COMUNICACIONES

SECRETARÍA DE INFRAESTRUCTURA, COMUNICACIONES Y TRANSPORTES

GUÍA DE CIBERSEGURIDAD DIRIGIDA A USUARIOS DE LOS SERVICIOS DE TELECOMUNICACIONES PARA IDENTIFICAR Y PREVENIR CIBERATAQUES DE MALWARE

Coordinación de Desarrollo Tecnológico

Agosto, 2023

Contexto

En los últimos años se ha experimentado una auténtica revolución en el mundo digital, el mayor uso de redes y dispositivos de telecomunicaciones, la adopción de nuevas tecnologías y la creación de nuevos ecosistemas digitales, ofrecen innumerables beneficios para las sociedades.

No obstante, la transformación digital y era post COVID-19 también han traído consigo la aparición de un gran número de riesgos y amenazas de ciberseguridad y una mayor vulnerabilidad y exposición a los ciberataques, tanto para para las personas como para las empresas y los gobiernos.

A tres años de la emergencia sanitaria por COVID-19, el mundo digital se ha visto amenazado por la proliferación de códigos maliciosos y campañas de phishing, que, en conjunto, definen el ambiente de amenazas cibernéticas en la actualidad[1].

Para el caso de México, el "Estudio sobre ciberseguridad en empresas, usuarios de Internet y padres de familia en México 2021", elaborado por la Asociación de Internet MX, indica lo siguiente[2]:

- **Más de la mitad de los internautas mexicanos** (el 53%) sufrió **alguna vulneración** de seguridad cibernética en los doce meses previos a la elaboración del estudio.

- Las principales afectaciones reportadas por las personas atacadas fueron:
    - Robo de información
    - Fraude y la pérdida financiera
    - Phishing
    - Fuga de información sensible
    - Robo de identidad

Sobre los hábitos de los usuarios, el estudio de referencia indica lo siguiente:

- El **60% de usuarios consultados considera que su equipo no está protegido frente a las ciberamenazas.**
- El **10% reconoce que no actualiza nunca su software antimalware**

Expertos en ciberseguridad concluyen que el problema de la propagación de malware radica no solo en la cantidad de ciberataques sino en la falta de medidas efectivas para la

[1] International Business Machines Corporation (IBM). "Índice de Inteligencia de Amenazas de X-Force 2022". https://www.ibm.com/downloads/cas/ADLMYLAZ
[2] Asociación de Internet Mx. https://irp.cdn-website.com/81280eda/files/uploaded/Estudio%20de%20Ciberseguridad%20AIMX%202021%20%28Pu%CC%81blica%29%2020210614.pdf

autoprotección, la concientización y la cultura de ciberseguridad de usuarios, empresas y organizaciones en general[3].

Los datos y conclusiones que presentan los estudios e investigaciones mencionados reflejan la importancia de fortalecer las capacidades de los usuarios y de la población en general, para identificar los diferentes riesgos de ciberseguridad asociados al Malware y, en consecuencia, adoptar medidas efectivas para prevenir ataques e incidentes de ciberseguridad.

Tomando en consideración lo anterior, la Secretaría de Infraestructura, Comunicaciones y Transportes (SICT) considera sumamente relevante la elaboración y difusión de materiales informativos, guías, lineamientos y mejores prácticas de higiene cibernética orientados a fomentar el uso responsable y seguro de redes, dispositivos, tecnologías y servicios de telecomunicaciones. Los cuales permitan a los usuarios prevenir incidentes de ciberseguridad y responder de forma adecuada una vez que éstos ocurren.

En este sentido, la SICT presenta:

La "Guía de ciberseguridad dirigida a usuarios de los servicios de telecomunicaciones para identificar y prevenir ciberataques de Malware".

El objetivo general de esta Guía es:

Difundir información relevante sobre el impacto negativo del malware en entornos laborales, académicos, familiares y personales, además de promover la adopción de mejores prácticas para prevenir y dar respuesta a incidentes ciberseguridad relacionados con la amenaza del malware.

Los objetivos específicos de esta Guía son:

- Ofrecer recomendaciones sencillas y prácticas para que los usuarios adopten buenos hábitos de higiene cibernética para prevenir incidentes de ciberseguridad provocados por Malware.

- Promover, entre la población, una cultura de ciberseguridad, así como la confianza en el uso de las telecomunicaciones, Internet y las TIC.

[3] ESET Security Report 2021. Empresa de ciberseguridad pioneras en Europa. https://www.eset.com/py/security-report. https://www.eset.com/py/security-report/

Conceptos básicos

¿Qué es el malware?

Es un programa informático (software, en inglés) cuya principal característica es que se ejecuta sin el conocimiento ni autorización del propietario o usuario del equipo o dispositivo infectado y realiza funciones perjudiciales.

El malware puede crearse para perseguir tres principales objetivos: robo de información, secuestro del equipo o de los datos del sistema, y "reclutamiento" de dispositivos para la creación redes de bots (botnets). En muchos casos, detrás de los ataques por malware, se encuentran motivaciones de tipo económico[4] .

¿Cómo pueden infectarse las redes, dispositivos y sistemas con malware?

Cualquier dispositivo puede infectarse con malware por medio de los siguientes métodos:

- Descarga de archivos o ingreso a enlaces sospechosos a través del correo electrónico o mensajes de texto.
- Descarga de mensajes o archivos en redes sociales
- Descarga de aplicaciones o actualizaciones poco confiables
- Visitas a sitios web sospechosos
- Conexiones a redes públicas o poco seguras
- Descargar archivos de música infectados
- Instalar nuevas barras de herramientas de un proveedor desconocido,
- Instalar software de una fuente dudosa

[4]Instituto Nacional de Ciberseguridad de España (INCIBE). "Aprende de Ciberseguridad: Malware" https://www.incibe.es/aprendeciberseguridad/malware

- Conexiones a Bluetooth
- Ejecución de USB, CD o DVD infectados
- Anuncios publicitarios falsos, entre otros.

Las amenazas de malware se presentan en una infinidad de formas, entre los tipos más comunes se encuentran los siguientes:

1. **Virus informáticos**[5]

¿Qué son?

Son códigos o programas informáticos maliciosos creados para infectar equipos, provocar problemas en el funcionamiento de éstos o robar información. Se encuentran en constante evolución y cada cierto tiempo aparecen nuevos tipos.

¿Cuál es su objetivo?

- Comprometer el rendimiento de los dispositivos y sistemas
- Son capaces de dañar, eliminar o corromper datos esenciales para su correcto funcionamiento. Tienen la capacidad de modificar o eliminar los archivos almacenados en el equipo.

¿Cómo se propagan o extienden?

- Un equipo o dispositivo puede infectarse con un virus informático a través de archivos o enlaces que el usuario descarga por medio del correo electrónico, las aplicaciones que utiliza, los mensajes de texto o bien pueden transmitirse por medio de dispositivos extraíbles, como memorias USB o archivos adjuntos, incluso a través de conexiones a redes.

- Cuando un virus infecta un equipo o dispositivo, hace copias de sí mismo y se adhiere a otros archivos o documentos. Posteriormente, modifica esos archivos y continúa propagándose.

[5] Oficina de Seguridad del Internauta (OSI-INCIBE). “Principales tipos de virus y cómo protegernos frente a ellos”. https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf

2. Adware

¿Qué es?

Código, programa o software malicioso cuyas características y funciones pueden ser variables. Según su diseño, pueden ejecutar las siguientes funciones[6]:

- Bombardear al usuario con anuncios publicitarios no solicitados
- Descargar complementos o de aplicaciones no solicitados
- Descargar actualizaciones falsas
- Rastrear las actividades que realizan los usuarios en internet

¿Cuál es su objetivo?

Recopilar información sobre las actividades de los usuarios en Internet y, de este modo, mostrarles anuncios dirigidos, lo que puede implicar molestias para los usuarios. No obstante, en muchos otros casos, su instalación repercute en el funcionamiento y buen rendimiento del equipo o dispositivo, además de que, por medio de este tipo de malware, el usuario puede dirigirse a páginas de Internet maliciosas.

¿Cómo se propaga o extiende?

Hay dos formas en las que los equipos o dispositivos pueden infectarse con adware[7]:

- Al visitar un sitio web no seguro (sitios falsos) que conducen a y conduce instalaciones no autorizadas de Adware.
- Al descargar software gratuito (shareware) por parte del usuario, ya sea en un formato limitado o en una versión de prueba.

3. Spyware (Programa espía)

¿Qué es?

Código, programa o software malicioso cuya función principal es rastrear y registrar la actividad de los usuarios tanto en equipos físicos como en dispositivos móviles. Incluso, existen "cepas" o tipos con comportamientos específicos como[8]:

- Registrar capturas de pantalla
- Obtener información del historial de navegación del usuario

[6] Avast. ¿Qué es el adware y cómo puede prevenirlo? https://www.avast.com/es-es/c-adware#topic-3
[7] Grupo Ático 34. "¿Qué es el Adware y cómo eliminarlo?". https://protecciondatos-lopd.com/empresas/adware/#:~:text=en%20el%20anuncio.-,%C2%BFC%C3%B3mo%20infecta%20los%20equipos%3F,e%20instalarse%20en%20el%20ordenador.
[8] Avast. "*Spyware: detección, prevención y eliminación*". https://www.avast.com/es-es/c-spyware

- Identificar las pulsaciones de teclas que realiza el usuario para obtener direcciones de correo electrónico, nombres de usuario y contraseñas, ingresar a datos de formularios y acceder a otros datos personales como números de tarjetas bancarias.

¿Cuál es su objetivo?

Acceder a información y datos del usuario por medio de la supervisión y copia todo lo que escribe, carga, descarga y almacena. Algunas cepas o tipos de spyware también son capaces de activar cámaras y micrófonos.

¿Cómo se propaga o extiende[9]?

Al navegar por páginas webs no seguras pueden aparecer mensajes en forma de anuncios emergentes o pop-ups[10] que, al hacer clic, descarguen este tipo de malware. También es común que se ejecute como programa adicional durante la instalación de un software.

4. Scareware o Rogueware

¿Qué es?

Código, programa o software malicioso que utiliza alertas de seguridad emergentes o supuestos avisos de las empresas de antivirus, así como otras técnicas de ingeniería social para alertar al usuario y motivarlo a que realice un pago para adquirir rápidamente una solución antivirus que promete resolver supuestas infecciones en los dispositivos. Además, este tipo de malware tiene la capacidad de afectar el rendimiento de los dispositivos[11].

¿Cuál es su objetivo?

Engañar a las víctimas para que "paguen por un software fraudulento", en este caso, el resultado es la descarga de otros tipos de malware para acceder a información confidencial del usuario como puede ser datos bancarios o personales y, con ello, concretar estafas mediante el robo de identidad y fraudes financieros.

¿Cómo se propaga o extiende[12]?

- Al navegar por páginas webs no seguras o apócrifas que automáticamente descargan e instalan en los dispositivos del usuario este tipo de malware.

[9] OSI-INCIBE. "Guía de ciberataques". https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf
[10] Un pop-up es un tipo de ventana o anuncio emergente que aparece en la pantalla de un sitio web o en el navegador de manera repentina. Se caracteriza por ser intrusivo ya que cubre otras ventanas, en particular la ventana que el usuario está tratando de leer.
[11] Avast. "¿Qué es scareware? Detección, Prevención y Eliminación" https://www.avast.com/es-es/c-scareware
[12] Karspersky Latinoamérica. "¿Qué es el scareware? Definición y explicación" https://latam.kaspersky.com/resource-center/definitions/scareware

- Al dar clic en ventanas emergentes o alertas que indican al usuario que su dispositivo está infectado.
- Al descargar correos electrónicos que solicitan al usuario registrarse a servicios o llenar un formulario.

Es importante considerar que los proveedores de software o soluciones de antivirus legítimos **NO** solicitan datos mediante tácticas de terror. Sin embargo, los cibercriminales se aprovechan del hecho de que muchas personas no cuentan con este tipo de sensibilización.

5. Ransomware de cifrado

¿Qué es?

Código, programa o software malicioso que, al introducirse a los dispositivos, tiene la capacidad de "secuestrar" la información de los usuarios (del inglés ransom), impidiendo el acceso a la misma por medio de técnicas de cifrado, es decir, por medio del uso de una contraseña que impide al usuario acceder a su información.

Una vez que el dispositivo ha sido infectado, se muestra un mensaje, exigiendo al usuario realizar un pago para acceder a la información "secuestrada"[13].

¿Cuál es su objetivo?

El objetivo del ransomware de cifrado es impedir el acceso de los usuarios legítimos a información almacenada en sus equipos o dispositivos que permite al atacante cobrar una compensación económica a cambio de liberar dicha información.

Este tipo de malware causa pérdidas temporales o permanentes de información de individuos y organizaciones e invariablemente, ocasiona pérdidas económicas y daños en la reputación de las organizaciones.

¿Cómo se propaga o extiende?

Se identifican diversos métodos de infección:

- Por medio de la descarga de archivos "trampa" que se encuentran adjuntos a correos electrónicos de spam (pueden ser archivos en PDF o Word).
- Al hacer clic en enlaces que contienen correos electrónicos de spam o de remitentes reconocidos.

[13] INCIBE. "*Ransomware, una guía de aproximación para el empresario*" (abril, 2021). https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf

- Al abrir archivos adjuntos o hacer clic en vínculos que llegan al usuario por medio la mensajería instantánea de redes sociales, WhatsApp y mensajes sms, que aparentan ser legítimos o bien, que proceden de una institución o persona de confianza.
- Al conectar los dispositivos personales a dispositivos infectados.

6. Fleeceware

¿Qué es?

El Fleeceware **no es un programa que corrompe archivos o roba información**. Es una práctica deshonesta de los desarrolladores de aplicaciones, que busca cobrar al usuario una cantidad económica abusiva por instalar un programa o aplicación.

Puede haber dos tipos de fleeceware: i) el que cobra una cantidad muy elevada al instalar el programa por primera vez y ii) el que cobra una cantidad excesiva por el uso de dicha aplicación y que continúa realizando cargos, incluso al desinstalar la aplicación. En este último caso, los desarrolladores de este tipo de aplicaciones pueden ocultar algún término abusivo donde indican que incluso si se desea desinstalar y dejar de utilizar ese programa o aplicación, el usuario tendrá que seguir pagando cada mes una cantidad de dinero.

Con frecuencia el Fleeceware opera como un **modelo de suscripción atractivo** para los usuarios con la promesa de pruebas gratuitas.

¿Cuál es su objetivo?

Motivar al usuario o descargar un programa o aplicación debido a una característica o promesa cautivadora y realizar cargos abusivos, inesperados y recurrentes. Su misión es la de cobrar de más a los usuarios por algo que en principio se ofrece de forma gratuita.

¿Cómo se propaga o extiende?

Un usuario puede descargar fleeceware por medio de anuncios publicitarios en las redes sociales y páginas de Internet. Pero también este tipo de aplicaciones están disponibles en las tiendas de aplicaciones de uso común.

7. Troyanos

¿Qué son?

Archivos, programas o fragmentos de código malicioso que funcionan haciéndose pasar por archivos legítimos, con el objetivo de engañar a las víctimas para que hagan clic en ellos, los abran o los instalen. Es decir, se empaquetan y entregan dentro de software legítimo

(de ahí su nombre). Cuando esto ocurre, el troyano comienza a instalar malware en los dispositivos[14].

Los troyanos pueden infectar a los dispositivos móviles del mismo modo que lo hacen con las computadoras de escritorio o portátiles.

A diferencia de los virus, que tienen la propiedad de replicación y autopropagación de un usuario a otro, los Troyanos no puede expandirse ni infectar archivos por sí solos, requieren de un proceso de instalación por parte del usuario.

¿Cuál es su objetivo?

Los troyanos pueden ejecutar diversas acciones maliciosas sin el permiso de los usuarios, por ejemplo[15]:

- Eliminar datos
- Bloquear datos
- Modificar datos
- Copiar datos
- Interrumpir el funcionamiento de computadoras o redes de computadoras
- Tener acceso remoto a un sistema

La mayoría de los troyanos tienen como objetivos controlar el equipo de un usuario, robar datos e introducir más software malicioso en los equipos.

¿Cómo se propagan o extienden[16]?

- Por medio de la descarga de archivos "trampa" que se encuentran adjuntos a correos electrónicos de remitentes desconocidos o poco confiables.
- Al navegar en páginas web que contienen contenido ejecutable[17]
- A través de la explotación de vulnerabilidades de seguridad que se presentan en aplicaciones no actualizadas (navegadores, reproductores multi-media, plataformas de mensajería instantánea).
- A través de la descarga de aplicaciones en mercados de aplicaciones piratas o no oficiales (juegos y películas, entre muchas otras aplicaciones).
- Al dar clic en archivos adjuntos a mensajería instantánea
- Al conectar a un equipo a un dispositivo externo infectado.

[14] Avast Academy. "¿Qué es un malware troyano? Guía definitiva" https://www.avast.com/es-es/c-trojan
[15] Idem.
[16] Ibidem.
[17] Los archivos o contenidos ejecutables están diseñados para poder iniciar un programa determinado o varios y contienen en su interior las instrucciones precisas para poder ejecutar dichos programas.

A continuación, se describen algunos tipos más comunes de troyanos[18]:

- **Troyanos de puerta trasera:** Utilizados por ciberdelincuentes para abrirse paso en los dispositivos y con ello, instalar otros tipos de malware o bien, conectar aquel dispositivo infectado a una red de bots maliciosos.

- **Troyanos bancarios:** Se introducen en los dispositivos y roban credenciales de inicio de sesión de aplicaciones o plataformas financieras para acceder a información de cuentas bancarias.

- **Troyanos de Denegación de Servicio Distribuido (DDoS):** Su objetivo es incluir al dispositivo en una red de bots (red de dispositivos enlazados y controlados de forma remota). Las redes de bots generalmente, son utilizadas para atacar sitios web y/o servicios de Internet.

- **Troyanos exploit:** Se encuentran diseñados para aprovechar las vulnerabilidades del software o hardware de los dispositivos, para infectarlos.

- **Troyanos infostealer:** Su objetivo es robar datos, para ello tienen la capacidad de revisar los dispositivos en busca de datos personales confidenciales y utilizarlos para fines maliciosos como fraudes o robo de identidad.

8. Gusanos

¿Qué son?

Software de tipo malicioso que tiene la capacidad de replicarse y expandirse rápidamente en los archivos y programas de una computadora, generando a su paso diferentes tipos de daño.

La existencia y expansión de los gusanos depende de la conectividad en red de varias computadoras, lo cual facilita su salida y multiplicación entre sistemas sin la necesidad de "llevar a cuestas un archivo para su transporte", lo que significa que tan pronto como un gusano ingresa en un equipo, puede extenderse a través de una red, sin necesidad de ayuda o de acciones externas[19].

[18] Karspersky. "¿Qué es un Troyano y qué daño puede causar?". https://latam.kaspersky.com/resource-center/threats/trojans

[19] A diferencia de los virus, los gusanos no necesitan usar la programación o el código de los equipos para ejecutarse y replicarse. Los gusanos informáticos son programas independientes que se replican a sí mismos y se ejecutan en segundo plano, mientras que los virus requieren un archivo de host para infectarlos.

Los gusanos, a diferencia de los virus, no suelen infectar los archivos de la computadora, sino que infectan otros equipos conectados a la red[20].

Los gusanos pueden utilizarse como mecanismos para la propagación de otros tipos de malware. En estos casos, el código adicional que lleva el gusano se conoce como «carga útil[21].

¿Cuál es su objetivo?

Los gusanos suelen colapsar al mayor número posible de dispositivos (ralentizar o incluso bloquear el equipo anfitrión usando demasiada potencia de procesamiento) y redes informáticas (saturación y uso de ancho de banda para propagarse).

Los gusanos, a través de su "carga útil"[22], pueden infectar a los dispositivos con cualquier tipo de malware y con ello, permitir a terceros tomar el control del sistema, recopilar datos personales confidenciales, instalar ransomware o convertir los dispositivos en «zombis» para usarlos en ataques de redes de bots (botnet)[23].

¿Cómo se propagan o extienden?

En general, los gusanos informáticos podrían clasificarse según el medio de propagación que utilizan, con base en esta clasificación, destacan los siguientes[24]:

- Gusano de Internet, que se propaga por las páginas de internet y los ordenadores.
- Gusano de email, infectan con sus archivos maliciosos el correo electrónico.
- Gusano de mensajería, se propaga a través de mensajería instantánea.
- Gusano de multimedia, aprovechan el intercambio de archivos multimedia.

9. Rootkits

¿Qué son?

Paquete de software malicioso diseñado para permitir el acceso no autorizado a un equipo o a otro software, a la vez que evita ser detectado en el dispositivo infectado[25].

[20] Hornet Security. "Gusanos informáticos: ¿Qué son los gusanos informáticos? ¿Cómo funcionan los gusanos informáticos?https://www.hornetsecurity.com/es/knowledge-base/gusanos-informaticos/
[21] On Retrieval. "¿Qué es un gusano informático? Principales características y tipos". *Las cargas útiles generalmente se crean para cambiar o eliminar archivos en una red de destino, extraer datos personales de ellos o cifrarlos y buscar un rescate de la víctima.* https://onretrieval.com/gusano-informatico/
[22] El Término de carga últil, se refiere al componente de un virus informático que ejecuta una actividad maliciosa.
[23] Avast. "¿Qué es un gusano informático?" https://www.avast.com/es-es/c-computer-worm
[24] On Retrieval. "¿Qué es un gusano informático? Principales características y tipos". https://onretrieval.com/gusano-informatico/
[25] Avast. ¿Qué es un rootkit? ¿Qué es un rootkit y cómo se elimina? | Avast

Cuando un rootkit ataca a un dispositivo, este dispositivo autoriza a terceros "no legítimos" el acceso remoto de administrador al sistema operativo. Los ciberatacantes utilizan este tipo de malware para acceder de forma remota a un equipo y manipularlo sin el conocimiento o consentimiento del usuario legítimo.

¿Cuál es su objetivo?

El rootkit puede contener una secuencia de herramientas para robar datos personales o financieros del usuario (contraseñas, información de tarjetas de crédito o banca online e información personal), instalar otras aplicaciones maliciosas o unir el equipo a una botnet para propagar spam o para sumarse a un ataque distribuido de denegación de servicio distribuido (DDoS).

Otras funciones que pueden realizar los rootkits son:

- Manipular o desactivar programas de seguridad, lo que dificulta su detección y eliminación
- Utilizarse como herramientas de seguimiento (espionaje)
- Crear en el sistema una puerta trasera de ciberseguridad para que el hacker pueda regresar más adelante.

Actualmente, existe una amplia variedad de Rootkits y cada uno ataca partes distintas de un dispositivo[26].

¿Cómo se propagan o extienden?

Los rootkits se instalan a través de una infinidad de métodos, pero el más común es a través del uso de una vulnerabilidad en el sistema operativo o de una aplicación que se ejecuta en el ordenador:

- A través de unidades USB
- Descarga de archivos trampa en correos electrónicos de remitentes desconocidos
- Acceso a vínculos sospechosos
- Descarga y uso de aplicaciones móviles infectadas

[26]Para conocer los tipos de rootkits más comunes, se sugiere revisar el siguiente enlace: Red Seguridad. "Rootkit': definición, tipos y protección ante este 'malware".
https://www.redseguridad.com/actualidad/cibercrimen/rootkit-definicion-tipos-y-proteccion-ante-este-malware_20210712.html

10. Ataques a Dispositivos IoT

Como la popularidad de los dispositivos IoT (Internet de las Cosas) ha aumentado, por ejemplo, altavoces inteligentes y timbres con cámaras de vídeo, los ciberatacantes buscan filtrarse en ellos para acceder a información de los usuarios.

Estos dispositivos a menudo poseen información de fácil acceso, como contraseñas y nombres de usuario, que después pueden ser utilizados por los ciberatacantes para iniciar sesión en las cuentas de los individuos y robar información importante, como, por ejemplo, datos bancarios.

Recomendaciones:

Existen una serie de recomendaciones sencillas y prácticas que cualquier usuario de equipos y dispositivos de telecomunicaciones puede implementar para evitar ser víctima de ataques de malware:

1. **Instalar un software antivirus- antimalware.**

- Instalar y mantener actualizados los antivirus, prefiriendo aquéllos que incorporan funcionalidades de protección contra malware y cortafuegos (firewall), también conocidos como suites de seguridad".

- Se recomienda activar funcionalidades de protección, como el cortafuegos (firewall), incorporadas en los sistemas operativos más comunes. Un cortafuegos es la primera línea de defensa ante un ataque a tu red desde Internet y permite proteger el equipo de programas maliciosos o de atacantes que intenten conectarse al equipo de forma remota. Además, permite establecer reglas para indicar qué conexiones de red se deben aceptar y cuáles no. Al mismo tiempo, admite el normal intercambio de datos entre la computadora y servicios verificados de Internet.

- Evitar tener dos antivirus en un mismo dispositivo. Tener dos antivirus activos no significa mayor protección; de hecho, puede ocasionar diferentes problemas en el sistema. Un antivirus que esté trabajando se convertirá en un "software malicioso" a los ojos del otro, el cual intentará bloquearlo y eliminarlo, y se corre el riesgo de afectar el desempeño del sistema por el consumo extra de recursos[27].

[27] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). ¿Sabías que utilizar tus dispositivos personales para trabajar puede ser peligroso? https://www.osi.es/es/actualidad/blog/2019/05/15/sabias-que-utilizar-tus-dispositivos-personales-para-trabajar-puede-ser

2. Ejecutar de manera periódica análisis de amenazas.

- Configurar el software o programa antivirus para que se ejecute a intervalos regulares, es preferible no esperar mucho tiempo entre cada ejecución.

- Configurar el software antivirus para que se ejecute en una noche específica y deje siempre el equipo en funcionamiento ese día.

3. Mantener el sistema operativo actualizado.

- Mantener actualizados los sistemas operativos y las aplicaciones de los dispositivos, incluidas las computadoras personales (PC), los teléfonos inteligentes y las tabletas. Estas actualizaciones incluyen cambios importantes que mejoran el rendimiento y la seguridad de los equipos; muchos de estos programas, incluso, se actualizan de manera automática.

- Todas las instalaciones y actualizaciones de programas y aplicaciones deben hacerse desde el sitio web oficial del fabricante[28] o desde las tiendas oficiales de apps -verificando la identidad del autor de la aplicación-, evitando descargar e instalar aquéllas de dudosa procedencia.

4. Proteger la red de internet en casa.

- Es cada vez más común que los usuarios cuenten en casa con un ruteador inalámbrico (Wi-Fi) para conectar sus dispositivos a Internet, sin necesidad de cables. Para evitar que usuarios no autorizados se conecten de forma inalámbrica al ruteador y tengan la posibilidad de acceder a la conexión, e incluso al resto de los dispositivos conectados y a la información que se transmite, es importante asegurar que la red Wi-Fi cuente con contraseña, que el usuario debe introducir, al conectar por primera vez un dispositivo.

- Asimismo, se recomienda que dicha contraseña incluya mayúsculas, minúsculas, números y símbolos. Cuanto mayor sea la longitud de la contraseña, más difícil será que un atacante pueda descubrirla.

[28] Ídem.

- Asegurarse de que cada uno de los equipos y dispositivos que se conectan a la red Wi-Fi, deban ingresar la contraseña cada vez que acceden a la red.

- Evitar compartir la clave de la red Wi-Fi con otras personas, pues quien tenga acceso a tu red inalámbrica podría tener acceso a todos los dispositivos conectados a ella.

- Evitar la conexión a redes Wi-Fi públicas abiertas (o hotspots Wi-Fi). Estas redes son inseguras ya que permiten que cualquier dispositivo se conecte al ruteador sin ningún tipo de seguridad, por lo que cualquier usuario podría capturar la información se transmita a través de dicha conexión. Piensa que, si puedes acceder a estas redes sin restricciones, ¿qué puede hacer un hacker?

5. Pensar antes de hacer clic y mantener la información personal segura

- Ingresar sólo a sitios web confiables, escribiendo uno mismo la dirección de la página a la que se quiere acceder y evitando utilizar ligas proporcionadas por terceros.

- Conocer y aplicar las funcionalidades de “navegación privada” o “navegación segura”, que impiden el almacenamiento del historial en el navegador, así como imágenes, nombres de usuario y contraseñas.

- Al realizar transacciones o intercambio de información sensible, asegurarse de que la dirección de la página web comience con “https” (no “http”), lo que contribuye a mantener segura la información que viaja por Internet.

- Desactivar la compartición de ubicación geográfica, a menos que sea estrictamente necesario.

- Evitar el ingreso de información personal en formularios dudosos. Si este tipo de formularios solicitan información sensible (por ejemplo, nombre de usuario y contraseña o datos bancarios), es recomendable verificar la legitimidad del sitio al que pertenece dicho formulario, antes de responder.

- Al terminar de navegar en Internet, es importante cerrar la sesión, sobre todo si se utiliza un equipo compartido, para evitar que otras personas tengan acceso a cuentas, contraseñas, información sensible o privada.

- Mantenerse alertas ante comunicaciones, como llamadas, correos electrónicos, mensajes cortos (SMS), enlaces de teleconferencias e invitaciones de calendario, de remitentes desconocidos.

- Antes de abrir cualquier enlace, archivo adjunto, mensaje de texto o llamada de un remitente desconocido, hay que preguntarse lo siguiente:

    - ¿Espero esa información? Si el mensaje proviene de un remitente desconocido (persona u organización), analizar bien antes de responder o hacer clic y/o descargar cualquier archivo adjunto.

    - ¿Reconozco al remitente? Comprobar si la dirección está bien escrita (verificar que no haga falta ninguna letra, por ejemplo) y si el dominio (la terminación del correo electrónico) es de confianza y corresponde al nombre de quien envía el mensaje.

    - ¿Solicitan que haga algo? Los correos electrónicos fraudulentos (phishing) o los mensajes de texto de este tipo (smishing) suelen pedir que se realice alguna acción como: hacer clic en un hipervínculo, descargar algún archivo, responder al mensaje proporcionando información personal, etc. Con frecuencia, buscan generar una sensación de urgencia y provocar una reacción inmediata e irracional. Es necesario analizar con calma antes de proporcionar cualquier información que pudiera resultar comprometedora.

    - Se debe desconfiar, particularmente, de los mensajes que parecerían genéricos (como “Estimados:”, “A quien corresponda:”, etc.).

    - En el caso de comunicaciones referentes a instituciones bancarias y financieras, se recomienda NUNCA dar clic en los enlaces contenidos en un correo o mensaje y NO proporcionar información de acceso a tus cuentas.

- Tener mucho cuidado de dónde se descargan las aplicaciones, procurar hacerlo de sitios oficiales y validando la firma de descarga.

- No descargar películas, juegos o música piratas, ya que los sitios que ofrecen este tipo de productos gratuitos son comúnmente los preferidos para añadir malware.

- No olvidar que los dispositivos del Internet of Things (IoT) forman parte de la red y necesitan también protección y mecanismos de seguridad.

6. Utilizar contraseñas seguras

Las contraseñas protegen la información que contienen los dispositivos y cuentas de los usuarios. No obstante, ante la cantidad de claves y combinaciones que cotidianamente se deben utilizar, la mayoría de las personas opta por contraseñas fáciles de recordar por la comodidad que esto implica, o bien, por la falta de conocimiento de lo fácil que puede ser para un ciberdelincuente obtenerlas.

Para asegurar la efectividad de las contraseñas y evitar el robo de éstas, es recomendable poner en práctica las siguientes acciones[29]:

- Al generar las contraseñas de los dispositivos y cuentas se deben utilizar claves largas y únicas para cada caso, evitando utilizar la misma contraseña para diferentes dispositivos o cuentas.

- Se deben evitar las combinaciones sencillas como fechas de nacimiento, secuencias consecutivas, repeticiones de un mismo dígito o palabras simples como “password” o “contraseña”.

- La mayor longitud de la contraseña, así como la incorporación de mayúsculas, minúsculas, números y caracteres especiales, contribuyen a que ésta sea más segura y difícil de vulnerar.

- Evitar escribir contraseñas en papeles o tener archivos con esa información que sean fácilmente accesibles para otros.

- Habilitar el doble factor de autenticación o verificación en dos pasos. Esta medida es una capa adicional de seguridad disponible para más servicios en la que, además de la contraseña, durante el inicio de sesión se solicita al usuario información por otro medio al que sólo el usuario autorizado tiene acceso (por ejemplo, verificación para entrar al correo electrónico mediante la recepción de un código vía SMS, llamada o mensaje de WhatsApp).

- Utilizar gestores de contraseñas. Son aplicaciones que sirven para almacenar credenciales (usuarios, contraseñas y los sitios web o aplicaciones a los que

[29] Oficina de Seguridad del Internauta del Instituto Nacional de Ciberseguridad de España (OSI-INCIBE). Campañas/ Contraseñas Seguras. https://www.osi.es/es/campanas/contrasenas-seguras

corresponden, etc.) en una base de datos cifrada mediante una contraseña "maestra". De este modo, los usuarios pueden gestionar todas sus cuentas de usuario desde una misma herramienta, memorizando únicamente una clave maestra[30].

En el mercado existe una gran variedad de aplicaciones con esta función, tanto para dispositivos móviles como para ordenadores Windows o macOS, también existen gestores de contraseñas que funcionan desde el navegador.

- No facilitar a nadie, por ningún medio, contraseñas y/o códigos personales.

- Es recomendable cambiar con frecuencia las contraseñas a efecto de evitar accesos no autorizados.

7. Hacer copias de seguridad.

- Realizar periódicamente copias de seguridad (respaldos) de la información que contienen los dispositivos, con el objetivo de disponer de un sistema de respaldo en caso de pérdida, deterioro o robo de información. Con ello, el usuario garantiza el acceso a su información en caso de que ocurra algún incidente.

- Existen diversos soportes en los que se pueden realizar copias de seguridad. La selección de éstos dependerá de algunos factores como la confiabilidad que la empresa necesita y la inversión económica que desea realizar. Los soportes más utilizados son:

    - Unidades USB y discos duros portátiles
    - Discos duros de equipos específicos
    - Soportes ópticos como DVD o CD
    - Almacenamiento de copias en la nube

- Es importante proteger con contraseña (encriptar) los dispositivos donde se almacene tu información (memorias USB o discos externos o archivos en la nube) para para proteger la información y siempre analizar los dispositivos extraíbles.

[30] OSI-INCIBE. *"Gestores de contraseñas: ¿cómo funcionan?* (enero de 2021). https://www.osi.es/es/actualidad/blog/2021/01/27/gestores-de-contrasenas-como-funcionan

8. Configurar adecuadamente las cookies

Al navegar por Internet o visitar un sitio web por primera vez, es común que se desplieguen mensajes como el siguiente: *"Este sitio web utiliza Cookies para mejorar y optimizar la experiencia del usuario, si continúas navegando consideramos que aceptas su uso. Más información en nuestra política de cookies"*.

Existen cookies que se encargan de autentificar a los usuarios (cookies de seguridad); o bien para asegurar el correcto funcionamiento de las páginas web (cookies de procesos) y cookies publicitarias, entre otras.

Entre las ventajas que ofrecen las cookies a los usuarios, se encuentran la navegación rápida y sencilla, la personalización del contenido para el usuario en función de sus preferencias y consultas o visitas anteriores. Por ello, es importante configurar correctamente en el navegador el uso que hace de las cookies:

- Ubicar en el navegador "Opciones" y después seleccionar la opción de "Privacidad y Seguridad".
- Dirigirse a "Cookies y datos del sitio", donde se puede la forma en la que el navegador gestiona las cookies.
- En el caso de las cookies de terceros, es recomendable aceptar sólo las que hay en las páginas que se han, o ninguna si el usuario prefiere que nadie pueda hacer un perfil publicitario o comercial personalizado.
- Eliminar cada cierto tiempo las cookies, sobre todo al navegar desde un dispositivo móvil.

Las telecomunicaciones y el acceso a Internet y a las nuevas tecnologías son parte de la vida cotidiana de las personas y, en ese sentido, su uso seguro y responsable cobra especial relevancia como un quehacer que nos atañe a todos los usuarios.

Por ello, es importante continuar el desarrollo de instrumentos que, como esta guía, contribuyan a la diseminación de buenas prácticas de higiene digital para empoderar a los usuarios en un uso seguro, productivo, ético y responsable de Internet y las nuevas tecnologías, ante los crecientes retos de ciberseguridad que plantea el mundo digital.