Revista Fidélitas, Vol. 2 (2). Noviembre 2021
http://revistas.ufidelitas.ac.cr/index.php/revista_fidelitas
Recibido: 09 julio 2021, Aprobado 26 octubre 2021

ISSN: 2215-6070
10.46450/revistafidelitas.v2i2.34

Protocolo para evitar robo de datos mediante encriptamiento de una red doméstica o de uso personal

Juan Alonso Arce Briceño
jarce70066@ufide.ac.cr

Abstract

This electronic/digital document is aimed at all kinds of people who are interested in learning about cybersecurity through the use of encryption, therefore, two elementary terms that will be relevant in the attached project will be explained: cyberspace and cybersecurity. In addition to the aforementioned, two types of encryption processes are implemented, which will be directed towards: private and domestic networks. Finally, the author offers a specific solution according to what has been investigated in a theoretical way, which will be the ideal steps that every individual must follow to have an environment without security breaches (intrusion detection protocol). In conclusion, it will refer to the results / conclusions made by the researcher, so that readers can have a clear and concise idea of what the writer has learned.

Keywords: Cybercrime, Malware, Hacker, Information security management, Spyware.

Resumen

Este documento electrónico/digital está dirigido a toda clase de persona que esté interesada en informarse en el tema de ciberseguridad mediante el uso de encriptación, por lo que se explicará dos términos elementales que tendrán relevancia en el proyecto adjunto: ciberespacio y ciberseguridad. En adición a lo mencionado anteriormente, se implementan dos tipos de procesos de encriptación, los cuales se verán dirigidos hacia: redes privadas y domésticas. Por último, el autor ofrece una solución determinada según lo investigado de forma teórica lo cual serán los pasos ideales que todo individuo debe seguir para poseer un ambiente sin brechas de seguridad (protocolo de detección de intrusiones). En conclusión, se referirá a los resultados/conclusiones realizadas por parte del investigador, con el fin de que los lectores puedan tener una idea clara y concisa de lo aprendido por parte del escritor.

Palabras clave: Cibercrimen, Malware, Hacker, Gestión de la seguridad de la información, Spyware.

1. Introducción

De acuerdo con Muñoz (2018) se puede definir el término de ciberseguridad como:

> "*La práctica de protección de dispositivos, sistemas, redes y datos de ataques u otros fines maliciosos. En otras palabras, se trata de la seguridad implementada en las tecnologías de la información y es aplicada en contextos diferentes. No obstante, siempre está presente en el siglo en que se vive hoy en día (vida cotidiana), muchos de los desarrollos cibernéticos se han dado debido a la ciberseguridad y su manera de desenvolverse en la vida cotidiana."*

De acuerdo a esta definición, en este artículo se presenta el término contra sus términos homólogos, con el fin de poder detener las brechas de seguridad en diferentes sitios web e inclusive en la computadora personal de cada persona, es importante que este término sea conocido por la ciudadanía en general y que se tenga claro acerca de los términos ciberespacio y ciberseguridad.

De acuerdo a Barboza Coto y Alvarado Fonseca (s.f) cuando se habla sobre la protección de datos de los usuarios, específicamente para el siglo XXI apuntan que:

> *"ha sido configurada por diferentes cortafuegos que tienen el fin de evitar el robo de datos, pero estos con frecuencia tienen fallas de configuración y ahí es donde entra el delincuente llamado "Hacker" o "Cracker". Estos últimos tipos de delincuente cibernético tienen distintas características; el "cracker" es más peligroso ya que este no tiene límites, usualmente no ocupa la información relevante del sistema, este individuo personaliza dicho sistema y lo hace a su disposición. En cambio, el "hacker" existen diferentes tipos, los*

cuales son: black-hat, white-hat, newbies y hacktivista. Usualmente todos son peligrosos y por eso se hace destacar la información a la población de todas las edades, que ser "hacker" o "cracker" es ilegal en cualquier país y es penado con cárcel."

Habitualmente la protección de datos que poseen una red doméstica o de uso personal es muy escasa, ya que es proporcionada por un contrato de servicio o bien por el desconocimiento de los usuarios, quienes no se protegen al no conocer sobre los peligros e infiltraciones de las que pueden ser objeto, lo cual lo convierte en un tema actual, para que se determine la importancia de informarse de manera recurrente sobre la necesidad y ventajas de considerar lo que la ciberseguridad puede ofrecer en este tipo de redes.

En la actualidad y a nivel mundial se destacan distintos artículos científicos que contribuyen a la comunidad informática, pero se necesita una continua formación académica en este campo, ya que este tema puede ayudar a una persona, a una organización o bien a un país completo. Lo peor que una organización o país puede enfrentar es un ataque cibernético (ciberataque), ya que este puede cortar todos los fondos de un país completo y dejarlo vulnerable ante sus deudas financieras e incluso causar una posible guerra.

El presente artículo muestra las capacidades de la ciberseguridad que han estado a lo largo de la historia y que continúan estando presentes en la actualidad. Se busca plantear que los lectores se puedan educar de una manera más crítica ante otros países competitivos en esta materia mencionada anteriormente. Dicho de otra manera, el objetivo general propuesto por el autor es demostrar en el campo de la ciberseguridad, la aplicación de una nueva metodología innovadora (disruptiva) con el fin de poder darle un propósito distinto a los resultados de la presente investigación. Por lo que se le pide a los lectores ver de una manera más innovadora el documento, debido a que se van a romper con los esquemas tradicionales de trabajos de investigación.

Adicionando a lo mencionado en el transcurso de la introducción, el proyecto de investigación tendrá dos objetivos específicos que buscarán cumplir con la metodología mencionada en el párrafo anterior: 1) Evaluar de manera eficaz y determinante la aplicación debida de los conceptos bases de la ciberseguridad y ciberespacio, con el fin de que el lector pueda adquirir el mayor conocimiento acerca del tema entablado. 2) Distinguir a la mayoría de las puestas en práctica, ya que éstas no poseen las características de conceptos elementales/básicos enfocados en CBSG que tendrán gran relevancia en el proyecto a tratar. Algunas de las diferencias que se podrán determinar luego de culminar la lectura podrán ser el valor real de las resistencias para que el dispositivo funcione correctamente.

Es importante mencionar que el estudio que se presenta a continuación no se aplicó en ninguna red local (privada) o doméstica, debido a las restricciones provocadas por la pandemia del COVID-19.

2. Referentes teóricos

Proceso de encriptación (Red Personal)

Por lo que se refiere al proceso de encriptación recomendado por el presente autor se declaran ciertos pasos que serán de suma importancia para el usuario final que tenga la intención de leer dicho artículo de carácter teórico informativo. En adición a este respecto encabezado, el autor declara su preocupación ante las fallas que han tenido las personas con las brechas de seguridad en diferentes ámbitos. Por lo que es de suma importancia advertir a los lectores leer con determinada paciencia cada análisis abordado.

Primeramente se explicará la encriptación en Linux que contiene una serie de diferentes aspectos importantes para tomar en cuenta. Debe ser por medio de aplicaciones o sistemas que permitan incluir los códigos o cifrados que corresponden en el momento de ejecutarlos, por lo que se recomienda utilizar GnuPG; este programa le facilita al usuario que requiere de su necesidad, incorporarlo en la base de archivos de su dispositivo para su respectivo uso.

El proceso de encriptación ha sido determinante para un número elevado de la población en todo el mundo, debido a que esta brinda confidencialidad a aquellos que necesitan proteger su privacidad de una manera simple y con un costo muy bajo. No obstante, se hace referencia a las características brindadas por el concepto de encriptación, ya que este hace enfoque a la privacidad de los usuarios poseedores de dicho material.

Proceso de encriptación (Red Doméstica)

Haciendo hincapié al proceso de encriptación mencionado anteriormente, se realiza una breve explicación de los modos en que se podría ayudar a una red doméstica:

Según Acosta (2016) "Uno de los controles establecidos por los estándares PCI DSS es la implementación de la encriptación o criptografía en redes, ya que, mediante un algoritmo asimétrico y simétrico se identifican las brechas en una red" (p. 1).

En adición a lo mencionado anteriormente, existen tres componentes principales en los que la encriptación se enfoca, Acosta (2016) menciona que "Se necesita que el texto sea claro, el éxito en la encriptación, y el texto encriptado" (p. 2).

Según INCIBE (s.f):

"*La encriptación en MACOS enfocada en una red doméstica, no es un gran problema.*

> *Debido a que los nuevos computadores Apple poseen una aplicación llamada FireVault, la cual tiene como función la encriptación del disco duro e inclusive la encriptación de datos individuales (p. 1).”*

Así mismo, cuando se trata del software desarrollado en Linux INCIBE (s.f) afirma que la encriptación

> “*no es algo de otro mundo, ya que esta es implementada en una serie de algoritmos los cuales tienen como fin la seguridad protocolaria del usuario. Depende del software libre que posea el usuario, se implementará de manera distinta el cifrado de extremo a extremo (p. 3).”*

A modo de cierre, la encriptación de una red es fundamental para que un usuario posea sus datos imponibles. Cuando un usuario se informa marca la diferencia, pero también abre los ojos, ya que este mal es de los más frecuentados entre la población mundial y es de suma preocupación para los editores de este artículo científico.

Pasos Protocolarios ante detección de robo de datos

Según Sánchez (2018), en un estudio realizado en el protocolo de ciberseguridad dirigido a la Universidad de Madrid, se realizaron diferentes actos protocolarios para la identificación de las brechas de seguridad en las redes locales (privadas), por lo que diferentes entes informáticos presentaron cambios sustanciales para evitar la propagación de vulnerabilidades cibernéticas. A continuación, se presentarán una serie de pasos protocolarios con el fin de detectar distintas brechas cibernéticas en redes personales o domésticas:

- Tener contraseñas complejas y distintas para diferentes recursos en que se utilice. Por ejemplo: entidades bancarias, correos electrónicos, entre otros. Esto es una causa muy frecuente, algo muy recurrente, por lo que es una brecha cibernética fácil de romper para los distintos tipos de malware.
- Cuando se recibe un correo revisar si posee enlaces o que sean correos ficticios. Ya que este es uno de los medios más usados por los hackers para robar información sensible.
- Es importante reforzar la seguridad de la red que se dispone en el hogar del usuario, ya sea cuando se compre algún dispositivo que ayude a la privacidad o se contrate a un técnico especializado.
- Actualizar el software de los dispositivos que se posean, es de mucha ayuda ya que en estas se ejecutan las últimas protecciones y seguridades que el fabricante dispone. Constatando que la actualización venga del fabricante y no de algún otro sitio de dudosa procedencia.
- Evitar comprar dispositivos de segunda mano, ya que no se sabe si ese dispositivo viene alterado.
- Investigar antes de comprar, ya que cuando el usuario no se informa de las técnicas de seguridad existentes, puede verse afectado. De esta forma se sabrá qué tan seguro es o qué anomalías podría detectar antes de un malware.
- Respaldar documentos que se tenga en los dispositivos, ya que si se pierde algún dato, este se podrá tener respaldado.
- Hacer una comprobación regular de la red que se posea en el lugar de residencia, de esta forma se podrá eliminar los dispositivos viejos que ya no se use o que ya no se conectan a la red, también, se podrá ver algún dispositivo que sea desconocido, eliminándolo y sin olvidar restablecer la configuración de fábrica. Esto ayudará a que si trata de conectarse de nuevo a la red, este no lo pueda hacer.
- Enseñar a los niños del hogar a no compartir información, ubicaciones, números de contacto o correos electrónicos que algunas aplicaciones solicitan. Guiar, supervisar y tener control de los dispositivos que puedan poseer los niños, ya que son aún más vulnerables ante los ataques y acosadores que se encuentran en internet.

A continuación, se mencionan distintas palabras claves o keywords, que se usan parcialmente en este documento:

Pequeñas y Medianas Empresas (PYMES): Según Westreicher (s.f) “Se usará el concepto anterior para referirse a un conjunto de personas que poseen una empresa pequeña o mediana” (p. 1).

Ataque dirigido persistente (APT): De acuerdo a Ramírez (2021): “Se emplea dicho término cuando los cracker o hackers tienen como objetivo al usuario durante un tiempo indefinido e incluso de la manera más imperceptible” (p. 2).

Estafa (scam): Según Muñoz (2018), “Esto se trata de un engaño o fraude, cometido ya sea por hackers o crackers, a un grupo de personas para que estos imprudentemente den su información, dinero, etc todo esto bajo falsas promesas de beneficios económicos” (p. 4).

Robo de identidad: Según Muñoz (2018),

> *“Los distintos crackers y hackers aprovechan el descuido de diferentes usuarios para obtener su información confidencial del usuario ya sea contraseñas para acceder a diferentes servicios. Y todo esto con el fin de que personas no autorizadas utilicen esta información para suplantar al usuario víctima del robo (p. 2).”*

Firewalls: Según Carles (2013),

> *“Es un software o hardware diseñado con un conjunto de reglas para bloquear el acceso a la red de usuarios no autorizados y así garantizar la seguridad del usuario” (p. 1)*

VPN: Según Ramírez (2021)

> *“Son las siglas de Virtual Private Network (red privada virtual), se aplican los túneles de datos y así estos rebotan en el país deseado” (p. 1).*

3. Metodología

Antes que nada se debe especificar que la razón primordial de este documento será la poca confiabilidad que tienen los usuarios en general de los protocolos de seguridad dentro de su ambiente tecnológico. Por lo que de una manera teórica, se le quiere hacer llegar al público meta para que sepan que existen protocolos que pueden ajustarse a sus necesidades. La pregunta a plantear por parte del autor será la siguiente: ¿Cómo llegar a tener un ambiente tecnológicamente amigable sin brechas de ciberseguridad?.

En primer lugar, el autor presenta investigaciones relevantes como Tesis de grado y documentos fiables para llegar a poseer información relevante ante cualquier eventualidad de brecha tecnológica. Se le agrega a lo mencionado anteriormente que el público meta enfocado en el documento será todo tipo de personas que quieran reforzar su conocimiento, e inclusive que tengan intenciones de comenzar a investigar en el presente tema tan amplio.

En segundo lugar, se aplicó en el estudio adjunto un equipo de revisión de literatura basada en las bibliotecas digitales de la Universidad de Costa Rica y la Universidad Fidélitas (EBSCO) con el fin de poder poseer documentos de alta categoría en el ambiente tecnológico, ya que el autor presenta diferentes contenidos temáticos con el fin de poder brindarle al lector los conocimientos adquiridos por este usuario. Y por último las variables y categorías adjuntadas en el documento de investigación, fueron acerca de cómo mejorar la protección del usuario final.

Para concluir, los instrumentos utilizados en el documento serán con fines informativos debido a que se ha detectado de una manera alarmante por parte del autor, que los usuarios que usualmente no confían tanto en la tecnología o que poseen muy pocos conocimientos acerca del peligro del ciberespacio, no encripta de manera eficaz sus dispositivos. Y esto beneficia a los ciberdelincuentes, debido a que sin estos pasos protocolarios se les hace más fácil el robo de datos del usuario final.

4. Resultados

Con respecto a los protocolos identificados para determinar una buena salud cibernética, se ha proporcionado por parte del autor algunos de los peligros correspondientes por la falta de cuido de los usuarios finales que poseen algún tipo de relación con el ámbito web (lo cual se considera sumamente peligroso), debido a las fallas cibernéticas/ delitos cibernéticos (ciberdelitos) que han ocasionado millones de estragos tanto económica como políticamente en distintas partes del globo terráqueo. No obstante, se hace énfasis que el estudio del que habla este documento no fue aplicado en redes domésticas o privadas debido a la pandemia del COVID-19, por lo que a futuro se espera que algún ente aplique dicho conocimiento brindado por el autor.

En adición a lo mencionado en los párrafos anteriores, la mayoría de la población adjunta posee el conocimiento de que las vulnerabilidades en los sitios webs/redes públicas y privadas son existentes, pero se ha identificado hasta cuál punto poseen el conocimiento acerca de lo anterior. Se justifica de manera extraordinaria, debido a que las vulnerabilidades son la causa de los ciberdelitos en la actualidad, por lo que el autor se tomó una reflexión acerca de cómo ayudar a lector y presentará de manera directa un conjunto de soluciones:

- Anteriormente se mencionó la definición de vulnerabilidad en la cual se explicó de manera concreta que todas las redes son vulnerables en algún aspecto, ninguna es perfecta ante los ojos cibernéticos.
- Usualmente, el Diagrama de Venn de una red según INCIBE (2017), "Está compuesto por tres factores, los cuales son: Amenaza, Sistema de Información y por último Vulnerabilidad" (p. 1).
- Según Cardona (s.f),

A la hora de realizar un análisis a fondo de una red se comienza desde los usuarios que la frecuentan, ya que, existen todo tipo de individuos con malas o buenas intenciones, por lo que generalmente, se necesita un personal especializado en el tema (p. 2).

- No obstante, también se realiza la estimación de riesgo, debido a que un análisis implementado sin previo aviso, puede molestar a los usuarios de esta red.

En resumen, los elementos brindados por el presente autor ayudarán a la población con sus problemas de seguridad (brechas cibernéticas), esto con el fin de poder reducir los ciberataques de una manera desigual. Se considera que esta problemática va a ir creciendo de manera exponencial conforme pasen los años y esto es sumamente preocupante para la comunidad de informática de todo el mundo, ya que esto se caracteriza como un evento de la vida cotidiana.

5. Discusión

Según el punto de vista del autor del presente documento se han obtenido grandes ganancias de conocimiento a nivel teórico-práctico, ya que se consideraba que los países no estaban aplicando algunas metodologías para combatir las brechas de seguridad. Pero se amplió la gama de conocimiento de que algunos países están aplicando su capital en el fortalecimiento de estos ambientes tecnológicos. No obstante, se recalca que falta mucho que mejorar, pero la iniciativa es sumamente innovadora.

En pocas palabras, se considera que las regiones se encuentran en una constante mejora en términos de ciberseguridad, debido a los acontecimientos tan lamentables que han sucedido a lo largo de los años anteriores. Adicionando a los sucesos, estos países se enfrentaron a una época donde la ciberseguridad se encuentra en un constante cambio.

En definitiva, la ciberseguridad ha causado grandes cambios en diferentes territorios de todo el globo terráqueo, ya sea de carácter positivo como de modo negativo. El autor encontró conocimientos teóricos que consideró de gran importancia para que los lectores comprendieran la necesidad de innovación en este ámbito. Se quiere mencionar de forma clara: Los países deben cambiar su visión y comenzar a fortalecer las áreas tecnológicas para que no se vean en enfrentamientos de brechas de seguridad.

6. Conclusiones

El concepto de ciberseguridad ha sido crucial debido a su desarrollo tan extraordinario a lo largo de los últimos años. No obstante, se le debe adicionar a este concepto que el paso para poseer una vida cotidiana saludable en palabras cibernéticas, será enfocarse en la encriptación que las personas podrán emplear en su vida cotidiana.

Algunos de los progresos de este escrito han sido la obtención de conocimientos por parte del autor y se ha notado el desarrollo que ha tenido toda la comunidad cibernética a través de los años.

La integridad o confidencialidad que proporciona, es debido a su clasificación y sus métodos que se utilizan para ejecutar cada una de las órdenes, ya que, cada uno de los archivos debe de seguir una serie de pasos y se utilizan diferentes sistemas para realizarlo, cada uno de los usuarios que lo realicen, deberán de generar usuarios y contraseñas complejas donde los archivos serán guardados y asegurados. Realizar cada uno de los pasos, promueve que los archivos no sean vistos por terceros y además no podrán ser robados (en otras palabras: codificación de archivos), distintas empresas los deben utilizar, debido a que la existencia de hackers y crackers en el mundo del internet que cada vez es más alta y lo que pretenden es posicionarse en estos archivos.

Lo más conveniente para el usuario es evitar el ingreso a páginas desconocidas o de poca fidelidad, ya que se ha determinado que los crackers o hackers utilizan las vulnerabilidades de distintas páginas web para que los usuarios ingresen sus datos y de esta manera ingresen a la información personal del usuario en general. Adicionando a lo mencionado en el texto anterior, se hace referencia a utilizar protocolos de seguridad en navegadores poco fiables como lo son la mayoría de los ofrecidos actualmente en el mercado.

Los recursos de determinada investigación se basarán exclusivamente en sitios web de alta fiabilidad como lo son: bibliotecas digitales, bases de datos (EBSCO), páginas web de fiabilidad e inclusive artículos de informativos acerca del tema mencionado a lo largo del documento. Se adiciona a dichas conclusiones que la ciberseguridad y tener buenos actos protocolarios ante cualquier intrusión han sido fomentadas como un buen hábito para cualquier usuario del mundo.

Los pasos protocolarios ayudarán al usuario a tener una mayor privacidad de sus datos en el computador e incluso poder encriptar el disco duro es uno de los objetivos primordiales de la seguridad del computador. Ya que se hace notar que más del cincuenta por ciento de la población no encripta, ni respalda el disco duro, y esto es de suma preocupación para el autor de este documento. Claro, muchos de los individuos poseen desconocimiento acerca de estos temas por lo que es de suma importancia que se den cuenta de los peligros cibernéticos que se realizan en la actualidad.

7. Referencias

Acosta, D. (2011, May). Definición de Cracker, Phreakin, Lammer. Definición ABC. Recuperado de https://www.definicionabc.com/tecnologia/cracker-phreakin-lammer.php

Barboza Coto, A. M., & Alvarado Fonseca, A. (s.f). Ciberseguridad en Costa Rica. Recuperado de https://www.kerwa.ucr.ac.cr/bitstream/handle/10669/500/libro%20completo%20Ciber.pdf?sequence=1&isAllowed=y

Darío Cardona A., O. (s.f). Evaluación de la amenaza, la vulnerabilidad y el riesgo. Recuperado de https://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

De Sistemas, I., Arias, G., Nelson, B., Almeida, M., Noriega García, N. (2021). Análisis y solución de las vulnerabilidades de la seguridad informática y seguridad de la información de un medio de comunicación audiovisual [Tesis de licenciatura no publicada] Universidad Politécnica Salesiana Sede Guayaquil Facultad de Ingenierías de Sistemas. Recuperado de https://dspace.ups.edu.ec/bitstream/123456789/5386/1/UPS-GT000497.pdf

Frutos, A. M. de. (2018). ¿Qué es scammer? ComputerHoy. Recuperado de https://computerhoy.com/noticias/software/que-es-scammer-73875

Hiperderecho (2018). Una breve historia de la ciberseguridad importada. Derechos Digitales. Recuperado de https://www.derechosdigitales.org/12329/una-breve-historia-de-la-ciberseguridad-importada/.

INCIBE. (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? INCIBE. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

Owaila, A. (2021). El robo de identidad aumentó durante la pandemia. WeLiveSecurity. Recuperado de https://www.welivesecurity.com/la-es/2021/02/04/el-robo-de-identidad-aumento-durante-la-pandemia/

Rochina, P. (2016). ¿Qué es el Hacktivismo? Ciberataques y grupos activistas. Canal Informática y TICS. Recuperado de https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

Rojano, E. (2015). Seguridad: Cómo cifrar y descifrar archivos en Linux. Sinologic.net. Recuperado de https://www.sinologic.net/2015-06/seguridad-como-cifrar-y-descifrar-archivos-en-linux.html

School, I. B. (2019). ¿Cuáles son los principales organismos relacionados con la ciberseguridad? Blog de Tecnología - IMF Smart Education. Recuperado de https://blogs.imf-formacion.com/blog/tecnologia/organismos-ciberseguridad-201904/

SinoLogic. (2015). Seguridad: Cómo cifrar y descifrar archivos en Linux. Sinologic.net. Recuperado de https://www.sinologic.net/2015-06/seguridad-como-cifrar-y-descifrar-archivos-en-linux.html

Wecheister, G. (2015). Pyme - Pequeña y mediana empresa. Economipedia. Recuperado de https://economipedia.com/definiciones/pyme.html