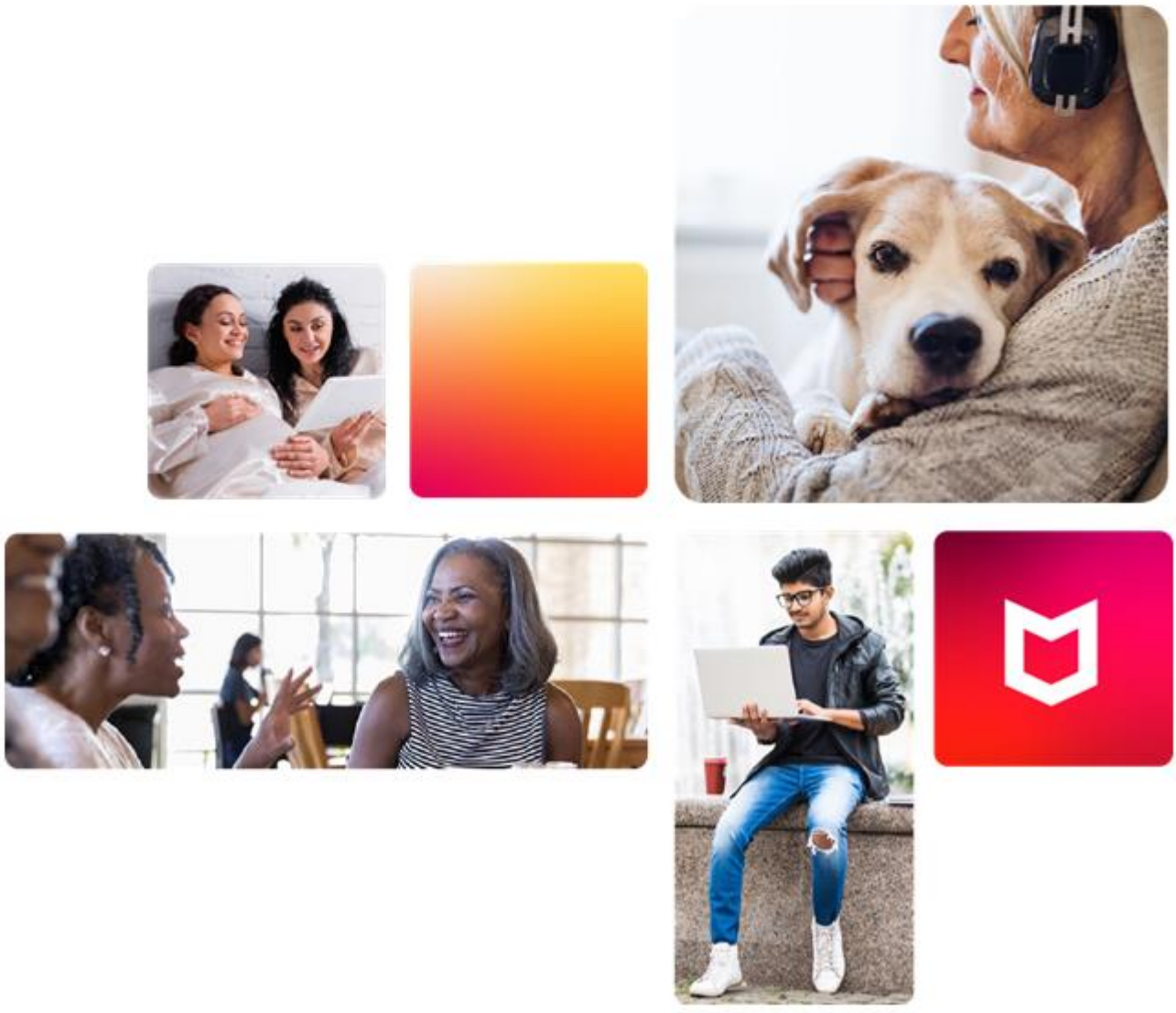
McAfee Multidispositivo
Preguntas Frecuentes (FAQ)



ESTE DOCUMENTO SÓLO PUEDE SER COMPARTIDO BAJO NDA.

ESTE DOCUMENTO ESTÁ DESTINADO ÚNICAMENTE A FACILITAR LA INFORMACIÓN ENTRE LAS PARTES. EL LENGUAJE EN ESTE DOCUMENTO NO PRETENDE CREAR, NI SE CONSIDERARÁ UN COMPROMISO LEGALMENTE VINCULANTE O EXIGIBLE, ACUERDO O SIMILARES DE CUALQUIER TIPO O NATURALEZA. ESTE DOCUMENTO CONTIENE INFORMACIÓN SOBRE PRODUCTOS, SERVICIOS Y/O PROCESOS QUE SIEMPRE ESTÁN EN DESARROLLO. TODA LA INFORMACIÓN PROPORCIONADA AQUÍ ESTÁ SUJETA A CAMBIOS SIN PREVIO AVISO A CRITERIO EXCLUSIVO DE MCAFEE. NINGUNA DE LAS PARTES TENDRÁ NINGUNA OBLIGACIÓN O RESPONSABILIDAD EN CUANTO A LOS ASUNTOS DESCRITOS EN ESTE DOCUMENTO A MENOS Y HASTA QUE LOS REPRESENTANTES DEBIDAMENTE AUTORIZADOS DE LAS PARTES EJECUTEN UN ACUERDO DEFINITIVO POR ESCRITO EN CUANTO A TALES ASUNTOS (UN "ACUERDO DEFINITIVO") Y NINGUNA PARTE TIENE ALGUNA RESPONSABILIDAD POR CUALQUIER INCUMPLIMIENTO O DENEGACIÓN DE LA EJECUCIÓN DE UN ACUERDO DEFINITIVO POR CUALQUIER MOTIVO.

Contenido

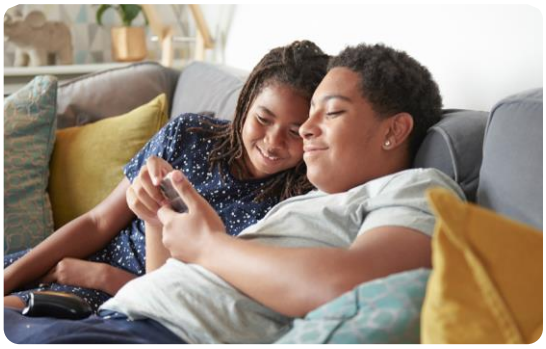
INTRODUCCIÓN

La visión de producto de McAfee es proteger al usuario de cualquier amenaza en cualquier dispositivo de cualquier red. Nuestra investigación de mercado muestra que los consumidores quieren una protección simple, perfecta y completa. Eso es lo que ofrece McAfee a través de la experiencia unificada.

Si bien McAfee ha creado un sólido portafolio de productos, ahora estamos reuniendo la experiencia del usuario para que sea lo más optimizada posible para aquellos usuarios que utilizan los distintos productos de nuestro portafolio o les ayuden a impulsar el uso de los productos adecuados en el punto que necesita.

De las características a:
Protecciones inteligentes que importan

Ahora tiene una protección inteligente de la privacidad y la identidad incorporada.



De muchas aplicaciones a:
Experiencias personalizadas y unificadas

Nuestro nuevo servicio de protección en línea le permite a usted y a su familia disfrutar libre y confiadamente de la vida en línea

De la protección de dispositivos a:
Protección de personas

Concéntrese en usted y en la seguridad de su familia en todas las actividades y dispositivos, dondequiera que se encuentre

¿QUÉ ES MCAFEE MULTI-ACCESS (MMA)?

McAfee Multi Dispositivos

Resumen de Características

Protección en línea todo en uno para su información personal y privacidad, para que pueda disfrutar de su vida en línea. Acceda a herramientas sólidas como el monitoreo preventivo de la Dark Web y la VPN segura automatizada desde cualquier dispositivo, y sea recibido con una experiencia consistente no importa si se conecta desde su PC o su dispositivo móvil.
Cumpliremos con nuestra promesa como líder confiable del mercado para proteger los datos personales y los dispositivos de todos en su hogar, ya sean usuarios avanzados de tecnología, usuarios esporádicos o intermedios.

Simplificamos la seguridad en línea para que pueda realizar operaciones bancarias, comprar, navegar y conectarse con confianza.

Conozca las nuevas características de McAfee, donde la protección es...

En todas partes
Nuestra aplicación móvil McAfee Security amplía su protección y privacidad en línea para protegerlo donde esté.
Conéctate con confianza desde la palma de tu mano, dondequiera que vayas.

Preventiva
Eres libre de vivir la vida en línea mientras monitoreamos la Dark Web, en busqueda de sus correos electrónicos y números de teléfono. Si alguna vez se ven comprometido, le daremos instrucciones fáciles de seguir para proteger su identidad.

Automatizada*
Ya sea que esté pagando facturas o simplemente explorando, Secure VPN lo ayuda a mantenerse privado. Tu VPN puede activarse automáticamente cuando lo necesites, ahora incluso en dispositivos móviles.

*Disponible solo en producto Premium

McAfee multi-Access ofrece una solución todo en uno fácil de implementar para familias de múltiples dispositivos que ayudan a evitar el daño digital. Ofrece una protección integral para PC, Mac, Android y dispositivos iOS.

¿CUÁLES SON LAS VENTAJAS PRINCIPALES DE MCAFEE® MULTI-ACCESS?

- Protege PCs, Mac, smartphones y tablets.
- La solución de seguridad fácil de usar defiende contra virus, ransomware y otras amenazas en línea.
- La navegación segura en la web le advierte sobre sitios web riesgosos y ayuda a prevenir descargas peligrosas y ataques de phishing
- La seguridad del firewall ayuda a impedir que los hackers y el malware ataquen su PC bloqueando el acceso a actividades sospechosas
- Rastree y realice una copia de seguridad remota de su dispositivo perdido o robado con protección antirrobo.

¿CUÁLES SON LAS CARACTERÍSTICAS DEL PRODUCTO?

Las características de McAfee Multi Access se dividen en tres categorías principales: Protección de Identidad, Seguridad y Privacidad.

CARACTERÍSTICAS PARA DISPOSITIVO DE ESCRITORIO

	PC	MAC
Anti-malware Bloquea virus, malware, ransomware, spyware y más. McAfee real Protect con aprendizaje automático (Machine learning) en el sistema operativo Windows y McAfee Active Protection™ en Mac OS.	✓	✓
Escáner de vulnerabilidad Asegura que su software informático y otras aplicaciones estén actualizadas y no sean vulnerables a las amenazas conocidas.	✓	
Firewall La seguridad del firewall ayuda a evitar que los hackers y el malware ataquen al ordenador bloqueando el acceso a actividades sospechosas.	✓	✓
Anti-phishing Le advierte de ataques de phishing y sitios web de phishing. Además, en PC, puede comprobar y alertar a los usuarios de sitios web riesgosos obtenidos a través de las redes sociales, correo electrónico y mensajes instantáneos, y bloquea el phishing en línea de la información personal y confidencial de un usuario.	✓	✓
Navegación web más segura Evita los sitios web riesgosos y ayuda a prevenir descargas peligrosas. Muestra iconos codificados por colores para indicar qué resultados de la búsqueda web pueden instalar código malicioso, phishing para la identidad de un usuario o enviar spam. Realiza análisis en cada sitio y los anota con clasificaciones, advirtiendo a los usuarios de posibles fallas de seguridad.	✓	✓
McAfee® WebAdvisor Bloquea sitios Web peligrosos, comprueba la protección activa de antivirus y Firewalls, escanea descargas, supervisa contraseñas y ayuda a los usuarios a tomar decisiones más inteligentes mientras usan Internet.	✓	
Gestión de redes domésticas Identifica los nombres de todos los dispositivos conectados a su Wi-Fi. Le notifica cuando los dispositivos desconocidos y nuevos obtienen acceso a su Wi-Fi.	✓	
McAfee® Shredder™ Protege su identidad y privacidad eliminando permanentemente archivos importantes de su PC: ideal para documentos tributarios, información financiera y otros archivos personales.	✓	
McAfee® QuickClean™ Ayuda a mantener su PC funcionando sin problemas eliminando las cookies y los archivos temporales que le rastrean en línea. Busca y repara problemas en la clave del registro de Windows para liberar espacio en disco y mejorar el tiempo de respuesta de la PC.	✓	
Administrador de contraseñas con autenticación multifactor (true Key) Reconoce tu huella dactilar, protege tus contraseñas y te inicia sesión instantáneamente en tus sitios web y aplicaciones en tus dispositivos.	✓	

CARACTERÍSTICAS PARA DISPOSITIVOS MÓVILES

	Android	iOS
Protección en tiempo real Con nuestro análisis de seguridad de un toque, verificaremos y protegeremos las fotos, los contenidos audiovisuales y los archivos de tu dispositivo contra malware, virus y otras amenazas	✓	
Protección de Identidad Buscaremos tu información personal en una base de datos de la Dark Web y te haremos saber si encontramos algo. Si encontramos que tu información personal ha sido filtrada, te mostraremos como protegerte. No te preocupes, mantendremos privada cualquier información que encontremos	✓	✓
Análisis de WiFi Cuando te conectas a una red WiFi, hacemos un análisis en segundo plano para comprobar si es insegura, incluso si la aplicación está cerrada.	✓	✓
Navegación Segura Antes que llegues a una página web sospechosa, te mostraremos una pantalla de advertencia, Podrás optar por continuar o evitar la página de forma segura	✓	✓
***VPN** Cuando envíes información personal a una aplicación o sitio, la cifraremos para que sea ilegible para todos menos para ti. Puedes tomar el control en cualquier momento que busques seguridad y privacidad adicionales mientras realizas operaciones bancarias, compras y navegas.	✓	✓

*VPN incluido solo en producto premium

PREGUNTAS FRECUENTES POR DISPOSITIVO

PC

¿CUÁLES SON LAS CARACTERÍSTICAS DEL PRODUCTO PARA PC?

Proporciona una protección esencial y galardonada para ordenadores con Windows. Protege las PC con Windows de las amenazas de Internet: protege la socialización, descarga y compra en línea. Salvaguarda Wi-Fi y ayuda a los usuarios a tomar decisiones más inteligentes sobre lo que hacen clic cuando están en línea. Proporciona protección antivirus esencial, ayuda a detener a los hackers y protege contra aplicaciones maliciosas y no certificadas.

¿Qué es la funcionalidad de Anti-virus — real Protect?
Protege contra los siguientes tipos de malware:

- Virus
- Troyanos
- Spyware
- Rootkits
- Gusanos (worms)
- Registradores de claves (Key Logers)

Ventajas:

- Analiza el malware que se sabe que interfiere con las instalaciones del producto
- Autentica en tiempo real para determinar si una aplicación es una amenaza
- Pone en cuarentena y elimina las amenazas mediante la comprobación cruzada de los archivos de firmas que se descargan automáticamente desde la nube de McAfee Global Threat Intelligence
- Mantiene los equipos funcionando más rápido y sin amenazas
- Impide a los ciberdelincuentes robar contraseñas
- Impide que los ciberdelincuentes tomar el control de la PC
- Protege los datos de la eliminación o la corrupción

¿Qué es la funcionalidad de **Firewall?**

- Monitorea el tráfico dentro y fuera del PC
- Ayuda a detener la transferencia de datos a destinos no seguros
- Niega que personas y programas no autorizados obtengan redes y Acceso al PC
- Protege contra hackers que accedan al PC
- Impide que PC propague malware y spam
- Salvaguarda información confidencial como nombres de cuenta y contraseñas

¿Qué es la funcionalidad de **Escáner de vulnerabilidad?**

- Identifica el software que necesita actualizarse comprobando la versión en nuestra base de datos
- Proporciona una solución de 1 clic para actualizar el software
- Permite a los usuarios actualizar más fácilmente el software para evitar agujeros de seguridad

¿Qué es la funcionalidad de **McAfee® WebAdvisor** - **Solución de protección de navegación?**

La próxima generación de protección de navegación que aprovecha la inteligencia de amenazas global de McAfee para proporcionar más valor y atraer positivamente a los usuarios para proteger sus actividades en línea.

- Identifica contraseñas comprometidas
  - Supervisa las contraseñas
  - Aconseja si una contraseña es una que es utilizada activamente por los hackers

- Comprueba la protección activa de antivirus y firewalls
  - Identifica si la configuración de seguridad está activada
  - Muestra la mensajería que se enciende desde el navegador

- Escanea descargas en busca de archivos peligrosos
  - Examina todos los archivos que un usuario intenta descargar desde el navegador
  - Muestra mensajes de advertencia si una descarga no es segura

- Bloquea sitios Web peligrosos
  - Identifica si el usuario intenta entrar en sitios web riesgosos y puede bloquear el acceso a una página

        - Muestra iconos codificados por colores para indicar qué resultados de búsqueda web pueden instalar código malicioso, phishing para robar la identidad de un usuario o enviar spam
        - Realiza análisis en cada sitio y los anota con clasificaciones, advirtiendo a los usuarios de posibles fallos de seguridad

- Protege el uso de las redes sociales
    - Ayuda a identificar si los mensajes de las redes sociales de "amigos" son seguros para hacer clic
    - Bloquea el usuario de visitar sitios Web maliciosos conocidos al hacer clic en las publicaciones
    - Ayuda a los usuarios a tomar decisiones más inteligentes sobre lo que hacen clic y descargan cuando usan sitios de redes sociales
    - Impide que los usuarios propaguen contenido malicioso a sus redes sociales
    - Protege de forma proactiva a los usuarios contra sitios Web maliciosos presentando la página de bloqueo como una advertencia de que hacer clic les conducirá a un sitio de riesgo conocido

¿Qué es la funcionalidad de **McAfee QuickClean?**

- Elimina las cookies innecesarias y los archivos temporales de Internet
- Vaciar papelera de reciclaje
- Busca y repara problemas en la clave del registro de Windows
- Limpia los archivos innecesarios del sistema que ocupa espacio valioso y ralentiza el PC
- Soluciona problemas de forma segura en el registro
- Libera espacio en disco
- Mejora el tiempo de respuesta del PC

¿Qué es la funcionalidad de **McAfee Shredder?**

- Destruye archivos de PC de forma segura como si nunca estuvieran allí en primer lugar
- Elimine manualmente documentos confidenciales como archivos de impuestos y copias de pasaportes
- Impide que un hacker pueda recuperar y restaurar los archivos que el usuario ha elegido para triturar

¿Qué es la funcionalidad de **TrueKey?**

- Guarda automáticamente las contraseñas mientras el usuario navega en la web
- Rellena las contraseñas y los registros al instante
- Los datos se sincronizan automáticamente entre plataformas, navegadores y dispositivos
- Genera contraseñas seguras con un solo clic
- Elimina la molestia de recordar todas las contraseñas diferentes
- Proporciona un lugar seguro para almacenar contraseñas utilizando el cifrado más potente disponible
- Ayuda a prevenir el acceso no autorizado a los datos verificando al usuario con autenticación multifactor

¿CÓMO DESCARGO E INSTALO LA SOLUCIÓN PARA PC?

Los métodos de instalación de los productos de software de McAfee para particulares varían según el producto y el dispositivo en que se va a instalar. Siga los pasos indicados a continuación para descargar e instalar en su dispositivo un producto de seguridad de McAfee.

Paso 1: En el equipo principal donde desea iniciar el proceso

1. Vaya a https://www.mcafee.com/.
2. Haga clic en Mi cuenta.
3. Haga clic en Sign In.
4. Escriba:
    - La **dirección de correo electrónico** de su cuenta de McAfee.
    - La contraseña de su cuenta de McAfee.
5. Haga clic en **Iniciar sesión**

Paso 2: Comenzar la instalación

1. Seleccione:
    - El tipo de **dispositivo** en el que desea realizar la instalación.
    - El **software** de McAfee que desee instalar.
2. Haga clic en **Descargar**.
3. Lea y acepte el **Acuerdo de licencia**.
4. Anote el **número de serie** mostrado. Puede que se le solicite más adelante.

SUGERENCIA: Mantenga la ventana del navegador abierta para que el número de serie siempre sea visible.

5. Siga las instrucciones para instalar el software de McAfee.

¿CÓMO INSTALAR EN UN PC DESDE UN DISPOSITIVO DIFERENTE?

Paso 1: En el equipo principal donde desea iniciar el proceso

1. Vaya a https://www.mcafee.com/.
2. Haga clic en **Mi cuenta**.
3. Haga clic en Sign In.
4. Escriba:
    - La **dirección de correo electrónico** de su cuenta de McAfee.
    - La **contraseña** de su cuenta de McAfee.
5. Haga clic en **Iniciar sesión**.

Paso 2: Enviar un vínculo de descarga al equipo secundario

1. Coloque el ratón sobre **Mi cuenta**.
2. Haga clic en **Suscripciones**.
3. Haga clic en **Agregar dispositivo** junto al producto que desee instalar.
4. Seleccione el tipo de dispositivo **Windows**.
5. Haga clic en **Enviar vínculo** y, a continuación:
    a. Escriba la **dirección de correo electrónico** de una cuenta de correo electrónico en el PC en el que desea realizar la instalación.
    b. Haga clic en **Enviar correo electrónico**.

    Se envía un correo electrónico con un vínculo de descarga al equipo en el que desea realizar la instalación.

Paso 3: En el equipo secundario

1. Abra la **aplicación de correo electrónico**.
2. Abra el **mensaje de correo electrónico** de McAfee.
3. Haga clic en el **vínculo de descarga** del mensaje.
4. Para completar la instalación, siga las indicaciones.

¿CUÁLES SON LOS REQUISITOS DEL SISTEMA PARA PC?

Windows

Sistemas Operativos	Windows 10 (32 bits y 64 bits) Windows 8.1 (32 bits y 64 bits) Windows 8 (32 bits y 64 bits)
Procesador	Procesadores compatibles con Pentium que admitan SSE2.
Espacio disponible en el disco duro	~ 500 MB
Conexión a Internet	Conexión a Internet de alta velocidad recomendada
Navegadores web (para la protección contra phishing)	Al menos uno de los siguientes: Internet Explorer 9 Firefox Chrome

¿CÓMO GESTIONAR EL FIREWALL DE MCAFEE EN WINDOWS?

Para deshabilitar el firewall en las nuevas versiones del software de McAfee:

1. Abra el software de McAfee.
2. Haga clic en el icono del **PC** o en el **icono de rueda dentada de configuración** en la esquina superior derecha.
3. Haga clic en el icono del **cortafuegos** o en la opción de menú **Cortafuegos**.
4. Haga clic en **Desactivar**.

   NOTA: Puede configurar el firewall para que se vuelva a activar automáticamente al cabo de un tiempo predefinido. Seleccione la hora deseada en la lista desplegable **Cuándo desea que continúe el firewall**.

Para habilitar el firewall en su PC:

1. Abra el software de McAfee.
2. Haga clic en el icono del **PC** o en el **icono de rueda dentada de configuración** en la esquina superior derecha.
3. Haga clic en el icono del **cortafuegos** o en la opción de menú **Cortafuegos**.
4. Haga clic en **Activar**.

MAC

¿CUÁLES SON LAS CARACTERÍSTICAS DEL PRODUCTO?

El componente de Mac – proporciona una protección esencial y galardonada para ordenadores Mac. Protege las Macs de amenazas en línea: asegura la navegación en redes sociales, descarga y compras en línea. Salvaguarda su conexión Wi-Fi y ayuda a los usuarios a tomar decisiones más inteligentes sobre donde hacen clic cuando están en línea. Proporciona protección antivirus esencial, ayuda a detener a los hackers y protege contra aplicaciones maliciosas y no certificadas.

¿Qué es la funcionalidad de **McAfee Active Protection™?**
Tipos de malware que McAfee protege contra:

- Virus
- Troyanos
- Spyware
- Rootkits
- Gusanos (Worms)
- Registradores de claves (Key loggers)

Ventajas

- Analiza el malware que se sabe que interfiere con las instalaciones del producto
- Autentica en tiempo real para determinar si una aplicación es una amenaza
- Pone en cuarentena y elimina las amenazas en tiempo real
- Mantiene las Macs corriendo y libre de amenazas
- Actualización automática de las últimas firmas de virus para una protección actualizada

¿Qué es la funcionalidad de **NetGuard?**

- Supervisa el tráfico tanto dentro como fuera de Mac
- Ayuda a detener la transferencia de datos a destinos no seguros

- Niega que personas y programas no autorizados obtengan acceso a la red y Mac
- Personaliza las reglas y la configuración del firewall
- Ayuda a impedir que los hackers accedan a Mac
- Impide que Mac propague malware y spam
- Salvaguarda información confidencial como nombres de cuenta y contraseñas

¿Qué es la funcionalidad de **Navegación web más segura?**

- Evite sitios web riesgosos
- Evitar descargas peligrosas

¿Qué es la funcionalidad de **Protección de aplicaciones?**

- Identifica las aplicaciones de software que no están autorizadas por, o no están firmadas con certificados de Apple
- Ajustes personalizables para el usuario (ejemplo: restringir el acceso a la red)
- Bloquea la ejecución de aplicaciones si no cumplen los criterios de seguridad
- Ayuda a garantizar que su Mac está a salvo de aplicaciones malas que podrían comprometer la función y la privacidad del usuario, así como su identidad

¿CÓMO DESCARGO E INSTALO LA SOLUCIÓN PARA MAC?

Los métodos de instalación de los productos de software de McAfee para particulares varían según el producto y el dispositivo en que se va a instalar. Siga los pasos indicados a continuación para descargar e instalar en su dispositivo un producto de seguridad de McAfee.

Paso 1: En el equipo principal donde desea iniciar el proceso

6. Vaya a https://www.mcafee.com/.
7. Haga clic en Mi cuenta.
8. Haga clic en Sign In.
9. Escriba:
    - La **dirección de correo electrónico** de su cuenta de McAfee.
    - La contraseña de su cuenta de McAfee.
10. Haga clic en **Iniciar sesión**

Paso 2: Comenzar la instalación

6. Seleccione:
    - El tipo de **dispositivo** en el que desea realizar la instalación.
    - El **software** de McAfee que desee instalar.
7. Haga clic en **Descargar**.
8. Lea y acepte el **Acuerdo de licencia**.
9. Anote el **número de serie** mostrado. Puede que se le solicite más adelante.

SUGERENCIA: Mantenga la ventana del navegador abierta para que el número de serie siempre sea visible.

10. Siga las instrucciones para instalar el software de McAfee.

¿CÓMO INSTALAR EN UN MAC DESDE UN DISPOSITIVO DIFERENTE?

Paso 1: En el equipo principal donde desea iniciar el proceso

6. Vaya a https://www.mcafee.com/.
7. Haga clic en **Mi cuenta**.
8. Haga clic en Sign In.
9. Escriba:
    - La **dirección de correo electrónico** de su cuenta de McAfee.
    - La **contraseña** de su cuenta de McAfee.
10. Haga clic en **Iniciar sesión**.

Paso 2: Enviar un vínculo de descarga al equipo secundario

6. Coloque el ratón sobre **Mi cuenta**.
7. Haga clic en **Suscripciones**.
8. Haga clic en **Agregar dispositivo** junto al producto que desee instalar.
9. Seleccione el tipo de dispositivo **MAC**.
10. Haga clic en **Enviar vínculo** y, a continuación:
    a. Escriba la **dirección de correo electrónico** de una cuenta de correo electrónico en el Mac en el que desea realizar la instalación.
    b. Haga clic en **Enviar correo electrónico**.

    Se envía un correo electrónico con un vínculo de descarga al equipo en el que desea realizar la instalación.

Paso 3: En el equipo secundario

5. Abra la **aplicación de correo electrónico**.
6. Abra el **mensaje de correo electrónico** de McAfee.
7. Haga clic en el **vínculo de descarga** del mensaje.
8. Para completar la instalación, siga las indicaciones.

¿CUÁLES SON LOS REQUISITOS DEL SISTEMA PARA MAC?

MAC

Sistemas operativos	macOS 11 (Big Sur) macOS 10.15 (Catalina) macOS 10.14 (Mojave) macOS 10.13 (High Sierra) macOS 10.12 (Sierra) Mac OS X 10.11 Mac OS X 10.10
Procesador	Equipos Apple con procesador Intel
Espacio disponible en el disco duro	~ 300 MB
Conexión a Internet	Conexión a Internet de alta velocidad recomendada
Navegadores web	Apple Safari

¿CÓMO GESTIONAR EL FIREWALL DE MCAFEE EN MAC?

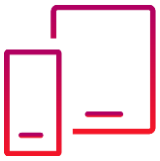
Para deshabilitar el firewall en su Mac:

1. Haga clic con el botón derecho del ratón en el icono **M** de McAfee en la barra de menús.
2. Haga clic en **Consola de (nombre del producto)**. Por ejemplo, **Consola de LiveSafe**.
3. Haga clic en **Seguridad para Mac** o en el **icono de rueda dentada** en la esquina superior derecha.
4. Haga clic en **Firewall**.
5. Haga clic en el **candado** para efectuar cambios y escriba su **contraseña**.
6. Haz clic en el **control deslizante** para **desactivar** el firewall.
7. Haga clic de nuevo en el **candado** para impedir más cambios.

En la parte superior de su producto de seguridad aparece una barra roja para indicar que su Mac está en peligro. También verá un triángulo rojo con un signo de exclamación.

Para habilitar el firewall en su Mac:

1. Haga clic con el botón derecho del ratón en el icono **M** de McAfee en la barra de menús.
2. Haga clic en **Consola de (nombre del producto)**. Por ejemplo, **Consola de LiveSafe**.
3. Haga clic en **Seguridad para Mac** o en el **icono de rueda dentada** en la esquina superior derecha.
4. Haga clic en el **candado** para efectuar cambios y escriba su **contraseña**.
5. Haga clic en el **control deslizante** para **desactivar** el firewall.
6. Haga clic de nuevo en el **candado** para impedir más cambios.



MÓVILES Y TABLETS

¿CUÁLES SON LAS CARACTERÍSTICAS DEL PRODUCTO?

El componente de teléfonos y tabletas – proporciona seguridad, privacidad y protección de identidad. Ofrece a los usuarios la tranquilidad de que siempre están protegidos de las actividades de malware que pueden poner en peligro su dispositivo o datos. Permite a los usuarios comprar y navegar de forma más segura y conectarse con confianza a cualquier red Wi-Fi.

¿Qué es la funcionalidad de **Análisis Antivirus**? (Solo Android)
Escaneo Antivirus no solo analiza las aplicaciones descargadas en su dispositivo en busca de amenazas, sino también puede analizar sus archivos.

Este escaneo verifica sus aplicaciones y archivos en busca de amenazas.

¿Qué es la funcionalidad de **Protección de identidad**?

La protección de identidad le permite verificar y monitorear continuamente sus direcciones de correo electrónico y la información adjunta, como contraseñas, que pueden estar a la venta en la dark web.
La protección de identidad está sincronizada en todos sus dispositivos, por lo que puede continuar donde lo dejó en otro dispositivo

¿Qué es la funcionalidad de **VPN**?

Utiliza una tecnología de cifrado, para proteger la información personal que se puede transmitir hacia y desde sitios web.

Al codificar los datos que se transmiten entre el consumidor y, por ejemplo, un sitio web de un banco, los ciberdelincuentes que interceptan el tráfico del consumidor se quedan con información indescifrable e imposible de interpretar.

Ayuda a navegar de manera anónima.

¿La funcionalidad de **VPN** está incluida en todos los paquetes?
No, solo está incluido en los paquetes premium

¿Qué es la funcionalidad de **Escaneo de WiFi**?
El escaneo de Wi-Fi escanea su red en busca de amenazas para garantizar que su información personal esté a salvo de los hackers.

¿Qué es la funcionalidad de **Navegación Segura**?
Cuando la navegación segura está habilitada, se muestra una página de bloqueo de McAfee si intenta visitar un sitio web malicioso.

Pero puede optar por abrir el sitio de todos modos si confía en él.

Consola de Muti dispositivos (Cross-device Console)
Los usuarios pueden administrar y extender su suscripción de MMA y comprobar el estado de seguridad de todos los dispositivos protegidos directamente desde MMS en el móvil.

¿CÓMO DESCARGO E INSTALO LA SOLUCIÓN PARA ANDROID?

Los métodos de instalación de los productos de software de McAfee para particulares varían según el producto y el dispositivo en que se va a instalar. Siga los pasos indicados a continuación para descargar e instalar en su dispositivo un producto de seguridad de McAfee.

Siga estos pasos en **el smartphone o tablet Android** donde desee instalar el producto.

Paso 1: Descargar McAfee Mobile Security en su dispositivo Android

1. Abra **Google Play Store**.
2. Busque **McAfee Mobile Security**.
3. Pulse **Instalar**. Espere a que se complete la instalación.
4. Abra **McAfee Mobile Security**.
5. Lea el Acuerdo de licencia de usuario final (EULA) y el Aviso de privacidad.
6. Pulse **Aceptar e iniciar la protección**.
7. Espere a que se complete el proceso de configuración.

Paso 2: Enviar un código de activación a su dispositivo.
Puede enviar el código desde su equipo:

1. Vaya a https://www.mcafee.com/.
2. Haga clic en **My Account**.
3. Haga clic en **Sign In**.
    - Si **ya tiene** una cuenta de McAfee:
        a. Escriba la **dirección de correo electrónico** de su cuenta de McAfee.
        b. Escriba la **contraseña** de su cuenta de McAfee.
        c. Haga clic en **Iniciar sesión**.
    - Si **no tiene** una cuenta de McAfee:
        a. Haga clic en **Registrarse ahora**.
        b. Siga las indicaciones.

SUGERENCIA: Cuando cree su cuenta, utilice una contraseña larga con letras y números, para mayor seguridad.

c. Haga clic en **Iniciar sesión**.

4. Haga clic en **Suscripciones**.
5. Haga clic en **Añadir dispositivo**.
6. Seleccione **Dispositivo móvil**.
7. Haga clic en **Enviar vínculo** y, a continuación:
    - Seleccione el tipo de dispositivo **Android**.
    - Seleccione el **tipo de suscripción**.
8. Haga clic en **Siguiente**.
9. En **How should we send the link**:
    - Elija **Por SMS** para que el vínculo del código de activación se envíe a su teléfono.
    - Elija **Por correo electrónico** para recibir el código de activación por correo electrónico.
10. Escriba la dirección de correo electrónico o el número de teléfono.
11. Haga clic en **Enviar SMS** o **Enviar correo electrónico**.

Paso 3: Activar McAfee Mobile Security

1. Abra la aplicación de **correo electrónico** o **mensajes** en el dispositivo Android.
2. Busque el mensaje de McAfee. El mensaje contiene su **código de activación**.
3. Abra **Mobile Security**.
4. Pulse el icono de **usuario** en la esquina superior derecha.
5. Pulse **¿Tienes un código de activación?**
6. Escriba el **código de activación** que ha recibido. Espere a que finalice la activación.
7. Pulse **Activar**.
8. Pulse **Finalizar**

¿CÓMO DESCARGO E INSTALO LA SOLUCIÓN PARA ANDROID DESDE UN DISPOSITIVO DIFERENTE?

Siga estos pasos para instalar McAfee Mobile Security en un dispositivo **secundario**, como el smartphone Android de su hijo, desde **su** smartphone, PC o Mac. Por ejemplo, puede enviar un vínculo de instalación desde su dispositivo y pedirle a su hijo que haga clic en el vínculo para completar la instalación en su smartphone o tablet.

Paso 1: En el dispositivo principal donde desea iniciar el proceso

1. Vaya a https://www.mcafee.com/.
2. Haga clic en **My Account**.
3. Haga clic en **Sign In**.
    - Si **ya tiene** una cuenta de McAfee:
        a. Escriba la **dirección de correo electrónico** de su cuenta de McAfee.
        b. Escriba la **contraseña** de su cuenta de McAfee.
        c. Haga clic en **Iniciar sesión**.
    - Si **no tiene** una cuenta de McAfee:
        a. Haga clic en **Registrarse ahora**.
        b. Siga las indicaciones.

SUGERENCIA: Cuando cree su cuenta, utilice una contraseña larga con letras y números, para mayor seguridad.

c. Haga clic en **Iniciar sesión**.

Paso 2: Enviar un vínculo de descarga al dispositivo secundario

1. En **Mi cuenta**, haga clic en **Suscripciones**.
2. Haga clic en **Añadir dispositivo**.
3. Seleccione **Dispositivo móvil**.
4. Haga clic en **Enviar vínculo** y, a continuación:
    - Seleccione el tipo de dispositivo **Android**.
    - Seleccione el **tipo de suscripción**.
5. Haga clic en **Siguiente**.
6. En **How should we send the link**:

    - Elija **Por SMS** para que el vínculo del código de activación se envíe a su teléfono.
    - Elija **Por correo electrónico** para recibir el código de activación por correo electrónico.
7. Escriba la dirección de correo electrónico o el **número de teléfono**.
8. Haga clic en **Enviar SMS** o **Enviar correo electrónico**.

Paso 3: Descargar, instalar y activar McAfee Mobile Security en el dispositivo secundario

1. Abra la aplicación de **correo electrónico** o **mensajes** en el dispositivo Android.
2. Busque el mensaje de McAfee. El mensaje contiene su **vínculo de descarga** y **código de activación**.
3. Pulse el vínculo de descarga para iniciar la instalación.
4. Cuando la instalación finalice, abra **McAfee Mobile Security**.
5. Pulse el icono de **usuario** en la esquina superior derecha.
6. Pulse **¿Tienes un código de activación?**
7. Escriba el **código de activación** que ha recibido. Espere a que finalice la activación.
8. Pulse **Activar** para finalizar el proceso.

¿CUÁLES SON LOS REQUISITOS DEL SISTEMA PARA ANDROID?

Android

Sistemas operativos	Google Android 2.3 posterior, incluido Android 5.x (Android L) y Android 6.x (Marshmallow)
Espacio de almacenamiento disponible	~ 35 - 50 MB
Conexión a Internet	Wi-Fi LTE 4G 3G 2G
Navegador web	Internet Explorer 9.0 o posterior Firefox 30 o posterior Safari 6.1 o posterior Google Chrome

¿CÓMO DESCARGO E INSTALO LA SOLUCIÓN PARA IOS?

Paso 1: Descargar McAfee Mobile Security en su dispositivo iOS

1. Vaya a la **App Store** de Apple.
2. Busque **McAfee Mobile Security**.

SUGERENCIA: Abra la cámara y escanee esta imagen en su iPhone o iPad para ir a McAfee Mobile Security en la App Store:

3. Pulse **Obtener**.
4. Si se le pide, **acepte la descarga** de la aplicación.
5. Espere hasta que McAfee Mobile Security se descargue y se instale.

Paso 2: Activar McAfee Mobile Security

1. Abra **McAfee Mobile Security**.
2. Inicie sesión usando la dirección de correo electrónico de su cuenta de usuario de McAfee y la contraseña.
3. Acepte el **Acuerdo de licencia y el Aviso de privacidad** de McAfee.
4. Pulse **Siguiente**. Espere a que se active la aplicación.

¿CÓMO DESCARGO E INSTALO LA SOLUCIÓN PARA IOS DESDE UN DISPOSITIVO DIFERENTE?

Siga estos pasos para instalar McAfee Mobile Security en un dispositivo **secundario**, como el iPhone de su hijo, desde **su** smartphone, PC o Mac. Por ejemplo, puede enviar un vínculo de instalación desde su dispositivo y pedir a su hijo que haga clic en el vínculo para completar la instalación en su iPhone o iPad.

Paso 1: En el dispositivo principal donde desea iniciar el proceso

1. Vaya a https://www.mcafee.com/ en el otro equipo o dispositivo.
2. Pulse **My Account**.
3. Pulse **Sign In**.
    - Si **ya tiene** una cuenta de McAfee:
        a. Escriba la **dirección de correo electrónico** de su cuenta de McAfee.
        b. Escriba la **contraseña** de su cuenta de McAfee.
        c. Haga clic en **Iniciar sesión**.
    - Si **no tiene** una cuenta de McAfee:
        a. Haga clic en **Registrarse ahora**.
        b. Siga las indicaciones.

SUGERENCIA: Cuando cree su cuenta, utilice una contraseña larga con letras y números, para mayor seguridad.

        c. Haga clic en **Iniciar sesión**.

Paso 2: Enviar un vínculo de descarga al dispositivo secundario

1. Pulse **Mi cuenta**.
2. Pulse **Suscripciones**.
3. Pulse **Agregar dispositivo**.
4. Seleccione **Dispositivo móvil**.
5. Pulse **Enviar vínculo** y, a continuación:
    - Seleccione el tipo de dispositivo **iOS**.
    - Seleccione el **tipo de suscripción**.
6. Pulse **Siguiente**.
7. En **How should we send the link**:

    - Elija **Por SMS** para que el código de activación se envíe a su teléfono.
    - Elija **Por correo electrónico** para recibir el código de activación por correo electrónico.
8. Escriba la **dirección de correo electrónico** o el **número de teléfono**.
9. Haga clic en **Enviar SMS** o **Enviar correo electrónico**.

Paso 3: En el dispositivo secundario

1. Abra la aplicación de **correo electrónico** o de **mensajes** en el dispositivo iOS.
2. Abra el **mensaje** de McAfee.
3. Pulse el **vínculo de descarga** del mensaje de correo electrónico de McAfee.
4. Para completar la instalación, siga las indicaciones.

¿CUÁLES SON LOS REQUISITOS DEL SISTEMA PARA IOS?

iOS

Sistemas operativos	Apple iOS 9 Apple iOS 8 Apple iOS 7 Apple iOS 6
Dispositivos admitidos	iPhone 6, 6s, 6+ y 6s+ iPhone 5 y 5s iPhone 4 y 4s iPhone 3GS iPad iPad Mini iPad Pro
Espacio de almacenamiento disponible	≈15 MB
Conexión a Internet	Wi-Fi LTE 4G 3G 2G
Navegador web	Apple Safari

GLOSARIO

Activación

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

Administración remota

La capacidad de administrar un sistema desde una ubicación remota.

ADSL

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

AES

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

Alerta

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

Antimalware

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

Antispam

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

Antivirus

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

API

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

proporciona una conexión sencilla y estándar a un componente de software particular.

Archivo de registro

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

Autenticación

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

Autenticador

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

Caballo de Troya

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

Caché

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

Categorías

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

Certificado

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

Cifrado

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

Clave privada

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

Clave pública

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

Complemento

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

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

Consola

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

Consola de administración

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

Correo web

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

Código PIN

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

DHCP

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

Dirección de red

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

Dirección IP

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

Directiva

Un conjunto de reglas que rigen las comunicaciones.

DNS

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

Dominio

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

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

Encabezado

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

Enrutador

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

Ethernet

Un protocolo de capa física basado en los estándares IEEE.

Exploit

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

Falsificación

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

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

Falso negativo

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

Falso positivo

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

Firma

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

FTP

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

Gravedad

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

Gusano

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

destruir dichos datos. Lo que con frecuencia parece una infección de un virus es, en realidad, un gusano.

Hash

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

HTML

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

HTTP

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

HTTPS

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

IMAP

Protocolo de acceso a mensajes de Internet. El método utilizado para acceder al correo electrónico de forma remota, normalmente, a través del correo web u otro protocolo que no descarga los mensajes al cliente. Permite mantener los mensajes en varias carpetas, admite el uso compartido de carpetas y permite la administración online del correo. IMAP es un método más avanzado de almacenaje de correo que POP, que se basa en la descarga de mensajes a una unidad local del usuario.

Independiente

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

Interfaz

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

Interfaz web

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

IPv6

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

LAN

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

Lista blanca

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

Lista negra

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

Malware

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

NIC

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

Nombre de host

El nombre o alias asignado a un sistema.

Nombre de sitio

El primer nombre de dominio (con su extensión) o el único en una cadena URL. Cuando un sitio web alberga otro sitio web, el primer nombre de dominio (con su extensión) es el del sitio y el último el del host. Por ejemplo, en la cadena URL

"www.SecureWeb.com/aaa/www.example.com/home.htm", el nombre del sitio es "www.SecureWeb.com" y el del host es "www.example.com".

Paquete

Una unidad de datos como se envía en una red.

Par de claves

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

Phishing

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

ping

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

POP3

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

PPP

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

Protocolo

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

Protocolo de Internet

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

Proxy

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

Puerto

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

Regla

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

Remitente de spam

Una persona que envía spam.

Retraso

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

Robos de identidad

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

RSA

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

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

Servidor de nombres

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

Servidor proxy

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

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

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

Servidor web

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

Sesión

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

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

Skype

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

SMTP

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

Spam

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

Spyware

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

SSL

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

Subred

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

TCP

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

TCP/IP

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

TLS

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

Transmisión

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

Transmisión multimedia en tiempo real

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

TrustedSource

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

UDP

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

URL

Localizador uniforme de recursos. Proporciona la dirección de documentos específicos en la Web. Cada archivo de Internet cuenta con una URL única, que indica el nombre del servidor, el directorio y el documento específico. La forma de una URL es

el protocolo://pathname. Por ejemplo: ftp://www.website.com y http://www.website.com.

Virus

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

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

VPN

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

WINS

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

AVISO DE PRIVACIDAD

El aviso de privacidad de McAfee se puede encontrar aquí:

http://www.McAfee.com/Common/Privacy/english/index.htm

McAfee se compromete a cumplir las leyes globales relacionadas con la inclusión, la notificación y la facturación.
Esperamos lo mismo de nuestros socios de facturación.

Cumplimiento del GDPR:

McAfee ha trabajado arduamente para estar preparado para la fecha de aplicación del GDPR, revisando nuestros productos, procesos, políticas de protección de datos y controles de seguridad. Estamos comprometidos con el cumplimiento de esta y todas las leyes aplicables. Hemos mejorado los procesos para prepararnos para abordar eficazmente los derechos particulares de las personas en la UE. Hemos generado una guía por escrito para ayudar a nuestros clientes a entender cómo nuestros productos recopilan y utilizan datos personales, y estamos preparados para responder a las preguntas de nuestros consumidores y clientes corporativos, así como de nuestros empleados.

Más información está disponible en https://www.McAfee.com/Enterprise/en-us/about/gdpr.html

Together is power.

Creemos que ninguna persona, producto u organización puede luchar solo contra el cibercrimen. Es por eso que reconstruimos a McAfee en torno a la idea de trabajar juntos.

Gente trabajando juntos. Productos que trabajan juntos.
Organizaciones e industrias que trabajan juntas.

Nuestro objetivo es difundir esta actitud colaborativa con nuestros clientes, socios e incluso competidores.

Todos los que se unen para superar el mayor desafío de la era digital —
ciberdelincuencia —
y hacer que el mundo conectado sea más seguro.