CONSIDERACIONES ESPECIALES, CONTRASEÑAS Y NOMBRES DE USUARIOS

AUTOR: HELLEN CUBERO

NOVIEMBRE: 2020

San Marcos

INTRODUCCIÓN

El usuario que navega en la Web, está prácticamente exigido a buscar la protección de sus datos. Sin embargo, pensar en esta seguridad implica una comprensión integral del universo de la Web y cada uno de sus componentes, desde espacios y conexiones virtuales hasta dispositivos físicos.

Numerosas aplicaciones surgen con las necesidades de seguridad. Los usuarios tienen la obligación de estar al corriente de las actualizaciones y mantener a sus dispositivos y software al tope de las mismas para lograr no solo un rendimiento adecuado, sino también la seguridad necesaria para evitar ataques de los delincuentes.

Los usuarios también deben estar conscientes de cuándo es necesario adquirir soporte técnico para proteger sus datos y sobretodo, normalizar la adquisición de estos servicios cuando sea necesario.

Contenido

Cómo proteger sus redes

Al iniciar con la instalación de una red de Internet generalmente existe un proveedor que se encarga de proporcionar el módem y el enrutador inalámbrico con cuatro puertos. Los técnicos no necesariamente tienen una formación especializada en seguridad por lo que, en muchas ocasiones, la instalación que realizan no considera con amplitud las posibilidades para proteger a la red de amenazas.

Además del aspecto anterior, es muy probable que tampoco se brinde un acceso privilegiado a la configuración del enrutador, por lo que, si un usuario desea mejorar su seguridad deberá contactarse con soporte, siendo ésta una situación no ideal.

Con un enrutador propio, se podría mejorar la seguridad de la red, sin tener que llamar a un departamento de soporte técnico. El enrutador debe conectarse al módem adquirido por el servicio externo; este aparato tiene un manual con instrucciones, una dirección IP y usuario y contraseña.

La clave para mejorar la seguridad de la red con un enrutador propio está en que se pueden actualizar los Firmware y cambiar las contraseñas. Las actualizaciones brindan incorporaciones de seguridad a los aparatos, y cambiar la contraseña por la original, le dará la autonomía en el manejo de su equipo y su red.

Cómo proteger las conexiones inalámbricas

La configuración de las conexiones inalámbricas de una red, puede llevar a mejorar su funcionamiento y evitar problemas. A veces existen elementos que generan interferencia en la red y afectan su latencia, como por ejemplo monitores de bebés, microondas, teléfonos inalámbricos o incluso otras redes inalámbricas; configurar adecuadamente un enrutador permitiría mejorar algunos aspectos para fortalecer una red.

Para fortalecer la seguridad, la opción de seguridad más recomendada (usualmente) es WPA2-PSK (AES). Se debe elegir dentro de la configuración de seguridad, disponible en la dirección IP de los manuales

de un enrutador y accesible con el usuario y contraseña que el mismo manual del aparato brinda.

Algunos enrutadores poseen la opción de generar redes de Invitados, para dividir la red local (de uso frecuente) y la red para los visitantes, y así no tener que compartir contraseñas de accesos con todas las personas. Esta acción permitirá entre otras cosas que, los usuarios invitados puedan utilizar internet pero no acceder a la red local, lo cual es un buen aspecto para la seguridad.

Es muy importante que las contraseñas sean diferentes y robustas, en ambas redes (invitado y local). También se recomienda cambiar las contraseñas cada cierto tiempo.

Seguridad física

Dispositivos móviles, tabletas o computadoras portátiles, tienen un riesgo físico y es el hurto. Ya sea por asalto o descuido, los ladrones cometen el acto de robar dispositivos físicos para reventa y sacar provecho económico.

Aunque sea doloroso la pérdida del aparato como tal, existe también un problema (quizá hasta más importante) de la pérdida de información. Aunque haya un respaldo en la nube, es hasta riesgoso que exista un robo o suplantación de información personal con claves o accesos a sitios privados.

El hurto de dispositivos tecnológicos requiere de una serie de medidas de prevención por parte de los usuarios dueños que implican siempre, eliminar la confianza que nada va a pasar. Dejar visible una tableta, computadora o celular en un carro, es suficiente para que un delincuente quiebre una ventana y se lo robe.

Existen aplicaciones como LoJack que permiten ubicar a un dispositivo físico en casos que esté perdido o se lo hayan robado. Instalar este tipo de aplicaciones es también una sugerencia para evitar la pérdida del

equipo físico. Aunque LoJack pueda identificar la locación donde está una computadora aunque se haya formateado el disco duro, no se recomienda de ninguna manera, localizarlo de forma individual, sino, hacer esa búsqueda en compañía de la policía.

Otra recomendación, es colocar una contraseña de escritorio que proteja al equipo mientras este haya sido desatendido por un tiempo, así se bloquearía la pantalla y si alguien desea ingresar, tendrá que colocar la contraseña.

Existen en los equipos una Ranura de Seguridad Universal. Está integrada al bastidor y tiene 1,27cm de largo y con frecuencia, tiene un símbolo de candado. La idea es atar el cable alrededor de algo sólido y meter la lengüeta en la ranura de la computadora. Utilizando una llave o combinación, el equipo se quedará fijo y asegurado al lugar donde se ató.

En el plano de seguridad física es importante también considerar la protección de los equipos por cargas eléctricas. Los picos de corriente eléctrica o apagones, pueden dañar la alimentación de un equipo y suceden por diferentes causas, como un rayo o inestabilidad en las fuentes. El uso de UPS (Fuentes de Alimentación Ininterrumpida) son recomendables para que esos picos de corriente no dañen las computadoras, ya que estas unidades son capaces de soportar esas sacudidas y además, brindan energía por un tiempo para evitar los apagones. El usuario tiene aquí la oportunidad de apagar debidamente los equipos hasta que regrese el flujo de corriente eléctrica.

Finalmente, cuando una persona va a deshacerse de un equipo físico, debe recordar que éste va a contener datos y que, debe borrarlos debidamente para que no deambulen con la persona que se adueñe de éste. Existen aplicaciones que facilitan la tarea de formateo de datos de la manera más correcta y segura, y brindando un panorama amplio a las personas usuarias sobre los datos que se borraron.

Su sistema operativo

Una computadora se compone esencialmente de Hardware y Software. Desde una perspectiva básica, el Sistema Operativo, es el software que permite al hardware operar y darle funcionamiento a las computadoras.

Existen tres sistemas operativos reconocidos para computadoras: Windows, Mac OS y Linux, siendo los dos primeros los más populares.

Cada sistema operativo, al igual que sucede con otro tipo de software, tiene actualizaciones con mejoras de seguridad y rendimiento. Esas mejoras, también significan en muchas ocasiones, demandas de capacidad y rendimiento para el Hardware. Existen usuarios que por diversas situaciones (como limitación de la capacidad del Hardware o limitaciones económicas para adquirir licencias), utilizan sistemas operativos anteriores a las últimas versiones disponibles.

Entre más desactualizado esté un Sistema Operativo, las opciones para recibir soporte o adquirir mejoras en seguridad, son más limitadas. En estos casos, se recomienda entonces generar respaldos de información en computadoras o dispositivos con sistemas operativos antiguos u obsoletos, ya que se vuelven más vulnerables y en cualquier momento podrían dejar de funcionar óptimamente. A pesar de esta recomendación, lo mejor es buscar actualizar el sistema operativo a las versiones más recientes.

La nube

La nube le ha dado ciertas ventajas a los usuarios en relación con el manejo y seguridad de los datos. Algunas de ellas son:

- Se puede visitar desde cualquier computadora (incluso varias al mismo tiempo) y desde diferentes partes del mundo.
- No requiere un espacio físico.

- Permite mejorar el servicio en términos de rendimiento y capacidad, con mucha facilidad.
- Los servicios de Nube pueden funcionar como respaldos de información.
- La seguridad de los servicios de Nube, generalmente, está muy bien garantizada.
- No hay Hardware que configurar, por lo que su acceso es más rápido y fácil.

Se pueden considerar algunas desventajas de los servicios de almacenamiento en nube:

- Si hay mala conexión, se complica el acceso a los servicios.
- Aunque generalmente la seguridad está garantizada, depende de otros. Esa situación puede que no alivie del todo a un usuario.
- Los servicios podrían llegar a tener un alto costo.

A pesar que la Nube es un servicio exitoso y seguro, siempre es recomendado poseer un respaldo del material. Las grandes compañías que brindan servicios en la nube como Google o Amazon, no dejarán que la reputación de su marca se caiga por lo que invierten en garantizar la calidad, continuidad y seguridad del servicio. En empresas más pequeñas, esto podría no ser una garantía.

Se recomienda también leer siempre las condiciones y términos del servicio adquirido.

La nube también tiene la capacidad de albergar una copia de la información en la computadora, de forma local, de manera que exista una duplicidad de los datos y cada vez que se modifiquen van a tener cambios en ambos espacios, lo cual representa una gran ventaja.

Los usuarios

La expansión de la Web y la constante experiencia de navegación de las personas usuarias, ha llevado a las corporaciones a generar cuentas para manejar los software, desde Sistemas Operativos, cuentas de correo, compras en línea, juegos, bancos, pagos personales, entre otros.

La especialización de las cuentas para cada acción, ha incorporado distintas modalidades de las mismas para incluso, proteger el acceso a los datos.

Por ejemplo, en sistemas operativos, se pueden tener cuentas con permisos de administración por completo y cuentas de usuarios invitados que no tienen un rol de administración total. Las cuentas administrativas no se recomiendan para roles de día a día, sino más bien, para cuando haya que generar cambios importantes dentro de la computadora o dispositivo.

Al existir tantas cuentas para tantos motivos, un usuario debe en la medida de lo posible generar contraseñas robustas y no repetirla en sus diferentes cuentas. Es decir, que la contraseña de la cuenta de correo no sea la misma del banco, por ejemplo. Una contraseña robusta implica la combinación de letras mayúsculas, minúsculas, números y símbolos y, en la medida de lo posible, que no sea conformada por datos fáciles de vincular a un usuario, como fechas de cumpleaños, nombres de la cuenta o que sean fácilmente relacionados con el usuario. Tampoco se recomiendan contraseñas cortas.

Existen aplicaciones que sirven para administrar las contraseñas de las múltiples cuentas que puede tener un usuario. Esto facilita de cierta manera al usuario el manejo de sus cuentas y sobretodo la seguridad de sus contraseñas, porque, podría aplicar una diferente para cada sitio sin temor a olvidarla y perder el acceso.

Generalmente, cuando se pierde una contraseña, para recuperarla el usuario asocia una cuenta de correo electrónico donde llegarán las

indicaciones respectivas. Se recomienda que, cada vez que se pierda una contraseña, se restaure la del correo asociado a la recuperación para evitar alguna posibilidad de rastreo o espionaje.

Debido a la gran cantidad de amenazas que tiene un usuario sobre sus contraseñas, muchos sitios solicitan condiciones de robustez y autenticaciones de doble factor, que, son la escritura de contraseñas y pero además, códigos que el usuario recibiría a un dispositivo móvil (por ejemplo) asegurando que solo la persona dueña de la cuenta tenga ese código de acceso. Los teléfonos móviles (algunos) incluyen la autenticación mediante huella dactilar como método de autenticación doble.

Aunque este método pueda significar una molestia para el usuario, es más efectivo en términos de seguridad, por lo que es recomendado.

Cómo prepararse para cualquier tipo de catástrofe

Un dispositivo puede fallar en cualquier momento y esto significa que los datos que tenga un usuario, se podrían perder súbitamente. Esta primicia indica que al menos, como medida, se debe de contar con una copia de seguridad en la Nube.

Las copias de seguridad, pueden ser físicas (en un disco duro externo) o en la Nube, mediante servicios como LiveDrive o Carbonite, que se instalan en la computadora y automáticamente generan respaldos. Algunos servicios cuentan incluso con la posibilidad de enviar un disco externo con la información de la computadora, en caso de catástrofe; ese servicio tiene un costo extra al normal.

Las amenazas son variadas para la salud de un computador: infección de virus, fallos del disco duro, mal uso de usuarios invitados, delincuentes que en físico o de forma remota estropean la computadora. El caso es que, una situación negativa puede suceder en cualquier momento y podría ser lo suficientemente lamentable para perder toda la información.

Es recomendable crear una copia de seguridad local, sin embargo esta tiene ciertas desventajas como que el dispositivo donde lo almacene pueda sufrir un daño o si la computadora tiene un virus, es probable que con el paso de archivos, el dispositivo también lo adquiera. Además de un daño físico, un dispositivo siempre está expuesto a robo. Tampoco va a gozar del beneficio de la actualización automática.

Acceso privado a internet

El acceso privado a Internet, garantiza la privacidad de los datos de un usuario mientras navega en la Red. Una Red Privada Virtual (VPN) crea un túnel cifrado y seguro entre el equipo del usuario y un servidor privado. El túnel oculta la dirección IP del usuario; garantizando así, privacidad en la transmisión de datos.

Existen varios proveedores en Internet que brindan el servicio VPN de forma paga o gratuita, en su gran mayoría con indicaciones claras sobre cómo acceder a la plataforma y comenzar a utilizar el servicio.

Los parches

En general, cada actualización de una aplicación como los sistemas operativos, contiene mejoras y nuevas cualidades. Sin embargo, algunas de esas nuevas incorporaciones podrían ser vulneradas o contener un error de funcionamiento posterior a su lanzamiento. Es ahí donde las casas corporativas que desarrollan las actualizaciones deben corregir. Ese paquete correctivo, se le llama popularmente como “parche”.

La aplicación de los parches resulta vital para la seguridad de la computadora, ya que evita que los piratas de la Web se aprovechen de las vulnerabilidades recientes y que el equipo esté a tope con la actualización aplicada, es decir, se cierra cualquier portillo que haga a la computadora vulnerable.

Entendida la importancia de este proceso de renovación de la seguridad de la computadora, los desarrolladores de sistemas operativos han

desarrollado software que se encarga solamente de incluir en la computadora, cada actualización. Así funciona Windows Update, que monitorea e incluye las actualizaciones apenas la corporación Microsoft la pone a disposición de los usuarios. Esta aplicación también tiene la habilidad de escanear la computadora para identificar software maliciosos con cada actualización aplicada, y lo mejor para el usuario es que lo realiza de forma automática.

Cada aplicación, más allá del sistema operativo, tiene también un proceso normal de actualización. En los menú, generalmente existe un apartado con la indicación de buscar actualizaciones disponibles. Es recomendable para el usuario mirar cada cierto tiempo si hay una nueva versión habilitada e instalarla.

Aplicaciones como Secunia, se encargan de monitorear actualizaciones en cada programa que contenga el sistema operativo, facilitando la labor al usuario de mantener siempre las últimas versiones.

Los programas antivirus

Contar con un programa antivirus siempre es pertinente para cualquier usuario, independientemente de su sistema operativo. Un antivirus se crea para proteger a las computadoras o dispositivos móviles de programas maliciosos ya identificados, por lo que si se crea uno completamente nuevo, su protección no será al 100%. Esta razón ha llevado a algunos usuarios, a pensar que este tipo de programas podrían ser prescindibles, lo cual supone un error.

Por lo general, un paquete de seguridad contiene un Firewall o cortafuegos, un antivirus, escáner de correo electrónico y descargas, un anti spam (mensajes no deseados) y un anti spyware (programas espía).

Hay aplicaciones en línea que generan un escaneo en la computadora sin necesidad de instalar el programa como tal. Generalmente estas aplicaciones identifican virus y brindan un informe de la salud de la computadora o dispositivo, pero no desinfectan del todo.

Los cortafuegos

Los cortafuegos o firewalls, sirven como barrera electrónica que protege a los equipos de los intentos constantes de dañarles. Es una protección necesaria y básica contra ataques de Internet.

Sistemas Operativos como Windows, ya incorporan un cortafuegos, sin embargo, en los paquetes de Antivirus los cortafuegos pueden ser más robustos, especializados y resistentes. Quitar un firewall, podría significar un error de seguridad muy alto.

Cómo blindar su equipo

Existen aplicaciones que podrían brindar seguridad extra a una computadora. Dos de ellas son DEP y EMET. La primera inhibe la ejecución de código percibido como malicioso.

EMET (por sus siglas en inglés) se encarga de detener cualquier aplicación que viole las reglas de seguridad que tiene implementada, por lo que funciona entonces como una capa de seguridad.

Ambas funcionalidades están incorporadas esencialmente para Windows por la compañía Microsoft y son configurables por el usuario.

CONCLUSIONES Y RECOMENDACIONES

La principal recomendación para un usuario que constantemente navega en Internet, exponiendo datos de diversa índole, es, estar alerta. Con esta condición, un usuario puede dimensionar la importancia de tomar medidas de seguridad adecuadas como contar con Antivirus, proteger las Redes de Internet con enrutadores, crear contraseñas robustas y diversas para sus múltiples cuentas y ser cuidadoso tanto con los respaldos de información físicos y virtuales.

Las amenazas en el mundo de la Web y la tecnología en general son las principales causantes de llevar a los usuarios a considerar múltiples aspectos vinculados con la seguridad.

En definitiva, una de esas consideraciones que resulta vital para la seguridad, es la actualización constante de los equipos y software, pero sobretodo, del conocimiento de las personas usuarias en materia de seguridad informática.

REFERENCIAS BIBLIOGRÁFICAS

Lower, R. (2016). *La seguridad informática es como el sexo seguro. Recuperado de* https://play.google.com/books/reader?id=SfH0DAAAQBAJ&hl=en&pg=GBS.PT117

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica