LOS CIBERDELITOS EN LA CUARTA TRANSFORMACIÓN EN MÉXICO

Sánchez García Alan Alejandro>
alansanchez972@hotmail.com
Sánchez Ramírez Brian Alexis
brian.0207@hotmail.com
Vicario Solórzano Claudia Marina
marina.vicario@gmail.com

Instituto Politécnico Nacional
Unidad Profesional Interdisciplinaria de Ingeniería
y Ciencias Sociales y Administrativas.

Resumen

Al pasar de los años se han buscado nuevas maneras para tener más segura nuestra información personal, por lo cual se crearon tecnologías con índole de combatir los ciberdelitos, puesto a que podemos ser víctima al navegar en internet sin nuestro consentimiento.

Los métodos de defensa creados cuentan con la función de mantener una barrera de protección de posibles ataques al usuario, de dicha innovación las más conocidas son la criptografía la cual se basa en la salvaguarda de nuestros datos en base al uso de códigos cifrados y la biometría la cual consiste en el uso de nuestras huellas dátiles, reconocimiento facial, reconocimiento de la voz como método de seguridad, lo cual nos aseguraría más seguridad y bien difícilmente alguien nos podría robar para el uso dañino. (Sánchez Calle, A, 2005). Puesto a que en la actualidad hay muchas personas con gran conocimiento de recursos digitales lo cual usan para la creación de programas para el robo de datos de usuario muchas veces con solo dar clic en un link, y bien no está de más el uso de antivirus o cortafuegos para asegurar aún más nuestra información y así prevenir el posible daño a nuestros dispositivos.

Palabras Clave: biometría, ciberdelitos, criptografía, informática, recursos digitales y reconocimiento.

Abstract

Over the years, new ways have been sought to make our personal information more secure, which is why technologies were created to combat cybercrime, since we can be a victim when browsing the Internet without our consent.

The defense methods created have the function of maintaining a protection barrier from possible attacks on the user, of this innovation the best known are cryptography which is based on the safeguarding of our data based on the use of encrypted codes and biometrics which consist of on the use of our fingerprints, facial recognition, voice recognition as a security method, which would ensure more security and it would be difficult for someone to steal from us for harmful use. (Sanchez Calle, A, 2005). Since there are currently many people with great knowledge of digital resources which they use to create programs to steal user data many times just by clicking on a link, and it does not hurt to use antivirus or firewalls to further ensure our information and thus prevent possible damage to our devices.

Keywords: : biometrics, biometrics, cybercrime, cryptography, computing, digital resources and recognition.

I. Introducción

pComo bien lo sabemos, existen distintas mejoras en la tecnología muchas de ellas nos ayudan para facilitarnos la vida, aunque algunas veces se encuentran diversos errores que personas con gran conocimiento en el tema aprovechan hackeando las propias aplicaciones para uso propio, crear diversas copias piratas o bien hasta la realización de un robo de identidades aprovechándose de estos fallos. (Latto Nico, 2020). Pero para prevenir todo esto se han creado a la vez, distintas formas de ciberseguridad para asegurar nuestra información y datos, pero aun con ello es indispensable que todos sepamos del tema, aunque sea un poco para no caer en un ciberdelito o bien no entrar en pánico y saber qué hacer (Gayoso Martínez Víctor, 2020).Ahora bien, en el caso de conocer a alguien que consideres vulnerable podrías aconsejarlo para que no sea una víctima más y así se logre disminuir la cantidad de agredidos, puesto a que en México vemos en aumento la cantidad de víctimas y en su mayoría no hacen nada al no saber qué hacer, o bien les da pena pedir ayuda tal vez por el que dirán o por orgullo, pero al final, los afectados serán estos y seguirá así si no se pone un alto.

II. Ciberdelito

Se le denomina ciberdelito a aquellas acciones ilegales que son hechas por un usuario o en su caso un grupo para la creación de programas o virus con el fin de perjudicar o bien robar información privada de distintas personas o bien el acoso vía internet. (Barrio Andrés Moisés, 2017).

Hablando más sobre los tipos de ciberdelitos, los más populares son el robo de dato bancarios que en su mayoría se realizan cargos de forma silenciosa al robar cantidades mínimas que al usuario le puede dar igual por lo cual pueden continuar haciéndolo y su sanción va de 6 meses a 3 años con multa que dependerá de la gravedad.

La ciberextorsión que consiste en amenazas para difundir cierta información obtenida a través de páginas web o mandarla a tus familiares la cual puede llegar a sanciones que rondan los 2 a 8 años en prisión que puede aumentar dependiendo del daño provocado en la victima y la multa de 40 a 170 días.

La venta y suplantación de datos personales la cual es considerada unos de los ciberdelitos más vistos en México para realizar compras o suscripciones aplicaciones que no solicitaste tú que en su mayoría no las puedes utilizar y suelen venir acompañadas de spam o cargos que van aumentando en caso de no realizarlos en las fechas dichas por lo cual se consideraría un fraude , o bien para la publicación de dicha información en páginas en internet o mandarlo a empresas para así mandarte publicidad que te ha estado interesando por las búsquedas que haces y algo que muchas personas desconocían desde hace tiempo es que la mayoría de redes sociales hacen dicho acto por lo cual ha provocado que sea una noticia muy sonada últimamente, sin embargo, este hecho no fue cuestión de nuevas actualizaciones puesto a que ya se viene realizando desde años atrás y no podemos realizar algo en contra en realidad al aceptar los términos de usuario al descargar la aplicación, en caso contrario y de que se cuente con pruebas de que no aceptaste ningún documento las sanciones van de 6 meses a 6 años, los cuales pueden aumentar dependiendo del tamaño del problema. (Barrio Andrés Moisés, 2018).

El sexting/cyberbullying que consta en el hostigamiento con la finalidad de hacer un daño mental provocado por insultos o pedir fotos intimas las cuales podrían ser divulgadas haciendo que la pena aumente, en su mayoría a infantes o adolescentes estos al ser los más vulnerables por problemas familiares o rebeldía, y al ser menores de edad las sanciones aumentan más las cuales rondan entre 1 a 5 años en prisión y bien en caso de que el agresor cuente con algún vínculo se aumentara la pena, al ser un delito grave se busca que las sanciones sean aún más grandes. (Área Digital Abogados, 2017).

En el año 2015 se hizo una encuesta sobre las personas que han reportado un caso de ciberdelito y de dichas personas un 70 % reportaron ser víctimas de que su imagen fuera suplantada o bien robada, otro 15 % está involucrado con fraudes que podemos encontrar al navegar en internet y el 15 % restante serían los hackeos. Con estas cantidades, México se consideró el 3er país con más ciberdelitos por no estar bien informados o navegar sin ninguna medida de prevención.

Como se ha mencionado antes, los ciberdelitos no son provocados siempre por desconocidos como muchos podrían llegar a pesar porque en su mayoría son provocados por personas que conviven constantemente con nosotros y nos han estudiado para saber qué medidas tomar para dañarnos (Romeo Casabona Carlos María,2007).

En caso de a ver sido víctima de algún tipo de ciberdelito antes mencionado o tú información privada fue divulgada sin tu consentimiento lo mejor sería mandar un reporte al CNS (Comisión Nacional de Seguridad) para llevar el seguimiento de tu caso y poder encontrar al agresor.

Figura 1. Principales tipos de fraudes en línea que se encuentran al navegar en internet. Fuente: (Guardia Nacional, 2

III. Virus informático

Si bien, la mayoría de dichos ciberdelitos son provocados por una persona o un conjunto se tiene que hablar de los programas que son utilizados para dicho acto y hablamos de los virus informáticos, muchos de estos se adquieren al descargar cosas de internet que no sean reconocidas como fiables y aun así muchos usuarios ignoran la advertencia o bien hasta dando un clic a aquel link que muchas veces nos llama la atención por tener un aspecto agradable, pero al no contar con un antivirus y medidas de seguridad, no nos enteramos hasta que nuestro dispositivo se ve afectado con fallas que pueden ser visibles como la disminución de velocidad a la cual trabaja el dispositivo, escuchar ruidos al llevar mucho tiempo siendo utilizado o bien el sobrecalentamiento, sin embargo, en otros casos no presenta daños visuales hasta que de pronto deja de servir a causa del virus. (López Matachana, Y, 2009).

Ahora bien, un virus informático es creado por un usuario utilizando un programa el cual permite la infección a partir de la adquisición y el lugar donde más los vemos situados serian en archivos de poco uso ocultos puesto a que los tenemos abandonados no le tomaremos interés, para así poder moverse o modificar a libertad sin que nosotros podamos visualizar cambios hasta después un cierto tiempo, ahora bien, dependiendo del tipo de virus sería los inconvenientes que tengamos.

Las acciones realizan son la eliminación de información que tengamos guardada o en algunos casos hasta nos dejarían sin la posibilidad de realizar algunas acciones como ejecutar nuestro antivirus para la eliminación de dicho virus para que este continúe haciendo su trabajo o bien hasta nos empezarían a dañar nuestros componentes para que nuestra máquina se vea dañada al estar utilizando más recursos de los que aguanta realmente nuestro dispositivo. (Roa Buendía, J. F, 2013).

Para prevenir un contagio de virus informáticos, lo mejor es acudir con algún conocido que sepa del tema y te recomiende algún antivirus, puesto a que se tiene una mal costumbre de investigar en internet y descargamos el primero que encontremos gratis, pero como nos podemos estar imaginando tal vez

este programa este infectado para que personas inocentes se vean afectadas utilizando supuestamente algo que nos ayudara pero realmente nos está perjudicando, y otra recomendación en caso de compartir el dispositivo seria bloquear el acceso a ciertas páginas para que así no puedan infectar tu información o bien comentarle que si sale una alerta de que la pagina o descarga no es de fiar, lo mejor sería buscar en otro sitio. (J. Sanok Daniel, 2005).

IV. Biometría

Con los distintos ciberdelitos que vemos en nuestro día a día, se han creado distintas formas para combatir dichos crímenes por lo cual se creó el reconocimiento biométrico el cual se basa en la identificación del usuario utilizando como base aquellos aspectos que nos identifican como lo sería el timbre de nuestra voz, huellas dactilares, reconocimiento visual o hasta el uso de un cabello. (L. Lai, S. Ho and H. V. Poor, 2011).

Se cuentan con diversas ventajas al utilizar la biometría como medida de seguridad como lo sería el costo bajo en el ámbito de la voz y huellas dactilares puesto a que en la mayoría de los celulares inteligentes actuales se cuenta con dicho servicio, posteriormente se vería el uso de la iris y reconocimiento facial los cuales al necesitar más recursos al ser más exactos y que necesita reconocer aún más facciones propias aumenta el costo ya que a pesar de que muchos dispositivos también lo cuentan en su mayoría son de gama alta lo cual dificulta la compra de dicho dispositivo por su costo elevado. (Ruiz Marín Milton, Rodríguez Uribe Juan, 2009). Por lo cual no todos los usuarios cuentan dicha cantidad para comprar uno; ahora en el aspecto de efectividad siempre se tendrán dificultades, pero en su mayoría hay 94 % al utilizar estos tipos de biometría por lo cual se están buscando distintas formas de mejorarlos a cada uno para que suba a 99.9 % y así aseguremos más nuestra información en caso de ser víctima de un robo. (Carrillo Benito Azahara, 2020).

V. Criptografía

Esta forma de proteger la información se ha ido mejorando ya que al estar navegando en una red la cual es inmensa se hace un gran tráfico de información lo cual provocaría ciertos inconvenientes a los usuarios porque no podrían hacer llegar el mensaje correctamente o habrá un choque en los canales de transmisión haciendo que lleguen a otros. (Ortega Triguero Jesús J, López Guerrero Miguel Ángel, 2006). Sin embargo, nuestra información llegaría cifrada lo cual es una ventaja ya que les costaría trabajo saber el contenido, esto sería en el ámbito de la comunicación, hablando en el ámbito empresarial vemos que ocupan este método para en caso de un robo, los agresores se les dificulte descifrar las claves de seguridad ya que las posibles contraseñas serian incalculables para un ser humano, y en el transcurso en lo que intentan hacer el delito podrían ser localizados con gran velocidad.

La criptografía a pesar de ser un tema muy relevante en la actualidad su historia va desde la época antigua y media donde se buscaba la creación de códigos para hacer el cifrado de los mensajes que se querían mandar desde un emisor hasta un receptor, en caso de que fuera encontrado por otras personas en el canal de envió estos se les dificultaría al no saber que significaban los distintos símbolos utilizados por lo cual su seguridad era más alta y el más claro ejemplo lo podemos ver en distintas guerras que se han dado en estos años, al enviar ciertos datos los encriptaban por si el bando enemigo interceptaba no supieran el significado de lo que se quería comunicar o bien entendieran otra idea para confundirlos. (Galende Díaz Juan C, 1995).

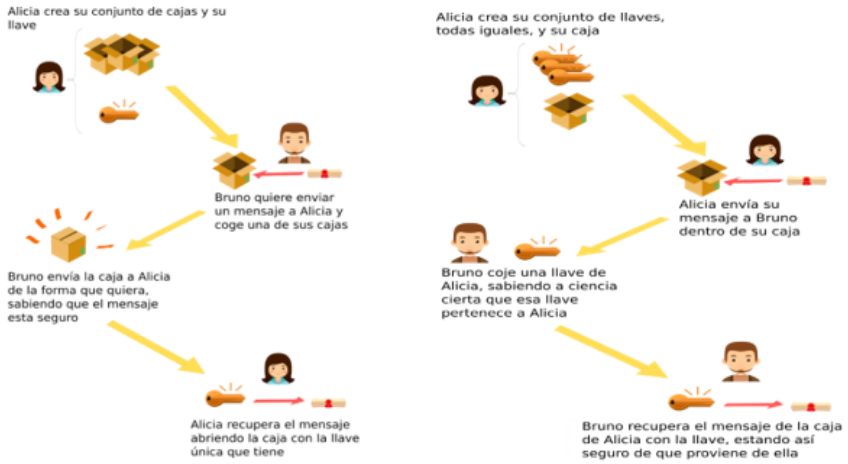

Figura 2. Criptografía básica para entender la tecnología blockchain. Fuente: (García de Mata Iñigo, 2018).

VI. Conclusión

Conociendo más sobre la importancia de un buen uso del internet, nos damos cuenta de varios errores que hemos cometido en el pasado como lo sería la búsqueda para realizar una tarea utilizando links que no sean de fiar con información errónea y muchas de las veces publicidad engañosa, lo cual podría provocar la adquisición de un virus. Sin embargo, desde la escuela nos van inculcando el hábito de buscar bien y saber elegir nuestras fuentes para así saber qué información puede ser verídica o bien saber las consecuencias de todo lo que hagamos, también de la importancia de conocer desde cosas sencillas hasta un poco más complicadas como las funciones del sistema operativo, donde se almacena toda nuestra información, y no menos importante conocer el proceso que se lleva un aparato inteligente para hacer una acción que estemos realizando para saber porque puede ser provocado algunas problemáticas en el transcurso, sin embargo, no todos hemos sido afortunados con dicha información. (Marco Galindo, M. J, 2012). Por lo cual vemos en la calle o en nuestra propia familia personas vulnerables a múltiples ataques informáticos por no estar enterados de los riesgos sobre todo gente de una edad mayor donde son víctimas de ciberdelitos que consisten en robarles dinero de sus cuentas bancarias al tenerlas vinculadas en su celular por lo cual pueden robar su información y ellos no se darán cuenta hasta después, o bien muchas veces vemos que nos han robado cantidades diminutas o que algún archivo que teníamos no lo encontramos y no le damos interés ya que es algo irrelevante pero podríamos ser víctimas de un crimen y al no reportarlo el atacante seguirá haciéndolo aún más porque nadie pretende ponerle un alto, también hacer conciencia a aquellos padres que consienten a sus hijos dejándolos hacer lo que gusten o bien no saber que hacen a sus espaldas, se comprueba que los secuestros a niños/adolescentes han ido aumentando por el uso de redes sociales donde se otorgan datos de más haciendo que sean vulnerables pero los padres por darles esa libertad prefieren evitarse problemas diciéndoles que hacen mal o que antes de hacer algo sepan las posibles consecuencias a futuro que podrían pasar. (Escrivá Gascó, G, 2013).

Referencias

Barrio Andrés Moisés (**2017**). *Ciberdelitos.Amenazas criminales del ciberespacio.* Editorial REUS, vol. 1 pp. 23-38. https://books.google.com.mx/books?id=hrxUDwAAQBAJ&pg=PA31&dq=ciberdelitos&hl=es-419&sa=X&ved=2ahUKEwiO4KCxpafuAhVOZc0KHQG3BgQQ6AEwAXoECAIQAg#v=onepage&q=ciberdelitos&f=false

Barrio Andrés Moisés (**2018**). *Delitos 2.0: aspectos penales, procesales y de seguridad de los ciberdelitos. Wolters Kluwer España.* https://elibro.net/es/lc/elibrocom/titulos/56038

Escrivá Gascó, G. (**2013**). *Seguridad informática.Macmillan Iberia, S.A.* https://elibro.net/es/lc/elibrocom/titulos/43260

Galende Díaz Juan C. (**1995**). *Criptografía. Historia de la escritura cifrada.* Editorial complutense, vol.1, pp. 75-85. https://books.google.com.mx/books?id=9jUjYLjJZCAC&pg=PA75&dq=criptografia&hl=es-419&sa=X&ved=2ahUKEwir7tnis9DtAhUIWq0KHS6tCrYQ6AEwAHoECAMQAg#v=onepage&q=criptografia&f=false

Gayoso Martínez Víctor. (**2020**). *Ciberseguridad.* Editorial CSIC, vol 1. https://books.google.com.mx/books?id=5sgKEAAAQBAJ&pg=PT28&dq=ciberseguridad&hl=es-419&sa=X&ved=2ahUKEwjGvLLRo6fuAhVOmK0KHZ6qC4UQ6AEwAHoECAEQAg#v=onepage&q=ciberseguridad&f=false

Autor (**año**). *Título del artículolibro,revista o nombre de la página web*texto restante. https://www.lipsum.com/feed/html

J. Sanok Daniel (**2005**). *An Analysis of how antivirus methodologies are utilized in protecting computer from malicious codeAssociation for computing machinery* (pp 142-144) New York USA. https://dl.acm.org/doi/10.1145/1107622.1107655

L. Lai, S. Ho and H. V. Poor (**2011**). *Privacy–Security Trade-Offs in Biometric Security SystemsIn IEEE Transactions on Information Forensics and Security* (vol. 6, no. 1, pp. 122-139) https://ieeexplore.ieee.org/document/5664787

López Matachana, Y. (**2009**). *Los virus informáticos: una amenaza para la sociedad. Editorial Universitaria.* https://elibro.net/es/lc/elibrocom/titulos/71403

Marco Galindo, M. J. (**2012**). *Escaneando la informática. Editorial UOC.* https://elibro.net/es/lc/elibrocom/titulos/33518

Ortega Triguero Jesús J, López Guerrero Miguel Ángel (**2006**). *Introducción a la criptografía. Historia y actualidad.* Editorial Ediciones De La Universidad de Castilla-La Mancha, vol.1, pp209-227. https://books.google.com.mx/books?id=fEV4Iffwt2oC&pg=PA9&dq=criptografia&hl=es-419&sa=X&ved=2ahUKEwjh-PHWydDtAhVBU80KHXjaCCMQ6AEwAXoECAIQAg#v=onepage&q=criptografia&f=false

Roa Buendía, J. F. (**2013**). *Seguridad informáticaMcGraw-Hill España.* https://elibro.net/es/lc/elibrocom/titulos/50243

Romeo Casabona Carlos María (**2007**). *De los delitos informáticos al cibercrimenUniversitas Vitae.* Editorial Universidad Salamanca, vol.1, pp.656

https://books.google.com.mx/books?id=ikq7AwAAQBAJ&pg=PA656&dq=cibercrimen&hl=es-419&sa=X&ved=2ahUKEwiV_NT6k9DtAhVKKawKHVl1BjMQ6AEwAHoECAIQAg#v=onepage&q=cibercrimen&f=false

Ruiz Marín Milton, Rodríguez Uribe Juan, Olivares Morales Juan C (**2009**). *Una mirada a la biometría Revista Avances en Sistemas e Informática,* vol. 6, núm. 2, pp. 29-38 https://www.redalyc.org/pdf/1331/133113598005.pdf

Sánchez Calle, A. (**2005**). *Aplicaciones de la visión artificial y la biometría informática. Dykinson.* https://elibro.net/es/lc/elibrocom/titulos/60927

Área Digital Abogados (**2017**). *¿Cuáles son los principales delitos informáticos?* Recuperado el 18/12/2020. De Área Digital Abogados ttps://adabogados.net/cuales-son-los-principales-delitos-informaticos/

Carrillo Benito Azahara (**2020**). *¿Qué es biometría? Concepto y tendencias.* Recuperado el 18/12/2020. De Blog de viafirma https://www.viafirma.com/blog-xnoccio/es/que-es-biometria/

Latto Nico (**2020**). *¿Qué es ciberdelito y cómo puedo prevenirlo?* Recuperado el 18/12/2020. De Avast https://www.avast.com/es-es/c-cybercrime

Guardia Nacional. (**2018**). *Conoce los principales tipos de fraudes en línea* Recuperado la imagen el 18/12/2020. De https://www.facebook.com/GUARDIA.NACIONAL.MX/posts/250214639693301/

García de Mata Iñigo. (**2018**). *Criptografía básica para entender la tecnología blockchain* (14/03/2018) Recuperado el 18/12/2020. De https://medium.com/@igmata/criptograf %C3 %ADa-b %C3 %A1sica-para-entender-la-tecnolog %C3 %ADa-blockchain-eb94cdd64158