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

5.2.4. Perfil de redes Wi-Fi públicas

Enviar correos electrónicos, escribir credenciales confidenciales o efectuar compras online mientras se está conectado a redes inalámbricas poco fiables puede poner en riesgo sus datos personales. El perfil de redes Wi-Fi públicas adapta los ajustes del producto para darle la posibilidad de realizar pagos online y hacer uso de información confidencial en un entorno protegido.

Configuración del perfil de redes Wi-Fi públicas

Para configurar Bitdefender de forma que aplique los ajustes del producto mientras está conectado a una red inalámbrica poco fiable:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del perfil de redes Wi-Fi públicas.

4. Deje marcada la casilla de verificación **Adapta los ajustes del producto para aumentar la protección cuando se conecta a una red Wi-Fi pública poco fiable**.
5. Haga clic en **Guardar**.

5.2.5. Perfil del modo Batería

El perfil del modo Batería está especialmente diseñado para usuarios de portátiles y tablets. Su objetivo es reducir al mínimo tanto el impacto del sistema como de Bitdefender en el consumo de energía cuando el nivel de carga de la batería esté por debajo del establecido por omisión o del que usted determine.

Configuración del perfil del modo Batería

Para configurar el perfil del modo Batería:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del perfil del modo Batería.
4. Elija los ajustes del sistema a aplicar marcando las siguientes opciones:
   - Optimizar los ajustes del producto para el modo Batería.
   - Posponer los programas en segundo plano y las tareas de mantenimiento.
   - Posponga las actualizaciones automáticas de Windows.
   - Adaptar los ajustes del plan de energía para el modo Batería.
   - Deshabilitar los dispositivos externos y los puertos de red.
5. Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Escriba un valor válido en el cuadro de número o selecciónelo con las teclas de flecha arriba y abajo para especificar cuándo debe empezar a funcionar el sistema en modo Batería. Por defecto, el modo se activa cuando el nivel de carga de la batería cae por debajo del 30%.

Cuando Bitdefender opera en el perfil del modo Batería, se aplican los siguientes ajustes del producto:

- Se pospone la actualización automática de Bitdefender.

- Se posponen los análisis programados.
- Se desactiva el Widget de seguridad.

Bitdefender detecta cuándo su portátil pasa a la alimentación con batería y, en función del nivel de carga de ésta, entra automáticamente en modo Batería. De la misma forma, Bitdefender sale automáticamente del modo Batería cuando detecta que el portátil ya no está siendo alimentado con la batería.

5.2.6. Optimización en tiempo real

La Optimización en tiempo real de Bitdefender es un plugin que mejora el rendimiento de su sistema discretamente, en segundo plano, asegurándose de que no se vea interrumpido mientras esté en un modo de perfil. Dependiendo de la carga de la CPU, el plugin monitoriza todos los procesos, centrándose en los que suponen una carga mayor, para adaptarlos a sus necesidades.

Para activar o desactivar la Optimización en tiempo real:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Desplácese hacia abajo hasta ver la opción de Optimización en tiempo real y, a continuación, utilice el conmutador correspondiente para activarla o desactivarla.

6. RESOLUCIÓN DE PROBLEMAS

6.1. Resolución de incidencias comunes

Este capítulo presenta algunos problema que puede encontrar cuando utiliza Bitdefender y le proporciona las posibles soluciones para estos problemas. La mayoría de estos problemas pueden ser resueltos a través de la configuración apropiada de los ajustes del producto.

- "*Mi sistema parece que se ejecuta lento*" (p. 155)
- "*El análisis no se inicia*" (p. 157)
- "*Ya no puedo usar una app*" (p. 159)
- "*Qué hacer cuando Bitdefender bloquea un sitio Web seguro o una aplicación online*" (p. 160)
- "*Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware*" (p. 161)
- "*Cómo actualizo Bitdefender en una conexión de internet lenta*" (p. 165)
- "*Los servicios de Bitdefender no responden*" (p. 165)
- "*El Filtro antispam no funciona correctamente*" (p. 166)
- "*El Autorrellenado de mi Wallet no funciona*" (p. 171)
- "*La desinstalación de Bitdefender ha fallado*" (p. 172)
- "*Mi sistema no se inicia tras la instalación de Bitdefender*" (p. 173)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Pedir ayuda*" (p. 286).

6.1.1. Mi sistema parece que se ejecuta lento

Normalmente, después de instalar un software de seguridad, puede aparecer una ligera ralentización del sistema, lo cual en cierto punto es normal.

Si nota una lentitud significativa, esta incidencia puede aparecer por las siguientes razones:

- **Bitdefender no es solo un programa de seguridad instalado en el sistema.**

Aunque Bitdefender busca y elimina los programas de seguridad encontrados durante la instalación, se recomienda eliminar cualquier otra solución de seguridad que pueda usar antes de instalar Bitdefender. Para más información, diríjase a "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 58).

- **No se cumplen los requisitos mínimos del sistema para ejecutar Bitdefender.**

  Si su PC no cumple con los requisitos mínimos del sistema, el equipo se ralentiza, especialmente cuando se ejecutan múltiples aplicaciones al mismo tiempo. Para más información, diríjase a "Requisitos mínimos del sistema" (p. 3).

- **Ha instalado apps que no utiliza**.

  Cualquier equipo tiene programas o apps que no utiliza. Y muchos programas no deseados se ejecutan en segundo plano ocupando espacio en disco y memoria. Si no utiliza un programa, desinstálelo. Esto también vale para otro software preinstalado o aplicación de evaluación que olvidó desinstalar.

  ! **Importante**
  Si sospecha que un programa o una aplicación forma parte esencial de su sistema operativo, no lo elimine y contacte con el departamento de Atención al cliente de Bitdefender para recibir asistencia.

- **Su sistema puede estar infectado**.

  La velocidad de su sistema y su comportamiento general también pueden verse afectados por las amenazas. Spyware, malware, troyanos y adware pasan todos factura al rendimiento de su equipo. Asegúrese de que puede analizar su sistema periódicamente, al menos una vez a la semana. Se recomienda utilizar el análisis de sistema Bitdefender porque analiza todo los tipos de amenazas que ponen en peligro la seguridad de su sistema.

  Para iniciar el análisis del sistema:

  1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
  2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
  3. Siga los pasos del asistente.

6.1.2. El análisis no se inicia

Este tipo de incidencia puede tener dos causas principales:

- **Una instalación anterior de Bitdefender la cual no fue desinstalada completamente o es una instalación Bitdefender defectuoso**.

  En este caso, reinstale Bitdefender:

  - En **Windows 7**:

    1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
    2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
    3. Haga clic en **REINSTALAR** en la ventana que aparece.
    4. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.

  - En **Windows 8 y Windows 8.1**:

    1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
    2. Haga clic en **Desinstalar un programa** o **Programas y características**.
    3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
    4. Haga clic en **REINSTALAR** en la ventana que aparece.
    5. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.

  - En **Windows 10**:

    1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
    2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
    3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
    4. Haga clic en **Desinstalar** para confirmar su elección.
    5. Haga clic en **REINSTALAR** en la ventana que aparece.
    6. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.

Nota
Siguiendo este procedimiento de reinstalación, se guardan los ajustes personalizados para que estén disponibles en el nuevo producto instalado. Puede que otros ajustes vuelvan a su valor por defecto.

- **Bitdefender no es solo una solución de seguridad instalada en su sistema**.

  En este caso:

  1. Eliminar las otras soluciones de seguridad. Para más información, diríjase a "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 58).
  2. Reinstalar Bitdefender:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
       c. Haga clic en **REINSTALAR** en la ventana que aparece.
       d. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
       d. Haga clic en **REINSTALAR** en la ventana que aparece.
       e. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
     - En **Windows 10**:
       a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
       b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
       c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.

d. Haga clic en **Desinstalar** para confirmar su elección.

e. Haga clic en **REINSTALAR** en la ventana que aparece.

f. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.

Nota
Siguiendo este procedimiento de reinstalación, se guardan los ajustes personalizados para que estén disponibles en el nuevo producto instalado. Puede que otros ajustes vuelvan a su valor por defecto.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.3. Ya no puedo usar una app

Esta incidencia ocurre cuando está intentado utilizar un programa el cual estaba trabajando de forma normal antes de instalar Bitdefender.

Tras instalar Bitdefender puede encontrarse con una de estas situaciones:

- Puede recibir un mensaje de Bitdefender que el programa está intentando realizar una modificación en el sistema.
- Puede recibir un mensaje de error del programa que intentando usar.

Este tipo de situación se produce cuando Defensa Contra Amenazas Avanzadas identifica erróneamente ciertas aplicaciones como maliciosas.

Defensa Contra Amenazas Avanzadas es una característica de Bitdefender que monitoriza constantemente las aplicaciones que se ejecutan en su sistema e informa de las que exhiben comportamientos potencialmente maliciosos. Dado que esta característica se basa en un sistema heurístico, pueden darse casos en los que Defensa Contra Amenazas Avanzadas informe sobre aplicaciones legítimas.

Si se produce esta situación, puede evitar que Advanced Threat Defense monitorice la app correspondiente.

Para añadir el programa a la lista de excepciones:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ADVANCED THREAT DEFENSE**, haga clic en **Ajustes**.

3. En la ventana **Excepciones**, haga clic en **Añadir aplicaciones a la lista blanca**.
4. Busque y seleccione la app que desea exceptuar y, a continuación, haga clic en **ACEPTAR**.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.4. Qué hacer cuando Bitdefender bloquea un sitio Web seguro o una aplicación online

Bitdefender ofrece una experiencia de navegación Web segura filtrando todo el tráfico de Internet y bloqueando cualquier contenido malicioso. No obstante, es posible que Bitdefender considere peligrosa una aplicación online o un sitio Web seguros, lo que hará que el análisis de tráfico HTTP de Bitdefender los bloquee erróneamente.

En caso de que la misma página o app se bloqueen en repetidas ocasiones, se pueden añadir a las excepciones para que los motores de Bitdefender no las analicen, lo que garantiza una navegación web sin problemas.

Para añadir un sitio web a las **Excepciones**:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Excepciones**.
3. Proporcione la dirección del sitio web o app online bloqueada en el campo correspondiente y haga clic en **AÑADIR**.
4. Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Solo debe añadir a esta lista aplicaciones y sitios Web en los que confíe plenamente. Estos se exceptuarán del análisis por parte de los siguientes motores: amenazas, phishing y fraude.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.5. Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Para mantener su sistema a salvo de situaciones desafortunadas, Bitdefender le da la posibilidad de proteger sus archivos personales.

Cuando una aplicación intente cambiar o eliminar alguno de sus archivos protegidos, se considerará poco fiable y Bitdefender bloqueará su funcionamiento.

En caso de que se añada alguna app a la lista de apps que no son de fiar y que esté seguro de que no hay problema en usarla, siga estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Acceso de las aplicaciones**.
3. Aparecen las apps que hayan solicitado cambiar archivos de sus carpetas protegidas. Haga clic en el conmutador **Permitir** junto a la app que considera segura.

6.1.6. No me puedo conectar a Internet

Tras instalar Bitdefender, quizás note que algún programa o navegador Web ya no pueden conectarse a Internet o acceder a servicios de red.

En este caso, la mejor solución es configurar Bitdefender para permitir automáticamente las conexiones hacia y desde la aplicación de software correspondiente:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.
3. En la ventana de **Reglas**, haga clic en **Añadir regla**.
4. Aparece una nueva ventana en la que puede añadir los detalles. Asegúrese de seleccionar todos los tipos de red disponibles y, en la sección de **Permiso**, seleccione **Permitir**.

Cierre Bitdefender, abra la aplicación de software y vuelva a intentar conectarse a internet.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.7. No puedo acceder a un dispositivo en mi red

Dependiendo de la red en la que esté conectado, el cortafuego de Bitdefender puede bloquear la conexión entre su sistema y otro dispositivo (como otro equipo o una impresora). En consecuencia es posible que no pueda compartir o imprimir archivos.

En este caso, la mejor solución es configurar Bitdefender para permitir automáticamente las conexiones desde y hacia el dispositivo correspondiente de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.
3. En la ventana de **Reglas**, haga clic en **Añadir regla**.
4. En la ventana **Ajustes**, active la opción **Aplicar esta regla a todas las aplicaciones**.
5. Haga clic en la pestaña **Avanzado**.
6. En el cuadro **Dirección remota personalizada**, escriba la dirección IP del equipo o la impresora a la que desea tener acceso sin restricciones.

Si todavía no puede conectarse al dispositivo, Bitdefender no puede ser el causante de su problema.

Comprobar otras causas potenciales, como las siguientes:

- El cortafuego en otro equipo puede bloquear los archivos e impresoras compartidos con su equipo.
  - Si se está utilizando Firewall de Windows, puede configurarse para que permita compartir archivos e impresoras de la siguiente forma:
    - En **Windows 7**:
      1. Haga clic en **Inicio**, vaya al **Panel de control** y seleccione **Sistema y seguridad**.
      2. Vaya a **Windows Firewall** y haga clic en **Permitir un programa a través de Firewall de Windows**.
      3. Marque la casilla de verificación **Compartir archivos e impresoras**.

- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Sistema y seguridad**, vaya a **Windows Firewall** y seleccione **Permitir una app a través de Firewall de Windows**.
  3. Marque la casilla de verificación **Compartir archivos e impresoras** y haga clic en **Aceptar**.
- En **Windows 10**:
  1. Escriba "Permitir una aplicación a través de Firewall de Windows" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
  2. Haga clic en **Cambiar configuración**.
  3. En la lista **Aplicaciones y características permitidas**, marque la casilla de verificación **Compartir archivos e impresoras** y haga clic en **Aceptar**.
- Si utiliza otro programa de cortafuego, por favor, consulte su documentación o archivo de ayuda.

- Condiciones generales que pueden impedir el uso o la conexión a la impresora compartida:
  - Puede necesitar iniciar sesión con una cuenta de Administrador de Windows para acceder a la impresora compartida.
  - Se establecen los permisos para permitir el acceso a la impresora compartida a los equipos y a los usuarios solamente. Si esta compartiendo su impresora, compruebe los permisos establecidos para esta impresora para ver si el usuario de otro equipo tiene permitido el acceso a la impresora. Si esta intentando conectarse a una impresora compartida, compruebe con el usuario del otro equipo si tiene permisos para conectarse a la impresora.
  - La impresora conectada a su equipo o a otro equipo no está compartida.
  - La impresora compartida no está agregada en el equipo.

> **Nota**
> Para aprender como administrar una impresora compartida (compartir una impresora, establecer o eliminar permisos para una impresora, conectar una impresora de red o compartir impresora), diríjase a la Ayuda de Windows y Centro de Soporte (en el menú Inició, haga clic en **Ayuda y soporte técnico**).

- El acceso a la impresora de la red puede estar restringido a equipo e usuarios solamente. Debería comprobar con el administrador de red si tiene permisos para conectarse con esta impresora.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.8. Mi conexión a Internet es lenta

Esta situación puede aparecer después de instalar Bitdefender. La incidencia puede ser causada por errores en la configuración del cortafuego de Bitdefender.

Para resolver esta situación:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, desactive el conmutador para desactivar la característica.
3. Compruebe si su conexión a Internet ha mejorado al deshabilitar el cortafuego de Bitdefender.
   - Si tiene una conexión a Internet lenta, el problema puede que no esté causado por Bitdefender. Debe contactar con su Proveedor de Servicios de Internet para verificar si la conexión funciona correctamente.

     Si recibe una confirmación de su Proveedor de Servicios de Internet que la conexión está activa y la incidencia continua, contacto con Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).
   - Si tras desactivar el cortafuego de Bitdefender la conexión a Internet mejora:
     a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
     b. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.

c. Acceda a la pestaña **Adaptadores de red** y establezca su conexión a Internet en **Hogar/Oficina**.

d. En la pestaña **Ajustes**, desactive la **Protección del análisis de puertos**.

En la zona **Modo oculto**, haga clic en **Editar los ajustes de invisibilidad**. Active el modo Oculto para el adaptador de red al que está conectado.

e. Cierre Bitdefender, reinicie el sistema y compruebe la velocidad de conexión a Internet.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.9. Cómo actualizo Bitdefender en una conexión de internet lenta

Si tiene una conexión a Internet lenta (tales como acceso telefónico), pueden ocurrir errores durante el proceso de actualización.

Para mantener su sistema actualizado con la última base de datos de información de amenazas de Bitdefender:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar**.
3. Desactive el conmutador de **Actualización silenciosa**.
4. La próxima vez que haya una actualización disponible, se le pedirá que seleccione la actualización que desea descargar. Seleccione solo **Actualización de firmas**.
5. Bitdefender descargará e instalará solo la base de datos de información de amenazas.

6.1.10. Los servicios de Bitdefender no responden

Este artículo le ayuda a solucionar problemas del error de **Los servicios de Bitdefender no responden**. Puede encontrar este error de la siguiente manera:

- El icono Bitdefender del área de notificación está en gris y se le informa de que los servicios de Bitdefender no responden.

- La ventana de Bitdefender le indica que los servicios de Bitdefender no responden.

El error puede ser causado por una de las siguientes condiciones:

- Errores temporales de comunicación entre los servicios de Bitdefender.
- algunos de los servicios de Bitdefender están detenidos.
- otras soluciones de seguridad se están ejecutando en su equipo al mismo tiempo que Bitdefender.

Para solucionar este problema, pruebe estas soluciones:

1. Espere unos momentos y mire si algo cambia. El error puede ser temporal.
2. Reinicie el equipo y espere unos momentos a que Bitdefender se inicie. Abra Bitdefender para ver si el error continua. Reiniciando el equipo normalmente soluciona el problema.
3. Compruebe si tiene alguna otra solución de seguridad instalada porque esta puede perturbar la ejecución normal de Bitdefender. Si este es el caso, le recomendamos que elimine todas las otras soluciones de seguridad y reinstale Bitdefender.

   Para más información, diríjase a "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 58).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.11. El Filtro antispam no funciona correctamente

Este articulo le ayuda a solucionar los siguientes problemas con el funcionamiento del Filtro Antispam de Bitdefender:

- Un número de mensajes de correo legítimos están marcados como [spam].
- Algunos mensajes spam no están marcados de acuerdo con el filtro spam.
- El filtro antispam no ha detectado ningún mensaje antispam.

Los mensajes legítimos se han marcado como [spam]

Mensajes Legítimos están marcados como [spam] simplemente porque el filtro Antispam de Bitdefender los ve como spam. Normalmente puede solventar este problema adecuando la configuración del filtro Antispam.

Bitdefender automáticamente añade los destinatarios de su mensajes de correo a la lista de Amigos. Los mensajes de correo recibidos de los contacto que estan en la lista de Amigos son considerados como legítimos. Estos no son verificados por el filtro antispam y, así, no serán marcados nunca como [spam].

La configuración automática de la lista de Amigos no previene la detección de errores que pueden ocurrir en estas situaciones:

- Puede recibir muchos correos comerciales como resultado de suscribirse en varias páginas web. En esta caso, la solución en añadir la dirección de correo de la cual recibe tales mensajes a la lista de Amigos.
- Una parte significativa de sus correos legítimos es de gente con los cuales nunca antes se ha contactado, como clientes, posibles socios comerciales y otros. Se requieren otras soluciones en este caso.

  Si está utilizando uno de los clientes de correo que Bitdefender integra, Indique detección de errores.

> **Nota**
> Bitdefender se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, diríjase a *"Clientes de correo electrónico y protocolos soportados"* (p. 89).

Añadir contactos a la lista de Amigos

Si esta utilizando un cliente de correo compatible, puede añadir fácilmente los remitentes de los mensajes legítimos a la lista de Amigos. Siga estos pasos:

1. En su cliente de correo, seleccionar el mensaje de correo del remitente que desea añadir a la lista de Amigos.
2. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Bitdefender.
3. Puede pedir que admita las direcciones añadidas a la lista de Amigos. Seleccione **No volver a mostrar este mensaje** y haga clic en**Aceptar**.

A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.

Si esta utilizando un cliente de correo diferente, puede añadir contactos a lista de Amigos desde la interfaz de Bitdefender. Siga estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTISPAM**, haga clic en **Gestionar amigos**.

   Aparece una ventana de configuración.
3. Escriba la dirección de correo electrónico en la que siempre desee recibir mensajes de correo electrónico y haga clic en **AÑADIR**. Puede añadir tantas direcciones de e-mail como desee.
4. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Indican errores de detección

Si está utilizando un cliente de correo compatible, puede corregir fácilmente el filtro antispam (indicando qué mensajes de correo no deben ser marcados como [spam]). Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccione el mensaje legítimos incorrecto marcado como [spam] por Bitdefender.
4. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Bitdefender para añadir los remitentes a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.
5. Haga clic en el botón **No es spam** de la barra de herramientas antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo). El mensaje de correo electrónico se moverá a la carpeta Bandeja de entrada.

No se han detectado muchos mensajes de spam

Si está recibiendo muchos mensajes spam que no están marcados como [spam], debe configurar el filtro antispam de Bitdefender, con el fin de mejorar su eficiencia.

Pruebe las siguientes soluciones:

1. Si está utilizando uno de los clientes de correo que Bitdefender integra, Indique mensajes spam no detectados.

   Nota

   Bitdefender se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, diríjase a "*Clientes de correo electrónico y protocolos soportados*" (p. 89).

2. Añadir spammers a la lista de Spammers. Los mensajes de correo recibidos de las direcciones que están en la lista de Spammer son marcados automáticamente como [spam].

Indicar mensajes de spam no detectados

Si esta utilizando un cliente de correo compatible, puede indicar fácilmente que mensajes de correo deben ser detectados como spam. Haciendo esto mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta Bandeja de Entrada.
3. Seleccione los mensajes spam no detectados.
4. Haga clic en el botón **Es spam** en la barra antispam de Bitdefender (localizada normalmente en la parte superior de la ventana del cliente de correo). Inmediatamente serán marcados como [spam] y trasladados a la carpeta de correo no deseado.

Añade spammers a la lista de Spammers

Si esta utilizando cliente de correo compatible, puede fácilmente añadir los remitentes de los mensajes spam a la lista de Spammers. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccione los mensajes marcados como [spam] por Bitdefender.

4. Haga clic en el botón **Añadir Spammer** en la barra de herramientas antispam de Bitdefender.
5. Puede pedir que reconozca las direcciones añadidas a la Lista de Spammers. Seleccione **No volver a mostrar este mensaje** y haga clic en**Aceptar**.

Si está utilizando un cliente de correo diferente, puede añadir manualmente spammers a la Lista de spammers desde la interfaz de Bitdefender. Es conveniente hacerlo sólo cuando ha recibido bastantes mensajes sapm desde la misma de dirección de correo. Siga estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTISPAM**, haga clic en **Gestionar emisores de spam**.

   Aparece una ventana de configuración.
3. Escriba la dirección de correo electrónico del emisor de spam y luego haga clic en **AÑADIR**. Puede añadir tantas direcciones de e-mail como desee.
4. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

El Filtro antispam no detecta ningún mensaje de spam

Si no se marca el mensaje spam como [spam], esto debe ser un problema con el filtro Antispam de Bitdefender. Antes de resolver este problema, asegúrese que no esta causado por una de las siguientes condiciones:

- Puede que esté desactivada la protección antispam. Para comprobar el estado de la protección antispam, haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender. Mire en el panel de **Antispam** si la característica está habilitada.

  Si Antispam está desactivado, esto es lo que está causando el problema. Haga clic en el conmutador correspondiente para activar su protección antispam.
- La protección Antispam de Bitdefender está disponible solo para clientes de correo configurados para recibir mensajes de correo mediante el protocolo POP3. Esto significa lo siguiente:
  - Los mensajes recibidos mediante servicios de correo basados en web (como Yahoo, Gmail, Hotmail u otro) no se filtran como spam por Bitdefender.

- Si su cliente de correo esta configurado para recibir mensajes de correo utilizando otro protocolo diferente a POP3 (por ejemplo, IMAP4), el filtro Antispam de Bitdefender no marcará estos como spam.

> **Nota**
>
> POP3 es uno de los protocolos más extensos utilizados para descargar mensajes de correo de un servidor de correo. Si no sabe el protocolo que utiliza su cliente de correo para descargas los mensajes, pregunte a la persona que ha configurado su correo.

- Bitdefender Total Security no analiza el tráfico POP3 de Lotus Notes.

Una posible solución esta para reparar o reinstalar el producto. Sin embargo, debería contactar con Bitdefender para soporte, como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.12. El Autorrellenado de mi Wallet no funciona

Ha guardado sus credenciales online en su Gestor de contraseñas de Bitdefender y se ha dado cuenta de que el autorrelenado no funciona. Normalmente, este problema se produce cuando la extensión Wallet Bitdefender no está instalada en su navegador.

Para resolver esta situación, siga estos pasos:

- En **Internet Explorer:**
  1. Abrir Internet Explorer.
  2. Haga clic en Herramientas.
  3. Haga clic en Barras de herramientas y extensiones.
  4. Haga clic en Barras de herramientas y extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.
- En **Mozilla Firefox:**
  1. Abra Mozilla Firefox.
  2. Haga clic en Herramientas.
  3. Haga clic en Complementos.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

- En **Google Chrome:**
  1. Abra Google Chrome.
  2. Vaya al icono Menú.
  3. Haga clic en Más herramientas.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

> **Nota**
> El complemento se habilitará después de que reinicie su navegador.

Ahora compruebe si el autorrelenado de Wallet funciona con sus cuentas online.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.1.13. La desinstalación de Bitdefender ha fallado

Si desea desinstalar su producto Bitdefender y observa que el proceso se cuelga o se bloquea el sistema, haga clic en **Cancelar** para cancelar la acción. Si esto no funciona, reinicie el sistema.

Cuando la desinstalación falla, alguna claves de registro y archivos de Bitdefender pueden permanecer en su sistema. Tales restos pueden impedir una nueva instalación de Bitdefender. Estas también pueden afectar al rendimiento y estabilidad del sistema.

Para eliminar Bitdefender de su sistema por completo:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. Haga clic en **ELIMINAR** en la ventana que aparece.
  4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
- En **Windows 8 y Windows 8.1**:

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
4. Haga clic en **ELIMINAR** en la ventana que aparece.
5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Haga clic en **ELIMINAR** en la ventana que aparece.
  6. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

6.1.14. Mi sistema no se inicia tras la instalación de Bitdefender

Si acaba de instalar Bitdefender y no puede reiniciar más su sistema en modo normal hay varias razones por las cuales puede pasar esto.

Lo más probable es que esto lo haya causado una instalación previa de Bitdefender que no fue desinstalada correctamente o por otra solución de seguridad que todavía está presente en el sistema.

Así es como puede abordar cada situación:

- **Ya tenía Bitdefender anteriormente y no lo desinstaló correctamente.**

  Para resolver esto:

  1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 60).
  2. Desinstalar Bitdefender de su sistema:

- En **Windows 7**:
  a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  b. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  c. Haga clic en **ELIMINAR** en la ventana que aparece.
  d. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
  e. Reinicie su sistema en modo normal.
- En **Windows 8 y Windows 8.1**:
  a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  b. Haga clic en **Desinstalar un programa** o **Programas y características**.
  c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  d. Haga clic en **ELIMINAR** en la ventana que aparece.
  e. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
  f. Reinicie su sistema en modo normal.
- En **Windows 10**:
  a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  c. Encuentre **Bitdefender Total Security** y seleccione **Desinstalar**.
  d. Haga clic en **Desinstalar** para confirmar su elección.
  e. Haga clic en **ELIMINAR** en la ventana que aparece.
  f. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
  g. Reinicie su sistema en modo normal.

3. Reinicie su producto Bitdefender.

- **Antes tenía instalada una solución de seguridad y no fue eliminada correctamente.**

  Para resolver esto:

  1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 60).
  2. Elimine las otras soluciones de seguridad de su sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
       c. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
       d. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
     - En **Windows 10**:
       a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
       b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
       c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
       d. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

Para desinstalar correctamente el otro programa, diríjase a su sitio Web y ejecute su herramienta de desinstalación o contacte con ellos directamente para que le proporcionen las indicaciones para desinstalar.

3. Reinicie su sistema en modo normal y reinstale Bitdefender.

Ya ha seguido los pasos anteriores y la situación no se ha solucionado.

Para resolver esto:

1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 60).
2. Utilice la opción Restaurar sistema de Windows para restaurar el equipo a un punto anterior antes de la instalación del producto Bitdefender.
3. Reinicie el sistema de modo normal y contacte con nuestros represetantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 286).

6.2. Eliminación de amenazas de su sistema

Las amenazas pueden afectar a su sistema de diversas formas y el enfoque de Bitdefender depende del tipo de ataque de amenazas. Dado que las amenazas modifican su comportamiento con frecuencia, es difícil establecer un patrón para sus comportamientos y sus acciones.

Hay situaciones en las que Bitdefender no puede eliminar automáticamente la infección de amenazas de su sistema. En cada caso, su intervención es requerida.

- "*Bitdefender Modo de Rescate (Entorno de rescate en Windows 10)*" (p. 177)
- "*¿Qué hacer cuando Bitdefender encuentra amenazas en su equipo?*" (p. 181)
- "*¿Cómo limpio una amenaza de un archivo?*" (p. 182)
- "*¿Cómo limpio una amenaza de un archivo de correo electrónico?*" (p. 183)
- "*¿Qué hacer si sospecho que un archivo es peligroso?*" (p. 184)
- "*¿Qué son los archivos protegidos con contraseña del registro de análisis?*" (p. 185)
- "*¿Qué son los elementos omitidos en el registro de análisis?*" (p. 185)
- "*¿Qué son los archivos sobre-comprimidos en el registro de análisis?*" (p. 185)

- "*¿Por qué eliminó Bitdefender automáticamente un archivo infectado?*" (p. 186)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Pedir ayuda*" (p. 286).

6.2.1. Bitdefender Modo de Rescate (Entorno de rescate en Windows 10)

El **modo Rescate** es una opción de Bitdefender que le permite analizar y desinfectar todas las particiones existentes del disco duro dentro y fuera de su sistema operativo.

Una vez que Bitdefender Total Security está instalado en **Windows 7, Windows 8 y Windows 8.1** y que se ha descargado el archivo de imagen de rescate de Bitdefender, puede utilizar el modo Rescate incluso si no es capaz de arrancar en Windows.

En Windows 10, el Entorno de rescate de Bitdefender está integrado con Windows RE, por lo que no es necesario descargar ninguna imagen del modo Rescate en este sistema operativo, y la característica no se puede usar si hay problemas de arranque. Para limpiar el sistema antes de cargar los servicios de Windows, le recomendamos que utilice Bitdefender Rescue CD.

Bitdefender Rescue CD es una herramienta gratuita que analiza y limpia su equipo cuando sospecha que alguna amenaza afecta a su funcionamiento. Tiene a su disposición útiles artículos con información sobre cómo crearlo y usarlo en la plataforma del centro de soporte de Bitdefender en https://www.bitdefender.com/support/consumer.html.

Descarga de la imagen del modo Rescate de Bitdefender

Para poder utilizar el modo Rescate en **Windows 7, Windows 8 y Windows 8.1**, primero tiene que descargar su archivo de imagen de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Modo Rescate**.
3. Haga clic en **Sí** en la ventana de confirmación que aparece para reiniciar su equipo.

Espere a que se descargue el archivo de imagen del modo Rescate de Bitdefender desde los servidores de Bitdefender. El equipo se reiniciará en cuanto finalice el proceso de descarga.

Aparece un menú que le pide que seleccione un sistema operativo. En esta fase, puede optar por iniciar su sistema en modo Rescate o de la forma normal.

Nota
Debido a la integración con el entorno de recuperación de Windows en **Windows 10**, no es necesario descargar ninguna imagen del modo Rescate en este sistema operativo.

Arranque del sistema en modo Rescate en Windows 7, Windows 8 y Windows 8.1

Puede acceder al Modo Rescate de dos maneras:

Desde la interfaz de Bitdefender

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Modo Rescate**.
3. Haga clic en **Sí** en la ventana de confirmación que aparece para reiniciar su equipo.
4. Una vez que reinicie su equipo, aparecerá un menú que le pedirá que seleccione un sistema operativo. Elija **Modo rescate Bitdefender** para arrancar en un entorno de Bitdefender desde el cual podrá limpiar la partición de Windows.
5. Si se le solicita, pulse **Intro** y seleccione la resolución de pantalla más cercana a la que usa normalmente. A continuación, pulse de nuevo **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

Inicie su equipo directamente desde el modo Rescate.

Si Windows no se inicia, puede arrancar su equipo directamente en el modo Rescate de Bitdefender, siguiendo los pasos detallados a continuación:

- En **Windows 7**:

1. Pulse la tecla **F8** hasta que aparezca la pantalla **Opciones de arranque avanzadas**.
2. Utilice las teclas de las flechas para seleccionar el modo Rescate de Bitdefender y, a continuación, pulse **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

- En **Windows 8 y Windows 8.1**:

  1. Pulse la tecla **Mayúsculas** hasta que aparezca la pantalla **Opciones de arranque avanzadas**.
  2. Seleccione la opción **Utilizar otro sistema operativo** y, a continuación, Modo Rescate de Bitdefender.

     El modo Rescate de Bitdefender se cargará en unos momentos.

> **Nota**
> Solo es posible cargar su equipo en modo Rescate si ha descargado previamente el archivo de imagen del modo Rescate tal como se describe en "Descarga de la imagen del modo Rescate de Bitdefender" (p. 177).

Inicio del sistema en el Entorno de rescate de Windows 10

Solo puede acceder al Entorno de rescate desde su producto Bitdefender de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Entorno de rescate**.
3. Haga clic en **REINICIAR** en la ventana que aparece.

   El Entorno de rescate de Bitdefender se cargará en unos instantes.

Análisis del sistema en el modo Rescate (Entorno de rescate de Windows 10)

Para analizar su sistema en modo Rescate (Entorno de rescate):

- En **Windows 7, Windows 8 y Windows 8.1**:

  1. Acceda al Modo Rescate, como se describe en "Arranque del sistema en modo Rescate en Windows 7, Windows 8 y Windows 8.1" (p. 178).

2. El logotipo de Bitdefender aparecerá y se empezarán a copiar los motores de la solución de seguridad.
3. Aparecerá una ventana de bienvenida. Haga clic en **Continuar**.
4. Se ha iniciado una actualización de la base de datos de información de amenazas.
5. Tras completarse la actualización, aparecerá la ventana del Análisis antivirus bajo demanda de Bitdefender.
6. Haga clic en **Analizar**, seleccione el objeto de análisis en la ventana que aparece y haga clic en **Abrir** para iniciar el análisis.

   Se recomienda analizar toda su partición de Windows.

   > **Nota**
   > Cuando trabaja en modo Rescate, trata con nombres de particiones de tipo Linux. Las particiones de disco aparecerán como sda1, probablemente correspondiendo con el tipo de partición de Windows (C:), sda2 que se corresponde con (D:) y así sucesivamente.

7. Espere a que se complete el análisis. Si se detecta cualquier tipo de amenaza, siga las instrucciones para eliminarla.
8. Para salir del Modo rescate, haga clic con el botón derecho en un área vacía del escritorio, seleccione **Salir** en el menú que aparece y después elija si desea reiniciar o apagar el equipo.

- En **Windows 10**:

1. Acceda al Entorno de rescate, según se describe en “Inicio del sistema en el Entorno de rescate de Windows 10” (p. 179).
2. El proceso de análisis de Bitdefender se inicia automáticamente en cuanto se carga el sistema en el Entorno de rescate.
3. Espere a que se complete el análisis. Si se detecta cualquier tipo de amenaza, siga las instrucciones para eliminarla.
4. Para salir del Entorno de rescate, haga clic en el botón **CERRAR** de la ventana con los resultados del análisis.

6.2.2. ¿Qué hacer cuando Bitdefender encuentra amenazas en su equipo?

Puede descubrir que hay una amenaza en su equipo de una de estas maneras:

- Ha analizado su equipo y Bitdefender ha encontrado elementos infectados en el.
- Una alerta de amenaza le informa de que Bitdefender ha bloqueado una o varias amenazas en su equipo.

En tal caso, actualice Bitdefender para asegurarse de contar con la última base de datos de información de amenazas y ejecute un Análisis del sistema para analizarlo.

Tan pronto como el análisis acabe, seleccione la acción deseada para los elementos infectados (Desinfectar, Eliminar, Trasladar a cuarentena).

Aviso
Si sospecha que el archivo es parte del sistema operativo Windows o que este no es un archivo infectado, no siga estos pasos y contacte con Atención al Cliente de Bitdefender lo antes posible.

Si la acción seleccionado no puede realizarse y el log de análisis muestra una infección la cual no puede ser eliminada, tiene que eliminar el archivo(s) manualmente:

El primer método puede ser utilizado en modo normal:

1. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
   c. En la ventana **Escudo**, desactive **Escudo de Bitdefender**.
2. Muestra los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 58).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Active la protección antivirus en tiempo real de Bitdefender.

En caso de que el primer método no lograse eliminar la infección:

1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 60).
2. Muestra los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 58).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Reiniciar su sistema e iniciar en modo normal.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.2.3. ¿Cómo limpio una amenaza de un archivo?

Una archivo es un archivo o una colección de archivos comprimidos bajo un formato especial para reducir el espacio en disco necesario para guardar los archivos.

Algunos de estos formatos son formatos abiertos, proporcionando así Bitdefender la opción de análisis dentro de ellos y luego tomar las acciones apropiadas para eliminar estos.

Otros formatos de archivo están parcial o totalmente cerrados y Bitdefender solo puede detectar la presencia de amenazas en ellos, pero no realizar ninguna otra acción.

Si Bitdefender le notifica que se ha detectado una amenaza en un archivo y no hay ninguna acción disponible, significa que no es posible eliminar la amenaza debido a restricciones en la configuración de permisos del archivo.

Aquí se explica cómo puede limpiar una amenaza almacenada en un archivo:

1. Identifique el archivo comprimido que incluye la amenaza realizando un Análisis del sistema.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
   c. En la ventana **Escudo**, desactive **Escudo de Bitdefender**.
3. Vaya a la ubicación del archivo y descomprímalo utilizando una aplicación de descompresión de archivos, como WinZip.

4. Identifique el archivo infectado y elimínelo.
5. Elimine el archivo original con el fin de asegurar que la infección está eliminada totalmente.
6. Recomprime los archivos en nuevo archivo utilizando una aplicación de compresión, como WinZip.
7. Active la protección antivirus en tiempo real de Bitdefender y ejecute un análisis del sistema para asegurarse de que no hay ninguna otra infección en el sistema.

Nota
Es importante saber que una amenaza almacenada en un archivo comprimido no es un peligro inmediato para su sistema, ya que esta debe descomprimirse y ejecutarse para poder infectarlo.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.2.4. ¿Cómo limpio una amenaza de un archivo de correo electrónico?

Bitdefender también puede identificar amenazas en bases de datos de correo electrónico y archivos de correo electrónico almacenados en el disco.

Algunas veces es necesario para identificar el mensaje infectados utilizando la información proporcionada por el informe de análisis, y eliminarlo manualmente.

Aquí se explica cómo puede limpiar una amenaza almacenada en un archivo de correo electrónico:

1. Analizar la base de datos de correo con Bitdefender.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
   c. En la ventana **Escudo**, desactive **Escudo de Bitdefender**.
3. Abra el informe de análisis y utilice la información de identificación(Asunto, De, Para) de los mensajes infectados para localizarlos en el cliente de correo.

4. Elimina los mensajes infectados. Muchos de los clientes de correo puede mover los mensajes eliminados a la carpeta de recuperación, desde donde se pueden recuperar. Debería asegurarse que el mensaje también se eliminará de esta carpeta de recuperación.
5. Compactar la carpeta que almacena el mensaje infectado.
   - En Microsoft Outlook 2007: En el Menú Archivo, haga clic Administración de Datos de Archivo. Seleccione los archivos (.pst) de las carpetas personales para intentar compactar, y haga clic en Configuración. Haga clic en Compactar agora.
   - En Microsoft Outlook 2010/2013/2016: En el menú Archivo, haga clic en Info y luego en Configuración de cuenta (Añada o elimine cuentas, o cambie los ajustes de conexión existentes). Luego haga clic en Archivo de datos, seleccione los archivos de carpetas personales (.pst) que desea compactar, y haga clic en Configuración. Haga clic en Compactar agora.
6. Active la protección antivirus en tiempo real de Bitdefender.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 286).

6.2.5. ¿Qué hacer si sospecho que un archivo es peligroso?

Puede sospechar que un archivo de su sistema es peligroso, incluso aunque su producto Bitdefender no lo haya detectado.

Para asegurarse de que su sistema está protegido:

1. Ejecute un **Análisis del sistema** con Bitdefender. Para averiguar cómo hacerlo, consulte "*¿Cómo analizo mi sistema?*" (p. 42).
2. Si el resultado del análisis parece limpio, pero todavía tiene dudas y quiere asegurarse sobre la naturaleza del archivo, contacte con nuestros representantes de soporte de forma que puedan ayudarle.

   Para averiguar cómo hacerlo, consulte "*Pedir ayuda*" (p. 286).

6.2.6. ¿Qué son los archivos protegidos con contraseña del registro de análisis?

Esto es solo una notificación la cual indica que Bitdefender ha detectado estos archivos y están protegidos con una contraseña o por alguna forma de cifrado.

Por lo general, los elementos protegidos con contraseña son:

- Archivos que pertenecen a otra solución de seguridad.
- Archivos que pertenecen al sistema operativo.

Con el fin de analizar el contenido, estos archivos necesitan ser extraídos o descifrados.

En caso de que dicho contenido sea extraído, Bitdefender análisis en tiempo real analizará automáticamente estos para mantener su equipo protegido. Si desea analizar estos archivos con Bitdefender, tiene que contactar con el fabricante del producto con el fin de que le proporcione más detalles de estos archivos.

Nuestra recomendación es que ignore estos archivos porque no son amenazas para su sistema.

6.2.7. ¿Qué son los elementos omitidos en el registro de análisis?

Todos los archivos que aparecen como Omitidos en el informe de análisis están limpios.

Para incrementar el rendimiento, Bitdefender no analiza archivos que no han sido cambiados desde el último análisis.

6.2.8. ¿Qué son los archivos sobre-comprimidos en el registro de análisis?

Los elementos sobrecomprimidos son elementos los cuales no pueden ser extraídos por el motor de análisis o elementos los cuales el tiempo de descifrado ha tomado demasiado tiempo haciendo el sistema inestable.

Los medios sobrecomprimidos que Bitdefender omite el análisis dentro de ese archivo, porque desempaquetando este tomó demasiados recursos del

sistema. El contenido será analizado al acceder en tiempo real si es necesario.

6.2.9. ¿Por qué eliminó Bitdefender automáticamente un archivo infectado?

Si se detecta un archivo infectado, Bitdefender intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se traslada a la cuarentena para contener la infección.

En ciertos tipos de amenazas, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

Este es normalmente el caso con archivos de instalación que son descargados de sitios web no fiables. Si se encuentra en tal situación, descargue el archivo de instalación desde la página web del fabricante u otra página web de confianza.

ANTIVIRUS PARA MAC

7. INSTALACIÓN Y DESINSTALACIÓN

Este capítulo incluye los siguientes temas:

- "*Requisitos del Sistema*" (p. 188)
- "*Instalando Bitdefender Antivirus for Mac*" (p. 189)
- "*Eliminando Bitdefender Antivirus for Mac*" (p. 193)

7.1. Requisitos del Sistema

Puede instalar Bitdefender Antivirus for Mac en equipos Macintosh que ejecuten OS X Mavericks (10.9.5), OS X Yosemite (10.10), OS X El Capitan (10.11), macOS Sierra (10.12), macOS High Sierra (10.13.0) o macOS Mojave (10.14 o posterior).

Su Mac también debe tener un mínimo de 1 GB de espacio disponible en disco duro.

Se requiere de una conexión a Internet para registrar y actualizar Bitdefender Antivirus for Mac.

Importante

Si está instalando Bitdefender Antivirus for Mac en OS X Mavericks 10.9.5, verá que el producto tiene una interfaz diferente a la que se describe en este documento. Esto sucede porque OS X Mavericks 10.9.5 no es compatible con la nueva interfaz que hemos diseñado. Sin embargo, su dispositivo seguirá estando protegido por Bitdefender y puede acceder a las características descritas en este documento siguiendo las instrucciones disponibles en la guía del usuario incluida en su producto. Para acceder a la guía del usuario, haga clic en **Ayuda** en la barra de menús y seleccione **Ayuda de Antivirus for Mac**.

Cómo averiguar la versión de macOS y la información de hardware de su Mac

Haga clic en el icono Apple en la esquina izquierda superior de la ventana y elija **Acerca de este Mac**. En la ventana que aparece puede ver la versión del sistema operativo y otra información útil. Haga clic en **Informe del sistema** para obtener información detallada sobre el hardware.

7.2. Instalando Bitdefender Antivirus for Mac

La app de Bitdefender Antivirus for Mac se puede instalar desde su cuenta Bitdefender de la siguiente manera:

1. Inicie sesión como administrador.
2. Diríjase a: https://central.bitdefender.com.
3. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.
4. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
5. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**

     Seleccione esta opción y guarde el archivo de instalación.
   - **Proteger otros dispositivos**

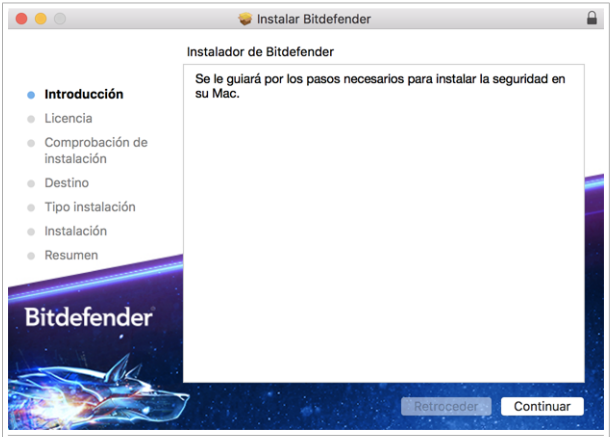
     Seleccione esta opción y, a continuación, haga clic en **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.
   - En el dispositivo en que desee instalar Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.
6. Ejecute el producto Bitdefender que ha descargado.
7. Siga los pasos de la instalación.

7.2.1. Proceso de instalación

Para instalar Bitdefender Antivirus for Mac:

1. Haga clic en el archivo descargado. Se iniciará un asistente que le guiará a través del proceso de instalación.
2. Siga el asistente de instalación.

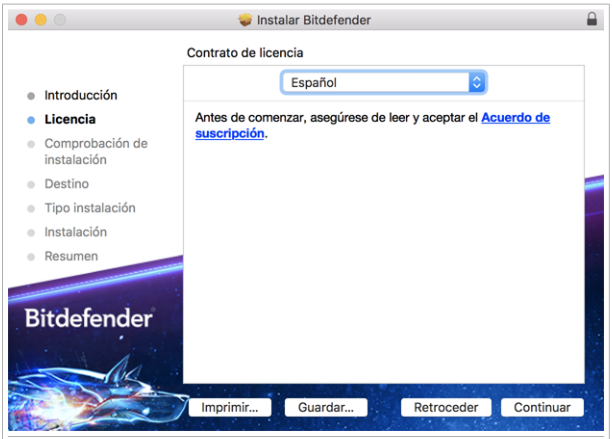
Paso 1 - Ventana de Bienvenida



Ventana de Bienvenida

Haga clic en **Continuar**.

Paso 2: Lea el Acuerdo de Suscripción



Lea el Acuerdo de Suscripción

Antes de continuar con la instalación, debe aceptar el Acuerdo de suscripción. Por favor, dedique un momento a leer el Acuerdo de suscripción, dado que

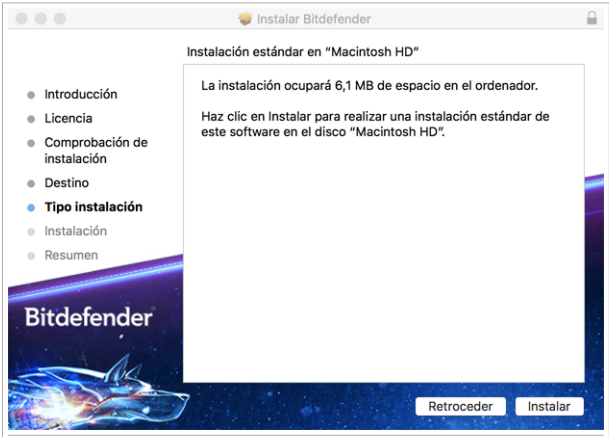
contiene los términos y condiciones bajo los cuales puede usar Bitdefender Antivirus for Mac.

Desde esta ventana también puede seleccionar el idioma en el que desea instalar el producto.

Haga clic en **Continuar** y, a continuación, haga clic en **Acepto**.

> **Importante**
> Si no está de acuerdo con estos términos, haga clic en **Continuar** y, a continuación, haga clic en **No acepto** para cancelar la instalación y salir del instalador.

Paso 3 - Iniciar la instalación

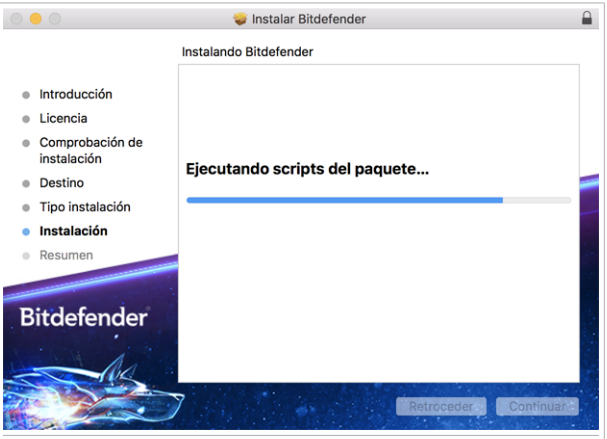


Inicio de la Instalación

Bitdefender Antivirus for Mac se instalará en Macintosh HD/Library/Bitdefender. La ruta de instalación no se puede cambiar.

Haga clic en **Instalar** para iniciar la instalación.

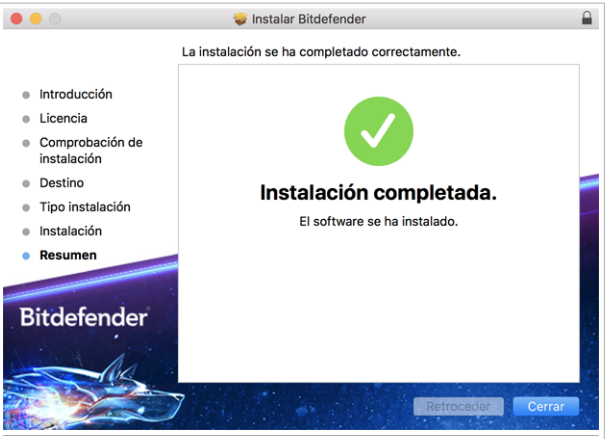
Paso 4 - Instalando Bitdefender Antivirus for Mac



Instalando Bitdefender Antivirus for Mac

Espere hasta que finalice la instalación y, a continuación, haga clic en **Continuar**.

Paso 5 - Finalizar



Finalizar

Haga clic en **Cerrar** para cerrar la ventana de instalación.

Ha finalizado el proceso de instalación.

Importante

- Si está instalando Bitdefender Antivirus for Mac en macOS High Sierra 10.13.0 o en una versión más reciente, aparecerá la notificación de **Bloqueo de extensión del sistema**. Esta notificación le informa de que las extensiones firmadas por Bitdefender han sido bloqueadas y deben activarse manualmente. Haga clic en **Aceptar** para continuar. En la ventana Bitdefender Antivirus for Mac que aparece, haga clic en el enlace **Seguridad y privacidad**. Haga clic en **Permitir** en la parte inferior de la ventana o seleccione Bitdefender SRL en la lista y, luego, haga clic en **Aceptar**
- Si está instalando Bitdefender Antivirus for Mac en macOS Mojave 10.14 o en una versión más reciente, aparecerá una notificación que le informa de que debe permitir manualmente que Bitdefender Antivirus for Mac cargue sus archivos en el sistema. Para continuar, haga clic en el enlace **Seguridad y privacidad** y, a continuación, haga clic en **Aceptar**. Haga clic en **Permitir** junto a Bitdefender SRL.

7.3. Eliminando Bitdefender Antivirus for Mac

Al ser una aplicación compleja, Bitdefender Antivirus for Mac puede ser eliminando de forma normal, arrastrando el icono de la aplicación de la carpeta de Aplicaciones a la Papelera.

Para eliminar Bitdefender Antivirus for Mac, siga estos pasos:

1. Abra una ventana del **Finder** y luego acceda a la carpeta Aplicaciones.
2. Abra la carpeta Bitdefender y, a continuación, haga doble clic en Desinstalador de Bitdefender.
3. Haga clic en **Desinstalar** y espere a que finalice el proceso.
4. Haga clic en **Cerrar** para terminar.

Importante

Si hay un error, puede contactar con Atención al Cliente de Bitdefendercomo se describe en "*Pedir ayuda*" (p. 286).

8. INICIANDO

Este capítulo incluye los siguientes temas:

- "*Acerca de Bitdefender Antivirus for Mac*" (p. 194)
- "*Abrir Bitdefender Antivirus for Mac*" (p. 194)
- "*Ventana principal de la app*" (p. 195)
- "*Icono de app del Dock*" (p. 196)
- "*Menú de navegación*" (p. 197)

8.1. Acerca de Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac es un potente analizador antivirus que puede detectar y eliminar todo tipo de software malicioso ("amenazas"), entre las que se incluyen:

- ransomware
- adware
- virus
- spyware
- Troyanos
- keyloggers
- gusanos

Esta aplicación detecta y elimina no solo amenazas de Mac, sino también de Windows, con lo que se evita que envíe accidentalmente archivos infectados a su familia, amigos y compañeros de trabajo que usen PC.

8.2. Abrir Bitdefender Antivirus for Mac

Hay diferentes maneras de abrir Bitdefender Antivirus for Mac.

- Haga clic en el icono Bitdefender Antivirus for Macen el Launchpad.
- Haga clic en el icono en la barra de menús y seleccione **Abrir la ventana principal**.
- Abra una ventana del Finder, acceda a Aplicaciones y haga doble clic en el icono de Bitdefender Antivirus for Mac.

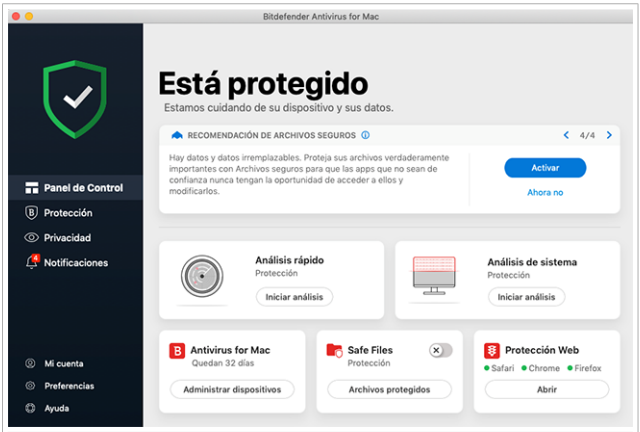
Importante

La primera vez que abra Bitdefender Antivirus for Mac en macOS Mojave 10.14 o en una versión más reciente, aparecerá una recomendación de protección porque necesitamos permisos para analizar todo el sistema en busca de amenazas. Para otorgarnos dichos permisos, debe iniciar sesión como administrador y seguir los pasos que se exponen a continuación:

1. Haga clic en el enlace **Preferencias del sistema**.
2. Haga clic en el icono y, a continuación, introduzca sus credenciales de administrador.
3. Se abre una nueva ventana. Arrastre el archivo **BDLDaemon** a la lista de apps permitidas.

8.3. Ventana principal de la app

Bitdefender Antivirus for Mac satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. Esta interfaz de usuario gráfica esta diseñada para satisfacer todas y cada una de las categorías de usuario.



Ventana principal de la app

Para que conozca la interfaz de Bitdefender, se muestra en la parte superior izquierda un asistente introductorio con información detallada sobre cómo configurar y manejar el producto. Seleccione Seleccione el soporte de ángulo recto para continuar, u **Omitir recorrido** para cerrar el asistente.

La barra de estado en la parte superior de la ventana le informa sobre el estado de seguridad del sistema mediante mensajes explícitos y colores asociados. Si Bitdefender Antivirus for Mac no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone roja. Para información detalla de incidencias y cómo repararlas, diríjase a "*Reparar Incidencias*" (p. 208).

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, ya esté trabajando o haciendo pagos por Internet, el 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 Antivirus for Mac.

Desde el menú de navegación del lado izquierdo, puede acceder a las secciones de Bitdefender para una configuración detallada y tareas administrativas avanzadas (pestañas **Protección** y **Privacidad**), notificaciones, su cuenta de Bitdefender y el área de Preferencias. Además, puede ponerse en contacto con nosotros (pestaña **Ayuda**) para obtener ayuda en caso de tener alguna pregunta o si sucede algo inesperado.

8.4. Icono de app del Dock

El icono de Bitdefender Antivirus for Mac puede verse en el Dock en cuanto abre la aplicación. El icono del Dock le proporciona una manera fácil para analizar archivos y carpetas en busca de amenazas. Simplemente arrastre y suelte el archivo o la carpeta en el icono del Dock y el análisis comenzará inmediatamente.

Icono del Dock

8.5. Menú de navegación

En el lado izquierdo de la interfaz de Bitdefender está el menú de navegación, que le permite acceder rápidamente a las características de Bitdefender que necesita para gestionar su producto. Las pestañas disponibles en esta área son las siguientes:

- **Panel de control**. Desde aquí puede solucionar rápidamente los problemas de seguridad, ver recomendaciones según las necesidades de su sistema y sus patrones de uso, realizar acciones rápidas y acceder a su cuenta de Bitdefender para administrar los dispositivos que ha añadido a su suscripción de Bitdefender.
- **Protección**. Desde aquí puede poner en marcha análisis antivirus, añadir archivos a la lista de excepciones, proteger archivos y aplicaciones frente a ataques de ransomware, salvaguardar sus copias de seguridad de Time Machine y configurar su protección mientras navega por Internet.
- **Privacidad**. Desde aquí puede abrir la aplicación de Bitdefender VPN.
- **Notificaciones**. Desde aquí puede ver detalles sobre las acciones realizadas en los archivos analizados.
- **Mi cuenta**. Desde aquí puede acceder a su cuenta de Bitdefender para comprobar sus suscripciones y realizar tareas de seguridad en los dispositivos que administra. También dispone de información acerca de la cuenta de Bitdefender y de la suscripción en uso.
- **Preferencias**. Desde aquí puede configurar los ajustes de Bitdefender.
- **Soporte**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su producto de Bitdefender, puede ponerse en contacto con el servicio de soporte técnico. También puede enviarnos sus comentarios para ayudarnos a mejorar el producto.

9. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Este capítulo incluye los siguientes temas:

- "*Buenas Prácticas*" (p. 198)
- "*Analizando Su Mac*" (p. 199)
- "*Asistente del Análisis*" (p. 200)
- "*Cuarentena*" (p. 201)
- "*Escudo de Bitdefender (protección en tiempo real)*" (p. 202)
- "*Excepciones de Análisis*" (p. 202)
- "*Protección Web*" (p. 203)
- "*Archivos seguros*" (p. 205)
- "*Protección de Time Machine*" (p. 207)
- "*Reparar Incidencias*" (p. 208)
- "*Notificaciones*" (p. 209)
- "*Actualizaciones*" (p. 210)

9.1. Buenas Prácticas

Para mantener su sistema protegido contra las amenazas y evitar la infección accidental de otros sistemas, siga estas recomendaciones:

- Mantenga activado el **Escudo de Bitdefender** para permitir que Bitdefender Antivirus for Mac analice automáticamente los archivos del sistema.
- Mantenga Bitdefender Antivirus for Mac actualizado con la última información de amenazas y actualizaciones de producto.
- Compruebe y repare regularmente las incidencias reportadas por Bitdefender Antivirus for Mac. Para información detallada, diríjase a "*Reparar Incidencias*" (p. 208).
- Verifique el registro detallado de eventos relativos a la actividad de Bitdefender Antivirus for Mac en su equipo. Siempre que sucede algo relevante para la seguridad de su sistema o de sus datos, se añade un nuevo mensaje al área de notificaciones de Bitdefender. Para más información, acceda a "*Notificaciones*" (p. 209).

- También debería seguir estas recomendaciones:
  - Acostúmbrese a analizar los archivos que descargue de una fuente de almacenamiento externa (como por ejemplo una memoria USB o un CD), especialmente cuando desconoce el origen de los mismos.
  - Si tiene un archivo DMG, móntelo y analice su contenido (los archivos del volumen/imagen montado).

  La vía fácil para analizar un archivo, una carpeta o un volumen es arrastrando&soltando sobre la ventana de Bitdefender Antivirus for Mac o al icono del Dock.

No se requiere otra acción o configuración. Sin embargo, si lo desea, puede ajustar la configuración de la aplicación y las preferencias para satisfacer mejor sus necesidades. Para más información, diríjase a "*Preferencias de Configuración*" (p. 213).

9.2. Analizando Su Mac

Además de la característica **Escudo de Bitdefender**, que monitoriza regularmente las apps instaladas en el equipo en busca de síntomas de amenazas e impide que las nuevas amenazas entren en su sistema, puede analizar su Mac o archivos concretos siempre que desee.

La vía fácil para analizar un archivo, una carpeta o un volumen es arrastrando&soltando sobre la ventana de Bitdefender Antivirus for Mac o al icono del Dock. El asistente de análisis aparecerá y le guiará a través del proceso de análisis.

También puede iniciar un análisis de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Antivirus**.
3. Haga clic en uno de los tres botones de análisis para iniciar el análisis deseado.
   - **Quick Scan**: busca amenazas en las ubicaciones más vulnerables de su sistema (por ejemplo, las carpetas que contienen los documentos, descargas, descargas de correo electrónico y archivos temporales de cada usuario).

- **Análisis completo**: realiza una comprobación exhaustiva en busca de amenazas en todo el sistema. Todos los dispositivos montados se analizarán también.

  > **Nota**
  >
  > Dependiendo del tamaño de su disco duro, analizar todo el sistema puede tardar bastante (hasta una hora o incluso más). Para mejorar el rendimiento, se recomienda no ejecutar esta tarea mientras se estén llevando a cabo otras tareas que consuman muchos recursos (como por ejemplo la edición de vídeo).
  > Si lo prefiere, puede escoger no analizar determinados volúmenes montados añadiéndolos a la lista de Excepciones en la ventana de Protección.

- **Análisis personalizado**: le ayuda a comprobar la existencia de amenazas en archivos, carpetas o volúmenes concretos.

También puede iniciar un Quick Scan o un Análisis del sistema desde el panel de control.

9.3. Asistente del Análisis

Cuando inicie una análisis, aparecerá el asistente de Análisis de Bitdefender Antivirus for Mac.

Análisis en Progreso

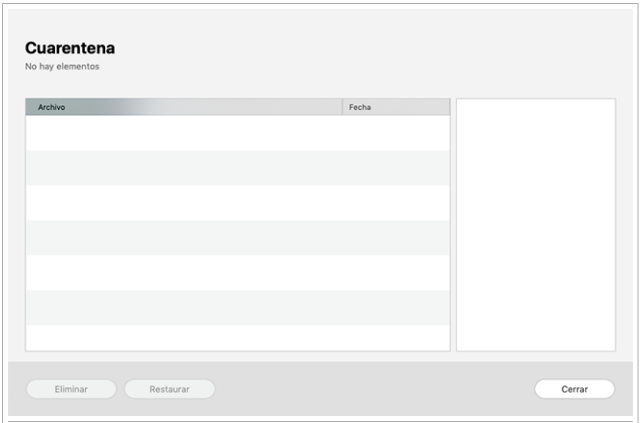
Durante cada análisis se muestra Información en tiempo real acerca de las amenazas detectadas y resueltas.

Espere a que Bitdefender Antivirus for Mac finalice el análisis.

Nota
El análisis puede llevar un tiempo, dependiendo de la complejidad del análisis.

9.4. Cuarentena

Bitdefender Antivirus for Mac le permite aislar los archivos infectados o sospechosos en una área segura, llamada cuarentena. Cuando una amenaza está aislada en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.



Archivos trasladados a la cuarentena

El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena.

Para borrar un archivo de la cuarentena, selecciónelo y haga clic en **Eliminar**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

Para ver una lista con todos los elementos añadidos a la cuarentena:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Se abre la ventana **Antivirus**.

Haga clic en **Abrir** en el panel de **Cuarentena**.

9.5. Escudo de Bitdefender (protección en tiempo real)

Bitdefender brinda protección en tiempo real contra un amplio abanico de amenazas mediante el análisis de todas las apps instaladas, sus versiones actualizadas y archivos nuevos y modificados.

Para desactivar la protección en tiempo real:

1. Haga clic en **Preferencias** en el menú de navegación de la interfaz de Bitdefender.
2. Desactive **Bitdefender Residente** en la ventana **Protección**.

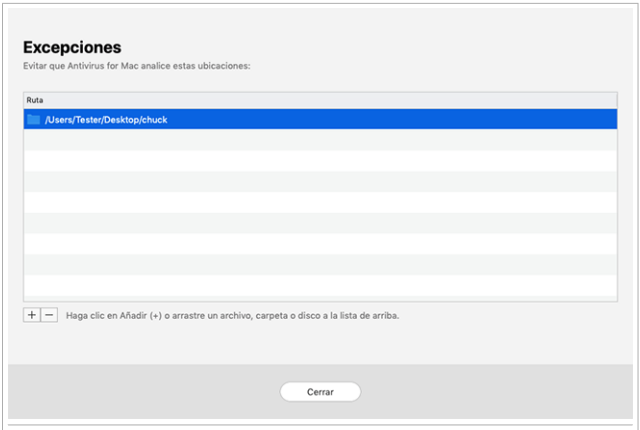
Aviso

Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Si desactiva la protección en tiempo real, no estará protegido contra las amenazas.

9.6. Excepciones de Análisis

Si así lo desea, puede hacer que Bitdefender Antivirus for Mac no analice ciertos archivos, carpetas o incluso un volumen entero. Por ejemplo, quizá querría excluir del análisis:

- Archivos que han sido identificados por error como infectados (conocidos como falsos positivos)
- Archivos que provocan errores de análisis
- Hacer copia de seguridad de los volúmenes



Excepciones de Análisis

La lista de excepciones contiene las rutas que se han exceptuado del análisis.

Para acceder a la lista de excepciones:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Se abre la ventana **Antivirus**.

   Haga clic en **Abrir** en el panel de **Excepciones**.

Existen dos modos de establecer una excepción de análisis:

- Arrastrar y soltar un archivo, carpeta o volumen sobre la lista de excepciones.
- Hacer clic en el botón etiquetado con el signo más (+), ubicado bajo la lista de excepciones. Luego, escoja el archivo, carpeta o volumen que desee exceptuar del análisis.

Para eliminar una excepción de análisis, selecciónela en la lista y haga clic en el botón etiquetado con el signo menos (-), ubicado bajo la lista de excepciones.

9.7. Protección Web

Bitdefender Antivirus for Mac utiliza las extensiones TrafficLight para proteger completamente su navegación Web. Las extensiones TrafficLight

interceptan, procesan y filtran todo el tráfico Web, bloqueando cualquier contenido malicioso.

Las extensiones funcionan y se integran con los siguientes navegadores: Mozilla Firefox, Google Chrome y Safari.

Habilitación de extensiones TrafficLight

Para habilitar las extensiones de TrafficLight:

1. Haga clic en **Reparar ahora** en la tarjeta de **Protección web** del panel de control.
2. Se abre la ventana **Protección web**.

   Aparece el navegador detectado que tiene instalado en su sistema. Para instalar la extensión Linkchecker en su navegador, haga clic en **Obtener extensión**.
3. Se le redirige a:

   https://bitdefender.com/solutions/trafficlight.html
4. Seleccione **Descarga gratuita**.
5. Siga los pasos para instalar la extensión TrafficLight correspondiente a su navegador.

Ajustes de administración de extensiones

Hay toda una serie de funciones disponibles para protegerle frente a todo tipo de amenazas que pueda encontrar mientras navega por la Web. Para acceder a ellos, haga clic en el icono TrafficLight junto a la configuración de su navegador y, a continuación, haga clic en **Ajustes**:

- **Ajustes de Bitdefender TrafficLight**
  - Filtro de amenazas avanzadas: Evita que acceda a sitios web empleados para ataques de phishing, fraudes y malware.
  - Detector de rastreadores: Detecta rastreadores en las páginas web que visita y le mantiene informado sobre su presencia.
  - Analizador de búsquedas: Proporciona una advertencia anticipada sobre sitios web peligrosos presentes en sus resultados de búsquedas.

    En caso de que todos los conmutadores de ajuste estén desactivados, no se analizará ningún sitio web.

- **Lista blanca**

  Se pueden exceptuar sitios web del análisis de los motores de Bitdefender. En el campo correspondiente, escriba el nombre del sitio web que desea añadir a la lista de excepciones y, a continuación, haga clic en **AÑADIR**.

  No se mostrará ninguna advertencia en caso de que haya amenazas en las páginas exceptuadas. Por eso solo debería añadir a esta lista sitios web en los que confíe plenamente.

Calificación de páginas y alertas

Dependiendo de la clasificación que TrafficLight otorgue a la página Web que esté viendo, mostrará en su área uno de los iconos siguientes:

Esta página es segura. Puede seguir trabajando.
Esta página web puede albergar contenido peligroso. Tenga cuidado si desea visitarla.
Debe abandonar la página web de inmediato, ya que contiene malware u otras amenazas.

En Safari, el fondo de los iconos de TrafficLight es negro.

9.8. Archivos seguros

El ransomware es un software malicioso que ataca a los sistemas vulnerables y los bloquea, con el fin de solicitar dinero al usuario a cambio de permitirle recuperar el control de su sistema. Este software malicioso actúa astutamente, mostrando mensajes falsos para que el usuario entre en pánico, instándole a efectuar el pago solicitado.

Gracias a la última tecnología, Bitdefender garantiza la integridad del sistema protegiéndolo contra ataques de ransomware sin afectar a su rendimiento. No obstante, puede que también desee evitar que apps que no sean de fiar accedan a sus archivos personales, como documentos, fotos o películas. Con Archivos seguros de Bitdefender puede poner a salvo sus archivos personales y configurar qué apps tienen permiso para realizar cambios en los archivos protegidos y cuáles no.

Para añadir posteriormente archivos al entorno protegido:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Contra ransomware**.

3. Haga clic en **Archivos protegidos** en el área de Archivos seguros.
4. Hacer clic en el botón etiquetado con el signo más (+), ubicado bajo la lista de archivos protegidos. A continuación, elija el archivo, la carpeta o el volumen que desea proteger en caso de que sufra un ataque de ransomware.

Para evitar que el sistema se ralentice, le recomendamos que añada un máximo de treinta carpetas, o que guarde varios archivos en una sola carpeta.

Las carpetas Imágenes, Documentos, Escritorio y Descargas están protegidas por defecto contra los ataques.

> **Nota**
> Se pueden proteger carpetas personalizadas solo para los usuarios actuales. No se pueden añadir al entorno de protección discos externos, archivos de aplicaciones y del sistema.

Se le informará cada vez que una aplicación desconocida con un comportamiento inusual intente modificar los archivos que ha añadido. Haga clic en **Permitir** o **Bloquear** para añadirlo a la lista de Aplicaciones administradas.

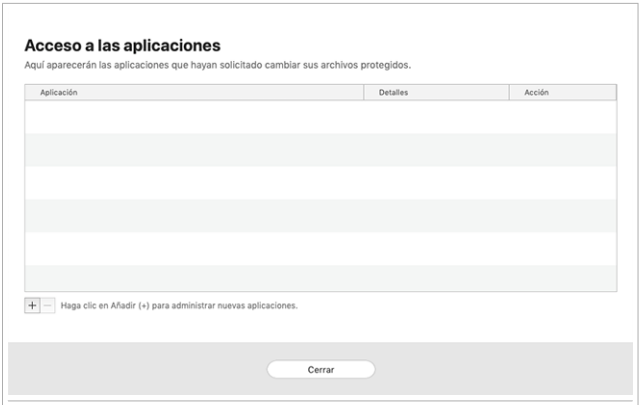
9.8.1. Aplicaciones administradas

Puede que las aplicaciones que intenten cambiar o borrar archivos protegidos se identifiquen como potencialmente poco fiables y se añadan a la lista de aplicaciones bloqueadas. Si se bloquease una aplicación y estuviese seguro de que su comportamiento es el adecuado, puede permitirla siguiendo estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Contra ransomware**.
3. Haga clic en **Acceso a aplicaciones** en el área de Archivos seguros.
4. Cambie el estado a Permitir junto a la aplicación bloqueada.

Las aplicaciones fijadas en Permitir también se pueden pasar a estado Bloqueado.

Utilice el método de arrastrar y soltar o haga clic en el signo más (+) para añadir más apps a la lista.



Archivos seguros

9.9. Protección de Time Machine

La Protección de Time Machine de Bitdefender actúa como una capa adicional de seguridad para su unidad de copia de seguridad, incluyendo todos los archivos que haya decidido almacenar en ella, al bloquear el acceso desde cualquier fuente externa. En caso de que un ransomware cifrara los archivos que tiene almacenados en su unidad de Time Machine, podría recuperarlos sin tener que pagar el rescate solicitado.

En caso de que necesite restaurar elementos de una copia de seguridad de Time Machine, consulte la página de soporte técnico de Apple para obtener instrucciones.

Activación y desactivación de la Protección de Time Machine

Para activar o desactivar la Protección de Time Machine:

1. Haga clic en **Protección** en el menú de navegación de la **interfaz de Bitdefender**.
2. Seleccione la pestaña **Contra ransomware**.
3. Active o desactive el conmutador de **Protección de Time Machine**.

9.10. Reparar Incidencias

Bitdefender Antivirus for Mac automáticamente detecta y le informa sobre una serie de incidencias que pueden afectar a la seguridad de su sistema y sus datos. De esta forma, puede evitar fácilmente y a tiempo riesgos para la seguridad.

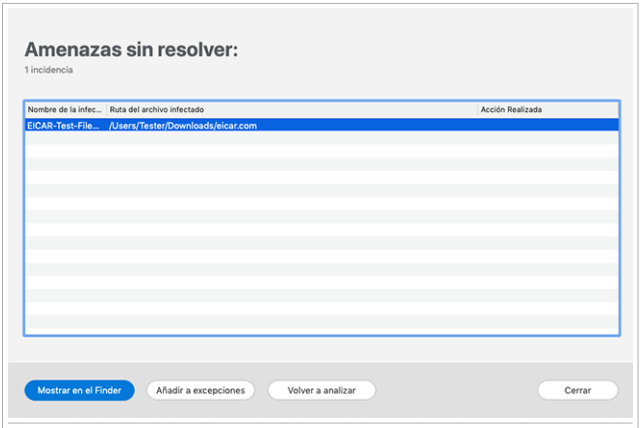
La reparación de incidencias indicadas por Bitdefender Antivirus for Mac es una manera rápida y sencilla de asegurarse una magnífica protección de su sistema y de sus datos.

Los problemas detectados incluyen:

- No se ha descargado de nuestros servidores la nueva actualización de la información de amenazas.
- Se han detectado amenazas en su sistema y el producto no puede desinfectarlas automáticamente.
- La protección en tiempo real está desactivada.

Para comprobar y reparar las incidencias detectadas:

1. Si Bitdefender no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone roja.
2. Compruebe la descripción para más información.
3. Si se detecta un problema, haga clic en el botón correspondiente para adoptar medidas.



Ventana de amenazas no solucionadas

La lista de amenazas no resueltas se actualiza tras cada análisis del sistema, independientemente de si el análisis se ha realizado automáticamente en segundo plano o si lo ha iniciado usted.

Puede escoger adoptar las siguientes medidas respecto a las amenazas no solucionadas:

- Eliminar manualmente. Lleve a cabo esta acción para eliminar manualmente las infecciones.
- Añadir a excepciones. Esta acción no está disponible para amenazas encontradas dentro de archivos comprimidos.

9.11. Notificaciones

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su PC. Siempre que ocurra algo relevante respecto a la seguridad de su sistema o información, se añadirá un nuevo mensaje a las Notificaciones de Bitdefender, de forma parecida a un nuevo e-mail apareciendo en su bandeja de entrada.

Las notificaciones son una herramienta importante en la supervisión y la gestión de la protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontraron vulnerabilidades o amenazas en su equipo, etc. Además, si es necesario

puede realizar acciones adicionales o cambiar las acciones que Bitdefender ha llevado a cabo.

Para acceder al registro de notificaciones, haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender. Cada vez que se produce un evento crítico, se puede ver un contador en el icono .

Dependiendo del tipo y la gravedad, las notificaciones se agrupan en:

- Los eventos **críticos** indican problemas críticos. Debe verificarlos inmediatamente.
- Los eventos de **Advertencia** indican incidencias no críticas. Cuando tenga tiempo debería comprobarlas y repararlas.
- Los eventos de **Información** indican operaciones que se han completado con éxito.

Haga clic en cada pestaña para obtener más información sobre los eventos generados. Con un simple clic en el título de cada evento se muestran algunos detalles: una breve descripción, la medida que Bitdefender adoptó cuando este se produjo, y la fecha y hora en que ocurrió. Si fuera necesario pueden proporcionarse opciones con el fin de tomar nuevas medidas.

Para ayudar a administrar fácilmente los eventos registrados, la ventana de Notificaciones proporciona opciones para eliminar o marcar como leídos todos los eventos en esta sección.

9.12. Actualizaciones

Todos los días se encuentran e identifican nuevas amenazas. Por este motivo es muy importante mantener Bitdefender Antivirus for Mac al día con las últimas actualizaciones de información de amenazas.

La actualización de información de amenazas se realiza al instante, reemplazándose progresivamente los archivos que haya que actualizar. De este modo, la actualización no afecta al funcionamiento del producto y, al mismo tiempo, se evita cualquier riesgo.

- Si Bitdefender Antivirus for Mac está actualizado, este puede detectar las últimas amenazas descubiertas y limpiar los archivos infectados.
- Si Bitdefender Antivirus for Mac no está actualizado, no podrá detectar y eliminar las últimas amenazas descubiertas por los laboratorios de Bitdefender.

9.12.1. Solicitando una Actualización

Puede solicitar una actualización manualmente en cualquier momento.

Se requiere conexión a Internet con el fin de comprobar las actualizaciones disponibles y descargarlas.

Para solicitar una actualización manual:

1. Haga clic en el botón **Acciones** en la barra de menús.
2. Elija **Actualizar la base de datos de información de amenazas**.

Como alternativa, puede solicitar manualmente una actualización pulsando CMD + U.

Puede ver el progreso de actualización y archivos descargados.

9.12.2. Obteniendo Actualizaciones a través de un Servidor Proxy

Bitdefender Antivirus for Mac puede actualizar solo a través de servidores proxy que no requiere autenticación. No tiene que configurar ninguna configuración del programa.

Si se conecta a Internet a través de un servidor proxy que requiera autenticación, debe pasar regularmente a una conexión directa a Internet para obtener actualizaciones de la información de amenazas.

9.12.3. Actualice a una nueva versión

De vez en cuando, lanzamos actualizaciones de producto para añadir nuevas características y mejoras o solucionar deficiencias del producto. Estas actualizaciones podrían requerir un reinicio del sistema para dar paso a la instalación de nuevos archivos. De forma predeterminada, si una actualización precisa un reinicio del equipo, Bitdefender Antivirus for Mac seguirá funcionando con los archivos anteriores hasta que se reinicie el sistema. Así, el proceso de actualización no interferirá con el trabajo del usuario.

Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si no lee esta notificación, puede también hacer clic en **Reiniciar para actualizar** en la barra de menús o reiniciar manualmente el sistema.

9.12.4. Encontrar información sobre Bitdefender Antivirus for Mac

Para hallar información sobre la versión de Bitdefender Antivirus for Mac que ha instalado, acceda a la ventana **Acerca de**. En la misma ventana, puede acceder al Acuerdo de suscripción, la Política de privacidad y las Licencias de código abierto y leer estos documentos.

Para acceder a la ventana Acerca de:

1. Abrir Bitdefender Antivirus for Mac.
2. Haga clic en Bitdefender Antivirus for Mac en la barra de menús y seleccione **Acerca de Antivirus for Mac**.

10. PREFERENCIAS DE CONFIGURACIÓN

Este capítulo incluye los siguientes temas:

- "*Preferencias de Acceso*" (p. 213)
- "*Preferencias de protección*" (p. 213)
- "*Preferencias avanzadas*" (p. 214)
- "*Ofertas especiales*" (p. 214)

10.1. Preferencias de Acceso

Para abrir la ventana de Preferencias de Bitdefender Antivirus for Mac:

1. Realice una de estas acciones:
   - Haga clic en **Preferencias** en el menú de navegación de la interfaz de Bitdefender.
   - Haga clic en la barra de menú de Bitdefender Antivirus for Mac y escoja **Preferencias**.
   - Presione el comando coma(,).

10.2. Preferencias de protección

La ventana de preferencias de protección le permite configurar el procedimiento general de análisis. Puede configurar las acciones a realizar en los archivos infectados y sospechosos detectados y otros ajustes generales.

- **Escudo Bitdefender.** El Escudo de Bitdefender brinda protección en tiempo real contra un amplio abanico de amenazas mediante el análisis de todas las apps instaladas, sus versiones actualizadas y archivos nuevos y modificados. Le recomendamos que no desactive el Escudo de Bitdefender, pero de ser necesario, hágalo durante el menor tiempo posible. Si desactiva el Escudo de Bitdefender, no estará protegido contra las amenazas.
- **Analizar archivos nuevos y modificados.** Seleccione esta casilla para que Bitdefender Antivirus for Mac analice sólo archivos que no han sido analizados antes o estos han sido modificados desde el último análisis.

  Puede optar por no aplicar este ajuste al análisis personalizado y al de arrastrar y soltar dejando sin marcar la casilla de verificación correspondiente.

- **No analizar el contenido de las copias de seguridad.** Seleccione esta casilla de verificación para excluir del análisis los archivos de copia de seguridad. Si posteriormente se restauran los archivos infectados, Bitdefender Antivirus for Mac los detectará automáticamente y adoptará las medidas oportunas.

10.3. Preferencias avanzadas

Puede elegir una acción general para todas las incidencias y elementos sospechosos hallados durante un proceso de análisis.

Acción para elementos infectados

Intentar desinfectar o mover a la cuarentena: Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso).

No realizar ninguna acción: No se realizará ninguna acción sobre los archivos detectados.

Acción para elementos sospechosos

Mover archivos a la cuarentena: Si se detectan archivos sospechosos, Bitdefender los moverá a la cuarentena.

No realizar ninguna acción: No se realizará ninguna acción sobre los archivos detectados.

10.4. Ofertas especiales

Cuando haya ofertas promocionales disponibles, el producto Bitdefender está configurado para que se lo notifique mediante una ventana emergente. Esto le da la oportunidad de beneficiarse de precios ventajosos y mantener sus dispositivos protegidos durante un mayor período de tiempo.

Para activar o desactivar las notificaciones de ofertas especiales:

1. Haga clic en **Preferencias** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Otros**.
3. Active o desactive el conmutador **Mis ofertas**.

La opción **Mis ofertas** está habilitada por defecto.

11. VPN

Este capítulo incluye los siguientes temas:

- "*Acerca de VPN*" (p. 215)
- "*Abrir VPN*" (p. 215)
- "*Interfaz*" (p. 216)
- "*Suscripciones*" (p. 218)

11.1. Acerca de 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 Bitdefender 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.

11.2. Abrir VPN

Hay tres formas de abrir la aplicación de Bitdefender VPN:

- Haga clic en **Privacidad** en el menú de navegación de la **interfaz de Bitdefender**.

Haga clic en **Abrir** en la tarjeta de Bitdefender VPN.

- Haga clic en el icono de la barra de menús.
- Acceda a la carpeta Aplicaciones, abra la carpeta Bitdefender y, a continuación, haga doble clic en el icono de Bitdefender VPN.

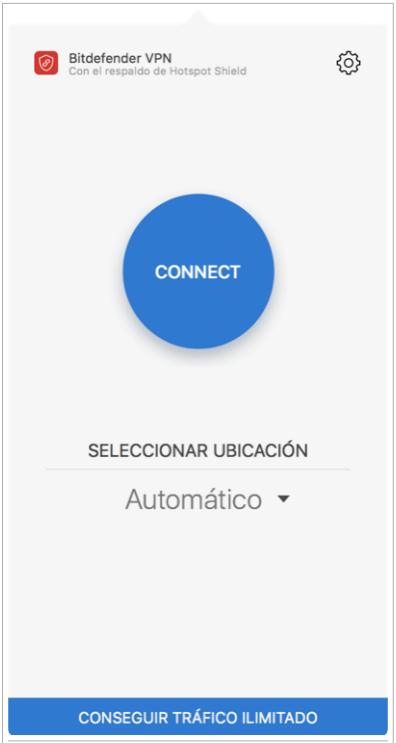
La primera vez que abra la aplicación, se le pedirá permiso para que Bitdefender añada configuraciones. Al permitir que Bitdefender añada configuraciones, acepta que toda la actividad de red de su dispositivo se podrá filtrar o monitorizar cuando use la aplicación de VPN.

Nota
La app Bitdefender VPN solo se puede instalar en macOS Sierra (10.12), macOS High Sierra (10.13.0) o macOS Mojave (10.14 o posterior).

11.3. Interfaz

La interfaz de VPN muestra el estado de la app: conectada o desconectada. Para los usuarios con la versión gratuita, Bitdefender configura automáticamente la ubicación del servidor a la más apropiada, mientras que los usuarios premium tienen la posibilidad de cambiar la ubicación del servidor al que deseen conectarse escogiéndola en la lista **SELECCIONAR UBICACIÓN**. Para más información sobre las suscripciones a VPN, consulte "*Suscripciones*" (p. 218).

Para conectarse o desconectarse, basta con hacer clic en el estado que se muestra en la parte superior de la pantalla. El icono de la barra de menús aparece en negro cuando VPN está conectado y en blanco cuando no.



Interfaz de VPN

Mientras está conectado, el tiempo transcurrido se muestra en la parte inferior de la interfaz. Para acceder a más opciones, haga clic en el icono ⚙ de la zona superior derecha:

- **Mi cuenta**: se muestran los detalles sobre su cuenta de Bitdefender y su suscripción a VPN. Haga clic en **Cambiar cuenta** si desea iniciar sesión con otra distinta.
- **Ajustes**: puede personalizar el comportamiento de su producto según sus necesidades:
  - Configurar la VPN para que se ejecute al iniciar el sistema.
  - Recibir notificaciones cuando la VPN se conecta o desconecta automáticamente.

- **Actualizar a Premium**: si utiliza la versión gratuita, puede actualizar al plan premium desde aquí. Haga clic en **ACTUALIZAR AHORA** para acceder a una página web desde donde podrá adquirir una suscripción.
- **Soporte**: se le redirige a la plataforma de nuestro Centro de soporte, donde puede leer un artículo sobre cómo usar Bitdefender VPN.
- **Acerca de** : Muestra información acerca de la versión instalada.
- **Salir**: para salir de la app.

11.4. Suscripciones

Bitdefender VPN ofrece gratuitamente una cuota de tráfico diaria de 200 MB por dispositivo para que proteja la conexión cuando su equipo lo necesite.

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

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento desde el panel **Mis suscripciones** disponible en su cuenta de Bitdefender.

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

Bitdefender VPN es un producto multiplataforma, disponible en 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.

12. BITDEFENDER CENTRAL

Este capítulo incluye los siguientes temas:

- "*Acerca de Bitdefender Central*" (p. 219)
- "*Mis suscripciones*" (p. 220)
- "*Mis dispositivos*" (p. 221)

12.1. 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:

- Descargue e instale Bitdefender en los sistemas operativos Windows, iOS, macOS y Android. Los productos disponibles para su descarga son:
  - Bitdefender Antivirus for Mac
  - La línea de productos de Windows de Bitdefender
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.

12.2. Acceso a Bitdefender Central

Existen varias formas de acceder Bitdefender Central. Dependiendo de la tarea que desee realizar, puede optar por cualquiera de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender Antivirus for Mac:
  1. Haga clic en el enlace **Ir a su cuenta** de la parte inferior derecha de la pantalla.
- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a internet.
  2. Diríjase 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.

12.3. Mis suscripciones

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

12.3.1. 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. Acceda a Bitdefender Central.

2. Haga clic en el icono ubicado en la esquina superior izquierda de la ventana y, a continuación, seleccione el panel **Mis suscripciones**.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Haga clic en **ACTIVAR** para continuar.

La suscripción ya está activada.

Para comenzar la instalación del producto en sus dispositivos, consulte "*Instalando Bitdefender Antivirus for Mac*" (p. 189).

12.3.2. Comprar suscripción

Puede adquirir una suscripción directamente desde su cuenta Bitdefender siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono ubicado en la esquina superior izquierda de la ventana y, a continuación, seleccione el panel **Mis suscripciones**.
3. Haga clic en el enlace **Comprar ahora**. Se le redirigirá a una página Web donde podrá realizar su compra.

En cuanto termine el proceso, la disponibilidad de la suscripción será visible en la esquina inferior derecha de la interfaz principal del producto.

12.4. Mis dispositivos

El área **Mis dispositivos** en su cuenta 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.

12.4.1. Personalice su dispositivo

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

1. Acceda a Bitdefender Central.
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, haga clic en **GUARDAR**.

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

1. Acceda a Bitdefender Central.
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 **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, haga clic en **ASIGNAR**.

12.4.2. Acciones remotas

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceda a Bitdefender Central.
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 **Actualización**.

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 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, haga clic en la flecha desplegable en el área de estado superior para obtener más información. Desde aquí puede solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.

- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis completo en sus dispositivos. Haga clic en 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. Para más información sobre estos dos procesos de análisis, consulte "*Analizando Su Mac*" (p. 199).

13. PREGUNTAS FRECUENTES

¿Cómo puedo probar Bitdefender Antivirus for Mac antes de solicitar una suscripción?

Es un nuevo cliente de Bitdefender y le gustaría probar nuestro producto antes de comprarlo. El periodo de evaluación es de treinta días y puede seguir utilizando el producto instalado con solo adquirir una suscripción de Bitdefender. Para probar Bitdefender Antivirus for Mac, tiene que:

1. Crear una cuenta Bitdefender siguiendo estos pasos:
   - Diríjase a: https://central.bitdefender.com.
   - Introduzca la información requerida en los campos correspondientes. Los datos que introduzca aquí serán confidenciales.
   - Antes de seguir adelante, debe aceptar los Términos de uso. Acceda a los Términos de uso y léalos detenidamente, ya que contienen los términos y condiciones bajo los cuales puede usar Bitdefender.

     Además, puede acceder a la Política de privacidad y leerla.
   - Haga clic en **CREAR CUENTA**.
2. Descargue Bitdefender Antivirus for Mac de la siguiente manera:
   - Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
   - Escoja una de las dos opciones disponibles:
     - **Proteger este dispositivo**

       Seleccione esta opción y guarde el archivo de instalación.
     - **Proteger otros dispositivos**

       Seleccione esta opción y, a continuación, haga clic en **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **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.

- En el dispositivo en que desee instalar Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.
- Ejecute el producto Bitdefender que ha descargado.

Tengo un código de activación. ¿Cómo puedo añadir su validez a mi 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. Acceda a Bitdefender Central.
2. Haga clic en el icono ☰ ubicado en la esquina superior izquierda de la ventana y, a continuación, seleccione el panel **Mis suscripciones**.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Haga clic en **ACTIVAR** para continuar.

La extensión se puede ver ahora en su cuenta Bitdefender, y en su producto Bitdefender Antivirus for Mac instalado, en la parte inferior derecha de la pantalla.

El registro de análisis indica que todavía hay elementos sin resolver. ¿Cómo los elimino?

Los elementos sin resolver en el registro de análisis pueden ser:

- archivos de acceso restringido (xar, rar, etc.)

  Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y borrarlo manualmente. Asegúrese de vaciar la Papelera.

- buzones de correo de acceso restringido (Thunderbird, etc.)

  Solución: Utilice la aplicación para eliminar la entrada que contiene el archivo infectado.

- Contenido de las copias de seguridad

  Solución: Activar la opción **No analizar el contenido de las copias de seguridad** en Preferencias de protección o **Añadir a excepciones** los archivos detectados.

Si posteriormente se restauran los archivos infectados, Bitdefender Antivirus for Mac los detectará automáticamente y adoptará las medidas oportunas.

Nota
Se entiende por archivos de acceso restringido aquellos que Bitdefender Antivirus for Mac solo puede abrir, pero no puede modificar.

¿Dónde puedo leer información detallada sobre la actividad del producto?

Bitdefender mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para acceder a esta información, haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.

¿Puedo actualizar Bitdefender Antivirus for Mac a través de un servidor proxy?

Bitdefender Antivirus for Mac puede actualizar solo a través de servidores proxy que no requiere autenticación. No tiene que configurar ninguna configuración del programa.

Si se conecta a Internet a través de un servidor proxy que requiera autenticación, debe pasar regularmente a una conexión directa a Internet para obtener actualizaciones de la información de amenazas.

¿Cómo puedo eliminar Bitdefender Antivirus for Mac?

Para eliminar Bitdefender Antivirus for Mac, siga estos pasos:

1. Abra una ventana del **Finder** y luego acceda a la carpeta Aplicaciones.
2. Abra la carpeta Bitdefender y, a continuación, haga doble clic en Desinstalador de Bitdefender.
3. Haga clic en **Desinstalar** y espere a que finalice el proceso.
4. Haga clic en **Cerrar** para terminar.

Importante
Si hay un error, puede contactar con Atención al Cliente de Bitdefendercomo se describe en "*Pedir ayuda*" (p. 286).

¿Cómo elimino las extensiones TrafficLight de mi navegador?

- Para eliminar las extensiones TrafficLight de Mozilla Firefox, siga los pasos siguientes:

1. Abra su navegador Mozilla Firefox.
2. Vaya a **Herramientas** y seleccione **Complementos**.
3. Seleccione **Extensiones** en la columna izquierda.
4. Seleccione las extensiones y haga clic en **Eliminar**.
5. Reinicie el navegador para completar el proceso de eliminación.

- Para eliminar las extensiones TrafficLight de Google Chrome, siga los pasos siguientes:
  1. Abra su navegador Google Chrome.
  2. En la esquina superior derecha, haga clic en **Más** .
  3. Vaya a **Más herramientas** y seleccione **Extensiones**.
  4. Haga clic en el icono **Desinstalar.....** junto a la extensión que desee eliminar.
  5. Haga clic en **Eliminar** para confirmar el proceso de eliminación.
- Para eliminar las extensiones Bitdefender TrafficLight de Safari, siga los pasos siguientes:
  1. Abra su navegador Safari.
  2. Haga clic en en la barra de herramientas del navegador y haga clic en **Preferencias**.
  3. Seleccione la pestaña **Extensiones** y localice en la lista la extensión **Bitdefender TrafficLight en Safari**.
  4. Seleccione la extensión y haga clic en **Desinstalar**.
  5. Haga clic en **Eliminar de Chrome** para confirmar el proceso de eliminación.

¿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.

MOBILE SECURITY PARA IOS

14. QUÉ ES BITDEFENDER MOBILE SECURITY FOR IOS

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 ser verse comprometidos. ¿Y qué hay más importante que proteger los datos almacenados en sus cuentas online y en su smartphone?

Bitdefender Mobile Security for iOS le permite:

- Proteja sus datos mientras usa redes inalámbricas inseguras..
- Comprobar si se ha producido alguna filtración en las cuentas online que utiliza a diario.
- Localizar, bloquear y borrar los datos de su dispositivo en caso de pérdida o robo.

Bitdefender Mobile Security for iOS se proporciona de forma gratuita y requiere su activación con una cuenta de Bitdefender.

15. INICIANDO

Requisitos del Dispositivo

Bitdefender Mobile Security for iOS funciona en cualquier dispositivo que ejecute iOS 10 o superior, y necesita disponer de conexión a Internet para activarse y detectar si se ha producido alguna filtración de datos en sus cuentas online.

Instalando Bitdefender Mobile Security for iOS

- **Desde Bitdefender Central**
  - Para iOS
    1. Diríjase a: https://central.bitdefender.com.
    2. Iniciar sesión con su cuenta de Bitdefender.
    3. Toque el icono ☰ de la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
    4. Toque **INSTALAR PROTECCIÓN** y, a continuación, toque **Proteger este dispositivo**.
    5. Se le redirigirá a la aplicación de **App Store**. En la pantalla de la App Store, toque la opción de instalación.
  - Para Windows, macOS y Android
    1. Diríjase a: https://central.bitdefender.com.
    2. Iniciar sesión con su cuenta de Bitdefender.
    3. Toque el icono ☰ de la esquina superior izquierda de la pantalla y, a continuación, **Mis dispositivos**.
    4. Pulse **INSTALAR PROTECCIÓN** y, a continuación, pulse **Proteger otros dispositivos**.
    5. Pulse **ENVIAR ENLACE DE DESCARGA**.
    6. 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.

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

- **En la App Store**

  Busque Bitdefender Mobile Security for iOS para encontrar e instalar la app.

Para finalizar el proceso de instalación, 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 for iOS.

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

Inicie sesión en su cuenta de Bitdefender

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

> **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.

Asistente

La primera vez que abra la app, aparecerá un asistente de introducción que le informa sobre las características del producto. Seleccione **SIGUIENTE** para continuar, u **Omitir** para cerrar el asistente.

Panel de Control

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

La primera vez que accede a la app, se le pide permiso para que Bitdefender le envíe notificaciones. Toque **Permitir** para estar informado cada vez que Bitdefender tenga que comunicarle algo relevante relacionado con su app. Para administrar las notificaciones de Bitdefender, acceda a Ajustes > Notificaciones > Seguridad móvil.

Para acceder a la información que necesita, toque el icono correspondiente en la parte inferior de la pantalla.

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*" (p. 235).

Privacidad de la cuenta

Averigüe si se ha filtrado o no la información de sus cuentas de correo electrónico. Para más información, diríjase a "*Privacidad de la cuenta*" (p. 238).

Antirrobo

Encuentre y bloquee su dispositivo para evitar que sus datos personales caigan en malas manos. Para más información, diríjase a "*Características Antirrobo*" (p. 240).

Para ver opciones adicionales, toque el icono en su dispositivo mientras esté en la pantalla principal de la aplicación. Aparecerán las siguientes opciones:

- Restaurar compras: desde aquí puede restaurar la suscripción Premium VPN que ha adquirido a través de su cuenta de iTunes.
- Primeros pasos: Desde aquí puede realizar un recorrido rápido del producto.

- Comentarios: Desde aquí puede ejecutar el cliente de correo electrónico por defecto para enviarnos sus comentarios acerca de la app.
- Información de la app: Desde aquí tiene acceso a la información sobre la versión instalada y el Acuerdo de suscripción, la Política de privacidad y el cumplimiento de las licencias de código abierto.

16. 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 Bitdefender 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 Bitdefender VPN por primera vez. Al seguir haciendo uso de esa característica, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

Para activar Bitdefender VPN:

1. Toque el icono en la parte inferior de la pantalla.
2. Toque **Conectar** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras.

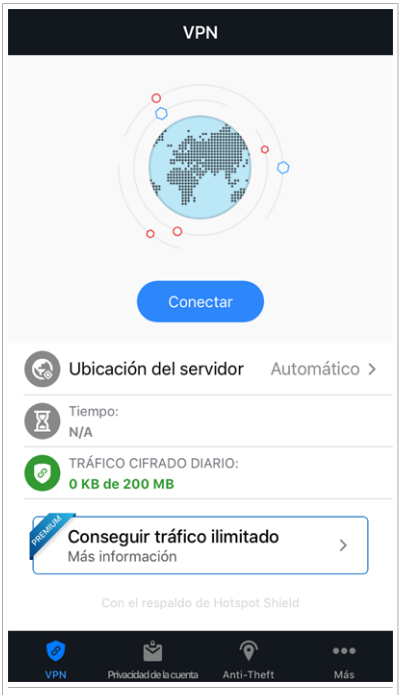
   Toque **Desconectar** cuando desee desactivar la conexión.

Nota
Cuando activa VPN por primera vez, se le pide que permita que Bitdefender configure las configuraciones VPN que monitorearán el tráfico de red. Toque **Permitir** para continuar. Si se ha configurado un método de autenticación (huella dactilar o código PIN) para proteger su smartphone, debe usarlo.

El icono VPN aparece en la barra de estado cuando VPN está activo.

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

Si posee una suscripción premium y quiere conectarse a determinado servidor, toque en **Ubicación del servidor** en la interfaz de VPN y, a continuación, seleccione el lugar que desee. Para más información sobre las suscripciones a VPN, consulte "*Suscripciones*" (p. 236).



VPN

16.1. Suscripciones

Bitdefender VPN ofrece gratuitamente una cuota de tráfico diaria de 200 MB por dispositivo para que proteja la conexión cuando su equipo lo necesite.

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

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento desde el panel **Mis suscripciones** disponible en su cuenta de Bitdefender.

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

Bitdefender VPN es un producto multiplataforma, disponible en 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.

17. PRIVACIDAD DE LA CUENTA

Privacidad de la cuenta de Bitdefender detecta si se ha producido alguna filtración de información 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.

Para comprobar si se ha filtrado alguna de las cuentas, toque **Buscar filtraciones**.

Para empezar a poner a salvo su información personal:

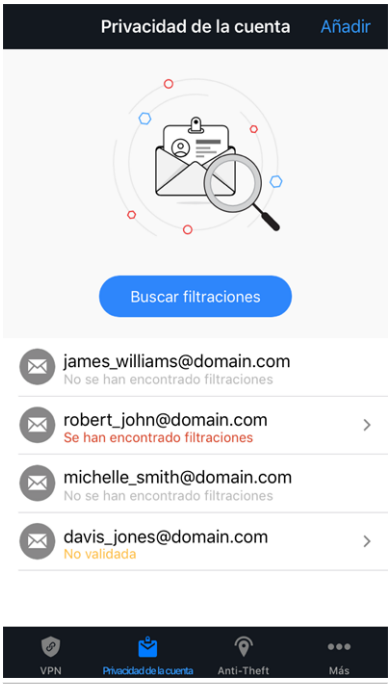
1. Toque el icono en la parte inferior de la pantalla.
2. Toque **Añadir** en la parte superior derecha de la pantalla.
3. Introduzca su dirección de correo electrónico en el campo correspondiente y, a continuación, toque **Siguiente**.

   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.
4. 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 también la carpeta de correo no deseado.

   Se muestra el estado de privacidad de la cuenta validada.

En caso de detectarse filtraciones 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 !.



Privacidad de la cuenta

18. 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.

Bitdefender Mobile Security for iOS ofrece las siguientes opciones Antirrobo:

Localización remota
Vea la ubicación actual de su dispositivo en Maps.

La precisión de la ubicación depende de cómo pueda determinarla Bitdefender:

- 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 a distancia.

Borrado remoto
Borrar todos los datos personales del dispositivo extraviado.

Activación de Antirrobo

Para habilitar las características Antirrobo:

1. Toque el icono en la parte inferior de la pantalla.
2. Active el conmutador.
3. Conceda acceso a la ubicación de su dispositivo para que Bitdefender pueda localizarlo en caso de pérdida o robo. Esta notificación aparece solo cuando activa por primera vez el Antirrobo de Bitdefender. Para

administrar el acceso a Bitdefender, vaya a Ajustes > Privacidad > Servicios de localización > Seguridad móvil.

4. La primera vez que active la característica Antirrobo en su dispositivo, también se le pedirá que instale un perfil MDM (Mobile Device Management). Por lo tanto, continúe con estos pasos:

   a. Toque **Permitir** para pasar al área de Ajustes.

   b. Toque **Instalar** para instalar el perfil de MDM (Mobile Device Management) que Bitdefender necesita para continuar con el proceso de activación.

      Si se ha configurado un código PIN para proteger su smartphone, debe usarlo.

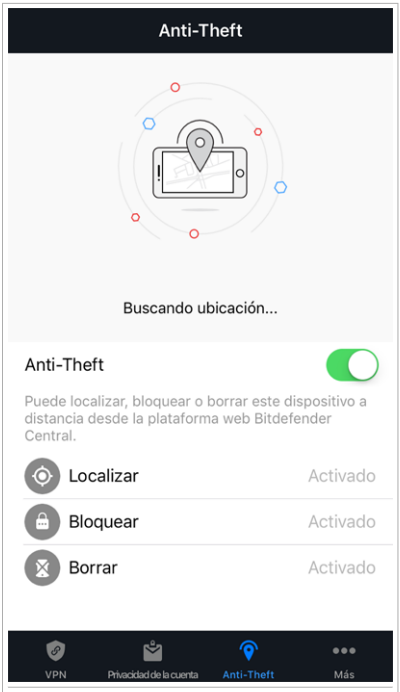
   c. Lea la información relacionada con el certificado raíz de CA y la administración de dispositivos móviles (Mobile Device Management).

   d. Si acepta los términos descritos, toque **Instalar**.

   e. Toque **Confiar** en la alerta de administración remota y, a continuación, en **Hecho** para cerrar la ventana.

Nota

Si fallase la instalación del perfil MDM actual de Bitdefender, puede que ya haya instalado un perfil MDM anterior que deba eliminarse. Por lo tanto, acceda a Ajustes > General > Administración de dispositivos > Bitdefender. Seleccione el perfil detectado y luego toque en **Eliminar administración**. Si se ha configurado un código PIN para proteger su smartphone, debe usarlo. Toque nuevamente en **Eliminar administración** para confirmar su elección. Intente activar el Antirrobo nuevamente. Si el problema persiste, envíenos un correo electrónico a bdios@bitdefender.com.



Antirrobo

Utilización de las funciones de Antirrobo desde Bitdefender Central (Control Web)

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

1. Diríjase a: https://central.bitdefender.com.
2. Iniciar sesión con su cuenta de Bitdefender.
3. Toque el icono ☰ de la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
4. Toque en la tarjeta del dispositivo deseado y, a continuación, en la pestaña **Antirrobo**.
5. En el campo inferior de la ventana, toque el icono correspondiente a la característica que desee utilizar:

Mostrar IP - Muestra la última dirección IP del dispositivo seleccionado.
Localizar: Muestra la ubicación de su dispositivo en Maps.

Bloquear - bloquee su dispositivo y establezca un código PIN para desbloquearlo.

Borrar - elimina toda la información de su dispositivo.

Importante
Después de borrar un dispositivo, todas las características de Antirrobo dejan de funcionar.

19. CUENTA BITDEFENDER

Hace falta una cuenta de Bitdefender para activar Bitdefender Mobile Security for iOS. Siempre que desee acceder a las características y servicios online del producto o realizar a distancia tareas importantes en dispositivos en los que Bitdefender esté instalado, puede iniciar sesión en su cuenta desde cualquier equipo o dispositivo móvil conectado a Internet con solo acceder a https://central.bitdefender.com.

Mis dispositivos

El área **Mis dispositivos** en su cuenta 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.

Para identificar y administrar fácilmente sus dispositivos, puede personalizar el nombre del dispositivo y crear o asignar un propietario a cada uno de ellos:

1. Toque el icono ☰ de la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.

2. Toque la tarjeta del dispositivo deseado y, a continuación, el icono ⋮ de la esquina superior derecha de la pantalla. Tiene las siguientes opciones a su disposición:

   - **Ajustes**: Desde aquí puede cambiar el nombre del dispositivo seleccionado.
   - **Perfil**: Desde aquí se puede asignar un perfil al dispositivo seleccionado. Toque **Añadir propietario** y, a continuación, rellene los campos correspondientes, establezca el nombre, dirección de correo electrónico, número de teléfono y fecha de nacimiento, e incluso añada una imagen al perfil.
   - **Eliminar**: Desde aquí se puede eliminar de su cuenta de Bitdefender un perfil junto con el dispositivo asignado.

Inicio de sesión con otra cuenta de Bitdefender

Para iniciar sesión con otra cuenta de Bitdefender:

1. Toque el icono en la parte inferior de la pantalla.
2. Toque **Cerrar sesión**.
3. Escriba su dirección de correo electrónico y contraseña de la cuenta de Bitdefender en los campos correspondientes.
4. Toque **INICIAR SESIÓN**.

MOBILE SECURITY PARA ANDROID

20. FUNCIONES DE PROTECCIÓN

Bitdefender Mobile Security protege su dispositivo Android con las siguientes funciones:

- Analizador malware
- Protección Web
- VPN
- Antirrobo, incluyendo:
  - Localización remota
  - Bloqueo de dispositivo remoto
  - Borrado de dispositivo remoto
  - Alertas de dispositivo remotas
- Privacidad de la cuenta
- Bloqueo de apps
- Informes
- Localizador

Puede usar el producto durante 14 días, sin cargo alguno. Tras expirar el período, ha de adquirir la versión completa para proteger su dispositivo móvil.

21. INICIANDO

Requisitos del Dispositivo

Bitdefender Mobile Security funciona en cualquier dispositivo que ejecute Android 4.0.3 y superior. Se necesita una conexión a Internet activa para el análisis de amenazas en la nube.

Instalando Bitdefender Mobile Security

- **Desde Bitdefender Central**
  - Para Android
    1. Diríjase a: https://central.bitdefender.com.
    2. Iniciar sesión con su cuenta de Bitdefender.
    3. Toque en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
    4. Toque **INSTALAR PROTECCIÓN** y, a continuación, toque **Proteger este dispositivo**.
    5. Se le redirigirá a la app **Google Play**. En la pantalla de Google Play, toque la opción de instalación.
  - En Windows, macOS, iOS
    1. Diríjase a: https://central.bitdefender.com.
    2. Iniciar sesión con su cuenta de Bitdefender.
    3. Toque en la esquina superior izquierda de la pantalla y, a continuación, **Mis dispositivos**.
    4. Pulse **INSTALAR PROTECCIÓN** y, a continuación, pulse **Proteger otros dispositivos**.
    5. Pulse **ENVIAR ENLACE DE DESCARGA**.
    6. 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.

7. 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:

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.

Inicie sesión en su cuenta de Bitdefender

Para usar Bitdefender Mobile Security debe vincular su dispositivo a una cuenta de Bitdefender, Facebook, Google 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 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.

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 aplicación 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 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.

Panel de Control

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

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 malware
Le permite iniciar un análisis bajo demanda y habilitar Analizar almacenamiento. Para más información, diríjase a "*Analizador malware*" (p. 253).

Protección Web
Le garantiza una navegación segura por Internet alertándole de posibles páginas web maliciosas. Para más información, diríjase a "*Protección Web*" (p. 256).

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*" (p. 258).

Antirrobo
Le permite activar o desactivar el Antirrobo, así como configurar sus ajustes. Para más información, diríjase a "*Características Antirrobo*" (p. 261).

Privacidad de la cuenta

Comprueba si se ha producido alguna vulneración de datos de sus cuentas en Internet. Para más información, diríjase a "*Privacidad de la cuenta*" (p. 265).

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*" (p. 267).

Informes

Mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con la actividad de su dispositivo. Para más información, diríjase a "*Informes*" (p. 272).

Localizador

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*" (p. 273).

22. ANALIZADOR MALWARE

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

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 en la instalación**

  Siempre que instale una aplicación, Bitdefender Mobile Security la analizará automáticamente usando 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 solicitado**

  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. Tras tocar el botón **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.

Análisis malware

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.

23. PROTECCIÓN WEB

Seguridad web, gracias a los servicios en la nube de Bitdefender, comprueba las páginas web a las que accede con el navegador predeterminado de Android, Google Chrome, Firefox, Opera, Opera Mini y Dolphin. Tiene a su disposición una lista completa con todos los navegadores compatibles en la sección de Seguridad web.

Si una URL apunta a un sitio Web conocido de phishing o fraudulento, o a contenido malicioso como spyware o virus, la página Web se bloquea temporalmente y se muestra una alerta.

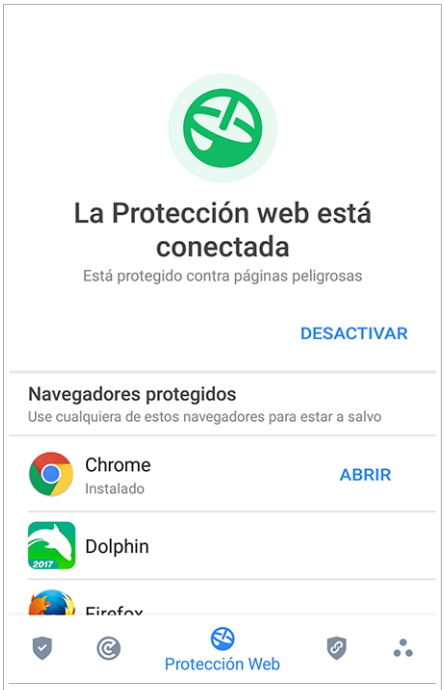
Puede elegir ignorar la alerta y entrar en la página Web o volver a una página segura.

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.

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



Protección Web

24. 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 Bitdefender 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 Bitdefender VPN por primera vez. Al seguir haciendo uso de esa característica, 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.

El icono aparece en la barra de estado cuando Bitdefender VPN está activo.

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 “Suscripciones” (p. 260).

VPN

Ajustes de VPN

Para una configuración avanzada de su VPN:

1. Toque **Más** en la barra de navegación inferior.

2. Toque **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.
- Red 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.

Suscripciones

Bitdefender VPN ofrece gratuitamente una cuota de tráfico diaria de 200 MB por dispositivo para que proteja la conexión cuando su equipo lo necesite.

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

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento desde el panel **Mis suscripciones** disponible en su cuenta de Bitdefender.

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

Bitdefender VPN es un producto multiplataforma, disponible en 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.

25. 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.

Bitdefender Mobile Security ofrece las siguientes opciones Antirrobo:

Localizar remotamente

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 pueda determinarla Bitdefender:

- 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.

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. Toque **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. Diríjase a: https://central.bitdefender.com.

ii. Inicie sesión en su cuenta.

iii. Toque ☰ en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.

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.

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. Toque en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
3. En la ventana **MIS DISPOSITIVOS**, seleccione la tarjeta de dicho dispositivo.
4. Seleccione la pestaña **Antirrobo**.
5. En el campo inferior de la ventana, toque y, a continuación, toque el botón correspondiente a la característica que desee utilizar:

   Localizar - muestra la ubicación de su dispositivo en Google Maps.

   Alerta - escriba un mensaje para mostrarlo en la pantalla de su dispositivo y/o haga que su dispositivo reproduzca una alarma sonora.

   Bloquear - bloquee su dispositivo y establezca un código PIN para desbloquearlo.

   Borrar - elimina toda la información de su dispositivo.

   Importante
   Después de borrar un dispositivo, todas las características de Antirrobo dejan de funcionar.

   Mostrar IP - Muestra la última dirección IP del dispositivo seleccionado.

Ajustes de Antirrobo

Si desea habilitar o deshabilitar los comandos remotos:

1. Toque **Más** en la barra de navegación inferior.
2. Toque **Antirrobo**.
3. Habilitar o deshabilitar las opciones deseadas.

26. PRIVACIDAD DE LA CUENTA

Privacidad de la cuenta 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 aplicaciones 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. Toque **Más** en la barra de navegación inferior.
2. Toque **Privacidad de la cuenta**.
3. Toque **PUESTA EN MARCHA**.
4. Aparece la dirección de correo electrónico utilizada para crear su cuenta de Bitdefender.

   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.
5. 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.

   Para añadir otras cuentas, toque **AÑADIR CUENTA** en la ventana de Privacidad de la cuenta y, a continuación, siga los pasos necesarios.

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

27. 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.

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.

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. Toque **Más** en la barra de navegación inferior.
2. Toque **Bloqueo de apps**.
3. Toque **ACTIVAR**.
4. Permitir el acceso a los datos de uso para Bitdefender.

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

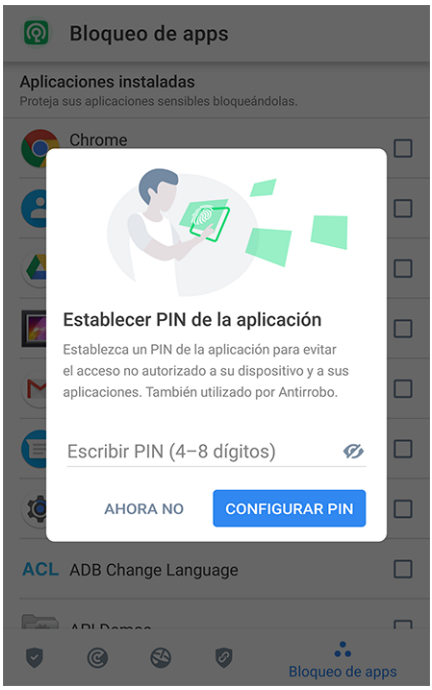
5. Vuelva a la app, configure el código de acceso y, a continuación, toque **ESTABLECER PIN**.

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

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



Bloqueo de apps

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

Opciones de Bloqueo de Apps

Para una configuración avanzada del Bloqueo de apps:

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

Hacer foto

Con Hacer foto de Bitdefender puede poner en una situación comprometida a sus amigos o familiares. De esta manera educará 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 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. Toque **Más** en la barra de navegación inferior.
2. Toque **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. Diríjase a: https://central.bitdefender.com.
2. Inicie sesión en su cuenta.
3. Toque en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
4. Seleccione su dispositivo Android y, a continuación, la pestaña **Antirrobo**.
5. Toque junto a **Consulte sus instantáneas** para ver las últimas fotos que se hicieron.

Solo se guardan las dos últimas fotos.

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

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

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. Toque **Más** en la barra de navegación inferior.
2. Toque **Bloqueo de apps**.
3. Toque **AÑADIR** para establecer la conexión Wi-Fi que utiliza actualmente como red de confianza.

Nota
Este ajuste solo está disponible si el Desbloqueo inteligente está activado.

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.

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

29. 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 está puesto 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.

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:

Start:<Where is my phone>

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. **Alerta**

   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.

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

31. BITDEFENDER CENTRAL

Bitdefender Central es la plataforma Web 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:

- Descargue e instale Bitdefender en los sistemas operativos Windows, iOS, macOS y Android. Los productos disponibles para su descarga son:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security for iOS
  - Bitdefender Antivirus for Mac
  - La línea de productos de Windows de Bitdefender
- 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.

Acceso a su cuenta de Bitdefender

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. Diríjase 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, se le proporcionan las opciones e instrucciones disponibles en la plataforma web.

Mis dispositivos

El área **Mis dispositivos** en su cuenta 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.

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

1. Acceda a Bitdefender Central.
2. Toque ☰ en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
3. Toque la tarjeta del dispositivo deseado y, a continuación, toque ⋮ en la esquina superior derecha de la pantalla.
4. Seleccione **Ajustes**.
5. Escriba un nuevo nombre en el campo **Nombre del dispositivo** y, a continuación, seleccione **GUARDAR**.

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

1. Acceda a Bitdefender Central.
2. Toque ☰ en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
3. Toque la tarjeta del dispositivo deseado y, a continuación, toque ⋮ en la esquina superior derecha de la pantalla.

4. Seleccione **Perfil**.
5. Toque **Añadir propietario** y, a continuación, rellene los campos correspondientes. Personalice el perfil añadiendo una foto y seleccionando una fecha de nacimiento.
6. Toque **AÑADIR** para guardar el perfil.
7. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, toque **ASIGNAR**.

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

Una vez que seleccione 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 solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis en su dispositivo. Toque en 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.
- **Antirrobo**. Si no se acuerda de dónde ha puesto su dispositivo, 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. Para más información sobre esta característica, consulte "*Características Antirrobo*" (p. 261).

Mis suscripciones

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

Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceda a Bitdefender Central.
2. Toque ☰ en la esquina superior izquierda de la pantalla y, a continuación, seleccione **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.

Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Mobile Security como se indica en “Instalando Bitdefender Mobile Security” (p. 248):

Renovar la suscripción

Si le quedan menos de treinta días a su suscripción y usted rechazó la renovación automática, puede renovarla manualmente siguiendo estos pasos:

1. Acceda a Bitdefender Central.
2. Toque ☰ en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis suscripciones**.
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.

32. 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 -> usado para la comunicación cloud.
- 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 Bitdefender cloud.
- Leer y guardar favoritos del navegador -> el módulo Seguridad Web elimina sitios peligrosos de su historial de navegación.
- Leer datos de registro -> Bitdefender Mobile Security detecta signos de actividades de amenaza desde los registros de Android.
- Localizar -> requerido 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?

De manera predeterminada, 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:

1. Toque **Más** en la barra de navegación inferior.
2. Toque **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. Toque **Más** en la barra de navegación inferior.
2. Toque **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. Acceda a Bitdefender Central.
2. Toque en la esquina superior izquierda de la pantalla y, a continuación, seleccione **Mis dispositivos**.
3. Toque la tarjeta del dispositivo deseado y, a continuación, toque en la esquina superior derecha de la pantalla.
4. Seleccione **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. Toque **Más** en la barra de navegación inferior.
2. Toque **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. Toque **Más** en la barra de navegación inferior.
2. Toque **Bloqueo de apps**.
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. Acceda a Bitdefender Central.
2. Toque en la parte superior derecha de la pantalla.
3. Toque **Mi cuenta** en el menú deslizante.
4. Seleccione la pestaña **Configuración**.
5. 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 Bitdefender asociada a mi dispositivo?

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

1. Toque **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 repercutirá Bitdefender Mobile Security en el rendimiento y en la autonomía de 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 función 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 completarse para eliminar 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:

- Vaya a los Ajustes de Android > 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 comprobar esto, diríjase a Ajustes > cuentas & sincronización y mire si existe una cuenta de Google bajo **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.

CONTACTO

33. PEDIR AYUDA

Bitdefender proporciona a sus clientes un nivel sin igual de soporte rápido y preciso. Si está experimentando cualquier incidencia o si tiene cualquier pregunta sobre su producto Bitdefender, puede utilizar varios recursos online para encontrar rápidamente una solución una respuesta. Al mismo tiempo, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

La sección "*Resolución de incidencias comunes*" (p. 155) le proporciona la información necesaria sobre las incidencias más frecuentes a las que se pueda enfrentar cuando utiliza este producto.

Si no encuentra una respuesta a su pregunta en los recursos proporcionados, puede llamarnos al **(+1) 800 839 6823** o enviarnos un correo electrónico a soho@bitdefender.com. Como alternativa, puede ponerse directamente en contacto con nosotros:

- "Póngase en contacto con nosotros directamente desde Bitdefender Total Security" (p. 286)
- "Póngase en contacto con nosotros a través de nuestro Centro de Soporte online" (p. 287)

Póngase en contacto con nosotros directamente desde Bitdefender Total Security

Si dispone de una conexión a internet, puede ponerse en contacto con Bitdefender directamente desde la interfaz del producto para obtener asistencia.

Siga estos pasos:

1. Haga clic en **Soporte** en el menú de navegación de la interfaz de Bitdefender.
2. Dispone de las opciones siguientes:
   - **GUÍA DE USUARIO**

     Acceda a nuestra base de datos y busque la información necesaria.
   - **SOPORTE TÉCNICO**

     Acceda a nuestros vídeos tutoriales y artículos online.

- **CONTACTAR SOPORTE**

  Haga clic en **CONTACTAR CON SOPORTE** para iniciar la Herramienta de soporte de Bitdefender y contactar con el departamento de atención al cliente.

  a. Rellene el formulario de envío con los datos necesarios:

     i. Seleccione el tipo de problema que ha experimentado.

     ii. Escriba una descripción del problema que se ha encontrado.

     iii. Haga clic en **TRATAR DE REPRODUCIR ESTE PROBLEMA** en caso de que se enfrente a un problema con el producto. Reproduzca el problema y luego haga clic en **FINALIZAR** en la zona REPRODUCIENDO EL PROBLEMA.

     iv. Haga clic en **CONFIRMAR TICKET**.

  b. Siga rellenando el formulario de envío con los datos necesarios:

     i. Escriba su nombre completo.

     ii. Escriba su dirección de correo electrónico.

     iii. Marque la casilla de verificación de aceptación.

     iv. Haga clic en **CREAR PAQUETE DE DEPURACIÓN**.

     Espere unos momentos mientras Bitdefender recopila información relacionada con el producto. Esta información ayudará a nuestros ingenieros a encontrar una solución a su problema.

  c. Haga clic en **CERRAR** para salir del asistente. Uno de nuestros representantes se pondrá en contacto con usted lo antes posible.

Póngase en contacto con nosotros a través de nuestro Centro de Soporte online

Si no puede acceder a la información necesaria utilizando el producto Bitdefender, consulte nuestro Centro de soporte online:

1. Visite https://www.bitdefender.com/support/consumer.html.

   El Centro de Soporte de Bitdefender alberga numerosos artículos que contienen soluciones de incidencias relacionadas con Bitdefender.

2. Utilice la barra de búsqueda en la parte superior de la ventana para encontrar los artículos que puedan proporcionar una solución a su

problema. Para hacer una búsqueda, simplemente escriba un término en la barra de Búsqueda y haga clic en **Buscar**.

3. Consulte los artículos o documentos relevantes e intente las soluciones propuestas.
4. Si la solución propuesta no resolviese el problema, acceda a

   https://www.bitdefender.com/support/contact-us.htmly póngase en contacto con nuestros representantes de soporte.

34. RECURSOS ONLINE

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

- Centro de soporte de Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Foro de Soporte de Bitdefender:

  https://forum.bitdefender.com

- El portal de seguridad informática HOTforSecurity:

  https://www.hotforsecurity.com

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

34.1. 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 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 comprensión que necesitan. Todas las solicitudes válidas de información o informes de errores provenientes de los clientes Bitdefender, finalmente acaban 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 Bitdefender está siempre disponible en

https://www.bitdefender.com/support/consumer.html.

34.2. Foro de Soporte de Bitdefender

El Foro de Soporte de Bitdefender proporciona a los usuarios de Bitdefender una manera fácil para obtener ayuda y ayudar a otros.

Si su producto de Bitdefender no funciona bien, si no puede eliminar determinadas amenazas de su equipo o si tiene preguntas sobre cómo funciona, publique en el foro su problema o pregunta.

El soporte técnico de Bitdefender monitoriza el foro para nuevos posts con el fin de asistirle. Podrá obtener una respuesta o una solución de un usuario de Bitdefender con más experiencia.

Antes de publicar su problema o pregunta, busque en el foro un tema similar o que tenga relación.

El Foro de Soporte de Bitdefender está disponible en https://forum.bitdefender.com, en 5 idiomas diferentes: Inglés, Alemán, Francia, España y Rumano. Haga clic en el enlace **Protección Doméstica** para acceder a la sección dedicada a los productos de consumo.

34.3. Portal HOTforSecurity

El portal HOTforSecurity es una preciada fuente de información de seguridad informática. Aquí puede saber las varias amenazas a las que está expuesto su pc cuando está conectado a Internet (malware, phishing, spam, cibercriminales).

Se postean nuevos artículos regularmente para que se mantenga actualizado sobre las últimas amenazas descubiertas, amenazas actuales y otra información de la industria de seguridad de equipos.

La página Web de HOTforSecurity es https://www.hotforsecurity.com.

35. INFORMACIÓN DE CONTACTO

La eficiente comunicación es la clave para un negocio con éxito. Desde 2001, BITDEFENDER se ha forjado una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectativas de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

35.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Centro de soporte:https://www.bitdefender.com/support/consumer.html
Documentación: documentation@bitdefender.com
Distribuidores Locales:https://www.bitdefender.com/partners
Programa de partners: partners@bitdefender.com
Relaciones con los medios: pr@bitdefender.com
Empleos: jobs@bitdefender.com
Envió de amenazas: virus_submission@bitdefender.com
Envíos de spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Página Web:https://www.bitdefender.com

35.2. Distribuidores locales

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

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite https://www.bitdefender.es/partners/partner-locator.html.
2. Elija su país y ciudad mediante las opciones correspondientes.
3. Si no encuentra un distribuidor Bitdefender en su país, no dude en contactar con nosotros por correo en comercial@bitdefender.es. Escriba su correo en inglés para que podamos ayudarle rápidamente.

35.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están lista para responder a cualquier pregunta sobre sus áreas de operación, tanto comerciales como de asuntos generales. Sus direcciones y contactos están listados a continuación.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Tel (oficina&comercial): 1-954-776-6262
Comercial: sales@bitdefender.com
Soporte Técnico: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Reino Unido e Irlanda

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Correo: info@bitdefender.co.uk
Teléfono: (+44) 2036 080 456
Comercial: sales@bitdefender.co.uk
Soporte Técnico: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Alemania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Oficina: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Comercial: vertrieb@bitdefender.de
Soporte Técnico: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Dinamarca

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Oficina: +45 7020 2282
Soporte Técnico: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

España

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Teléfono: +34 902 19 07 65
Comercial: comercial@bitdefender.es
Soporte Técnico: https://www.bitdefender.es/support/consumer.html
Página Web: https://www.bitdefender.es

Rumania

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax: +40 21 2641799
Teléfono comercial: +40 21 2063470
Correo comercial: sales@bitdefender.ro
Soporte Técnico: https://www.bitdefender.ro/support/consumer.html
Página Web: https://www.bitdefender.ro

Emiratos Árabes Unidos

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Teléfono comercial: 00971-4-4588935 / 00971-4-4589186
Correo comercial: mena-sales@bitdefender.com
Soporte Técnico: https://www.bitdefender.com/support/consumer.html
Página Web: https://www.bitdefender.com

Glosario

ActiveX

ActiveX es un modo de escribir programas de manera que otros programas y el sistema operativo puedan usarlos. La tecnología ActiveX es empleada por el Microsoft Internet Explorer para hacer páginas web interactivas que se vean y se comporten como programas más que páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, apretar botones, interaccionar de otras formas con la página web. Los mandos de ActiveX se escriben generalmente usando Visual Basic.

ActiveX es notable por la ausencia absoluta de mandos de seguridad; los expertos de la seguridad computacional desaprueban desalientan el empleo de ActiveX en Internet.

Actualización de información de amenazas

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

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.

Adware

El adware habitualmente se combina con aplicaciones que son gratuitas a cambio de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan el propósito de la aplicación, no se comete ningún delito.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas

de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

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.

Amenaza persistente avanzada

Una amenaza persistente avanzada (Advanced Persistent Threat, APT) explota vulnerabilidades de los sistemas para robar información importante que se entrega a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el objetivo primordial de esta amenaza.

El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo, para poder monitorizar y recopilar información importante sin dañar las máquinas objetivo. El método empleado para inyectar la amenaza en la red es un archivo PDF o un documento de Office que parezca inofensivo, para que cualquier usuario decida ejecutarlo.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Archivo Comprimido

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Archivo de informe

Es un fichero que lista las acciones ocurridas. Bitdefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

Área de notificación 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.

Backdoor

Es una brecha de seguridad dejada intencionalmente por los diseñadores o los administradores. La motivación no es siempre maléfica; algunos sistemas operativos funcionan con unas cuentas privilegiadas, concebidas para el uso de los técnicos del service o para los responsables con el mantenimiento del producto, de parte del vendedor.

Botnet

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

Cliente de mail

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

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.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Correo

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Descargar

Para copiar información (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal. También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

Elementos en 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.

Eventos
Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Explorador
Abreviatura de navegador web, una aplicación de software utilizada para localizar y mostrar páginas web. los navegadores más populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren plugins para ciertos formatos.

Extensión de un archivo
La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

Falso positivo
Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.

Gusano
Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede añadir a otros programas.

Heurístico
Un método basado en reglas para identificar nuevas amenazas. Este método de análisis no se basa en una determinada base de datos de información de amenazas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de una amenaza existente. Sin embargo,

puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

Honeypot (sistema trampa)
Un sistema informático que sirve como señuelo para atraer a los piratas informáticos con el fin de estudiar cómo actúan e identificar los métodos delictivos que utilizan para recabar información del sistema. Las empresas y grandes corporaciones están más interesadas ??en implementar y utilizar estos sistemas trampa para mejorar su estado general de seguridad.

IP
Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

Keylogger
Un keylogger es una app que registra todo lo que usted escribe.

Los keyloggers en su esencia no son maliciosos. Pueden ser utilizados para propósitos legítimos, como monitorizar la actividad de los empleados o niños. Sin embargo, son cada vez más utilizados por cibercriminales con fines maliciosos (por ejemplo, para recoger datos privados, como credenciales y números de seguridad social).

Línea de comando
En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Memoria
Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

No Heurístico
Este método de análisis se basa en una determinada base de datos de información de amenazas. La ventaja del análisis no heurístico es que

no se deja engañar por lo que podría parecer una amenaza y no genera falsas alarmas.

Phishing

El acto de enviar un email a un usuario simulando pertenecer a una empresa legítima e intentar estafar al usuario solicitándole información privada que después se utilizará para realizar el robo de identidad. El email conduce al usuario a visitar una página web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, de la seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Photon

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

Programas Empaquetados

Son ficheros en formato comprimido. Muchos sistemas operativos y varias aplicaciones contienen comandos que le permiten a usted empaquetar un fichero para que ocupe menos espacio en la memoria. Por ejemplo: tiene un fichero de texto conteniendo diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

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.

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.

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 hacía referencia a herramientas recompiladas que proporcionaba a los intrusos de derechos de administrador, permitiéndoles ocultar su presencia para no ser visto 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 periféricoa, 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.

Ruta

Las rutas exactas de un archivo en un equipo. Esta suma de información es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

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.

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Spam

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

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.

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.

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.

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 viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar Troya.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Virus de boot

Una amenaza que infecta el sector de arranque de un disco fijo o disquete. Un intento de arranque desde un disquete infectado con un virus en el 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.

Virus de macro

Un tipo de amenaza informática codificada como una macro incrustada en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

Estas aplicaciones permiten introducir un macro en un documento y también que el macro se ejecute cada vez que se abra el documento.

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.