Machine Translated by Google



# Mejores prácticas para proteger su red doméstica

Resumen ejecutivo ¡No seas una

víctima! Los actores cibernéticos malintencionados pueden aprovechar su red doméstica para obtener acceso a información personal, privada y confidencial. Ayude a protegerse a sí mismo, a su familia y a su trabajo practicando comportamientos conscientes de la seguridad cibernética, observando algunas pautas básicas de configuración e implementando las siguientes mitigaciones en su red doméstica, que incluyen:

Actualice y actualice todo el equipo y el software regularmente, incluido el enrutamiento.
dispositivos

• Ejercer hábitos seguros haciendo una copia de seguridad de sus datos y desconectando los dispositivos cuando no se necesitan conexiones

• Limitar la administración solo a la red interna

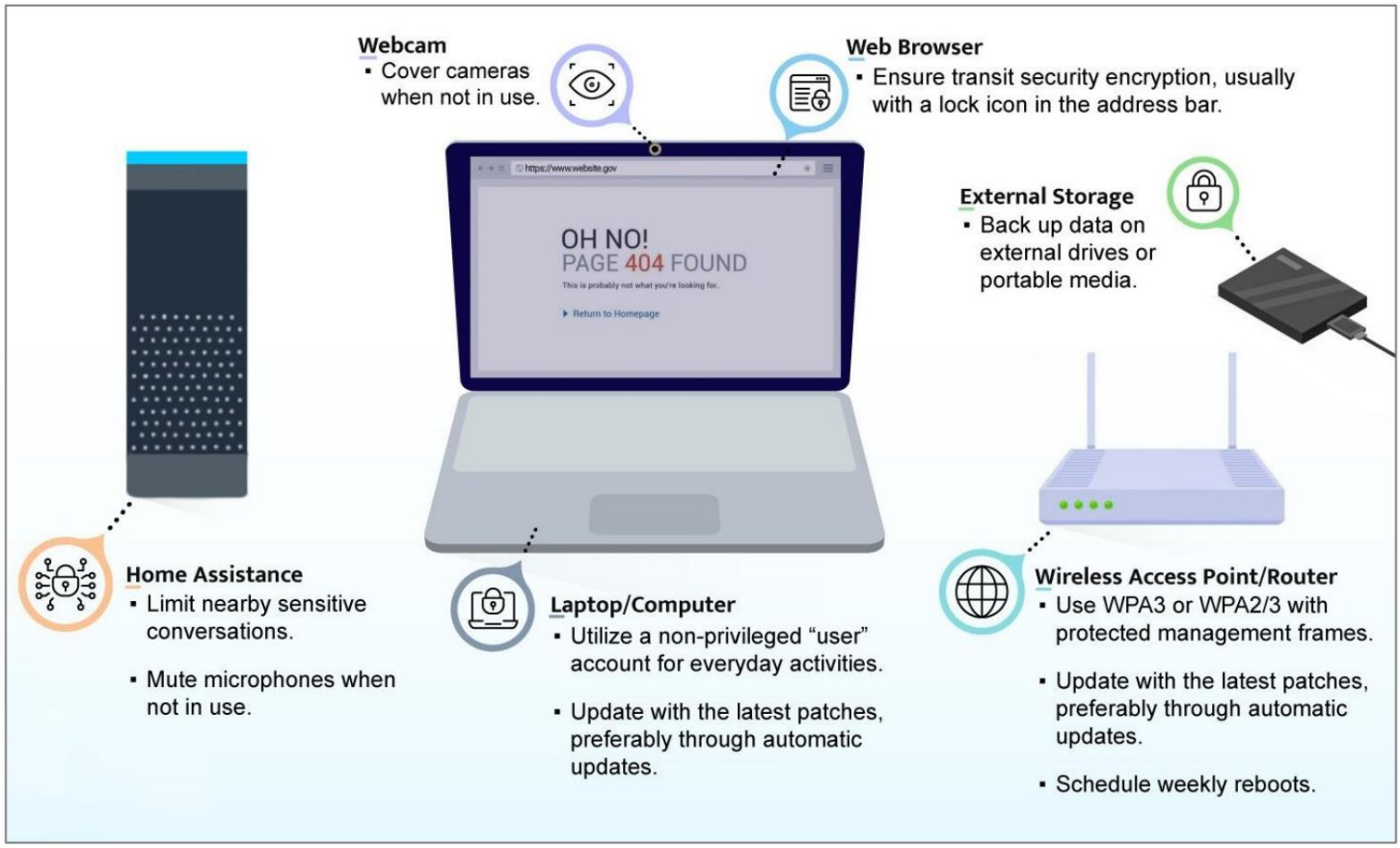


Figura: Varias prácticas recomendadas para proteger su red doméstica

Machine Translated by Google



## Recomendaciones para la seguridad del dispositivo

Los dispositivos informáticos electrónicos, incluidos ordenadores, portátiles, impresoras, teléfonos móviles, tabletas, cámaras de seguridad, electrodomésticos, automóviles y otros dispositivos de "Internet de las cosas" (IoT), deben protegerse para reducir el riesgo de compromiso. La mayoría de los dispositivos de servicios públicos y entretenimiento en el hogar, como sistemas de monitoreo del hogar, monitores para bebés, dispositivos IoT, dispositivos inteligentes, reproductores de Blu-ray™, reproductores de transmisión de video y consolas de videojuegos, pueden acceder a Internet, grabar audio y/o captura de vídeo. La implementación de medidas de seguridad puede garantizar que estos dispositivos no se conviertan en el eslabón débil de la protección de su hogar.

### Actualice a un sistema operativo moderno y manténgalo actualizado

La versión más reciente de cualquier sistema operativo (SO) contiene funciones de seguridad que no se encuentran en versiones anteriores. Muchas de estas funciones de seguridad están habilitadas de forma predeterminada y ayudan a prevenir los vectores de ataque comunes. Aumente la dificultad para que un adversario obtenga acceso privilegiado mediante el uso del sistema operativo más reciente disponible y compatible para computadoras de escritorio, portátiles y dispositivos inteligentes. Los dispositivos IoT en una red doméstica a menudo se pasan por alto, pero también requieren actualizaciones. Habilite la función de actualización automática cuando esté disponible. Si las actualizaciones automáticas no son posibles, descargue e instale parches y actualizaciones de un proveedor de confianza mensualmente.

### Asegure los dispositivos de enrutamiento y manténgalos actualizados

Su proveedor de servicios de Internet (ISP) puede proporcionarle un módem/enrutador como parte de su contrato de servicio. Para maximizar el control administrativo sobre el enrutamiento y las funciones inalámbricas de su red doméstica, considere usar un dispositivo de enrutamiento de propiedad personal que se conecte al módem/enrutador proporcionado por el ISP. Además, utilice las funciones de los enrutadores modernos para crear una red inalámbrica separada para invitados, para separar la red de sus dispositivos más confiables y privados.

Su enrutador es la puerta de entrada a su red doméstica. Sin la seguridad y los parches adecuados, es más probable que se vea comprometido, lo que también puede comprometer otros dispositivos en la red. Para minimizar las vulnerabilidades y mejorar la seguridad, los dispositivos de enrutamiento de su red doméstica deben actualizarse con los parches más recientes, preferiblemente a través de actualizaciones automáticas. Estos dispositivos también deben reemplazarse cuando lleguen al final de su vida útil (EOL) para obtener soporte. Esto garantiza que todos los dispositivos puedan continuar actualizándose y parchándose a medida que se descubren vulnerabilidades.

Machine Translated by Google



## Implementar WPA3 o WPA2 en la red inalámbrica

Para mantener la confidencialidad de sus comunicaciones inalámbricas, asegúrese de que su WAP personal o proporcionado por su ISP sea compatible con Wi-Fi Protected Access 3 (WPA3). Si tiene dispositivos en su red que no admiten WPA3, puede seleccionar WPA2/3 en su lugar. Esto permite que los dispositivos más nuevos usen el método más seguro al tiempo que permiten que los dispositivos más antiguos se conecten a la red a través de WPA2.

Al configurar WPA3 o WPA2/3, utilice una frase de contraseña segura con una longitud mínima de veinte caracteres. Cuando estén disponibles, los marcos de administración protegidos también deben habilitarse para mayor seguridad. La mayoría de las computadoras y dispositivos móviles ahora admiten WPA3 o WPA2. Si planea comprar un nuevo dispositivo, asegúrese de que tenga la certificación WPA3-Personal. Cambie el identificador de conjunto de servicios predeterminado (SSID) a algo único. No oculte el SSID ya que esto no agrega seguridad adicional a la red inalámbrica y puede causar problemas de compatibilidad.

## Implementar la segmentación de redes inalámbricas

Aproveche la segmentación de la red en su red doméstica para mantener segura su comunicación inalámbrica. Como mínimo, su red inalámbrica debe estar segmentada entre su red Wi-Fi principal, Wi-Fi para invitados y la red IoT. Esta segmentación evita que los dispositivos menos seguros se comuniquen directamente con sus dispositivos más seguros.

## Emplear capacidades de firewall

Asegúrese de que su dispositivo de enrutamiento de propiedad personal sea compatible con las capacidades básicas del firewall. Verifique que incluya la traducción de direcciones de red (NAT) para evitar que los sistemas internos se escaneen a través del límite de la red. Los puntos de acceso inalámbrico (WAP) generalmente no brindan estas capacidades, por lo que puede ser necesario comprar un enrutador.

Si su ISP es compatible con IPv6, asegúrese de que su enrutador sea compatible con las capacidades de firewall de IPv6.

## Aproveche el software de seguridad

Aproveche el software de seguridad que proporciona defensa en capas a través de capacidades antivirus, antiphishing, antimalware, navegación segura y firewall. El paquete de seguridad puede estar integrado en el sistema operativo o estar disponible para instalar como un producto separado en computadoras, laptops y tabletas. Sin embargo, es posible que algunos dispositivos, como asistentes domésticos, dispositivos inteligentes y otros dispositivos IoT, no admitan la instalación de suites de seguridad. El software moderno de detección y respuesta de endpoints utiliza servicios de reputación basados en la nube para detectar y

evitando la ejecución de malware. Siempre que sea posible, se debe implementar el cifrado de disco completo en computadoras portátiles, tabletas y teléfonos móviles para evitar la divulgación de datos si el dispositivo se pierde o es robado; muchos dispositivos móviles permiten el cifrado de disco de forma predeterminada y el software de seguridad puede hacerlo tan fácil como presionar un botón.

## Proteger contraseñas

Asegúrese de que las contraseñas y las respuestas a las preguntas de seguridad estén debidamente protegidas, ya que brindan acceso a la información personal. Las contraseñas deben ser seguras, únicas para cada cuenta y difíciles de adivinar. Las contraseñas y las respuestas a las preguntas de seguridad no deben almacenarse en forma de texto sin formato en el sistema o en cualquier lugar al que pueda tener acceso un actor malicioso. Se recomienda encarecidamente utilizar un administrador de contraseñas porque le permite usar contraseñas únicas y complejas sin necesidad de recordarlas.

## Limitar el uso de la cuenta de administrador

La cuenta de administrador altamente privilegiada puede acceder y potencialmente sobrescribir todos los archivos y configuraciones en su sistema. Debido a que puede acceder a más archivos, el malware puede comprometer su sistema de manera más efectiva si se ejecuta mientras está conectado como administrador. Para evitar esto, cree una cuenta de "usuario" sin privilegios para las actividades cotidianas normales, como la navegación web, el acceso al correo electrónico y la creación/edición de archivos. Solo use la cuenta privilegiada para mantenimiento, instalaciones y actualizaciones.

## Protección contra escuchas

Tenga en cuenta que los asistentes domésticos y los dispositivos inteligentes tienen micrófonos y escuchan conversaciones, incluso cuando no está interactuando activamente con el dispositivo. Si se ve comprometida, el adversario puede espiar las conversaciones. Limite las conversaciones confidenciales cuando esté cerca de monitores para bebés, juguetes de grabación de audio, asistentes domésticos y dispositivos inteligentes. Considere silenciar sus micrófonos cuando no estén en uso. Para dispositivos con cámaras (por ejemplo, computadoras portátiles, dispositivos de monitoreo y juguetes) cubra las cámaras cuando no las esté usando. Desconecte el acceso a Internet si un dispositivo no se usa con frecuencia, pero asegúrese de actualizarlo cuando lo use.

### Ejercer hábitos de usuario seguros

Para minimizar los riesgos de ransomware, haga una copia de seguridad de los datos en unidades externas o medios portátiles. Desconecte y almacene de forma segura el almacenamiento externo cuando no esté en uso. Minimice la carga de dispositivos móviles con computadoras; utilice el adaptador de corriente en su lugar. Evite conectarse

Machine Translated by Google



dispositivos a estaciones de carga públicas. Deje las computadoras en modo de suspensión para permitir la descarga e instalación de actualizaciones automáticamente. Reinicie regularmente las computadoras para aplicar las actualizaciones. Apague los dispositivos o desconecte sus conexiones a Internet cuando no se vayan a utilizar durante un tiempo prolongado, como cuando se va de vacaciones.

## Limite la administración solo a la red interna

Deshabilite la capacidad de realizar administración remota en el dispositivo de enrutamiento. Solo realice cambios en la configuración de la red desde su red interna. Deshabilite Universal Plug-n-Play (UPnP). Estas medidas ayudan a cerrar agujeros que pueden permitir que un atacante comprometa su red.

## Programe reinicios frecuentes del dispositivo

Para minimizar la amenaza de código malicioso no persistente en su dispositivo personal, reinicie el dispositivo periódicamente. Se ha informado que los implantes maliciosos infectan los enrutadores domésticos sin persistencia. Como mínimo, debe programar reinicios semanales de su dispositivo de enrutamiento, teléfonos inteligentes y computadoras. Los reinicios regulares ayudan a eliminar los implantes y garantizan la seguridad. Para obtener más orientación sobre cómo proteger mejor su teléfono inteligente, consulte las "Prácticas recomendadas para dispositivos móviles" CSI.

## Garantice la confidencialidad durante el teletrabajo

La seguridad de la red de tu hogar puede afectar directamente no solo a tu información personal, sino también a tu información y redes laborales cuando teletrabajas. El uso de una red privada virtual (VPN) para conectarse de forma remota a su red corporativa interna a través de un túnel seguro es una solución para acceder de forma segura a la información del trabajo. Esto proporciona una capa adicional de seguridad al mismo tiempo que le permite aprovechar los servicios que normalmente se ofrecen a los usuarios en el sitio. Para obtener más orientación sobre cómo proteger su VPN, consulte "Selección y fortalecimiento de soluciones VPN de acceso remoto" Guía de información de ciberseguridad (CSI).

Cuando se conecte a otros servicios de trabajo, como sitios web y aplicaciones de oficina basadas en la nube, asegúrese de que también sea a través de un túnel seguro buscando un ícono de candado en la barra de direcciones del navegador web. Si utiliza servicios de colaboración comercial, elija uno que proporcione un cifrado fuerte, preferiblemente cifrado de extremo a extremo. Para ver en profundidad algunas plataformas de colaboración comerciales, consulte "Selección y uso seguro de los servicios de colaboración para el teletrabajo". CSI.

Machine Translated by Google



## Recomendaciones para el comportamiento en línea

La suplantación de identidad (spearphishing), los anuncios maliciosos, los archivos adjuntos de correo electrónico y las aplicaciones que no son de confianza pueden presentar preocupaciones para los usuarios domésticos de Internet. Para evitar revelar información confidencial, cumpla con las siguientes pautas al acceder a Internet.

### Siga las mejores prácticas de correo electrónico

El correo electrónico es un vector de ataque potencial para los piratas informáticos. Las siguientes recomendaciones ayudan a reducir la exposición a las amenazas:

- Evite abrir archivos adjuntos o enlaces de correos electrónicos no solicitados. ejercicio cibernético higiene; no abra correos electrónicos desconocidos ni haga clic en sus archivos adjuntos o enlaces web. Verifique la identidad del remitente a través de métodos secundarios (llamada telefónica, en persona) y elimine el correo electrónico si falla la verificación. Para aquellos correos electrónicos con enlaces incrustados, abra un navegador y navegue al sitio web directamente por su dirección web conocida o busque el sitio usando un motor de búsqueda de Internet.

- Para evitar la reutilización de contraseñas comprometidas, utilice una contraseña diferente para cada cuenta. Considere usar un administrador de contraseñas para crear y recordar contraseñas seguras y únicas.

- Evite usar la función de mensaje de fuera de la oficina a menos que sea necesario. Haz que sea más difícil para personas desconocidas aprender sobre tus actividades o estado.

- Utilice siempre protocolos de correo electrónico seguros, especialmente si utiliza una red inalámbrica. Configure su cliente de correo electrónico para usar la opción de seguridad de la capa de transporte (TLS) (IMAP seguro o POP3 seguro) para cifrar su correo electrónico en tránsito entre el servidor de correo y su dispositivo.

- Nunca abra correos electrónicos que hagan afirmaciones extravagantes u ofertas que sean "demasiado buenas para ser verdadero."

## Actualice a un navegador moderno y manténgalo actualizado

Los navegadores modernos son mucho mejores para avisar a los usuarios cuando las funciones de seguridad no están habilitadas o no se utilizan. Los navegadores modernos ayudan a proteger la confidencialidad de la información confidencial en tránsito por Internet. El navegador debe mantenerse actualizado. Al realizar actividades como inicios de sesión en cuentas y transacciones financieras, la pestaña URL del navegador indica que la seguridad de tránsito está en su lugar, generalmente con un ícono de candado.

Machine Translated by Google



## Tome precauciones en los sitios de redes sociales

Los sitios de redes sociales son un medio conveniente para compartir información personal con familiares y amigos. Sin embargo, esta comodidad también conlleva un nivel de riesgo. Para protegerse, consulte "Mantenerse seguro en las redes sociales" orientación de CSI y haga lo siguiente:

- Evite publicar información, como direcciones, números de teléfono, lugares de empleo y otra información personal, que puede usarse para atacarlo o acosarlo. Algunos estafadores utilizan esta información, junto con los nombres de las mascotas, la marca o el modelo del primer automóvil y las calles en las que ha vivido, para averiguar las respuestas a las preguntas de seguridad de la cuenta.
- Limite el acceso a su información a "solo amigos" y verifique cualquier nuevo amigo solicitudes fuera de las redes sociales.
- Tenga cuidado con los perfiles duplicados o imitados de amigos, familiares o compañeros de trabajo Los actores maliciosos pueden usar cuentas suplantadas para solicitarle información privilegiada o atacarlo para phishing.
- Revise las políticas y configuraciones de seguridad disponibles de su proveedor de red social trimestralmente o cuando cambie la política de Términos de uso del sitio, ya que los valores predeterminados pueden cambiar. Optar por no exponer información personal a los motores de búsqueda.
- Tome precauciones con respecto a las solicitudes y enlaces no solicitados. Los adversarios pueden intentar que haga clic en un enlace o descargue un archivo adjunto que puede contener software malicioso.

## Garantías de autenticación

- Habilite la autenticación fuerte en su enrutador. Proteja sus contraseñas de inicio de sesión y tome medidas para minimizar el uso indebido de las opciones de recuperación de contraseña.
- Deshabilitar funciones que permiten que sitios web o programas recuerden contraseñas. Usar en su lugar, un administrador de contraseñas.
- Muchos sitios en línea usan recuperación de contraseña o preguntas de seguridad. Para evitar que un atacante aproveche la información personal para responder preguntas de seguridad, considere proporcionar una respuesta falsa a una pregunta basada en hechos, suponiendo que la respuesta sea única y memorable.

Machine Translated by Google



- Utilice la autenticación multifactor (MFA) siempre que sea posible. Los ejemplos de autenticación multifactor incluyen un teléfono/correo electrónico de confirmación secundario, preguntas de seguridad e identificación basada en aplicaciones/dispositivos. Algunas formas de MFA, como la identificación basada en aplicaciones/dispositivos, son más seguras y deben utilizarse en lugar de métodos menos seguros, como la confirmación por teléfono o correo electrónico. Cuando esté disponible, prefiera usar MFA resistente al phishing opciones

## Tenga cuidado al acceder a puntos de acceso público

Muchos establecimientos, como cafeterías, hoteles y aeropuertos, ofrecen puntos de acceso inalámbricos o quioscos para que los clientes accedan a Internet. Debido a que se desconoce la infraestructura subyacente de estos y la seguridad puede ser débil, los puntos de acceso público son más susceptibles a la actividad maliciosa. Si debe acceder a Internet mientras está fuera de casa, evite el uso directo de redes inalámbricas públicas. Cuando sea posible, use un punto de acceso Wi-Fi corporativo o personal con autenticación y encriptación sólidas. Si es necesario el acceso público, consulte "Protección de dispositivos inalámbricos en entornos públicos" CSI para obtener orientación y hacer lo siguiente:

- Si es posible, use la red celular (es decir, Wi-Fi móvil, servicios 4G o 5G) para conectarse a Internet en lugar de puntos de acceso públicos. Esta opción generalmente requiere un plan de servicio con un proveedor celular.
- Si debe utilizar Wi-Fi público, utilice una VPN de confianza. Esta opción puede proteger su conexión de actividades maliciosas y monitoreo.
- Ejercer la seguridad física en el lugar público. No deje los dispositivos desatendidos.

## No intercambies contenido doméstico y laboral.

El intercambio de información entre los sistemas domésticos y los sistemas de trabajo a través de correo electrónico o medios extraíbles puede aumentar el riesgo de compromiso de los sistemas de trabajo. Idealmente, use el equipo y las cuentas proporcionados por la organización para realizar el trabajo mientras está fuera de la oficina. Si usa un dispositivo personal, como a través de un programa Traiga su propio dispositivo (BYOD), use los productos de seguridad exigidos por la empresa y la guía para acceder a los recursos y redes de la empresa. Intente conectarse a un escritorio remoto o servidor terminal dentro de la red corporativa en lugar de hacer copias de archivos y transportarlos entre dispositivos. Evite el uso de cuentas y recursos personales para interacciones comerciales. Utilice siempre una VPN u otro canal seguro para conectarse a redes y servicios corporativos para asegurarse de que sus datos estén protegidos a través del cifrado.

Machine Translated by Google



### Use dispositivos separados para diferentes actividades

Establezca un nivel de confianza basado en las características de seguridad de un dispositivo y su uso. Considere segregar tareas dividiéndolas entre dispositivos dedicados a diferentes propósitos. Por ejemplo, un dispositivo puede ser para uso de información financiera/de identificación personal (PII) y otro para juegos o entretenimiento para niños.

## Orientación adicional

Guía de ciberseguridad de la NSA:

- Prácticas recomendadas para dispositivos móviles • Plataformas de colaboración seguras • Indicadores y mitigaciones de redes personales comprometidas • Las diez principales estrategias de mitigación de ciberseguridad de la NSA • MFA resistente al phishing • Mantenerse seguro en las redes sociales • Protección de dispositivos inalámbricos en público

Temas generales:

- Asociación Nacional de Aseguramiento de la Información

Normas:

- NIST SP 800-124 Directrices para la gestión de la seguridad de los dispositivos móviles en el Empresa •

NIST SP 800-63 Pautas de identidad digital

### Descargo de responsabilidad

La información y las opiniones contenidas en este documento se proporcionan "tal cual" y sin garantías ni garantías. La referencia en este documento a cualquier producto, proceso o servicio comercial específico por nombre comercial, marca comercial, fabricante o de otro modo, no constituye ni implica su respaldo, recomendación o favorecimiento por parte del gobierno de los Estados Unidos, y esta guía no se utilizará para publicidad. o fines de promoción de productos.

### Marcas registradas

Blu-ray es una marca comercial de Blu-ray Disc Association.

### Objetivo

Este documento se desarrolló para promover las misiones de seguridad cibernética de la NSA, incluidas sus responsabilidades para identificar y difundir amenazas a los sistemas de información de los Sistemas de Seguridad Nacional, el Departamento de Defensa y la Base Industrial de Defensa, y para desarrollar y emitir especificaciones y mitigaciones de seguridad cibernética. Esta información puede compartirse ampliamente para llegar a todas las partes interesadas apropiadas.

### Contacto

Consultas generales sobre ciberseguridad: CybersecurityReports@nsa.gov Consultas de bases industriales de defensa y servicios de ciberseguridad: DIB_Defense@cyber.nsa.gov Consultas de los medios / Mesa de prensa: 443-634-0721, MediaRelations@nsa.gov