Fotografía: Peshkov para Adobe Stock

Robo de datos personales a través de ciberdelitos en jalisco

Luis Abraham Rincón Prieto
Coordinador de Archivos del Consejo Municipal del Deporte de Zapopan, Jalisco

Resumen

En este artículo se expone el avance que Jalisco ha obtenido en el tema de las tecnologías de la información y las comunicaciones, así como en tecnología e innovación. Consecuentemente los habitantes de Jalisco haciendo uso de las herramientas tecnológicas y del internet, han creado hábitos de conexión de 24 horas al día.

Los ciudadanos Jaliscienses por falta de capacitación respecto a prevenir los ciberdelitos, y la omisión de una normatividad severa para castigar a los practicantes ciberdelincuentes, hace que sean víctimas de robo de datos personales. Siendo vulnerables en redes sociales, aplicaciones, plataformas digitales, wifi o dispositivos con sensores de monitoreo.

Los Jaliscienses en sus roles de vida interactúan con dispositivos electrónicos que cuentan con sensores que lo monitorean todo y almacenan grandes cantidades de datos personales. Se trate de un reloj (SmartWatch), celular o una bocina inteligente que en muchas ocasiones los conectan con plataformas digitales para realizar diversos servicios como: solicitar transporte; un trámite ante el gobierno; realizar pagos; comprar productos para el hogar; dar mayor productividad en el trabajo o simplemente por entretenimiento, lo que hace que sean más vulnerables en el ciberespacio.

Los ciberdelitos más comunes que se dan en Jalisco son: ciberacoso o ciberbullyng, suplantación de identidad o robo de identidad, cibergrooming o groooming, sexting o packs, ransomware, phishing.

Es necesario que la legislación estatal de Jalisco evolucione y de alcance a regular las tecnologías de comunicación y de la información, y el avance tecnológico e innovador. En especial que regule las redes sociales, aplicaciones, plataformas digitales, wifi o dispositivos con sensores de monitoreo (Internet de las Cosas).

PALABRAS CLAVES:
Ciberdelincuente, Ciberdelitos, Datos Personales, Ciberresilencia, Ciberespacio, Internet de las Cosas

Introducción

En el constante avance de la materia de transparencia y protección de datos personales, nuestros legisladores han emitido reformas a nuestro ordenamiento, me refiero a la Constitución Política de los Estados Unidos Mexicanos en sus artículos 6º y 16, y han emitido Leyes Generales reglamentarias de dichos preceptos constitucionales, para garantizar los derechos humanos de Transparencia y Acceso a la Información Pública, y a la Protección de Datos Personales. Sin embargo, la tecnología e invocación al paso del tiempo ha influido considerablemente en la vida de los mexicanos, facilitando la conexión a internet a través de dispositivos electrónicos inteligentes, que están equipados con aplicaciones y sensores. Logrando ingresar a un ciberespacio que es nutrido cada día con grandes cantidades de información, incluyendo datos personales que se comparten en redes sociales; al momento de descargar aplicaciones; al realizar compras con dispositivos inteligentes con sensores y que se conectan a las redes wifi.

Ciberespacio donde los ciudadanos mexicanos como internautas intercambian y comparten información con libertad y rapidez, y mayor aun con un plus el anonimato. Anonimato que motiva a que se realice un mal uso de la fuente ilimitada de información contenida en el ciberespacio y llamando la atención a los practicantes de ciberdelitos para obtener datos personales y con ello tener beneficios. Derivado de lo anterior, se analizarán estudios del uso del internet en México, así como de Jalisco para determinar que avance han tenido en la tecnología de la información y las comunicaciones, así como se investigará cuáles son las principales redes sociales utilizadas, y que tipos de datos personales recopilan. Incluso se investigará el internet de las cosas y su forma de captar datos personales a través de sensores de monitoreo y qué tipo de ciberdelitos son las más comunes en Jalisco.

La falta de regulación jurídica respecto a las redes sociales, el internet de las cosas e incluso de las wifi públicas y los sitios web falsos como medios por los cuales con consentimiento y sin verificar la seguridad se conectan los usuarios, para compartir información e incluso datos personales, hacen vulnerables a los ciudadanos Jaliscienses.

Surge la necesidad de conocer las definiciones de ciberdelitos cometidos en Jalisco, y su tipificación en el Código Penal para el Estado Libre y Soberano de Jalisco; y conocer algunas recomendaciones de cómo prevenirlos. De aplicar cuestionarios a menores para adquirir qué tanto conocimiento se tiene del tema de ciberseguridad y ciberdelitos, para acreditar la necesidad de crear conciencia de capacitarse en dichos temas, y a su vez se analizará un estudio de hábitos de los usuarios en ciberseguridad.

Finalmente, se emitirán conclusiones para mejorar la problemática encontrada como propuestas, y se genere concientización respecto al uso de internet y sus consecuencias de compartir datos personales en redes sociales; al momento de descargar aplicaciones; al realizar compras con dispositivos inteligentes con sensores y que se conectan a las redes wifi. Proponiendo se emita una Ley de Ciberseguridad y Ciberdelitos en el Estado de Jalisco, y el contenido que podría integrarla.

Desarrollo

México ha tenido un considerable avance respecto a hábitos de uso de internet tal y como se advierte a continuación: 1.- Aumento del 82.7% al 2018 respecto a los usuarios de internet; 2.- El perfil del internauta mexicano es 51% femenino y 49% masculino; 3.- Respecto a la edad el mayor porcentaje es de 25 a 34 años; 4.- El 67% de los internautas en México, perciben que se encuentran conectados en internet las 24 horas; 5.- El 84% de los usuarios se conectan en su hogar; 6.- Las redes sociales son la mayor actividad en línea teniendo un 82%, siendo la principal el facebook; 7.- El 41% de los usuarios de internet solicitan transporte, esto por mayor comodidad y seguridad; y El smartphone es el principal dispositivo para acceder a alguna red social.[1]

Ahora bien en Jalisco, una de las obligaciones del Estado, es garantizar y promover el acceso a la sociedad de la información y economía del conocimiento, mediante el uso y aprovechamiento de las tecnologías de comunicación y de la información. Así como se reconozca, entre otros derechos el de acceso a la tecnología e innovación, con el objetivo de elevar el nivel de vida de los habitantes jaliscienses (Constitución Política del Estado de Jalisco, 2019, art. 4).

Debido al importante avance tecnológico de comunicaciones y de información que ha tenido el Estado de Jalisco, el 70,4 % de los habitantes de Jalisco disponen de conexión a internet en sus hogares. De acuerdo a la Encuesta Nacional realizada por el INEGI respecto a hogares que disponen de conexión a internet por ciudad seleccionada.[2]

La edad de los usuarios de internet en Jalisco media de entre los 6 años a 55 años o más, destacando los usuarios de 25 a 34 años de edad con mayor conexión. Según se advierte de la Encuesta Nacional realizada por el INEGI respecto a usuarios de internet por entidad federativa, según grupos de edad, 2018.[3]

Jalisco ha buscado impulsar la competitividad, y productividad de las PYMES, a través de iniciativas como La Estrategia Estatal de Internet of Things[4], cuyo objetivo es:

> *Desarrollar, fomentar y acelerar en Jalisco, la integración de una plataforma tecnológica de IoT, especializada en innovación de aplicaciones productivas con la colaboración de las empresas globales de IoT, empresas locales tecnológicas, universidades y centros de investigación y desarrollo. La estrategia está impulsada por la Secretaria de Innovación, Ciencia y Tecnología del Estado, a través del Centro de Innovación y Aceleramiento para el Desarrollo Económico (CIADE), el cual ha definido como sectores estratégicos al sector Agroalimentario, Salud y Farma, TIC's e Industrias creativas y Biotecnología en donde a través de Internet of Things se buscará potencializar dichos sectores buscando su innovación y la creación de productos que puedan competir a nivel global (Díaz, 2014).*

En el Estado de Jalisco se encuentra la Ciudad Creativa digital, y ha realizado eventos tan importantes como Talent Land 2019, por lo que siempre los jaliscienses están a la vanguardia de la tecnología.

Sin embargo, el hábito cotidiano que tienen tan arraigado los Jaliscienses de la adicción a la conexión de 24 horas a redes sociales como el facebook, así como chatear mediante WhatsApp y Telegram desde su smartphone o teléfono inteligente para compartir en el ciberespacio imágenes, videos, archivo de sonido e incluso videollamadas, los involucra en riesgos

1 Asociación de Internet. MX. 15º Estudio sobre los Hábitos de los Usuarios de Internet en México 2019. Mayo, 13, 2019. Recuperado de: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/15-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2019-version-publica/lang,es-es/?Itemid=

2 INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares. (ENDUTIH),2018. Recuperado de: https://www.inegi.org.mx/temas/ticshogares/default.html#Tabulados.

3 INEGI, Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares. (ENDUTIH),2018. Recuperado de: https://www.inegi.org.mx/temas/ticshogares/default.html#Tabulados.

4 Internet de las Cosas.

como perdida de datos personales[5], por desconocimiento de aspectos importantes como: la privacidad en las comunicaciones, por riesgo de suplantación, y no realizan una simple comparación de dichos aspectos. Se analizaron las redes sociales de WhatsApp y Telegram, para determinar qué red social es más vulnerable para que le roben los datos personales:

> *WhatsApp cuenta con 450 millones de usuarios. También destaca por su facilidad de uso, con un diseño simple y fácil de utilizar. En cuanto a seguridad ha ido mejorando, se puede configurar información privada, como hora de conexión, el estado o foto de perfil. Sin embargo, las comunicaciones, que ya van cifradas siguen siendo un punto débil. Su mayor problema relacionado con la seguridad es la facilidad con la que se puede suplantar la identidad de otra persona, debido al sistema que utiliza la aplicación para identificarnos. Pues para conectarte e iniciar sesión WhatsApp sólo necesita un número de teléfono y la dirección MAC (iPhone) o el IMEI (Android), logrando que alguien se haga pasar por nosotros (Oficina de Seguridad del Internauta, 2019).*

> *Telegram cuenta con el número más bajo de usuarios. Es idéntica a WhatsApp. En cuanto a seguridad cuenta con un cifrado calificado de "indescifrable". Y puede utilizar un chat secreto. El código de Telegram es abierto y libre. (Oficina de Seguridad del Internauta, 2019).*

Se determina de las anteriores citas, que WhatsApp es más vulnerable porque se puede suplir la identidad de sus usuarios, sin olvidar que solicita el número de smartphone, así como los demás contactos de la libreta de direcciones y por el contrario Telegram cuenta con más seguridad tiene sistema robusto de cifrado de comunicaciones, tiene chat secreto y es de código libre y abierto.

Consejos para prevenir robo de datos personales, mediante mensajería instantánea:

- No difundir el número de teléfono móvil de otras personas sin su consentimiento.
- Instalar un antivirus en el dispositivo (PC, tableta, smartphone) donde se utilice la aplicación de mensajería instantánea.
- Asegurar de que la persona con la que se comunica es quien dice ser. No caer en engaños.
- Establecer una contraseña de bloqueo en el dispositivo.
- Revisar siempre los ficheros que se descarguen. Tener cuidado de no difundir contenido ilegal.
- No facilitar información privada.
- Eliminar el historial de las conversaciones con frecuencia. De esta forma se evitara que, si alguien accede al dispositivo de manera no autorizada, pueda leerlas y obtener información del usuario que no desea.
- Tener cuidado con las redes WiFi a las que se conectan para chatear. Si no están debidamente protegidas o son redes públicas, una persona malintencionada conectada a la misma red podría capturar las conversaciones y descifrarlas.
- Actualizar la aplicación siempre que aparezca una nueva versión por si ésta, además de incorporar alguna nueva funcionalidad, corrigiese algún fallo de seguridad.
- No olvidar leer la política de privacidad y las condiciones del servicio antes de usarlo.
- Si la aplicación de mensajería instantánea que usas ofrece alguna opción de chat secreto, acostumbrarse a utilizarla (Oficina de Seguridad del Internauta, 2019).

Se analizó la aplicación más comúnmente utilizada en el ámbito del internet en Jalisco, siendo el facebook, al momento de descargarla y para efectos de realizar el registro y gozar del servicio de dicha red social, solicita entre otros datos personales: correo electrónico,

5 Debe recordarse que los datos personales son toda aquella información concerniente a una persona física identificada o identificable.

número de teléfono smartphone y una vez registrado puedes agregar más datos personales como: empleo, formación académica, lugares donde viviste, información de contacto, si eres hombre o mujer, fecha de nacimiento, apodo, situ ación sentimental, gustos, a quien decides seguir dentro del servicio de dicha red social, eventos agendados, además puedes agregar, fotos y videos, estado de ánimo. Pero este es el inicio de compartir datos personales porque muchas de las veces los usuarios publican, eventos a los que asisten sean estos familiares o sociales, fotos intimas, lugares que visitan con frecuencia, su ubicación en tiempo real[6], sus riquezas, videos, tipo de religión, los nombres de sus familiares, en pocas palabras hasta el tipo de sangre.

> *Facebook es la red social que más controversia genera en sus condiciones de uso. Principalmente deja claro en sus términos de uso que todo lo que se suba a su red social (fotos, videos, estados, información) pasa a ser de su propiedad. De hecho, si se sube una foto, y se quiere borrar, la puedes deshabilitar, para que no sea accesible desde el muro, pero queda en sus servidores. (Internauta, Instituto Nacional de Ciberseguridad de España M.P., S.A. , 2015).*

De la anterior cita, se advierte que la información incluyendo datos personales, no se eliminan inmediatamente de los servidores de Facebook. Las condiciones de servicio de Facebook, en la sección denominada “Permisos que se Conceden”, claramente explican que aun eliminando el contenido de la cuenta puede seguir existiendo en parte de sus sistemas hasta por 90 días[7].

También muchas de las veces entre aplicaciones se comparten información, como el caso de whatsapp que trabaja con la empresa de facebook. En ocasiones los datos personales son utilizados para venderlos con fines de mercadotecnia y otras veces se venden en el mercado negro para cometer delitos de extorción o fraudes. “Lo que quiere decir que manipulan, venden y comparten información en las aplicaciones más utilizadas”. (Aguilar., 2017). Como se advierte los usuarios son proveedores de datos personales para dichas aplicaciones y lo peor muchas de las veces otorgan su consentimiento, por no leer los términos y condiciones para hacer uso de los servicios, con tan solo dar un click.

Aquí no termina el tema de las aplicaciones pues algunas dan las opciones de configurar la privacidad[8] del usuario, pero al no realizar la configuración por falta de interés o desconocimiento quedamos vulnerables a ciberdelitos.

> *En 2018, la ENDUTIH indica que 45.5 millones de los usuarios de Internet mediante celular inteligente (Smartphone) instalaron aplicaciones en sus teléfonos. De estos, el 89.5% instaló mensajería instantánea, el 81.2% para acceder a redes sociales y el 71.9% instaló aplicaciones para acceder a contenidos de audio y video. Por otra parte, el 18.1% de los usuarios utilizaron su dispositivo para instalar alguna aplicación que les permitiera acceder a la banca móvil (Social, 2019).*

6 39% pública su ubicación en redes sociales.

7 Información Legal de WhatsApp. 2019. Recuperado de: https://www.whatsapp.com/legal/#terms-of-service

8 El Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales. Emitió Recomendaciones para mantener segura tu privacidad y datos personales en el entorno digital. Recuperado en: http://inicio.inai.org.mx/Guias/5RecomendacionesPDP_Web.pdf

Otra manera mediante la cual los Jaliscienses proporcionan datos personales son mediante dispositivos con sensores de monitoreo y aplicaciones, que están conectados a internet. Que gracias a la gran cantidad de información que almacenan de sus usuarios, una vez analizada, son capaces de detección de objetos, transmitir, tomar decisiones y actuar. Este tipo de dispositivos los utilizan el 29% de los usuarios.[9] Es lo que se llama Internet de las Cosas (IoT), una definición es:

> *Tecnología basada en la conexión de objetos cotidianos a internet que intercambian, agregan y procesan información del entorno físico para proporcionar servicios de valor añadido a los usuarios finales. También reconoce eventos o cambios, y tales sistemas pueden reaccionar de forma autónoma y adecuada. Su finalidad es, por tanto, brindar una infraestructura que supere la barrera entre los objetos en el mundo físico y su representación en los sistemas de información (Andrés, 2018).*

Esta nueva forma de conexión cambiará totalmente la forma en que vivimos, la comunicación y revolucionará el mercado, la educación, la salud. Pues la interoperabilidad entre dispositivos inteligentes se impulsará, en consecuencia se captará mayor información, que se utiliza para optimizar procesos y análisis de datos, será de gran beneficio para la sociedad, por lo que se está ante otra etapa de la revolución industrial. “La Cuarta Revolución Industrial es el Internet de las Cosas (IoT, por sus siglas en inglés)”, (Schwab, 2016).

Entre los dispositivos inteligentes de este tipo, los más comúnmente usados son los wearables[10] como las pulseras inteligentes, los smartwatches, los smart rings. Que guardan información personal como monitoreo de actividad física, calorías quemadas, ritmo cardiaco, pulso, temperatura, movimientos, niveles de glucosa, presión arterial, nivel de estrés, detección de deshidratación, preferencias en televisión. Dicha información es almacenada en servidores de la compañía creadora del artículo o captada por aplicaciones como la fitbit para almacenarla en el smartphone.

Así para gozar del servicio que brinda fitbit, solicita datos personales como: su nombre, dirección de correo electrónico, contraseña, fecha de nacimiento, sexo, altura, peso y, en algunos casos, su número de teléfono móvil, rol de alimentación, el peso, los hábitos de sueño. Y si se permite realizar pagos y efectuar transacciones, se debe proporcionar como: número de tarjeta de crédito, débito, fecha de vencimiento de las tarjetas y código CVV[11].

Esto además de que puede conectar con servicios de terceros como facebook de donde obtiene datos como: nombre, dirección email y lista de amigos. Claro está que para poder hacer uso de estos servicios las compañías siempre solicitan el consentimiento de los usuarios, el cual viene en los términos y condiciones que la mayoría de usuarios no lee[12]. No se revisa la política de privacidad. No se configura correctamente para estar protegidos, o se vende el teléfono inteligente sin antes borrar los datos personales, nuevamente son vulnerables a ser víctimas de ciberdelitos.

> *Los fabricantes utilizan tecnología Bluetooth de baja energía para permitir al wearable sincronizarse de forma inalámbrica a un smartphone lo que puede provocar que éste pueda ser monitorizado o rastreado sin necesidad de tener muchos conocimientos técnicos. ¿Riesgos? Por poner un ejemplo, un simple ladrón podría*

9 Asociación de Internet. MX. 15º Estudio sobre los Hábitos de los Usuarios de Internet en México 2019. Mayo, 13, 2019. Recuperado de: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/15-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2019-version-publica/lang,es-es/?Itemid=

10 Wearables es el conjunto de aparatos y dispositivos electrónicos que se incorporan a alguna parte de nuestro cuerpo interactuado de forma continua y con otros dispositivos con la finalidad de realizar alguna función concreta.

11 El Código CVV es un grupo de 3 o 4 números situado en el reverso de la tarjeta de crédito. Recuperado de: https://www.bbva.com/es/que-es-el-ccv-o-cvc-en-las-tarjetas-de-credito/

12 Estudio Hábitos de los usuarios en ciberseguridad en México 2019. Recuperado de: https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf pag. 14. Donde el 42.05 indicó que no revisa el contenido de los permisos requeridos antes de instalar aplicaciones.

saber perfectamente dónde se encuentra una persona para decidir cuál es el mejor momento para entrar a robar a su casa. También hay vulnerabilidades en los sistemas de almacenamiento relacionados con las contraseñas. Se ha visto que en algunos se transmite en claro (sin utilizar ningún tipo de cifrado) y que la gestión de usuarios es deficiente. ¿Riesgos? Si alguien consigue esa contraseña, accederá a nuestra información privada, entre la que se encuentra, ¡datos médicos relacionados con nuestra salud! En algunos casos, se detecta la ausencia de políticas de privacidad que expliquen de forma clara y sencilla para qué se recogen los datos de los usuarios y qué hacen con ellos. En otros, aunque sí que existen, no están del todo accesibles. ¿Riesgo? Tus datos podrían ser "cedidos" a empresas de terceros. ¿Qué pasa si fuese a una aseguradora médica? Quién sabe, igual podría subir el precio de la póliza contratada de una persona, si gracias a una smartband sabe que practica mucho deporte y tiene más riesgos de sufrir un accidente… Al margen del estudio, tampoco debemos olvidarnos de que los servidores que almacenan todos los datos que voluntariamente facilitamos a las empresas a través de sus wearables, pueden ser objetivo de ataques. Si están correctamente configurados y protegidos, no debería suponernos ningún riesgo de seguridad, pero, ¿qué pasa si encuentran un agujero de seguridad en los sistemas y consiguen acceder a nuestros datos? Eso igual ya no nos hace tanta gracia… (Internauta, Instituto Nacional de Ciberseguridad de España M.P., S.A. , 2015)

Los ciberdelincuentes, que ya han obtenido el número de tarjeta por otros medios, intentan hacerse con el código CVV usando distintos métodos, como correos electrónicos falsos o incluso llamadas de teléfono, haciéndose pasar por la entidad emisora de la tarjeta, por ejemplo (OCU Ediciones, 2009).

En México cada día es más común observar estos tipos de pulseras inteligentes más en el ámbito deportivo. México es ubicado en la posición 18 de los 24 países considerados, con 6.8 dispositivos (IoT) por cada 100 habitantes, donde el 43% de los mexicanos están interesados en controlar dispositivos a través de smartphone, como objetos relacionados con la salud como pulseras y sensores. (Gobierno de México, 2019)

Otros dispositivos son las bocinas inteligentes capaces de reconocer las características físicas del lugar en el que está ubicado, como la marca Apple que funciona con "Siri" lo que da comodidad a sus usuarios pues puede leer mensajes, hacer y contestar llamadas. (SUN, 2018)

Al igual que la bocina inteligente que funciona con "Alexa" capaz de reconocer la voz de los usuarios, controlar diversos dispositivos de la casa como focos, ventiladores, cerradura, cámaras, el refrigerador, el televisor inteligente. (Mariana R. Fomperosa, 2018)

Estos dispositivos con sensores de monitoreo almacenan gran cantidad de datos personales[13], ya que del análisis que realizan a los mismos, van conociendo nuestra voz, nuestros gustos, nuestra agenda diaria, nuestras ubicaciones, nuestros destinos. La justificación de las compañías en general es para rendir un mejor servicio personalizado al usuario.

Estos tipos de altavoces pueden ser hackeados a través del router, que es la puerta de entrada a toda tu red doméstica. Si el pirata informático entra en el router, él o ella pueden comprometer potencialmente cada computadora y dispositivo conectado a la red. Y si alguno de esos dispositivos además del altavoz

[13] Big data. Recuperado de: https://www.webopedia.com/TERM/B/big_data.html

inteligente tiene capacidades de audio, el hacker[14] puede hacer que el dispositivo emita comandos para el altavoz inteligente, por ejemplo, para que desbloquee la puerta delantera o abra el garaje. Antes de que te des cuenta, todos tus pequeños dispositivos se comunican entre sí como un ejército de traidores (Avast, 2018).

Hoy en día es muy común que en los cafés, restaurantes, plazas, tiendas comerciales, hoteles, librerías existan wifi de libre acceso (wifi pública), en las que es muy fácil conectarse.

> *La mayor amenaza para la seguridad de las redes Wi-Fi gratuitas es la capacidad que tiene el hacker de interponerse entre ti y el punto de conexión. Por lo tanto, en lugar de hablar directamente con el punto de acceso, envías tu información al hacker, quien luego vuelve a transmitirla (Kaspersky, 2019).*

También es muy común que desde la laptop al estar realizando investigaciones se entre a sitios webs y una vez que se da click, nos aparece una ventanilla que nos indica ingrese por medio de facebook, y se vuelve nuevamente un riesgo para que nos roben datos personales, pues se otorga el consentimiento para que accedan a información. No se realiza el cercioramiento para verificar que en realidad se trate del sitio web que buscamos. No se verifica que se trate de un formulario que utilice un ciberdelincuente. Se esta tan acostumbrado a dar click y click que se es víctima de sitios webs falsos.[15]

La realidad es que se otorgue o no consentimiento en el ciberespacio[16] nuestros datos personales son oro molido para el practicante ciberdelincuente, experto en acceder de forma no autorizada a sistemas informáticos sean privados o del Estado que formen parte de una laptop, teléfono inteligente, smartphone, pulseras inteligentes, entre otros dispositivos electrónicos, con el objetivo de apoderarse de datos personales a través de ciberdelitos.

A nivel nacional en México en el Código Penal Federal, en sus artículos 211 bis1 al 211 bis 7, tipifican la conducta de acceso ilícito a sistemas y equipos de informática, y establece que se sancionará al que tenga acceso, destruya, conozca o copie la información sin autorización a sistemas particulares o del Estado que cuenten con algún mecanismo de seguridad. Incluyendo la modificación, y los Sistemas Financiero del Estado y las instituciones que forman parte del mismo.

Entre los ataques a Sistemas Informáticos más destacados en México se encuentran el caso del Sistema de Pagos Electrónicos Interbancarios (SPEI), donde se registró en abril y mayo del 2018 un ataque cibernético a los sistemas de conexión al (SPEI), cuyo objetivo fue generar transferencias electrónicas de fondos a cuentas específicas, con el fin de sustraer ilegalmente recursos monetarios. Donde el modus operandi fue: Inserción de operaciones apócrifas, Uso de cuentas beneficiarias válidas y Eliminación de evidencia. Los ataques, utilizaron técnicas comunes como robo de credenciales, escalamiento de privilegios, movimientos laterales entre servidores, inserción de archivos o ejecución de instrucciones y borrado de bitácoras.[17] Al respecto el Banco de México en su carácter de administrador del (SPEI) en su Informe Anual emitido en marzo 2019 informa que: implementó medidas con el objetivo de mitigar los riesgos de materialización de eventos similares a los ocurridos

[14] Ciberdelincuente.

[15] Los virus troyanos pueden atacar los ordenadores de las víctimas y mostrar un cuadro de diálogo o una imagen en los ordenadores de cada usuario. La ventana será una imitación del sitio web del banco del usuario y le solicitará que introduzca su nombre de usuario y contraseña. Recuperado en: https://www.kaspersky.es/resource-center/threats/online-banking-theft

[16] El conjunto de información digital y a la comunicación que se realiza a través de las redes, un espacio en el cual casi todo lo que contiene es información. Término concebido por el escritor William Gibson en su novela de ciencia ficción “Neuromancer” (1984) con el propósito de describir un mundo de redes de información. Recuperado en: https://www.internetglosario.com/90/Ciberespacio.html

[17] Reporte de análisis forenses. Recuperado en: https://www.banxico.org.mx/spei/d/%7B4A977A24-0889-3F24-A717-DF9DBBA118C1%7D.pdf

durante 2018 y reducir las afectaciones a los usuarios de los servicios de transferencias electrónicas, a los participantes del (SPEI), entre los que destacan: Migración de participantes afectados, así como de un perfil de mayor riesgo a una plataforma de operación contingente; Implementación de alertas para detectar anomalías en los mensajes de pagos; Emisión de regulación con el fin de que las entidades que otorgan el servicio de transferencias de fondos implementen medidas de control; Establecimiento de protocolos y procedimientos que documenten las acciones a tomar en caso de que se materialicen riesgos de ciberseguridad; Designación de oficial de seguridad de la información responsable de las políticas de riesgos de ciberseguridad; Implementación de un proceso de autoevaluación. Lo anterior, para solventar las deficiensas de los Sistemas de conexión a (SPEI) y para fortalecer otros Sistemas Financieros.

El ciberdelincuente busca aprovecharse de los fallos de seguridad y sacar un beneficio, es ese hacker negro que busca sacar beneficios, actúa en ocasiones por razones económicas, razones ideológicas o por venganza. El ciberdelincuente tiene amplios conocimientos de seguridad informática, quien utiliza herramientas para llevar a cabo ciberataques (Internauta, Instituto Nacional de Ciberseguridad de España M.P., S.A., 2019)

El ciberdelincuente una vez accediendo a la wifi fácilmente, utiliza herramientas y roba nuestros datos personales, para cometer ciberdelitos o venderlos para su propio beneficio tales como: ciberacoso o ciberbullyng, suplantación de identidad, grooming, sexting, ransomware, phishing. Se analizará cada ciberdelito, su definición, se investigará si hay noticias respecto a esos delitos en Jalisco, se determinará qué datos personales son robados, se determinará si este ciberdelito está contemplado en la legislación estatal, y por último se describirán recomendaciones para evitar cada ciberdelito.

Ciberacoso o ciberbullyng:

> *Acto intencionado, ya sea por parte de un individuo o un grupo, teniendo como fin el dañar o molestar a una persona mediante el uso de tecnologías de la información y la comunicación (TIC) en específico el internet o teléfono celular (Inegi.Org.Mx, 2017).*

Jalisco es el cuarto lugar con más jóvenes de 12 a 19 años que han sido ciberacosados. (Informador Mx, 2019).

El ciberdelincuente roba fotos de desnudos, mensajes íntimos, videos íntimos, descifra contraseñas simples, se hace pasar por menor de edad, solicita datos personales utilizando artimañas.

El ciberacosador puede enviar mensajes a través de redes sociales[18] o correos electrónicos, los cuales en cuestión de minutos llegan a muchos compañeros, con el fin de burlarse o amenazar a su víctima. Las víctimas de ciberacoso se pueden sentir heridas, enojadas, odiadas y con ganas de suicidarse.

En ocasiones la práctica del ciberdelincuente por venganza, crea una identidad digital falsa de su víctima al extremo de hacerla pasar en ocasiones por dama de compañía e inclusive realiza publicaciones de fantasías de su víctima, provocando con ello que la usuaria ponga en riesgo su integridad.

El ciberacoso es un peligro que debemos reconocer, es una realidad que forma parte del mundo digital (Nora Muñiz, 2019).

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Quinto, Capítulo I, que habla de los ultrajes a la moral o a las buenas costumbres e incitación a la prostitución, artículo 135 bis, establece:

> *Quien obtenga de persona mayor de edad, material con contenido erótico sexual y sin su consentimiento lo divulgue original o alterado, se le impondrá una pena de dos*

18 La fábrica de engaños-redes sociales. Recuperado en: https://www.youtube.com/watch?v=i2tSrvLxYbE

a cinco años de prisión. Cuando el ultraje señalado en el párrafo anterior se cometa a través de las tecnologías de la información y la comunicación, se le impondrá al responsable una pena de cuatro a ocho años de prisión. Este delito se perseguirá por querella de la parte ofendida. Se estará a lo previsto en el Código Penal Federal cuando los hechos se adecuen al delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo (Código Penal para el Estado Libre y Soberano de Jalisco, 2019).

Como se advierte del artículo antes citado, prevé cuando se hace uso de las tecnologías de la información y la comunicación. Se considera que este tipo de ciberdelito debe estar en una Ley referente a Ciberseguridad y Ciberdelitos, en el cual se otorgue mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Algunas recomendaciones para evitar el ciberacoso son: Mantener en el caso de los menores de edad la comunicación con sus padres[19], recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, no aceptar invitaciones en redes sociales de desconocidos, mantener cuidado con los datos personales que se suben al internet, en caso de recibir mensajes ofensivos comunicarlo a la autoridad competente,[20] no seguir el juego a los acosadores hay que romper el silencio, configura la privacidad de tus redes sociales[21], descarga antivirus en tu smartphone, computadora, elabora contraseñas robustas, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle que herramientas puede utilizar para su protección.

Suplantación de identidad o robo de identidad:

"El robo de identidad se produce cuando alguien obtiene ilegalmente la información personal de otra persona y la utiliza para cometer fraude o un robo". El tipo de información personal podría ser cualquier cosa, desde datos generales, como tu nombre o dirección, hasta datos más específicos, como los registros de los hospitales, los detalles de la declaración fiscal o la información bancaria. Existen varias maneras habituales de las que se puede cometer el robo de identidad (Karpersky, 2019).

En Jalisco en los últimos días es muy común el robo de identidad en el infonavit[22], víctimas revelan que desconocidos falsificaron su información y pidieron créditos para adquirir viviendas (Informador. Mx, 2019). También es muy común escuchar que han creado un perfil de facebook utilizando tus datos personales. Se aprovecha de la anonimidad que le otorga el ciberespacio.

En Jalisco de acuerdo a un reporte llamado "Roban identidad a Pensiones en Jalisco" realizado por Luis Herrera en Reporte Índigo, informa que los fraudes por suplantación de identidad están desfalcando al Instituto de Pensiones de Jalisco y sus afiliados. Durante el 2019 se han registrado cinco casos y en el pasado sexenio hubo 14, este último dato lo sustenta con un informe que se brindó vía solicitud de transparencia identificada con el folio 04056619.[23] Lo anterior, hace evidente que los practicantes de ciberdelitos cada día roban más datos personales.

19 Prevención del Abuso Infantil. Video Recuperado en: https://www.educacionpas.org/Lobo/Basico/Civismo-Digital/Ciberbullying

20 Policía Cibernética, dependiente de la Fiscalía General de Jalisco.

21 Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

22 Instituto del Fondo Nacional de la Vivienda para los Trabajadores.

23 Roban identidad a Pensiones en Jalisco. Recuperado en: https://www.reporteindigo.com/reporte/roban-identidad-a-pensionados-en-jalisco-fraudes-prestamos-desfalco-infonavit/

El ciberdelincuente vende los datos personales al mejor postor, inclusive en la dark web[24], sitio donde se puede acceder con buscadores de internet especiales y conseguir información ilegal (Netflix, 2017). En ocasiones envían un mensaje de texto para que se visite una página web para robar datos personales, es lo que se denomina Smishing (Condusef, 2019).

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Sexto, Capítulo IV, que habla suplantación de identidad, artículo 143 quáter, establece:

> *Comete el delito de suplantación de identidad quien suplante con fines ilícitos o de lucro, se atribuya la identidad de otra persona por cualquier medio, u otorgue su consentimiento para llevar la suplantación de su identidad, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona. Este delito se sancionará con prisión de tres a ocho años y multa de mil a dos mil veces el valor diario de la Unidad de Medida y Actualización. Serán equiparables al delito de suplantación de identidad y se impondrán las penas establecidas en este artículo:*
>
> *I. Al que por algún uso de medio electrónico, telemático o electrónico obtenga algún lucro indebido para sí o para otro o genere un daño patrimonial a otro, valiéndose de alguna manipulación informática o intercepción de datos de envío, cuyo objeto sea el empleo no autorizado de datos personales o el acceso no autorizado a base de datos automatizados para suplantar identidades;*
>
> *II. Al que transfiera, posea o utilice datos identificativos de otra persona con la intención de cometer, favorecer o intentar cualquier actividad ilícita; o*
>
> *III. Al que asuma, suplante, se apropie o utilice, a través de internet, cualquier sistema informático o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca, produciendo con ello un daño moral o patrimonial, u obteniendo un lucro o un provecho indebido para sí o para otra persona.*
>
> *Se aumentará hasta en una mitad las penas previstas en el presente artículo, a quien se valga de la homonimia, parecido físico o similitud de la voz para cometer el delito; así como en el supuesto en que el sujeto activo del delito tenga licenciatura, ingeniería o cualquier otro grado académico en el rubro de informática, computación o telemática (Código Penal para el Estado Libre y Soberano de Jalisco, 2019).*

Como se advierte del artículo antes citado, prevé en su fracciones I y II ya involucra términos como medio electrónico, telemático o electrónico e internet. Este tipo de ciberdelito debe estar en una Ley referente a Ciberseguridad y Ciberdelitos, en el cual se otorgue mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Para prevenir la suplantación de identidad o robo de identidad: Mantener en el caso de los menores de edad la comunicación con sus padres, recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, no aceptar invitaciones en redes sociales de desconocidos, no dar click a correos que te ofrezcan premios tentadores, en caso de recibirlos hacerlo del conocimiento a la autoridad competente,[25] tener cuidado con los datos personales que se suben al internet, revisa tus estados de cuen-

[24] La web obscura, los sitios ocultos de internet.

[25] Policía Cibernética, dependiente de la Fiscalía General de Jalisco.

tas, configura la privacidad de tus redes sociales[26], descarga antivirus en tu smarphone, computadora, elabora contraseñas robustas, mantén actualizado tu smartphone o computadora, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle qué herramientas puede utilizar para su protección, utilizar las guías emitidas por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[27].

La Condusef respecto a este tipo de ciberdelito recomienda: No ingresar nombres de usuario y contraseñas en sitios desconocidos. Evitar compartir información financiera. Utilizar sólo páginas electrónicas que cuenten con certificados de seguridad. En caso de extravío de documentos personales presentar una denuncia ante la autoridad correspondiente. Evitar proporcionar datos personales a encuestadores vía telefónica. Revisar periódicamente tus estados de cuenta para detectar a tiempo cualquier operación irregular.

Cabe destacar que en este artículo del Código Penal para el Estado Libre y Soberano de Jalisco, también contiene la figura del ciberdelito llamado Phishing que es un tipo de fraude mediante el cual hacen pasar por una institución financiera y te envían un mensaje indicándote un error en tu cuenta bancaria, al ingresar tus datos, obtienen tu información confidencial como: números de tus tarjetas de crédito, claves, datos de cuentas bancarias, contraseñas. (Condusef, 2019). El ciberdelincuente realiza llamadas telefónicas o envía correos electrónicos a los usuarios, solicitando datos financieros o datos personales.

Otra forma en la que los ciberdelincuentes roban datos financieros o datos personales, es mediante el ciberdelito Vishing o phishing telefónico, mediante el cual te llaman para comunicarte si tus tarjetas tienen cargos y derivado de ello el usuario proporcione información (Condusef, 2019).

En Jalisco el phishing, vishing, suplantación de identidad son muy comunes en el mes de diciembre, cuando los usuarios realizan compras en el buen fín. (Informador M.X., 2017)

Anteriormente he comentado que los más vulnerables en las redes sociales para que les roben sus datos personales son los menores de edad, son víctimas fáciles en el ciberespacio, tal es el caso que el ciberdelincuente una vez que se empodera de los datos personales los vende a adultos pedófilos que practican el Grooming, en el internet.

Grooming o Cibergrooming:

> *Es el acoso o acercamiento a un menor ejercido por un adulto con fines sexuales. Concretamente, se refiere a acciones realizadas deliberadamente para establecer una relación y un control emocional sobre un niño o niña con el fin de preparar el terreno para el abuso sexual del menor, incluyéndose en este desde el contacto físico hasta las relaciones virtuales y la obtención de pornografía infantil (Inteco, 2019).*

En Jalisco también se dan casos de grooming, pues entre enero y julio de 2018, se sumaron 53 investigaciones por casos de acoso, principalmente en las redes sociales de facebook y whatsapp (Informador Mx, 2018), en las anteriores aplicaciones el ciberdelincuente crea perfiles falsos en caso de facebook o envía mensajes para iniciar una relación con los menores de edad, el objetivo es incitar al menor a participar en actos de naturaleza sexual, solicitándole le envié fotos intimas o videos. Poco a poco el practicante de ciberdelitos va aplicando estrategia para lograr su objetivo. La primera fase seria el sexo virtual y en su caso aplica ciberacoso. La segunda y última fase sería el contacto físico con el menor de edad y logran el abuso infantil.

[26] Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

[27] Guía para prevenir robo de identidad. Recuperado en: http://inicio.inai.org.mx/nuevo/Guia%20Robo%20Identidad.pdf

En el tema que nos ocupa, el ciberdelincuente accede a la red social del menor, roba sus datos personales a través de juegos de aplicaciones como roblox y los vende o utiliza para lograr el grooming.

Cabe destacar que en la mayoría de los casos cambia la conducta del menor a la de víctima, y por la falta de comunicación con sus padres no hace del conocimiento lo que está sufriendo, por lo que es necesario observar al menor porque regularmente cambia sus hábitos respecto al uso de internet pues lo hará a escondidas, perderá el interés por el estudio, tal vez hasta pérdida de apetito, manifestará cambios de humor, manifestará miedos, problemas de salud.

En virtud de que en este ciberdelito el objetivo principal son los menores, la Fundación de la Prevención del Abuso Infantil, en su sección de civismo digital, da a conocer un video dirigido a menores para que conozcan más sobre el grooming.[28]

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Quinto bis, Capítulo I, que habla de Corrupción de Menores, artículo 142-A, establece:

> *Se impondrá de tres a seis años de prisión y multa de cien a doscientas veces el valor diario de la Unidad de Medida y Actualización a la persona que facilite, provoque, induzca o promueva en persona menor de edad o con quien no tenga capacidad para comprender el significado del hecho:*
>
> *I. El hábito de la mendicidad;*
>
> *II. El hábito de consumir alcohol, drogas o sustancias similares;*
>
> *III. La iniciación o práctica de la actividad sexual, la realización de actividades sexuales explícitas, actos con connotación sexual, el envío de imágenes o sonidos de sí misma con contenido sexual o a la aceptación de un encuentro sexual, o*
>
> *IV. La comisión de cualquier delito.*
>
> *Cuando se trate de los actos mencionados y el sujeto activo del delito empleare cualquier tipo de violencia, o se valiese de alguna situación de mando, poder, función pública o autoridad que tuviere, la pena será de cuatro a siete años de prisión y multa de doscientos a quinientas veces el valor diario de la Unidad de Medida y Actualización.*
>
> *Cuando el acto de corrupción se realice a través de las tecnologías de la información y la comunicación, al responsable se le impondrá de seis a doce años de prisión y multa de doscientos cincuenta a quinientos cincuenta veces el valor diario de la Unidad de Medida y Actualización, sin perjuicio de las penas correspondientes a los demás delitos que en su caso se cometan.*
>
> *Se aumentará en una cuarta parte de la pena que corresponda, cuando la víctima u ofendido de los delitos de este capítulo, sea persona menor de doce años.*
>
> *Cuando la corrupción de la víctima conlleve un beneficio económico para el corruptor se estará a lo previsto en la Ley General para Prevenir, Sancionar y Erradicar los Delitos en Materia de Trata de Personas y para la Protección y Asistencia a las Víctimas de estos Delitos.*

[28] Prevención del Abuso Infantil. Video Recuperado en: https://www.educacionpas.org/Lobo/Intermedio/Civismo-Digital/Grooming

Como se advierte del artículo antes citado, prevé cuando se hace uso de las tecnologías de la información y la comunicación. Ciberdelito que debe estar contemplado en una Ley referente a Ciberseguridad y Ciberdelitos, en el cual se otorgue mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Para evitar el grooming son: mantener en el caso de los menores de edad la comunicación con sus padres[29], recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, no aceptar invitaciones en redes sociales de desconocidos, tener cuidado con los datos personales que se suben al internet en especial con las fotos y videos íntimos, configura la privacidad de tus redes sociales[30], descarga antivirus en tu smarphone, computadora, elabora contraseñas robustas, mantén actualizado tu smartphone o computadora, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle que herramientas puede utilizar para su protección.

Sexting definiciones:

> *Es un término tomado del inglés que une sex (sexo) y texting (envió de mensajes de texto vía SMS desde teléfonos móviles. El término sexting es un nuevo concepto que significa, recibir, enviar, o reenviar mensajes de texto, imágenes o fotografías, que presentan un contenido sexual explícito, vía internet o teléfono celular (Martínez, 2017).*

> *Práctica de riesgo, sobre todo cuando implica a los menores de edad. Mediante el sexting, se envían a través del teléfono móvil u otro dispositivo con cámara, fotografías o vídeos producidos por uno mismo con connotación sexual. El riesgo está en que una vez enviados estos contenidos, pueden ser utilizados de forma dañina por los demás (Is4k, 2019).*

En Jalisco en la mayoría de las escuelas primarias, secundarias, preparatorias e incluso en centros universitarios está presente el ciberdelito de sexting o mejor conocido como packs, pues incluso los usuarios de internet practicantes de esta conducta, forma sus propios grupos en las redes sociales (Informador Mx, 2018), en principio los usuarios los hacen por juego, satisfacción o simplemente para sentirse que son parte del grupo. De hecho en internet en buscador de google si capturamos packs en Jalisco, nos remite a una página de facebook (packs Jalisco.com)[31].

Packs[32] es una modalidad potencializada del sexting (textear respecto al sexo), es un "paquete" de dos o más imágenes. Para intercambiarlas, algunos jóvenes han creado grupos privados en redes sociales. Y de acuerdo con especialistas consultados, alguien del grupo puede traicionar la confianza de los involucrados y difundir las fotografías sin consentimiento de las afectadas. Como consecuencia, surge el bullying (acoso escolar) y, en el peor de los casos, hay riesgo de ser víctima de la trata de blancas. (Universidad de Guadalajra, 2017)

En este ciberdelito el principal dato personal robado son las fotos y videos intimas de las redes sociales como facebook , whatsapp, snapchat, instagram que los usuarios mismos producen, puede ser por voluntad propia del usuario de internet formando grupos muy reservados o porque un ciberdelincuente logró conexión con los dispositivos de los usuarios y roba los datos personales. Datos personales que vende al mejor postor, que en ocasiones son del crimen organizado dedicados a trata de blancas o red de prostitución infantil.

[29] Engaños por internet video ¿Nos conocemos? Recuperado en: https://www.youtube.com/watch?v=NuuppRGDUNk

[30] Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

[31] https://es-la.facebook.com/Packs-Jalisco-com-485705978595311/

[32] Prevención del Abuso Infantil. Video Recuperado en: https://www.educacionpas.org/Lobo-Jovenes/Basico/Civismo-Digital/Que-Hay-de-Los-Nudes-o-Packs

La obtención de datos personales por este ciberdelito, motiva a que se origine el ciberchantaje, que consiste en que una persona exija un beneficio a cambio de no divulgar fotografías o material audiovisual que afecte el honor del amenazado. Nuestro Código Penal para el Estado Libre y Soberano de Jalisco, pronto contemplará dicho ciberdelito (Informador M.X., 2019).

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Quinto, Capítulo I, que habla de los ultrajes a la moral o a las buenas costumbres e incitación a la prostitución, artículo 135 bis, establece:

> *Quien obtenga de persona mayor de edad, material con contenido erótico sexual y sin su consentimiento lo divulgue original o alterado, se le impondrá una pena de dos a cinco años de prisión. Cuando el ultraje señalado en el párrafo anterior se cometa a través de las tecnologías de la información y la comunicación, se le impondrá al responsable una pena de cuatro a ocho años de prisión. Este delito se perseguirá por querella de la parte ofendida. Se estará a lo previsto en el Código Penal Federal cuando los hechos se adecuen al delito de pornografía de personas menores de dieciocho años de edad o de personas que no tienen capacidad para comprender el significado del hecho o de personas que no tienen capacidad para resistirlo (Código Penal para el Estado Libre y Soberano de Jalisco, 2019)*

El artículo antes citado, prevé cuando se hace uso de las tecnologías de la información y la comunicación. La Ley referente a Ciberseguridad y Ciberdelitos que se propone debe prever este tipo de ciberdelito, y otorgar mayor información a los usuarios de internet para que tengan mayores indicios para denunciar y se lleve una correcta integración de la carpeta de investigación correspondiente.

Recomendaciones preventivas para evitar el sexting o packs son: mantener en el caso de los menores de edad la comunicación con sus padres, recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar, concientizar a los menores del riesgo de tomarse fotos y videos íntimos y el riesgo que esto conlleva, tener cuidado con los datos personales que se suben al internet en especial con las fotos y videos íntimos que suben en facebok, whatsapp, configura la privacidad de tus redes sociales[33], descarga antivirus en tu smarphone, computadora, elabora contraseñas robustas, mantén actualizado tu smartphone o computadora, no des click a páginas que no cuenten con https://w.w.w. y que tengan candado color verde, enseñar a usar al menor con responsabilidad las redes sociales, internet y comentarle que herramientas puede utilizar para su protección. Explicar al menor que el hecho de compartir fotos y videos íntimos de una persona desconocida es un delito.

Ransomware:

> *Software malicioso que infecta el ordenador y muestra mensajes que exigen el pago de un rescate para que el sistema funcione de nuevo. Esta clase de malware es un sistema de obtención de dinero criminal que puede instalarse mediante enlaces engañosos en un mensaje de correo electrónico, mensaje instantáneo o sitio web. Tiene la capacidad de bloquear la pantalla de un ordenador o cifrar determinados archivos importantes con una contraseña (Kaspersky, 2019).*

El pasado 18 de marzo del presente año, la Fiscalía General de la República alertó, mediante su cuenta de twitter sobre la entrada de un código que tomaba el control de nuestra computadora con tan solo dar un clic. (Informador M.X., 2019)

[33] Utiliza la guía para la configuración de privacidad en redes sociales, emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. Recuperado en: http://inicio.inai.org.mx/Guias/Guia_Configuracion_RS.PDF

El ciberdelincuente ingresa a nuestra laptop y encripta toda nuestra información, solicita rescate pero por lo general no se recupera información y queda en su poder.

El Código Penal para el Estado Libre y Soberano de Jalisco, actualmente en su Título Sexto, Capítulo II, que habla de la obtención ilícita de información electrónica, artículo 143 bis, establece:

> *Al que sin autorización y de manera dolosa, copie, modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días de multa (Código Penal para el Estado Libre y Soberano de Jalisco, 2019).*

Las penas previstas en este artículo se incrementarán en una mitad cuando el sujeto pasivo del delito sea una entidad pública o institución que integre el sistema financiero.

Para prevenir se debe realizar un respaldo de la información, actuar con precaución al seguir los enlaces de correos electrónicos, mensajes o en redes sociales, realizar actualizaciones de seguridad, utilizar herramientas anti-ransomware, mantener en el caso de los menores de edad la comunicación con sus padres, recabar toda la evidencia necesaria para acreditar circunstancias de modo, tiempo y lugar.

Los anteriores son los ciberdelitos más comunes en Jalisco. Sin embargo, el ciberespacio es tan amplio y nuestra sociedad Jalisciense va avanzando tan rápido en el tema de las tecnologías de comunicación y de la información, que se originarán nuevos ciberdelitos, los cuales en Jalisco no son muy documentados, como:

Cracking:

> *El término "cracking" hace referencia a la práctica que consiste en atacar sistemas informáticos y software con intención maliciosa. Por ejemplo, se puede crackear una contraseña para acceder a la cuenta de un usuario, o una red Wi-Fi pública para interceptar los datos que circulan por ella. Se puede prevenir utilizando un administrador de contraseñas e instalando antivirus. (Avast, 2019).*

Spyware:

> *"Tipo de malware que los hackers utilizan para espiarle con el fin de acceder a su información personal, detalles bancarios o actividad en línea". Se previene instalando actualizaciones recientes, instalando parches de seguridad recientes, estableciendo niveles altos de seguridad y privacidad, extremando precauciones al momento de llevar intercambio de archivos, no dando click a ventanas emergentes. (Avast, 2019).*

Malware y Antimalware:

> *Malware hace referencia a cualquier tipo de software malicioso que trata de infectar un ordenador o un dispositivo móvil. Los hackers utilizan el malware con múltiples finalidades, tales como extraer información personal o contraseñas, robar dinero o evitar que los propietarios accedan a su dispositivo. Se previene utilizando antivirus o antimalware. (Avast, 2019).*

Keylogger:

> *Tipo de spyware que registra en secreto las pulsaciones de su teclado para que los ladrones pueden obtener información de su cuenta, datos bancarios y tarjetas de crédito, nombres de usuario, contraseñas*

y otros datos personales. Se previene utilizando un software anti-keylogger. (Avast, 2019).

Por lo que es necesario preparase tanto en capacitación y normatividad en el tema, caso contrario se estará ante el inminente riesgo de ser víctimas de nuestras propias circunstancias, porque como se cita anteriormente, los usuarios cada segundo que pasa proporcionan datos personales al internet, esos datos que seguramente son almacenados en servidores gigantescos, y que alguien estará analizando los metadatos[34] y creando nueva tecnología (inteligencia artificial).

Inteligencia artificial:

Conjunto de disciplinas de software, lógica, informática y filosofía que están destinadas a hacer que los PC realicen funciones que se pensaba que eran exclusivamente humanas, como percibir el significado en el lenguaje escrito o hablado, aprender, reconocer expresiones faciales, etc. El campo de la inteligencia artificial tiene una larga historia tras de sí, con muchos avances anteriores, como el reconocimiento de caracteres ópticos, que en la actualidad se consideran como algo cotidiano (Hewlett Packard, 2019).

De acuerdo al Estudio de Hábitos de los Usuarios en Ciberseguridad en México 2019, realizado mediante mesas de trabajo los días 28 y 30 de enero, así como el 1de febrero del presente año. Que contó con 5,011 asistentes a las mesas de ciberseguridad la mayoría menores de edad estudiantes de primaria y secundaria. De los cuales 150 fueron participantes de Jalisco. Estudio que reveló que no existe una conciencia clara del uso de redes sociales e internet. Y que día a día en ese tipo de plataformas comparten fotografías, ubicaciones u opiniones, con el fin de relacionarse. Siendo uno de los problemas más preocupantes el que un menor tenga acceso libre a la tecnología, dando click y click a todo lo que encuentra en internet. Dando como resultado la importancia de seguir fomentando las capacidades digitales de los usuarios de forma integral, donde se incluya el uso seguro y responsable de las tecnologías, además de crearse políticas públicas, leyes y programas sociales que lo apoyen. (Gobierno de México, 2019). De lo anterior se advierte que en Jalisco hace falta capacitarse en el tema de ciberseguridad, para consecuentemente no ser víctimas de robo de datos personales a través de ciberdelitos.

[34] Video. Red en Defensa de los Derechos Digitales M.X. ¿Qué son los metadatos? Recuperado en: https://www.youtube.com/watch?v=iKccR3E6jn4

Es importante mencionar que se realizó una encuesta sencilla, cuya vitrina metodológica es:

- Se entrevistó a menores de entre 13 a 16 años de edad, de algunas calles de una colonia del municipio de Zapopan, Jalisco, asegurando el anonimato a los entrevistados y se aplicó de forma aleatoria.
- El trabajo de campo se realizó en el mes de Junio del 2019.
- La muestra se compuso de 96 cuestionarios.
- El margen de error de las estimaciones de la encuesta es de ¬+/-5% en la colonia.
- La encuesta fue llevada por un servidor.
- El número de habitantes de dichas calles es de 500 menores.
- Cuya fórmula es:

N: Población. De calles 500 menores.

n: Muestra.

p: Probabilidad a favor.

q: Probabilidad en contra.

z: Nivel de confianza. 95%

e: Error de muestra.

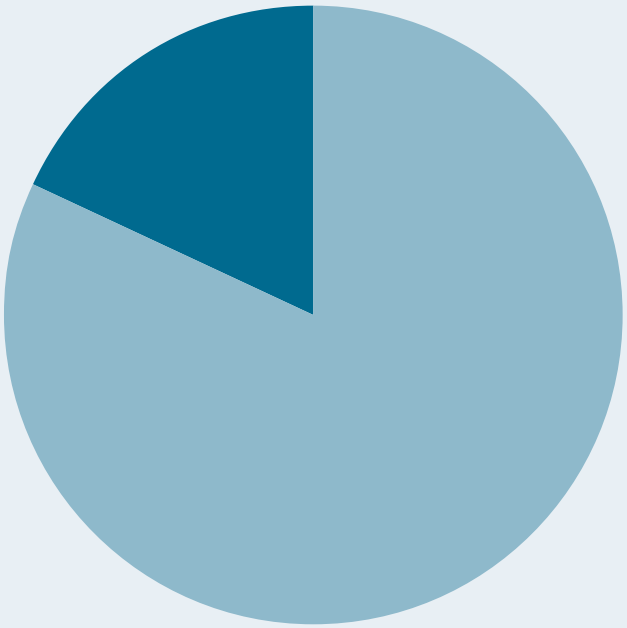
$$n = \frac{z2*p*q*N}{e2(N-1)+z2*p*q} \qquad n = \frac{1.96\text{^}(2)x0.5x0.5x500}{0.05\text{^}(2)x(500-1)+1.96\text{^}(2)x0.5x0.5} = 96 \text{ personas}$$

Las preguntas de cuestionario son respecto: Al tema de ciberseguridad y ciberdelitos, consistentes en:

1. ¿Conoce el ramsomware?, la mayoría de las respuestas fue: no.
2. ¿Comparte datos personales mediante wifi públicas?, la mayoría de las respuestas fue: sí.
3. ¿Conoces los cookies?, la mayoría de las respuestas fue: no.
4. ¿Cómo proteges tu router wifi?, la mayoría de las respuestas fue desconozco.
5. ¿Utilizar una misma contraseña para todos tus sitios?, la mayoría de las respuestas fue: utilizó una distinta.
6. ¿En facebook compartes fotos y videos?, la mayoría de las respuestas fue: sí.
7. ¿En facebook configuras tu privacidad?, la mayoría de las respuestas fue: no.
8. ¿Tienes instalado antivirus en tu laptop?, la mayoría de las respuestas fue: no.
9. ¿Conoces qué es un packs?, la mayoría de las respuestas fue: sí.
10. ¿Sabes qué es el ciberacoso?, la mayoría de las respuestas fue: no.
11. ¿Te han molestado mediante alguna red social?, la mayoría de las respuestas fue: sí.

Lo anterior se puede apreciar en la grafica siguiente:

Respuestas de 96 entrevistados =100%



Derivado de lo anterior, se sugiere que se debe expedir una Ley de Ciberseguridad[35] y Ciberdelitos en el Estado de Jalisco, que en sustancia responda al desarrollo de internet, de las redes sociales y la tecnología y que en el tema de las sanciones remita a nuestro Código Penal para el Estado Libre y Soberano de Jalisco.

Para emitirse deber realizarse en colaboración con autoridades internacionales especializadas en temas de ciberdelitos, toda vez que la tecnología ha tenido un rápido avance y debe existir armonización en las leyes contra ciberdelitos. Y así obtener beneficios para nuestra Ley Estatal.

[35] Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término es amplio y se aplica a numerosos elementos, desde seguridad informática hasta recuperación ante desastres y educación del usuario final. Recuperado en: https://latam.kaspersky.com/resource-center/definitions/what-is-cybersecurity

Autoridades Internacionales con normatividad en temas de ciberseguridad:

En Colombia tienen: CONPES 3701 DE 2011 Lineamientos Ciberseguridad y Ciberdefensa. Ley 527 de 1999- Validez jurídica y probatoria de la información electrónica; Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad; Ley 679 de 2001 – Pornografía Infantil – Responsabilidad ISPs; Ley 962 de 2005 -Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas; Ley 1150 de 2007 – Seguridad de la información electrónica en contratación en línea; Ley 1266 de 2008 – Habeas data financiera, y seguridad en datos personales; Ley 1273 de 2008 – Delitos Informáticos y protección del bien jurídico tutelado que es la información; Ley 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad; Ley 1437 de 2011 – Procedimiento Administrativo y aplicación de criterios de seguridad; Ley 1480 de 2011 – Protección al consumidor por medios electrónicos. Seguridad en transacciones electrónicas; Decreto Ley 019 de 2012 Racionalización de trámites a través de medios electrónicos. Criterio de seguridad; Ley 1581 de 2012, Ley estatutaria de Protección de datos personales; Ley 1623 de 2013 – Ley de Inteligencia – Criterios de seguridad; Ley 1712 de 2014 – Transparencia en el acceso a la información pública (CERTICAMARA SA, 2014).

En Chile tienen: Respuestas y Comentarios a Consulta Ciudadana Política Nacional sobre Ciberseguridad; Respuestas y Comentarios a Consulta Ciudadana Política Nacional sobre Ciberseguridad; Texto consulta pública Política Nacional de Ciberseguridad (2016); Documento Bases Política Nacional sobre Ciberseguridad (2015); DTO-533_17-JUL-2015 Crea Comité Interministerial sobre Ciberseguridad (2015); Reglamento Funcionamiento Comité Interministerial sobre Ciberseguridad (2015); Agenda Digital 2020 (CSIRT CHILE, 2019).

En Unión Europea: "Reglamento 2019/881" (Viafirma, 2019).

En México contamos con la Policía Federal, la cual de conformidad con el Manual de organización General, establece que contará con:

- División Científica que establecerá los mecanismos, lineamientos, políticas, protocolos y procedimientos que permitan la aplicación de herramientas técnico-científicas en las funciones que desarrolla la Institución, mediante la selección e implementación de tecnologías a los procesos y los servicios en especialidades de criminalística, investigación de delitos electrónicos y seguridad de sistemas de información, y aquellos en los que se requiera la aplicación.

- Coordinación para la Prevención de Delitos Electrónicos que conducirá las acciones de investigación de las conductas delictivas que utilicen medios electrónicos para su comisión, así como aquellas que representen amenazas y ataques a los sistemas de información, a través de la respuesta a solicitudes de colaboración, monitoreo de la red pública de Internet y aplicación tecnológica, electrónica, informática y de telecomunicaciones, desarrollada por los laboratorios de innovaciones, para prevenir y combatir aquellas conductas posiblemente constitutivas de delito en el territorio nacional.

- Dirección General de Prevención de Delitos Cibernéticos que dirige las acciones y procedimientos basados en el análisis de la información de la operación de actores o grupos delictivos, así como hechos delictivos en cuya comisión se utilicen medios cibernéticos, mediante el uso de herramientas especializadas para la vigilancia, monitoreo y rastreo de la red pública de Internet, así como la identificación, recolección y análisis de la información contenida en indicios digitales, con la finalidad de prevenir e investigar los delitos en coadyuvancia con las áreas de

la Institución y autoridades competentes conforme a las disposiciones aplicables.

- Dirección General del Centro Especializado en Respuesta Tecnológica que coordinará las respuestas a incidentes de seguridad informática en la estructura informática crítica de México, en colaboración con los diferentes órdenes de gobierno y actores sociales, mediante la aplicación de técnicas científicas para la identificación y mitigación de incidentes cibernéticos, así como de métodos avanzados de investigación y análisis, a fin de prevenir y combatir delitos que se cometan utilizando medios electrónicos o tecnológicos.

- Dirección General de Laboratorios en Investigación Electrónica y Forense que determinará los mecanismos de protección para la infraestructura informática crítica del país en tiempo real, a través de la operación de los laboratorios en investigación electrónica y forense, con la finalidad de implementar canales seguros para el intercambio de información de las investigaciones, con organismos homólogos nacionales y extranjeros conforme a las disposiciones aplicables.

Además la Coordinación para la Prevención de Delitos Electrónicos tendrá la atribución de establecer alianzas de cooperación con organismos y autoridades nacionales e internacionales relacionados con la prevención de delitos electrónicos.[36]

En Jalisco se cuenta con la Policía Cibernética que fue creada con la finalidad de detectar por medio del patrullaje en la red, los sitios, procesos y responsables de las diferentes conductas delictivas que se puedan cometer en contra y a través de medios informáticos y electrónicos. La Fiscalía General del Estado a través de la coordinación de Policía Cibernética brinda orientación a la ciudadanía respecto de los pasos que deberá seguir para presentar una denuncia en caso de ser víctima de un delito cometido a través del uso de las tecnologías de la información, además de que la Policía Cibernética colabora con el Ministerio Publico de así requerirlo en las investigaciones.

Es necesario destacar que al tener conexión con internet se ingresa al ciberespacio donde el usuario adquiere una identidad digital e incluso una vida que en ocasiones es anónima, y hace cosas que en su vida física no se atreve hacer o decir.

Se propone que entre los temas que debe contener la Ley de Ciberseguridad y Ciberdelitos en el Estado de Jalisco, se consideren los siguientes:

1.- Disposiciones Generales:

En las que se establezca la naturaleza e interpretación de la Ley.

2.- Objetivos de la Ley:

Donde se establezca que regulará las plataformas digitales, las redes sociales, aplicaciones, el internet de la cosas, entre otras comunicaciones digitales.

3.- Glosario de la Ley:

Que se deberá entender por amenaza, sujeto activo, sujeto pasivo, activo de información, ciberdefensa, datos personales, riesgo, entre otros.

Donde se explique conceptos propios de la Ley.

4.- Supletoriedad.

5.- De la comunicación digital:

Donde con apoyo de expertos en ciberseguridad que formen parte de las mesas de trabajo se establezca en específico cada tema referente a: Plataformas digitales, aplicaciones, redes sociales, del internet de las cosas, de la inteligencia artificial, el wifi público, sitios web.

6.- De las autoridades cibernéticas:

En este apartado se debe establecer qué autoridades deben intervenir en caso de ciberdelitos, sus obligaciones, funciones y facultades. Centro de reacción a incidentes. Policías cibernéticas.

[36] Artículo 27, fracción VII, del Reglamento la Ley de la Policía Federal.

7.- De la Cooperación de asociaciones privadas en temas de ciberseguridad:

En virtud de que en un futuro muy cercano todo será digital, por lo que es necesario involucrar a las asociaciones privadas, recordando que la ciberseguridad es un compromiso de todos.

8.- De la cooperación de autoridades internacionales.

9.- Capacitación en temas de Ciberseguridad:

Este apartado deberá establecerse que se otorgará presupuesto a las autoridades cibernéticas para efectos de capacitar en temas de ciberseguridad, manejo de portales, registro de identidades digitales, el internet de las cosas y sus riesgos, estudio de ciberdelitos, prevención de ciberdelitos, inteligencia artificial, big data, creando guías, videos educativos, se lleven a cabo campañas para elaborar contraseñas seguras, se den herramientas para detectar las fake news en redes sociales, como proteger wifi, como hacer compras seguras en internet, como proteger a nuestro menores en internet, como descargar antivirus, como proteger nuestros smartphone, como cifrar nuestros datos personales, crear juegos educativos para menores en temas de ciberseguridad, ciberdelito y cómo prevenirlos, celebrar convenio con autoridades internacionales para formar perito ciberforenses y porque no ciberabogados, formas de autenticación en el ciberespacio.

El ciberabogado deberá tener conocimientos informáticos y en ciberseguridad, puesto que todo se encontrará en la red, para asesorar a su cliente desde el ciberespacio; con formación digital; y con conocimientos de las normas que intentan ordenar el ciberespacio, donde asesora a ciudadanos, organizaciones y empresas en materias TIC (Tecnologías de la Información y la Comunicación) y por otro lado asesora a ciberciudadanos y ciberempresas en el nuevo entorno, con nuevos paradigmas, conflictos y normas (Campus Internacional Ciberseguridad, 2019).

La capacitación de ser de acuerdo al sector que vaya dirigida, sea seguridad pública, militar, educacional, ambiental, entre otras.

Con el objetivo de lograr la ciberresilencia: capacidad de los sectores público, privado, y de la sociedad para enfrentar este entorno sin que afecte su habilidad de operar día con día se denomina (McKinsey&Company, 2018). Es importante invertirle a la educación ya que no hay tiempo, la tecnología nos está superando y debemos tener el control.

10.- De los ciberdelitos, apartado donde se establezca:

Descripción, en específico de cada ciberdelito con apoyo de experto en la materia.

11.- Evidencia digital:

Donde se establezca qué elementos son necesarios para acreditar el tipo de ciberdelito, procedimiento para llevar acopio de evidencia, si deben ser certificaciones de publicaciones ante notario, cómo ofrecer peritos o informes, cómo llevar la actuación mediante orden de un juez, análisis de imágenes y videos, qué métodos debemos utilizar para análisis de evidencia, cómo deducir a qué redes sociales estuvo conectado el ciberdelincuente, cómo acreditar si la evidencia fue borrada intencionalmente, cómo descubrir las huellas en el ciberespacio. Valdría la pena agregar un apartado de ciberforense e informática forense.

Informática forense: Aplicación de técnicas científicas y analíticas especializadas en la infraestructura y dispositivos tecnológicos que permite identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal. En la actualidad la estructura documental de presentación de cualquier reclamación judicial, querellas o escrito tiene una estructura clara y definida, que permanece invariable, y que de no ser así se rechaza por defecto de forma (Es Ciber, 2019).

12.- Sanciones:

Donde se establezca que se aplicarán las penas establecidas en nuestro Código Penal para el Estado Libre y Soberano de Jalisco, pero haciendo reformas en el sentido de que serán más severas, dependiendo del modus operandi del ciberdelincuente.

Conclusiones

Ante el evidente y acelerado avance de las tecnologías de información y comunicaciones, es necesario concientizar a las autoridades y a los usuarios de internet, de los riesgos que hay en el ciberespacio, pues como quedó demostrado en el contenido del presente artículo, los practicantes ciberdelincuentes se ponen a la vanguardia de la tecnología para obtener robo de datos personales, ingresando de forma no autorizada a sistemas informáticos y financieros, creando aplicaciones y sitios webs falsos, accediendo a dispositivos inteligentes que se conectan a internet y están vinculados a los smartphone o teléfonos inteligentes como las pulseras inteligentes, enviado correos electrónicos falsos, por medio de bocinas inteligentes, y todo para obtener un beneficio económico, idealista o por venganza.

Es de suma importancia otorgar información de los ciberdelitos a los ciudadanos Jalisciense tales como: 1.- Ciberacoso o ciberbullyng; 2.- Suplantación de identidad; 3.- Grooming; 4.- Sexting; 5.- Ransomware; 6.- Phishin; 7.- Smishing; y 8.-Vishing. Los ciudadanos Jalisciense deben conocer las amenazas y riesgos que enfrentarán cuando utilizan la tecnología y el ciberespacio.

Se debe estar a la vanguardia en tecnología porque surgirán nuevos ciberdelitos, por lo que es necesario cooperar con autoridades internacionales como Estonia, Colombia, Chile, España, Singapur, Estados Unidos, Japón respecto al tema de ciberdelitos, de acuerdo a informes de la Condusef en el primer trimestre de 2019, las quejas por fraudes cibernéticos crecieron un 19% respecto al 2018 y representan cada año una mayor proporción[37].

Es necesario destinar mayor presupuesto a campañas de publicidad respecto a la cultura de ciberseguridad, para lograr que se realice vía radio, televisión, redes sociales, sitios webs, realizar foros, infografías, folletos que lleguen como coloquialmente se menciona al ciudadano de a pie.

[37] Fraudes cibernéticos y tradiciones. Consultado en: https://www.condusef.gob.mx/gbmx/?p=estadisticas

Se generen políticas públicas donde se involucren a las autoridades de los tres niveles Federal, Estatal y Municipal competentes en el sector educativo y tecnológico, para que se establezca como materia en las escuelas el tema de ciberseguridad y ciberdelitos, toda vez que los menores son los más expuestos a ciberdelitos. Y se capacite respecto al uso de wifi seguras, antivirus, sitios webs, compras online, cuidado de datos personales, redes sociales, correos electrónicos infectados, servicios en la nube seguros, herramientas para dispositivos para evitar robo de datos personales.

Es necesario se expida una Ley de Ciberseguridad y Ciberdelitos en el Estado de Jalisco, que en sustancia responda al desarrollo de internet, de las redes sociales y la tecnología y que en el tema de las sanciones remita a nuestro Código Penal para el Estado Libre y Soberano de Jalisco.

Dar al Internet de las cosas, uso responsable, por ejemplo en el caso de pulseras inteligentes pueden ayudar para integrar debidamente el expediente clínico de los usuarios. El análisis de las grandes cantidades de información puede ser utilizada para un fin positivo mejoraría nuestra calidad de vida e incluso nuestro planeta, seriamos un Jalisco digital de primer mundo y tendríamos control en: ciberambiente, cibereducación, cibergobierno, cibercomercio, cibersanidad.

Debemos estar muy preparados en temas de ciberseguridad y ciberdelitos, es necesario que nuestras normas evolucionen, caso contrario la gran información que es almacenada, puede ser utilizada para obtener el control total de todos los servicios.

Se debe cuidar a los menores cuando estén usando la conexión de internet, porque son los más vulnerables, se debe hablar y tratar los temas de ciberdelitos para lograr concientizarlos, y lograr que cuando haya reuniones familiares convivan y no estén únicamente conectados a las redes sociales.

Luis Abraham Rincón Prieto

Abogado egresado de la Universidad de Guadalajara. Egresado de la Especialidad en Gestión, Publicación y Protección de Información por el CESIP del ITEI. Notificador en Juzgados de Primera Instancia del Poder Judicial. En el Supremo Tribunal de Justicia del Estado como encargado del archivo en la Sala Auxiliar Mixta. Litigante en despacho jurídico. Coordinador Especializado “A” en el Despacho del C. Gobernador. Coordinador de archivos del OPD Consejo Municipal del Deporte de Zapopan, Jalisco.

Referencias

(s.f.).

Aguilar., R. (27 de julio de 2017). *Andro4 Cill.* Obtenido de Así es como te la cuelan con los términos y condiciones de usuario.: Ricardo Aguilar (27 de julio de 2017). Así es como te la cuelan con los términos y condiciones de usuario. Andro4all. Recuperado de https://andro4all.com/2017/07/terminos-condiciones-problemas-android

Andrés, M. B. (2018). *Internet de las Cosas.* Madrid: Reus.

Avast. (24 de Septiembre de 2018). *¿Podrián los altavoces inteligentes desmontar tu hogar inteligente?* Obtenido de https://blog.avast.com/es/podrian-los-altavoces-inteligentes-desmontar-tu-hogar-inteligente

Avast. (2019). *Cracking.* Obtenido de https://www.avast.com/es-es/c-cracking

Avast. (2019). *Keylogger.* Obtenido de https://www.avast.com/es-es/c-keylogger

Avast. (2019). *Malware y Antimalware.* Obtenido de https://www.avast.com/es-es/c-malware

Avast. (2019). *Spyware.* Obtenido de https://www.avast.com/es-es/c-spyware

Campus Internacional Ciberseguridad. (2019). *¿Por qué son necesarios los ciberabogados en la nueva ciber-realidad?* Obtenido de https://www.campusciberseguridad.com/blog/item/123-por-que-son-necesarios-los-ciberabogados-en-la-nueva-ciber-realidad

CERTICAMARA SA. (01 de Marzo de 2014). *Instrumentos Normativos de Ciberseguridad.* Obtenido de https://web.certicamara.com/app/webroot/media/import/normativa-colombiana-en-materia-de-ciberseguridad-y-ciberdefensa-1-marzo-2014.pdf

Código Penal para el Estado Libre y Soberano de Jalisco. (11 de Mayo de 2019). Periódico Oficial “El Estado de Jalisco”. México, Jalisco, México: Congreso del Estado de Jalisco.

Condusef. (2019). *Portal de fraudes financieros.* Obtenido de https://phpapps.condusef.gob.mx/fraudes_financieros/informate.php

Constitución Política del Estado de Jalisco. (09 de Abril de 2019). Periódico Oficial “El Estado de Jalisco”. México, Jalisco, México: Congreso del Estado de Jalisco.

CSIRT CHILE. (2019). *Ciberseguridad.* Obtenido de https://www.ciberseguridad.gob.cl/documentos/

Díaz, F. N. (Diciembre de 2014). *Promexico. Mx.* Obtenido de http://promexico.mx/documentos/mapas-de-ruta/internet-of-things.pdf

Es Ciber. (29 de Mayo de 2019). *Curso Forense.* Obtenido de https://www.es-ciber.com/ciberseguridad/cursos-forense/

Gobierno de México. (2019). *Estudio "Hábitos de los usuarios en ciberseguridad en México 2019".* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

Gobierno de México. (15 de marzo de 2019). *Procuraduría Federal del Consumidor.* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/445899/DIA_MUNDIAL_DE_LOS_DERECHOS_DEL_CONSUMIDOR_2019.pdf

Hewlett Packard. (2019). *¿Que es la inteligencia artificial?* Obtenido de https://www.hpe.com/mx/es/what-is/artificial-intelligence.html

Inegi.Org.Mx. (2017). *Módulo sobre ciberacoso 2017.* México.

Informador M.X. (29 de Diembre de 2017). *Crecen denuncias por fraude en Jalisco; diciembre es el mes con más casos.* Obtenido de https://www.informador.mx/Crecen-denuncias-por-fraude-en-Jalisco-diciembre-es-el-mes-con-mas-casos-l201712290001.html

Informador M.X. (18 de Marzo de 2019). *Alertan sobre programa malicioso que toma control dela computadora.* Obtenido de https://www.informador.mx/mexico/Alertan-sobre-programa-malicioso-que-toma-control-de-la-computadora-20190318-0112.html

Informador M.X. (05 de Febrero de 2019). *Congreso de Jalisco aprueba que el "ciberchantaje" sea delito.* Obtenido de https://www.informador.mx/jalisco/Congreso-de-Jalisco-aprueba-que-el-ciberchantaje-sea-delito--20190205-0146.html

Informador Mx. (22 de Agosto de 2018). *Tras reforma, crecen denuncias porciberdelitos contra menores de edad.* Obtenido de https://www.informador.mx/Tras-reforma-crecen-denuncias-por-ciberdelitos-contra-menores-de-edad-l201808220001.html

Informador Mx. (06 de Mayo de 2019). *Jóvenes jaliscienses, de los más ciberacosados.* Obtenido de https://www.informador.mx/jalisco/Jovenes-jaliscienses-de-los-mas-ciberacosados-20190506-0020.html

Informador. Mx. (24 de Abril de 2019). *Sufren calvariopor fraude en créditos del Infonavit.* Obtenido de https://www.informador.mx/Sufren-calvario-por-fraude-en-creditos-del-Infonavit-l201904240001.html

Inteco. (2019). *Instituto Nacional de Tecnologías de la Comunicación.* Obtenido de https://www.adolescenciasema.org/usuario/documentos/sos_grooming.pdf

Internauta, O. d. (16 de Febrero de 2015). *Instituto Nacional de Ciberseguridad de España M.P., S.A.* . Obtenido de https://www.osi.es/es/actualidad/blog/2015/02/16/lee-antes-de-aceptar-lo-que-no-leemos-de-las-condiciones-y-terminos-de-uso

Internauta, O. d. (18 de Diciembre de 2015). *Instituto Nacional de Ciberseguridad de España M.P., S.A.* . Obtenido de https://www.osi.es/es/actualidad/blog/2015/12/18/la-privacidad-en-wearables-en-que-punto-se-encuentra

Internauta, O. d. (2019). *Instituto Nacional de Ciberseguridad de España M.P., S.A.* Obtenido de Los ciberdelincuentes, ¿quiénes son?: https://www.osi.es/es/campanas/los-ciberdelincuentes-quienes-son

Is4k. (2019). *Internet Segura ForkiDs.* Obtenido de https://www.is4k.es/necesitas-saber/sexting

Karpersky. (2019). *Robo de Identidad: hechos y preguntas frecuentes.* Obtenido de https://www.kaspersky.es/resource-center/threats/identity-theft-facts-and-faq

Kaspersky. (2019). *¿Qué es el clickjacking?* Obtenido de https://www.kaspersky.es/resource-center/definitions/clickjacking

Kaspersky. (2019). *¿Que es el ransomware?* Obtenido de https://www.kaspersky.es/resource-center/definitions/what-is-ransomware

Kaspersky. (2019). *Cómo evitar los riesgos de seguridad asociados a las redes Wifi públicas.* Obtenido de https://latam.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks

Mariana R. Fomperosa. (21 de Diciembre de 2018). *Milenio.* Obtenido de https://www.milenio.com/tecnologia/resena-echo-amazon-bocina-inteligente-alexa

Martínez, J. G. (2017). *Bullyingg, sexting y grooming .* Colombia: San Pablo.

McKinsey&Company. (2018). *Perspectiva de ciberseguridad en México.* México: Comexi.

Netflix. (2017). *La red obscura.* Obtenido de https://www.netflix.com/mx/title/80182553

Nora Muñiz. (25 de Junio de 2019). *Plumas Atomicas.com.* Obtenido de https://plumasatomicas.com/noticias/extraordinario/que-hacer-ante-el-ciberacoso/

OCU Ediciones, S. (06 de Novimembre de 2009). *Organización de Consumidores y Usuarios.* Obtenido de https://www.ocu.org/dinero/tarjetas/noticias/tarjetas-cuidado-con-el-cvv-472704

Oficina de Seguridad del Internauta. (2019). *Mensajeria Instantanea.* Obtenido de https://www.osi.es/es/mensajeria-instantanea

Oficina de Seguridad del Internauta. (2019). *WhatsApp, Telegram y Line. ¿Cuál es más segura para chatear?* Obtenido de https://www.osi.es/es/actualidad/blog/2014/05/09/whatsapp-telegram-y-line-cual-es-mas-segura-para-chatear

Red en Defensa de los Derechos Digitales M.x. (28 de Mayo de 2015). *¿Que son los metadatos?* Obtenido de https://www.youtube.com/watch?v=iKccR3E6jn4

Schwab, K. (2016). *La Cuarta Revolución Industrial.* Suiza: Penguin Randon House.

Social, C. (02 de Abril de 2019). *INEGI.* Obtenido de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2019/OtrTemEcon/ENDUTIH_2018.pdf

SUN. (28 de Octubre de 2018). *Informador MX.* Obtenido de https://www.informador.mx/tecnologia/Apple-HomePod-el-nuevo-sonido-de-la-casa-20181028-0048.html

Universidad de Guadalajra. (27 de Diciembre de 2017). *La Red Universitaria de Jalisco.* Obtenido de http://www.udg.mx/es/noticia/packs-intercambio-imagenes-eroticas-redes-sociales-pasatiempo-alto-riesgo

Viafirma. (20 de Junio de 2019). *La nueva Ley de Seguridad Cibernética de la Unión Europea .* Obtenido de https://www.viafirma.com/blog-xnoccio/es/ley-seguridad-cibernetica-union-europea/