Revista NEYART
ISSN: 2992-7161

LA SEGURIDAD COMPUTACIONAL EN LA FRONTERA NORTE MEXICANA, CASO DE ESTUDIO: CD. JUAREZ, CHIHUAHUA, MEXICO

COMPUTER SECURITY IN MEXICAN BORDER. CASE STUDY: CD. JUAREZ, CHIHUAHUA, MEXICO

Nafarrate Bustillos Jorge
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0009-0007-9294-068X
jb_nafa@hotmail.com

Hurtado Solís Martha Magdalena
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0000-0003-2434-1902
martha.hs@cdjuarez.tecnm.mx

Ruiz Isis
University of Texas at El Paso
https://orcid.org/0009-0004-3435-9828
isis.anru@hotmail.com

Reyes Uribe Viridiana
Tecnológico Nacional de México/I. T. De Ciudad Juárez
https://orcid.org/0009-0007-9793-3367
viridiana.ru@cdjuarez.com

DOI: https://doi.org/10.61273/neyart.v2i1.45 | **Recibido:** 28/11/2023 | **Aceptado:** 08/02/2024 | **Publicado:** 29/02/2024

Esta obra está bajo
una licencia internacional
Creative Commons Atribución 4.0.

Resumen: Existen diversas compañías que se encargan de crear soluciones para las tiendas de ultramarinos que se encuentran en la ciudad, la mayoría de estos ultramarinos gestionan información valiosa o realizan algún tipo de transacción como el pago de servicios o compras de tiempo aire mediante puntos de venta. Una de las compañías que acaba de llegar a la ciudad es NAUTILUS, la cual una empresa que mediante los puntos de venta recolecta información estadística de las ventas que ultramarinos, dicha información es comprada por diferentes compañías, además de que es útil para la misma empresa ya que pertenece a una cadena de productos en el mundo y esta maneja diferentes marcas de productos propios. La información estadística sirve para saber cómo se encuentra el mercado, cuáles son las áreas de oportunidad y tener monitoreada a la competencia para así poder de alguna manera crear ofertas o promociones que ayuden a tener mayor control sobre la NAUTILUS no es la única compañía de puntos de venta que se dedica a este tipo comercio, pero es una de las empresas que acaban de llegar a Cd. Juárez aproximadamente en mayo y aunque su matriz se encuentra en Guadalajara, Jalisco, México actualmente tiene presencia en la mayoría de los estados mexicanos.

Palabras Clave: Puntos de venta, estadística, mercado, tiendas de conveniencia, seguridad informática.

Resumen: There are some companies that are responsible for creating solutions for grocery stores located in the city. Most of these grocers manage valuable information or conduct some type of transaction such as paying for services or purchasing airtime through points of sale. One of the companies that has just arrived in the city is NAUTILUS, which is a company that, through points of sale, collects statistical information on the sales that grocery stores make every day. This information is purchased by different companies and is also useful for the same company since it belongs to a product chain in the world, and it manages assorted brands of its own products. Statistical information is used to know how the market is, what the areas of opportunity are and to monitor the competition to somehow create offers or promotions that help to have greater control over the competition. NAUTILUS is not the only point of 27 sale company that is dedicated to this type of trade but it is one of the companies that just arrived in Ciudad Juárez in May 2019, and although its headquarters

is in Guadalajara, Jalisco, Mexico It currently has a presence in most Mexican states.

Keywords: Point of sale, statistics, market, convenience stores, sales, informatic security, risks.

INTRODUCCIÓN

Existen una mayoría de personas que tienen un punto de venta desconocen en su totalidad el valor que tiene la información que generan y no solo eso realizan transacciones por cantidades a veces considerables y no tienen precauciones ya que no tienen conocimientos acerca de la seguridad informática y esto es algo preocupante ya que podrían ser blancos fáciles para algún ataque cibernético, la empresa en sí no proporciona un antivirus que proteja a sus asociados de algún virus informático, robo de información, o un ataque informático.

La seguridad informática en México tiene muchas áreas de oportunidad y es un tema que está tomando fuerza en el ámbito laboral, las empresas hoy en día son un poco más consientes, pero desafortunadamente los usuarios informáticos no tienen hábitos ni conocimientos de la situación actual en la que se encuentra el país con respecto a la ciberseguridad.

En la actualidad no es necesario tener todo un equipo de cómputo para manejar un punto de venta ya que con el simple uso de una aplicación móvil se pueden realizar los diferentes movimientos que se requieren para cumplir con las necesidades de un punto de venta, tal es el caso de NAUTILUS, todo se maneja mediante una aplicación móvil instalada en una tablet que utiliza un sistema operativo Andriod®. Recientemente la compañía de seguridad informática ESET® realizo un análisis y revelo interesantes datos acerca de la protección de dispositivos móviles que utilizan sistema operativo Android® y en dicho análisis según (Olmedo, 2019) México encabeza la lista en Latino América con el 26% de detecciones de malware. Esto indica que los usuarios informáticos en nuestro país no toman precauciones con el uso adecuado de la tecnología que ayuden a prevenir virus o ataques cibernéticos que perjudiquen o roben información.

Uno de los objetivos de este documento es la concientización del lector acerca de la importancia de estar protegido, al interactuar con los medios informáticos al momento de navegar por el ciberespacio, teniendo la certeza de que la información manejada en el mismo estará segura.

La rapidez con la que crece la tecnología es impresionante y eso es algo muy bueno para la sociedad

en general, pero, a su vez, es algo muy preocupante debido a que, en la actualidad, prácticamente toda la información relativa a personas físicas, jurídicas y organizaciones estatales, se transmite a través de internet.

Como afirma Herrera (2019) Según datos del Instituto Federal de Telecomunicaciones, al final del 2018,se cuentan con 120 millones de líneas celulares, el 54% de casas tiene internet fijo. Mientras tanto, nuestro país tiene una tasa de penetración nacional de banda ancha del 87% y 61 millones de usuarios de Facebook, lo que lo convierte en el quinto país con más usuarios de esta red., por lo tanto México ya ha expuesto una parte importante de su panorama social, económico y político a diversas formas de delitos cibernéticos.

Actualmente la mayoría de las personas que interactúan con los medios informáticos, desconocen los riesgos a los cuales se exponen, utilizan las redes sociales y algunas aplicaciones sin tomar precauciones, muchas de las ocasiones en que los usuarios informáticos resultan ser víctimas de virus y ataques informáticos, son originadas por el mismo usuario dado que excluye la forma en que operan los ciberdelincuentes.

La mayoría de las veces, los atacantes o virus informáticos utilizan información tramposa que parece ser real, provocando que los usuarios informáticos inconscientemente instalen o ejecuten programas perniciosos en sus computadoras o teléfonos celulares.

Otro de los orígenes por la cual los usuarios informáticos, no le dan importancia a la seguridad informática ni tomen conocimiento, es que en su mayoría desconocen totalmente las leyes que existen actualmente en nuestro país y esto provoca que no estén dispuestos para cualquier ataque cibernético, robo de identidad o secuestro de información.

Realmente las personas que interactúan con los medios informáticos pocas veces invierten en seguridad informática y están habituados a utilizar aplicaciones gratuitas, o software pirata, elevando así los riesgos de ser un blanco fácil de virus o espías informáticos.

Pocas veces se imparten pláticas o cursos sobre seguridad informática y esto puede perjudicar a futuro a las nuevas generaciones. Según (Treviño, 2015), socio director en Lex Informática Abogados™, los delitos informáticos son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación, es decir, es donde la informática es el medio o el instrumento para realizar un delito.

La Seguridad Computacional en México

En el mes de abril del presente año 2019, el partido político Morena presentó el desarrollo de una Agencia Nacional de Seguridad Informática (ANSI) perteneciente a la Secretaría de Seguridad y Protección Ciudadana Federal, todo esto fue por una iniciativa sobre la Ley de Seguridad Informática.

Conforme a la lista de países que conforman el índice global de seguridad de la Unión Internacional de Telecomunicación (ITU), México durante los últimos dos años ha sido desplazado del 1 lugar 28 de 175 en 2017 al lugar 63 de 175 en 2018. El indie consta de cinco puntos principales qu califican a los países:

1. Cooperación
2. Organizaciones
3. Legales
4. Habilidades Técnicas
5. Desarrollo de cada una de estas9

Dentro del ámbito legal, se puede notar la deficiencia del país, sirve como referencia el Plan Nacional de Desarrollo 2019 – 2024 que fue recién mostrado por el actual presidente de México (Andrés Manuel López Obrador) que trata de la cobertura de internet para todo el país y del desarrollo integral de la economía digital, pero a ninguno de esto dos puntos mencionados se le da alguna orientación de seguridad informática siendo que hay grandes antecedentes como el problema del ciberataque que se presentó al Sistema de Pagos Interbancarios (SPEI) en el mes de abril de 2018 y los análisis de grandes empresas de seguridad que revelan a México está dentro de los primeros lugares con más ciberataques en el mundo.

Sin embargo, en la Estrategia Digital Nacional presentada en marzo del 2019, se menciona a la ciberseguridad como principal tema a atender tomando encargos de la industria y organizaciones.

Las organizaciones y la cooperación son algunos de los pilares de la ITU y hay varias cuestiones clave.

Uno de ellos, que no se limita a México, sino que es un tema global, es la cooperación entre organizaciones.

Este problema se toma como una base muy sólida para la propuesta de la creación de la ANSI ya que, dentro de su propuesta, esta agencia estaría correspondida a determinar y coordinar políticas en materia de ciberseguridad aplicando lineamientos centralizados en acciones del ámbito social, económico y político.

Esta necesidad de centralización se da como respuesta a la diversidad de Equipos de Respuesta ante Emergencias Informáticas (CERT), policías cibernéticas y su problema de coordinación al momento de

acudir al ministerio público adema de una falta de sincronización y generando distintas interpretaciones a un mismo problema dando como resultados retrasos en conclusiones jurídicas.

Esta carencia de combinación entre organizaciones, el gobierno mexicano, en colaboración con la Organización de Estados Americanos (OEA), pretende mejorar la situación con el documento "Estrategia Nacional de Ciberseguridad" difundido en noviembre de 2017, y uno de sus principales enfoques es a través del involucramiento de la OEA en las organizaciones.

Cooperación entre varios grupos internacionales y nacionales, y el compromiso del Gobierno de proporcionar medios para mejorar la cooperación y la colaboración. Implementar políticas es muy importante para mejorar y fortalecer la seguridad informática. Sin embargo, el proceso burocrático es muy lento y los usuarios finales son los más afectados.

Sobre estas circunstancias, la Estrategia Nacional de Ciberseguridad integra como primer punto de sus ejes transversales la cultura de ciberseguridad. Este punto consiste esencialmente en concientizar a la mayoría de la población sobre sus interacciones e influencias en el ciberespacio a través de campañas publicitarias, educación y capacitación. En México se tienen dos vertientes principales asociadas a esto:

El phishing, una actividad de fraude cibernético que engaña a las personas para obtener beneficios económicos, ha aumentado un 81 % en comparación con 2017.

En 2018, tenemos una variedad de ataques donde la obsolescencia y el uso de tecnología antigua fueron los principales problemas. Específicamente, ransomware, cryptojacking y exploits.

El profesor de delitos cibernéticos de la Universidad de Harvard, Israel Reyes, señala con bastante precisión que México no puede responder a los ataques cibernéticos porque no existe una ley que regule este tipo de actividad criminal, y su importancia es crítica para la economía mexicana.

Cuanto más importante es estabilizarse, más probable es escalar.

Un exploit es un fragmento de código que un ciberatacante utiliza para explotar una vulnerabilidad en su sistema, también están incluidos. Cabe destacar que SMB/Exploit.DoublePulsar.B ocupa el sexto lugar entre las amenazas más comunes en México en 2018.

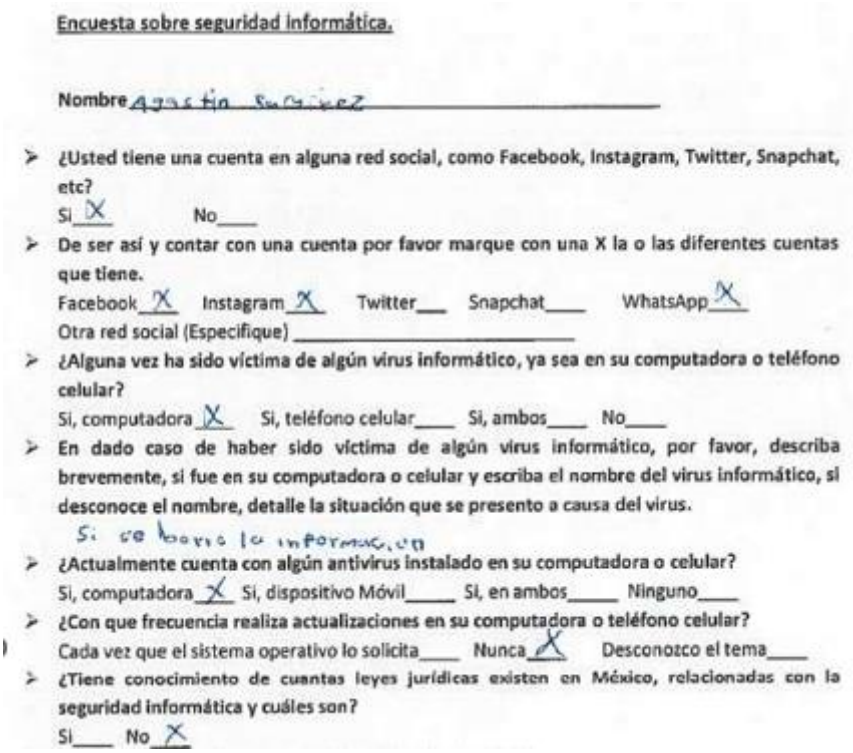
Este es un exploit que puede aprovechar una vulnerabilidad en Server Message Block (SMB), un protocolo para compartir archivos o impresoras dentro de una cuadrícula.

Según el sitio WeLiveSecurity by ESET, México es el país Latinoamericano con más localización de este exploit (22,5% del total de las localizaciones regionales), según se muestra en el siguiente gráfico:

Figura 1. Detecciones durante el año 2018.

DESARROLLO

Dado que se busca comprobar que los usuarios informáticos desconocen los riesgos a los cuales se exponen, al utilizar las redes sociales y algunas aplicaciones ya que no toma precauciones, muchos de los momentos en que los usuarios informáticos resultan ser víctimas de virus y ataques informáticos, son causadas por el mismo usuario ya que desconoce la forma en que los ciberdelincuentes operan; el actual trabajo fue hecho bajo el enfoque metodológico cuantitativo, y para lo cual utilizó la Recopilar y analizar datos para responder preguntas de investigación y probar hipótesis establecidas previamente, confiando en la medición numérica, el conteo y repetidamente en el uso de la estadística para crear con exactitud patrones de comportamientos en una población. (Hernández, Fernández & Baptista, 2003). El método de recolección de datos, que se utilizó en este trabajo, es probabilístico mediante una investigación de campo. La técnica de recolección de información de esta investigación es a través de encuestas, ya que se pretende generalizar los resultados a una población. Las encuestas estuvieron formadas por un total de 14 preguntas donde todas las respuestas tienen la misma probabilidad de ser elegidas.



Encuesta sobre seguridad informática.

Nombre Agustin Sanchez

- ¿Usted tiene una cuenta en alguna red social, como Facebook, Instagram, Twitter, Snapchat, etc?
  Si X No___
- De ser así y contar con una cuenta por favor marque con una X la o las diferentes cuentas que tiene.
  Facebook X Instagram X Twitter___ Snapchat___ WhatsApp X
  Otra red social (Especifique) _____
- ¿Alguna vez ha sido víctima de algún virus informático, ya sea en su computadora o teléfono celular?
  Si, computadora X Si, teléfono celular___ Si, ambos___ No___
- En dado caso de haber sido víctima de algún virus informático, por favor, describa brevemente, si fue en su computadora o celular y escriba el nombre del virus informático, si desconoce el nombre, detalle la situación que se presento a causa del virus.
  Si se borro la informacion
- ¿Actualmente cuenta con algún antivirus instalado en su computadora o celular?
  Si, computadora X Si, dispositivo Móvil___ Si, en ambos___ Ninguno___
- ¿Con que frecuencia realiza actualizaciones en su computadora o teléfono celular?
  Cada vez que el sistema operativo lo solicita___ Nunca X Desconozco el tema___
- ¿Tiene conocimiento de cuantas leyes jurídicas existen en México, relacionadas con la seguridad informática y cuáles son?
  Si___ No X

Figura 2. Evidencia de instrumento.

Fuente. Elaboración propia (2023)

Para la definición del universo se buscó enfocarse en las personas que utilizan medios informáticos para sus diferentes propósitos. La muestra que se sacó son personas que normalmente utilizan los medios informáticos para asuntos laborales, concretamente en negocios pequeños y medianos como lo son los ultramarinos y mini super's de Ciudad Juárez, Chihuahua, México. La indagación de este trabajo se logró a través individuos que utilizan un punto de venta de la compañía NAUTILUS, ya que día con día generan, modifican y envían información mediante el sistema que tienen instalado en sus puntos de venta. Para evaluar el tamaño preciso se utilizó un nivel de confianza del 95% y un margen de error del 5%, un tamaño de la población de 129, debido a que son los puntos de venta instalados en Ciudad Juárez actualmente pertenecientes a NAUTILUS y una proporción de éxito del 0.5 y una proporción de fracaso del 0.5, como se muestra a continuación en la siguiente formula de Ecuación Estadística para Proporciones Poblacionales:

no = Tamaño de la muestra

z = Nivel de confianza deseado

p = Proporción de la población con la característica deseada (éxito)

q = Proporción de la población sin la característica deseada (fracaso)

e = Nivel de error dispuesto a cometer

N= Tamaño de la población.

Una vez identificados todos los datos necesarios se procedió a realizar la operación: no $= Z^2 * p * q / e^2$, donde no, es igual a: $(1.96)^2 *(.5)*(.5) / (.05)^2 = 384$.

n'= no / 1 + (no -1) / N, donde N, es igual a: 384 / 1 + (384-1) / 129 = 384 / 3.9689

n'= 96.75

El tamaño de la muestra que se utilizó para este proyecto de investigación fue de 97 encuestas que se aplicaron a las personas, que interactúan con el punto de venta NAUTILUS y que se encuentran distribuidas por Ciudad Juárez.

CONCLUSIÓN

A partir de los hallazgos detectados, coincidimos con la descripción de la problemática que relata de 26 manera detallada, la ausencia de información en la gran parte de las personas que día con día interactúan con los sistemas informáticos, así como también, el desinterés por parte de comercios pequeños y medianos en cuestiones de seguridad informática.

Por otra parte, los resultados guardan relación con la información publicada por la compañía de seguridad informática ESET, quienes señalan cuales fueron las 10 amenazas más detectadas en México durante el año (2018), pero en lo que no coincide la investigación es en la posición, que obtuvieron estos virus informáticos con respecto a la frecuencia con la que se presentaron.

Las encuestas que se realizaron a los 97 usuarios informáticos, arrojaron los siguientes datos: Los virus LNK/Agent.DV y LNK/Agent.DA encabezaron los primeros 2 lugares, siendo los más frecuentes en nuestras encuestas, para la compañía de seguridad informática ESET estos dos virus informáticos ocuparon los puestos número 8 y numero 10 según las detecciones que obtuvieron en sus antivirus, otros virus informático que tampoco coincidió, fue el virus JS/Adware.Agent.AA que ocupo el segundo lugar en las detecciones del virus ESET, para los resultados obtenidos por la investigación, este virus ocupó el puesto número 3. Otro de los resultados obtenidos por nuestra investigación es, el virus TML/ScrInject.B el cual

ocupó el quinto lugar de los virus con mayor presencia en las encuestas realizadas a los usuarios informáticos, siendo el virus informático con séptimo lugar en las detecciones del antivirus ESET. Así como también el tercero y quinto lugar de las detecciones más frecuentes por el antivirus ESET las obtuvieron los virus informáticos JS/Coinminer.F y JS/Coinminer.D, que, en las encuestas realizadas a los 97 usuarios informáticos, ocuparon el puesto número 6 y 7.

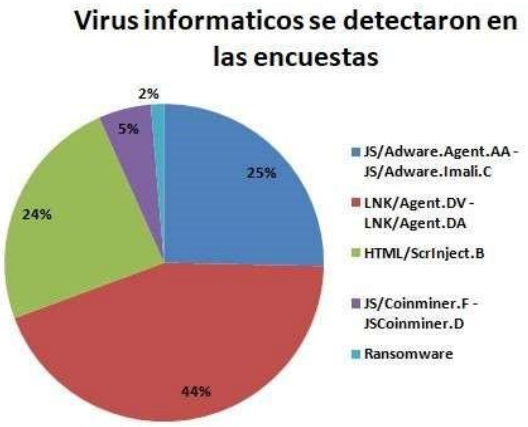


Figura 3. Porcentaje de virus detectados.

Fuente: Elaboración propia (2023).

Y por último en la encuesta realizada a los 97 usuarios aparece una variante del virus informático Ransomware, ocupando el puesto número 8, mientras que en la información publicada por la compañía 20 de seguridad informática ESET no aparece en el top diez, simplemente hace mención, que México fue el tercer país con más afectación en Latinoamérica por este virus informático, pero no ocupo algún puesto dentro de las 10 más detectadas.

Por otra parte, Israel Reyes, catedrático de Harvard, experto en seguridad informática, explica que en México no existe legislación que se encuentre actualizada, en este rápido crecimiento de tecnología.

Durante la investigación que se realizó, se explica el contenido del Código Penal Federal, capítulo II "Acceso ilícito a sistemas y equipos de informática", y básicamente lo que se castiga es lo siguiente:

"Al que sin autorización o esté autorizado, modifique, destruya o provoque perdida de información contenida en sistemas o equipos informáticos, particulares, estatales o financieros protegidos por algún mecanismo de seguridad, será acreedor a una pena determinada.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática, particulares, estatales o financieros, resguardados por algún mecanismo de seguridad será acreedor a una pena determinada."

Pero cuales son realmente los problemas que tiene la legislación mexicana? en lo que tenemos hoy actualmente vigente como delincuencia informática, primero el titulo donde están contemplados estos ilícitos, el tema es acceso ilícito y algunos ilícitos se cometen sin necesidad de tener propiamente un acceso, hay ilícitos que se cometen desde afuera, el ataque de negación de servicios es el ejemplo más claro, simplemente se necesita un gran número de personas mandando peticiones de servicios a una página web para tratar de mermar o ralentizar el servidor hasta que falle el equipo.

Luego tenemos algo muy particular, nuestro Código Penal Federal castiga a aquellos movimientos ilícitas que tienen que ver específicamente, con accesos no autorizados o alteración o pérdida de información no autorizada, siempre y cuando, los equipos estén protegidos por mecanismo de seguridad. Lo cual concuerda con la explicación anteriormente dada por el catedrático de Harvard en seguridad informática, Israel Reyes, las leyes sobre seguridad informática no están a la altura de la tecnología que existe actualmente.

La seguridad informática no solo es un tema de efectuar leyes jurídicas perfectas, sino también, concientizar a los consumidores informáticos, y crear el hábito de formar el uso correcto de los dispositivos informáticos, ya que la gran mayoría de los casos de infecciones por virus se dan a través de los usuarios.

Los antivirus no deberían figurar un gasto económico sino una inversión, proteger la información personal y mantener los dispositivos informáticos renovados, ayudara a reducir los índices de contagio y como consecuencia se impedirán gastos innecesarios en compensaciones técnicas por daños a punto de conexión infectados.

Las pláticas o cursos sobre la ciberseguridad, convendría que fuesen un tema de suma relevancia en las diferentes áreas de trabajo que existen, así como también en los institutos y dependencias gubernamentales.

Necesitamos leyes jurídicas que se ajusten a los problemas actuales que se están presentando en cuestiones de ciberseguridad.

RECOMENDACIONES

Se pide utilizar software original, además de realizar actualizaciones constantes para contar con parches de seguridad renovados y eficaces a la hora de prevenir ataques informáticos.

Igualmente se recomienda tener instalado algún antivirus en la computadora o teléfono celular y realizar periódicamente escaneos de rutina.

Otra recomendación es evitar abrir correos electrónicos de remitentes no conocidos y mucho menos proporcionar información acerca de nuestras cuentas, contraseñas y datos personales, a páginas web o aplicaciones que sean de dudosa procedencia.

La creación de contraseñas alfanuméricas que no sean fácil de predecir y cambiarlas cada cierto tiempo para prevenir algún hackeo exitoso.

Es importante también, no conectarse a redes Wi-Fi públicas (Red no seguras) y aún más, no realizar consultas o transacciones bancarias, o algún otro tipo de actividades que requieran información privada como usuarios y contraseñas.

La siguiente recomendación es realizar la correcta configuración de redes sociales con respecto a la seguridad, es decir, tener configuraciones de tal manera que solo las personas que se desea que vean nuestra información sean las únicas con acceso a nuestras cuentas.

Por último, se recomienda invertir en tecnología y cultura, porque la protección tecnológica puede ayudar, pero no garantiza que sea 100% seguro por sí solo.

REFERENCIAS BIBLIOGRÁFICAS

Alonzo, S. (18 de enero de 2018). *Excelsior*. Obtenido de México, cuarto lugar a nivel mundial en uso de redes sociales: https://www.excelsior.com.mx/hacker/2018/01/18/1214650#view-1

Baeta, M. (11 de agosto de 2017). *Softonic*. Obtenido de Conocer Crepper, el primer virus de la historia: https://www.softonic.com/articulos/creeper-historia-primer-virus

Becerra, B. (10 de febrero de 2019). *El Sol de México*. Obtenido de México no está preparado para detener un ciberataque: Catedrático de Harvard: https://www.elsoldemexico.com.mx/finanzas/mexico-no-esta-preparado-para-detenerunciberataque-catedratico-de-harvard-3036526.html

Bortnik, S. (4 de noviembre de 2013). *We live security by eset*. Obtenido de 5 Curiosidades sobre el gusano de Morris en su 25 aniversario: https://www.welivesecurity.com/laes/2013/11/04/5curiosidades-gusano-morris-25-aniversario/

Foltýn, T. (19 de diciembre de 2018). *We live security by eset.* Obtenido de Las 25 contraseñas más populares del 2018: https://www.welivesecurity.com/la-es/2018/12/19/las-25contrasenas-maspopulares-del-2018/

Hernández, J. (9 de junio de 2019). *Solo es ciencia.* Obtenido de La ciberseguridad en México, ¿Cómo estamos?: https://soloesciencia.com/2019/06/09/la-seguridad-informatica-enmexico-comoestamos/

Herrera, M. V. (12 de agosto de 2019). *Forbes México*. Obtenido de La Ciberseguridad: el reto de México: https://www.forbes.com.mx/la-ciberseguridad-el-reto-de-mexico/

INAI. (diciembre de 2017). Introducción a la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. México, Coyoacán, México.

León, A. D. (18 de mayo de 2018). El gobernador de Banxico explica el ciberataque a bancos de México. (L. d. Mola, Entrevistador)

Line, F. (2019). *Line branding*. Obtenido de Las 5 redes sociales más usadas en México este 2019: https://www.linebranding.com/redes-sociales-mas-usadas-en-mexico/

Mendoza, M. Á. (11 de enero de 2019). *We live security*. Obtenido de Las amenazas informáticas que más se detectaron en México: https://www.welivesecurity.com/laes/2019/01/11/amenazasinformaticas-mas-detectadas-mexico/

Milenio Digital. (18 de diciembre de 2018). *Milenio.* Obtenido de Las peores contraseñas de 2018: https://www.milenio.com/tecnologia/las-peores-contrasenas-de-2018

Olivarez, F. J. (febrero de 2010). Manual de Informática I. Morelia, Michoacán, México.

Olmedo, C. (7 de octubre de 2019). *wradio*. Obtenido de http://wradio.com.mx/radio/2019/10/07/tecnologia/1570462029_125485.html

Riquelme, R. (22 de enero de 2018). *El Economista*. Obtenido de ¿Que es un Equipo de ¿Respuesta ante Emergencias Informáticas?: https://www.eleconomista.com.mx/tecnologia/Que-es-un-Equipo-de-Respuesta-ante-Emergencias-Informaticas-CERT-20180122-0009.html

Riquelme, R. (2 de abril de 2019). *El Economista*. Obtenido de Morena propone la creación de una agencia nacional de ciberseguridad: https://www.eleconomista.com.mx/tecnologia/Morena-propone-la-creacion-de-unaagencianacional-de-ciberseguridad-20190402-0044.html

Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Àlava Cruzatty, J. E., Parrales Anzúles, G. R., Àlava Mero, J. C., y otros. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Cantón Jipijapa: 3 Ciencias.

Stallings, W. (2004). *El gusano Morris.* Madrid: Pearson Education.

Treviño, J. A. (2015). *Delitos informáticos en México y el mundo*. Obtenido de AbogadoDigital.TV: https://www.abogadodigital.tv/?s=delitos+informaticos

Tabla Trabajo Colaborativo

Rol	Autor (es)
Conceptualización	Jorge Nafarrate Bustillos y Martha Magdalena Hurtado Solís
Metodología	Jorge Nafarrate Bustillos y Martha Magdalena Hurtado Solís
Software	Jorge Nafarrate Bustillos
Validación	Isis Ruiz y Viridiana Reyes Uribe
Análisis Formal	Martha Magdalena Hurtado Solís
Investigación	Jorge Nafarrate Bustillos
Recursos	No aplica
Curación de datos	Isis Ruiz y Viridiana Reyes Uribe
Escritura - Preparación del borrador original	Jorge Nafarrate Bustillos, Martha Magdalena Hurtado Solis e Isis Ruiz
Escritura - Revisión y edición	Jorge Nafarrate Bustillos, Isis Ruiz, Viridiana Reyes Uribe y Miguel Gerardo Mireles Centeno