UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

POSGRADO EN DERECHO

FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

SEGURIDAD INFORMÁTICA Y BLOCKCHAIN COMO INSTRUMENTO DE PREVENCIÓN DE DELITOS DE ROBO DE INFORMACIÓN EN INSTITUCIONES BANCARIAS EN MÉXICO

TESIS

QUE PARA OPTAR POR EL GRADO DE:

MAESTRO EN POLÍTICA CRIMINAL

PRESENTA:

CALLES MELÉNDEZ JOSÉ ROMÁN

TUTOR

MTRO. ROBERTO ALVARÉZ MANZO
(FES ACATLÁN)

MIEMBROS DEL SÍNODO

Dr. Eduardo Alfonso Rosales Herrera (Presidente)
Mtro. Antonio Cholley Nakahodo Rivera (Secretario)
Mtro. Roberto Álvarez Manzo (Vocal)
Dr. Héctor Cantú Lagunas (1er Suplente)
Mtro. Jaime Cárdenas Camacho (2do Suplente)
(FES ACATLÁN)

Sta Cruz Acatlán, Estado de México, Septiembre 2021

“Las ciencias tienen las raíces amargas, pero muy dulces los frutos”

Aristóteles

AGRADECIMIENTOS

A MI MAMÁ: MARICÉLA MELÉNDEZ

Muchas gracias mamá por apoyarme en todas mi metas, gracias por estar al pendiente de mí desde que era pequeño. Sin ti no hubiera cumplido este sueño.

A MI PAPÁ: JOSÉ CALLES

En dónde quiera que estés papá gracias por darme la vida espero que estés viendo este momento tan importante de mi vida. Muchas gracias por todos esos momentos de felicidad.

A MIS HERMANAS:

Les doy gracias por estar conmigo en las buenas y en las malas, por tolerarme y sobre todo por ser las mejores hermanas, Elena, Vanessa y Valeria.

A MI TÍO: EDUARDO CASTRO

Gracias por ser parte de mi formación, por escucharme, por ponerme toda la atención necesaria cuando la necesité.

A MI TUTOR: MTRO. ROBERTO ÁLVAREZ

Muchas gracias por el apoyo y sus asesorías, por darme la oportunidad de profundizar en mi tema de investigación. Muchas gracias.

A MI SÍNODO: DR. EDUARDO ROSALES

Gracias por ayudarme a cosechar los frutos del conocimiento, por ayudarme a desarrollar uno de los temas más importantes de la actualidad. Gracias por la confianza

A MI SÍNODO: MTRO. ANTONIO NAKAHODO

Gracias por su asesorías por el apoyo y por todo el entusiasmo que pone en sus clases, le agradezco por su profesionalismo.

A MI SÍNODO: DR. HÉCTOR CANTÚ

Su seriedad hizo que mi tema de investigación tuviera uno de los mejores enfoques, sin su apoyo no hubiera sido posible esto. Muchas gracias.

ÍNDICE

INTRODUCCIÓN

Dentro de los intereses profesionales se pudo desarrollar y brindar una solución referente a la Seguridad Informática, dándole un enfoque social y después forense; la línea de investigación por la que se pudo indagar relacionado a la Maestría en Política Criminal fue la detección de problemas relacionados a la extracción y robo de información de plataformas digitales, en específico en Bancos. Desafortunadamente nuestra identidad en el ámbito digital está quedando marcada por toda la cantidad de datos generados todos los días. Ante este escenario se trabajó con una de las Ciencias Forenses más jóvenes de nuestros tiempos "La Informática Forense".

Mejor conocido por el "computo forense" se encontró con diferentes alternativas en materia de prevención del robo y extracción de datos personales en al ámbito bancario una de ellas fue las plataformas de seguridad informática.

Dentro de las soluciones posibles se inclinó por el sector de la Criptografía y en específico el tema del Blockchain como posible solución para poder prevenir el delito de extracción de datos personales en el ámbito Bancario a partir de técnicas en materia de Informática forense.

Primero para poder dar una visión sociológica del problema me fui por Urlich Beck con su Teoría del Riesgo en dónde nos habla de los "Males públicos globales", El Riesgo a la Modernización, el Riesgo a la Tecnología. De la misma forma se explicó del riesgo del Internet, la informática, la telemática y los virus informáticos. Se revisó también lo referente a la Ciberseguridad con perspectiva de Criminología en dónde se analizó los Tipos de Seguridad Informática, sus principios y las políticas de seguridad informática. Y finalmente se vio el tema de Seguridad Informática y Derechos Humanos, derivado de la Protección de datos personales como un derecho Humano y el primer principio de la Estrategia de Ciberseguridad.

En el segundo capítulo se dio el desarrollo de la legislación y el marco jurídico, reuní evidencia para sustentar la problemática del robo y extracción de datos personales en el ámbito bancario. Consulté la CPEM, el Código Penal Federal, el Código Penal

de Sinaloa, el Código Civil, la Ley Federal de Derechos de Autor y finalmente la Ley Federal de Protección de Datos Personales.

Mientras que en el ámbito internacional revise lo que corresponde a los Organismos Internacionales como: EL Convenio de Budapest, la pronunciación de la ONU de los crímenes por Internet y la Organización de Estados Americanos.

Por ultimo consulte varios cuerpos normativos y realice una “Marco Normativo Comparado” en materia de Seguridad Informática de la Unión Europea (España) y Estados Unidos.

En el tercer capítulo se analizó la problemática, revisé a nivel internacional los principales Bancos, los cuales han sido vulnerados en los últimos años; primeramente empecé con Estonia como uno de los primero países que usó la Banca Electrónica como sistema seguro para hacer transferencias Bancarias y su vulneración de su sistema de pagos a través de la denegación de servicio.

De la misma forma se analizó el problema del ataque cibernético que sufrió HSBC de Londres, EL Banco Griego, el Banco de Bangladesh y por último el Banco Ruso.

En el segundo bloque de este capítulo traté el tema referente a los Ciberataques a Bancos Mexicanos se tomó como punto de referencia el SPEI (Sistemas de Pagos Electrónico Interbancario) y el efecto que está teniendo con otras organizaciones las cuales se ven vulnerados por la misma disyuntiva.

En el tercer bloque se analizó “al Sujeto en la figura de robo informático en Instituciones Bancarias” en dónde se analiza el Sujeto Activo y Pasivo del delito.

En el cuarto bloque se revisó lo referente a Phreaker, Craker, Lammers Bucanas y Gurus Newbie, los cuales son figuras muy importantes del sujeto del delitod.

En el cuarto capítulo se brinda una propuesta basada en Blockchain en la que analizo su aplicación para los datos Bancarios, pero antes de eso explico la definición propia de Blockchain, sus antecedentes y sus elementos más importantes, dentro de la propia descripción de estos conceptos destaco la importancia de la “Usabilidad de plataformas como Blockchain para la prevención

en robo y extracción de datos Bancarios. En este último tema se destacó la importancia del uso de dicha tecnología que brinda seguridad a toda persona que tenga sus datos principalmente afiliado a plataformas electrónicas en las que se pueda consultar la Banca Electrónica.

En el segundo apartado de este capítulo se plantea una planeación para enfrentar al tipo de delincuente Bancario, para ello hago la clasificación de estos tipos de delincuentes como son: Delincuentes comunes, delincuentes políticos, sabiendo la intención de estas dos figuras se analizan los elementos principales que se deben de tomar en cuenta para formular una **"Estrategias de información en materia de encriptación"**

En la tercera sesión se ve el análisis de la "Estrategia preventiva de Política Criminal para el tratamiento del robo de extracción de datos Bancarios". Esta se basa principalmente en una planilla de investigación de cómputo forense en Bancos, se utilizan técnicas de informática forense como la geolocalización y se involucra a la cadena de custodia y la participación de Blockchain para poder obtener evidencia digital para resolver casos en materia de robo y extracción de datos personales en el ámbito bancario, así como prevenir con tecnología de blockchain el robo de lo antes mencionado.

Por último se propone la "Aplicación de una estrategia de ciberseguridad, encriptación de Datos Bancarios" la cual se fusiona con tecnología Blockchain y ayuda a la sociedad.

CAPÍTULO I

1.1 Teoría del riesgo con perspectiva en Política Criminal

1.1.1 El riesgo a la modernización

El concepto de riego y sociedad del riesgo combina lo que en otros tiempos era mutuamente excluyentes: sociedad y naturaleza, ciencias sociales y ciencias de la materia, construcción discursiva del riesgo y materialidad de amenazas.

El enfoque de política criminal es cuando se ven las causas de los riesgos, es decir la modernidad trae como consecuencia riesgos de criminalidad. Iñaki nos menciona que "la política criminal no es solamente un concepto complejo; es también un concepto problemático"[1] De Sola nos dice que "la inserción de la política criminal en el campo de la política cabría empezar diciendo que aquélla hace referencia al conjunto de actividades del Estado encaminadas a reducir -ya que no eliminar- la criminalidad"[2]

La Sociedad del Riesgo Mundial es el elemento articulador de los temas colaterales desarrollados en sus reflexiones sobre el presente y el futuro de la sociedad; "el tipo, el modelo y los medios del reparto de los riesgos se diferencian sistemáticamente de los del reparto de la riqueza."[3]

Urlich Beck nos menciona que hay desgracias globales que impactan en las clases sociales, uno de ellos es el sector industrial en el que se ve reflejado el poder fáctico de las empresas y los organismos mundiales.

En la actualidad uno de los problemas es enfrentarse a las cosas nuevas, sobre todo cuando hablamos de la Tecnologías de la Información, las cuales tienen un impacto en la modernización y el progreso de los países. El miedo al manejo de las tecnologías y el cambio ha puesto a muchas personas a dudar de su usabilidad.

[1] Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 153
[2] A. de Sola, "El pensamiento Criminológico", Edit. Temis, Colombia, 1983, Pág. 247
[3] Beck, Ulrich, "La Sociedad del Riesgo", Barcelona, Edit. Paidos, Iberica, 1986, Pág. 40

Cada vez que una persona va al cajero automático existe un miedo interno al equivocarse y teclear dígitos confidenciales; el pánico que genera enfrentarse a nuevas formas en que se maneja la información, es difícil comprender el nivel de abstracción, sobre todo a usuarios que no saben utilizarlo al momento de usar nuevas modalidades de tecnología.

El riesgo está latente cada vez que se crean nuevas tecnologías, mientras que en China están sacando al mercado un software- conjunto de programas, instrucciones y reglas para ejecutar ciertas tareas en una computadora u ordenador[4]- que identifica personas a partir de reconocimiento facial, en (EUA) están creando un software que sirve como defensa para elevar la protección en materia de seguridad Informática. El mercado de las Tecnologías de la Información no deja de detenerse y es símbolo de la modernización imparable.

En la actualidad muchos países están migrando a la digitalización, es el caso de Estonia que en los últimos años ha sido nombrado como el país que está en la **"nube",** este concepto se refiere al "Espacio de almacenamiento y procesamiento de datos y archivos ubicado en internet, al que puede acceder el usuario desde cualquier dispositivo"[5], este es usado para determinar, por sus procesos administrativos que los lleva acabo de forma digital como: elecciones populares, pagos electrónicos, juicios en línea, abertura de una empresa en línea, internet en todo el país incluyendo las zonas inaccesibles, mejor desarrollador de sistemas informáticos y creador del programa Skype el cual es un software propietario distribuido por Microsoft tras haber comprado la compañía homónima que permite comunicaciones de texto, voz y vídeo sobre Internet.

El mundo de las aplicaciones está cambiado la forma de operar; la modernidad de esta nueva tecnología ha impactado en el proceso histórico y social, es decir, que en esta etapa de "La modernidad" existe otra formas de control social, la cuales se está desbordando debido que no se tiene un seguimiento detallado de los procesos informáticos. El término "mal global" de la Teoría del Riesgo se presenta en que no

[4] Real Academia Española http://lema.rae.es/dpd/srv/search?key=software Marzo del 2019
[5] Real Academia Española https://dle.rae.es/?id=QgpwJRv Marzo del 2019

se tiene un mecanismo de control claro para que cualquier individuo pueda navegar por la red y cometa “Actos no regulados por la ley” y que por lo tanto sea imposible su sanción. El riesgo de contar con diferentes plataformas “Sin seguridad informática, evidentemente lleva a pensar que se seguirán cometiendo muchos delitos informáticos y seguirán apareciendo figuras nuevas, representadas por sujetos “anónimos” que cometan actividades ilícitas.

La modernidad exige nuevas formas de enfrentar a los riesgos de la tecnología y para ello se creó la Ciberseguridad como medio de prevención y combate a los ataques cibernéticos. La ciberseguridad “es un conjunto de técnicas o procedimientos que velan por la seguridad de los usuarios que comparten información entre sistemas computables”[6]

1.1.2 Males públicos globales

Urlich Beck menciona que existen una serie de “Males Públicos Globales” los cuales se caracterizan por ser problemáticas que surgen dentro de los “Estados Trasnacionales”.

El autor menciona que para que se pueda resolver “Los Males Públicos Globales” se debe de seguir el siguiente Método Contrario a lo que seguía: “Problemas Globales soluciones globales”[7], nos menciona que se debe dejar de atender asuntos globales pensados que son locales.

En la vida diaria podemos ver que, como producto de la mundialización, ahora muchos asuntos se involucran a nivel trasnacional, desde un asunto comercial, hasta un convenio diplomático en el que se dirimirán controversias de carácter global-internacional. Urlich Beck nos menciona que estos asuntos se ven reflejados

[6] Economía simple .net https://www.economiasimple.net/glosario/ciberseguridad Consulta : 3 de Marzo del 2019
[7] Beck, Ulrich (1998), “*La sociedad del riesgo. Hacia una nueva modernidad”*, Barcelona, Paidós. Pág. 70

en males globales; es evidente que estos se ven expresados en problemas que no se han podido resolver y que urge una solución.

Es aquí donde se puede explicar el problema de las conductas que aún no están reguladas dentro de la ley en materia informática. En la Red se realizan miles de operaciones informáticas, se suben archivos, se descargan archivos a algo que se llama “La nube”, ciertos paquetes de información no tienen la seguridad necesaria para poder transitar en la red porque pueden ser extraídos, copiados o en su caso robados. La información transita por diferentes servidores del mundo y hay personas físicas que se encargan de recoger esa información con la finalidad de lucro. El miedo global se ve reflejado al momento de que la información puede ser robada en otra parte y ser utilizada para poder cometer delitos tipificados o realizar conductas que aún no están descritas como delitos por los códigos penales.

No hay un control por las redes mundiales y esto ha generado muchos problemas como los denominados ciberataques a diferentes dependencias de gobiernos. Según el periódico Universal “se han registrado 51 millones 649 min hackeos a 23 instituciones públicas, entre secretarías, bancos del Estado, universidades y partidos políticos en México, provenientes de Europa y Asia. [8]

El mal público de las Tecnologías de Información ha pegado a las instituciones y se debe de atender con urgencia a partir del uso de la “seguridad Informática”. Esta es la única vía para poder combatir este mal público que está afectando a miles de personas que tienen acceso a ellas.

Varias instituciones de gobierno y privadas viven con temor ante las amenazas de ciberataques. El problema global se ve representado por estos ciberataques que roban en ocasiones dinero depositado del sector Bancario de México. Es muy fácil con una tecla hacer daño a las instituciones. Muchas veces son bandas criminales organizadas, en otros términos “bandas de hackers” que operan en la red con equipos sofisticados que soportan buena cantidad de información. Un problema

[8] Cibergrafía, Villa y Caña Pedro, “Ciberataques, una amenaza exterior contra organismos”, El Universal, 14 de Octubre del 2018 https://www.eluniversal.com.mx/nacion/ciberataques-una-amenaza-exterior-contra-organismos Consulta 2 de Abril del 2019

global de la misma naturaleza es cuando Hackean algo tan importante como el suministro de agua y electricidad, en la actualidad un hacker podría crear una guerra civil por la escasez de agua, tan sólo infiltrándose al sistema de aguas nacionales.

Estamos hablando que los cibercriminales son más peligrosos que incluso una banda que asalta una institución bancaria, los primeros podrían robar varias cuentas bancarias haciendo uso de una buena programación, mientras que los segundos su botín podría ser 90 % menor y arriesgando la vida.

Por ejemplo, un robo muy grande propagado por una banda criminal fue:

"Robo cibernético a banco de Bangladesh

Durante 2016, cibercriminales robaron 81 millones de dólares a un banco de Bangladesh mediante el uso de un código malicioso detectado por ESET como una variante de Win32/Agent.XZH. Se trata de un código altamente complejo que presenta una funcionalidad sofisticada y que permitió a los cibercriminales acceder al software de mensajería utilizado por más de 11.000 bancos e instituciones financieras de más de 200 países conocido como SWIFT Alliance Access"[9]

1.1.3 Riesgo a la Tecnológica

Según Alexandra Ramírez Castro "El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad"[10]

[9]Harán, Manuel, Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 6 de Abril del 2019

[10] Cibergrafía, Ramírez Castro Alexandra , "Riesgo Tecnológico y su impacto para las organizaciones parte 1"Seguridad, cultura de prevención para TI" UNAM, https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i Consulta: 7 de Abril del 2019

Ramírez nos menciona algo muy interesante que es la gestión, una herramienta dentro de la Administración Pública que lleva a que los procedimientos estén bien establecidos.

Ulrich nos habla respecto a las grandes transformaciones que estaba experimentando el mundo occidental a partir de la década de los ochenta del siglo XX, comentaba que "Desde el punto de vista de la teoría social y de la historia social, lo que aparece y es lamentado como «terror de la intimidad» son, pues, las contradicciones de una modernidad demediada en el proyecto de la sociedad industrial, que siempre ha partido ya los principios indivisibles de la modernidad libertad individual e igualdad más allá de la limitación del nacimiento[11]

El autor señala claramente que se está vulnerando la individualidad y la intimidad de las personas y si se asumen el enfoque de las Tecnologías de la Información, se puede dar cuenta que, al ser parte de las redes sociales, la información está siendo comprometida. Al crear un perfil en una plataforma, existe el riesgo de que otras personas tengan conocimiento de la existencia y que por tanto se obtenga información completa de cualquier persona. Al momento de generar una cuenta en alguna plataforma, cualquier persona vulnerable a que se nos pueda robar la información, no obstante, por los cambios globales tenemos-por necesidad- que hacer uso de estas plataformas.

El riego tecnológico está ahora en las aplicaciones, las cuales son usadas todo el tiempo. Hay aplicaciones para hacer compras en los supermercados, aplicaciones para solicitar servicio particular de taxi, aplicaciones para poder saber ubicación de lugares, aplicaciones para hacer pagos por vía bancaria, aplicaciones para bajar música, video, escuchar programas internacionales, etc. El riesgo es que todo esto se pueda usar para fines de dudosa naturaleza. Por ejemplo, es sector más atacado por los hackers son las instituciones bancarias:

---

[11] Beck Ulrich, "La Sociedad del Riesgo" , Barcelona, Edit. Paidos,Iberica, 1986, Pág. 144

“Ataque dirigido a bancos polacos e instituciones en Latinoamérica

A inicios de 2017, investigadores de ESET identificaron un malware dirigido contra bancos polacos e instituciones en Latinoamérica, ya que tras atacar en Polonia se dirigió a instituciones ubicadas en México y Uruguay. La amenaza se envió con sigilo a través de un ataque watering hole, con lo cual un sitio de confianza que fue comprometido redirigió a las víctimas hacia una página fraudulenta que escondía un exploit.[12]

Ciberataque a bancos de México

El último hasta el momento fue el ataque dirigido a bancos de México, donde se estima que los cibercriminales robaron cerca de 300 millones de pesos al explotar una vulnerabilidad en el software que utilizan bancos e instituciones financieras para conectar sus sistemas con el Sistema de Pagos Electrónicos Interbancarios (SPEI); una plataforma del Banco de México que permite realizar transacciones por Internet”[13].

1.2 Teoría del Riesgo y el uso de Nuevas Tecnologías con perspectiva de Derecho Penal.

1.2.1 Riesgo en Internet

La orientación de la perspectiva va enfocada directamente hacia un ámbito penal De Sola nos decía que “el derecho penal es el último recurso al que se permite acudir, dentro del esquema del Estado de derecho, para salvaguardar determinados intereses individuales y colectivos, la política criminal no puede limitarse al análisis

[12] Harán Manuel Juan, “Los ciberataques dirigidos a bancos más importantes de los últimos tiempo”, Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 10 de Abril del 2019
[13] Harán Manuel Juan, “Los ciberataques dirigidos a bancos más importantes de los últimos tiempo”, Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 11 de Abril del 2019

de los resultados obtenidos o por obtener del funcionamiento de las instituciones penales" [14]

Enfocado al ámbito penal y las nuevas tecnologías en época contemporánea exige comunicación abierta en todo el planeta, las redes se han ampliado y el internet juega un papel muy importante para las operaciones. El internet es un medio de comunicación; es la cuarta forma de sistema de control (Medios masivos de Comunicación), la cual tiene consecuencias, debido a que no está del todo regulado y las conductas se pueden diversificar. La sociedad se mueve a través de la búsqueda de información, el riesgo que se corre de explorar estos ciberespacios es de encontrarse con posibles sitios vulnerables.

Jorge Vasconcelos Santillana nos dice que internet es "Un conjunto de elementos tecnológicos que permiten enlazar masivamente redes de diferentes tipos para que los datos puedan ser transportados de una a otra red"[15]

El Internet es una revolución de las comunicaciones, gracias a este sistema todas las personas pueden gozar de mejoras constantes. No obstante, a pesar de ser uno de los mayores inventos de la humanidad, está teniendo fallas en la misma; se refiere elementalmente a que gracias a internet ahora las organizaciones criminales pueden operar de forma más fácil. Resulta que se ha creado una fuerza cibernética de criminalidad que comete muchos delitos, así como conductas aún no tipificadas. La era del Internet ha logrado construir una red organizada de sujetos que saben perfectamente como robar información desde cualquier parte del mundo. Entran a los sistemas de forma clandestina y extraen datos sin el conocimiento y muchos menos la autorización de las y los usuarios.

Los peligros de internet van desde tener dinero electrónico "Criptomonedas" hasta tener un "Secreto industrial", muchos sujetos que saben programación y que navegan en internet, por lo regular encuentran la forma para poder entrar a sitios lo cuales son hackeados. Navegar en internet es peligroso y no sabemos que

[14] A. de Sola, "El pensamiento Criminológico", Edit. Temis, Colombia, 1983, Pág. 247
[15] Vasconcelos Santillana Jorge, "Informática II Sistemas de Información", Publicaciones culturales, México 2002, Pág. 30

podamos encontrar; desde páginas que explican cómo hacer armas hasta sitios en dónde se proporciona la pornografía. El riesgo de recorrer paginas puede ocasionar problemas, por ejemplo, en los últimos años se juegan videojuegos en línea y muchas personas quieren llevar a la realidad el video juego, ocasionando tal vez homicidios o lesiones a sujetos.

El internet tiene un peligro, porque se puede realizar plataformas de ventas clandestinas, sobre todo sitios que están en la Deep web; sitio de red obscura en dónde se puede conseguir cualquier cosa.

Según Grossman lev “La internet profunda es un conjunto de sitios web y bases de datos que buscadores comunes no pueden encontrar ya que no están indexadas. El contenido que se puede hallar dentro de la internet profunda es muy amplio”

1.2.2 Riesgo en la Informática

Otro riesgo importante es la informática, su nivel de vulnerabilidad ha sido de gran alcance debido a que se comparten datos de forma automatizada a partir de un servidor central. El Problema público se ve manifestado cuando en la red está la información de las personas y muchas veces son utilizados para fines desconocidos.

La vulnerabilidad de las y los usuarios ha superado la expectativa, cada vez que uno teclea su número de cuenta del banco y su contraseña este puede estar siendo observado en otra parte del mundo a partir de programas alternativos que se usan para espiar las actividades de otros “Malware”. Con un teclado y la información necesaria se puede hacer mucho daño, el riesgo en la informática se ve vulnerable principalmente al momento de compartir la información. Esto se parece mucho al correo que se usaba anteriormente y los paquetes no llegaban a su destino y eran robados por bandas; ahora sabemos que estos paquetes- físicos- cuentan con un código de barras y con una guía lo que hace imposible-en la mayoría de los casos- desaparecer. Está pasando lo mismo en las Redes Informáticas en pleno siglo 21;

esto se ve reflejado porque aún no se tiene una "estratificación en materia de redes informáticas"

Julio Téllez Valdés es un pensador mexicano, líder en materia de Derecho Informático en México y nos da esta definición, la cual es muy objetiva al momento de querer poner en práctica: "La informática es un conjunto de técnicas destinadas al tratamiento lógico y automatizado de la información con miras a una adecuada toma de decisiones"[16]

La informática cambió nuestro mundo y nuestra forma de pensar, antes se tenía que usar tarjetas perforadoras para poder realizar procesos contables, ahora existen muchos programas que facilita el uso de la contabilidad. La informática se hizo necesaria cuando se dieron cuenta que se podía ahorrar pasos y procesos. En la era analógica se tenía rendimiento y en la era digital se tiene aún más, es decir que el escenario de la informática está cada vez mejorando, no obstante, se tiene que implementar siempre una estrategia de ciberseguridad, para que el tratamiento lógico y automatizado sea el adecuado

1.2.3 Riesgo en la Telemática

La sociedad adquiere conceptos diferentes, los cuales se deben adoptar dentro de nuestro vocabulario, en este caso es la Telemática, rama de las ciencias exactas que se distingue por referirse a las redes de carácter informático, cualquier protocolo de comunicación virtual en el cual se use ceros y unos. El Dr. Beck puso énfasis a la "Configuración del Estado Trasnacional" el cual la sociedad civil mundial tiene que adoptar ciertos procedimientos y protocolos de las nuevas tecnologías.

La Telemática es otro nivel y nos habla de protocolos de comunicación que van a permitir ejecutar operaciones a gran escala en materia de compartir datos a través de la Red.

[16] Téllez Valdés Julio, "Derecho Informático", Edit. Mc Graw Hill, 2009, México, Pág. 21

El riesgo de los protocolos de comunicación se ve reflejado en una compleja Red Mundial. En diferentes casos se ha escuchado de la intervención de teléfonos, muchas veces son intervenidas por agencias de dudosa procedencia o bien por personas que lo único que quieren lograr es un fin de lucro, espiando llamadas, interceptando información por esta vía de las telecomunicaciones.

Según Martínez Echeverría "Lo más característico de estos nuevos medios es, sin duda, la posibilidad de constituir grandes «bases de datos», es decir, gigantescos ficheros en soporte magnético, a los que se puede acceder con gran velocidad, son' fácilmente modificables, pueden ser consultados simultáneamente por muchos usuarios, y todo ello a costes económicos que se reducen de día en día."[17]

La Telemática según la Real Academia Española nos dice que es "La aplicación de las técnicas de las telecomunicaciones y de la informática a la transmisión a larga distancia en la información computarizada"[18]

Según Marc Goodman "En la red tenemos el problema de las direcciones de protocolo. Los IP son un tipo de dirección existente en la red; cada computadora que se conecta en la red posee su propia dirección IP, es una manera de identificarse en la red y de localizar a la gente que buscamos, el problema es que las direcciones de IP también son fáciles de falsificar"[19]

Hoy en día el uso de las redes es indispensable para la economía, las operaciones de la bolsa de valores se pueden efectuar de forma rápida gracias a la telemática y a través de satélites, podemos saber que operaciones financieras se están realizando en Hong Kong. El riesgo es no brindar seguridad informática a estas redes; el cuidado de las plataformas y sistemas que comunican a las redes, deben ser monitoreados constantemente para que no sean hackeados. Los satélites transmiten información que muchas veces es captada por piratas informáticos. Por ejemplo, si un secreto industrial es transmitido desde Singapur a EUA, si no se tiene

[17] Martínez Echeverría A. Miguel, "Informática y Derechos Humanos", Pág. 99
[18] Diccionario de la Real Academia Española, "Diccionario de la Lengua Española", Edit. Vox, España, 2002, Pág. 70

[19] Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 14

la seguridad informática suficiente, se puede correr el riesgo de que ese secreto se pueda conocer y tal vez ser de dominio público, permitiendo que cualquier usuario/a pueda descargarlo. La protección de la información no está garantizada debido a que no se puede combatir de forma rápida estos ciberataques.

1.2.4 Riesgo de Virus Informático

Rosa Eliza Elizondo define al virus informático "Cómo programas Informáticos como cualquier otro software, excepto que son creados por personas con propósitos mal intencionados, cuyo objetivo es provocar las fallas en el funcionamiento del sistema o corromper o destruir parte o la totalidad de los datos almacenados en el disco.[20]

En la era de la informática nos encontramos con muchos problemas para proteger la información; la industria crea productos para el uso de los procesos informáticos de las organizaciones, Bancos, Escuelas, Hospitales y cualquier empresa pública o privada; no obstante, se presenta un mercado opuesto, el cual se caracteriza por infringir la ley y toda ley de informática conocida. Las organizaciones se están quejando constantemente de esto debido a que se están presentando pérdidas millonarias en diferentes sectores. Los llamados "virus" son programas creados para poder abrir otros programas y desconfigurarlos. Lo que hacen es entrar directo en el lenguaje modificando su status y su modo de operación, ocasionando que se infecte el sistema y que por lo regular se muestre vulnerable, mostrando como característica -en el caso de una computadora- comportamiento anómalo y de dudosa procedencia.

Cómo podemos ver Rosa nos brinda una idea respecto a las intenciones con los datos y esto es alarmante; se corre un riesgo mayor de robo de datos según José de Jesús del periódico Excélsior en la sección de "Dinero"

"En la última década según especialistas de organizaciones que manejan miles de datos como la IFT, SCT OEA y Microsoft afirman que ha crecido exponencialmente

[20] Elizondo Elisa Rosa, "Informática I", Edit. Mc. Graw. Hill, 2006, México Pág. 25

300%, más de 45 millones de personas han sido víctimas de ciberataques y principalmente el robo de identidad. Desagraciadamente hasta hoy no hay penalidad, es decir este tipo de actos no están tipificados por la ley."[21]

Los datos nos arrojan que la cantidad de infecciones en la Red trae como consecuencia ciberataques, afectando significativamente el cuadro económico, político y social de las instituciones.

Según Marc Goddman "Los países más ricos piensan en la seguridad informática, pero los pobres no por lo tanto los gobiernos deben trabajar con la policía. Un ejemplo de eso sucedió con el virus "*I love you*", que luego de ser creado en Manila Filipinas, ha atacado a las computadoras de todo el planeta. Los daños mundiales han sido cuantificados entre 2,000 y 3,000 millones de dólares. En unos días el FBI en coordinación con la policía de Manila identificó al sospechoso, un joven de apellido Goosman que estudiaba en la Universidad de Manila y decidió escribir el programa del virus. La policía detuvo al individuo, pero según la ley en Filipinas se puede causar daño sólo a cosas físicas, tangibles. En la red es difícil entender un daño porque no es algo físico; el joven salió libre y no hubo algo que pudiera hacer la policía ni en Filipinas ni en Estados Unidos".[22]

Desde que inicio el proyecto de las Tecnologías de la Información, se tenía miedo a los virus y a pesar de la creación de nuevas alternativas de solución, los piratas cibernéticos, idean a nuevas formas para violar contraseñas e infectar sistemas. La fobia a usar las tecnologías precisamente viene de este hecho. Las personas temen usar plataformas bancarias por miedo a que un malware se meta a la terminal y este le extraiga todo el dinero.

Como ya hemos mencionado las instituciones bancarias han sido los blancos por ejemplo esto pasó en Londres:

[21] Guadarrama José de Jesús, "Nada detiene el robo de Identidad", Edit. Excélsior, 2019, México, Pág.14 https://www.excelsior.com.mx/periodico/flip-dinero/17-03-2019/portada.pdf Consulta: 20 de Abril del 2019

[22] Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 14

"**Ataque DDoS a plataforma online de filial del HSBC en Reino Unido**

En enero de 2016, la filial del Reino Unido del banco HSBC reveló que los servicios en línea de su sitio fueron blanco de ataques DDoS. Si bien la institución aseguró que pudo defenderse de manera exitosa, sus sistemas quedaron fuera de servicio por un tiempo"[23]

Otro ataque fue perpetrado con un código malicioso: "**Ataques DDoS a bancos griegos,** en él años 2015, tres bancos griegos fueron blanco de ataques distribuidos de denegación de servicio (DDoS) donde cibercriminales del grupo que se hacen llamar Armada Collective demandaron el pago de un rescate en bitcoins."[24]

1.3 Ciberseguridad con perspectiva de Criminología.

1.3.1 Teoría de Complejos de Seguridad Regional

Debido al problema del escenario de los ciberataques se tiene que trabajar un modelo que se caracterice para prevenir, combatir y frenar los ataques, Iñiaki nos menciona que "Los niveles se elevan con modelos de criminología crítica, en la medida en que esta recoge el **paradigma del "Etiquetamiento"** o de la reacción social, lo mejora y lo torna adecuado la aplicación práctica"[25] El etiquetamiento lo podemos clasificar por el grupo exclusivo de hackers y crackers.

La Teoría propuesta por Barry Buzan en su libro People, States and Fear en el año de 1991 nos menciona respecto la ampliación de una agenda de seguridad debido a que la seguridad ya no se puede abordar desde un punto de vista tradicional y estatocéntrico. La aplicación pretendería asistir a sectores vulnerables, incluyendo

[23] Harán Manuel Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 21 de Abril del 2019
[24] Harán Manuel Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 21 de Abril del 2019
[25] Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 153

el Sector Cibernético. La Teoría CSR tiene una perspectiva neorrealista y perspectiva globalista.[26]

La evolución y la modernización del hombre ha sido sorprendente y la tecnología nos ha traído muchos beneficios, pero también problemas. Marc Goodman asesor de la interpol y FBI nos dice que dentro de la Ciberseguridad se analiza la "Cibercriminalidad, va más allá de los hackers y los piratas, pues hay muchas otras formas de causar daño en la red y de atacar sus sistemas, como, por ejemplo, los criminales trasnacionales. El hacker puede tener acceso a la página que quería en cualquier parte del globo terráqueo, cuando está en el sistema pueda manipular los datos con fines criminales y eso pasa cada día".[27]

Con esto último podemos analizar que dentro de la seguridad pública hay una necesidad por evitar la manipulación de datos. Hoy de día muchos datos son públicos y cualquier persona puede tener acceso, por ejemplo, una fecha de nacimiento puede ser muy peligrosa darla, debido a que los cibercriminales pueden extraer información, meterse a cuentas bancarias y realizar ciberataques.

Existe en México una Estrategia Nacional de Ciberseguridad que atiende al público cuando tiene un problema. Esta idea surgió por "el marco del Plan Nacional de Desarrollo 2013-2018, dentro del Programa para un Gobierno Cercano y Moderno 2013-2018, se estableció la Estrategia Digital Nacional cuya finalidad es impulsar la digitalización de México, a través de acciones como: gobierno digital, datos abiertos, inclusión y habilidades digitales, servicios de salud y educación a través de las TIC, el uso de TIC en servicios financieros, entre otras"[28].

[26] Barry Buzan, People, States and Fear, 1983, Inglaterra, Pág. 16
[27] Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 15

[28] SEGOB, "Estrategia de Ciberseguridad", 2018
https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf
Consulta 23 de Abril del 2019

1.3.2 Tipos de Seguridad Informática

Según el Instituto Nacional de Ciberseguridad de España existen 3 tipos:

Técnico: se refiere a los sistemas, los dispositivos, el software y cualquier elemento, mecanismo o aparato, que permite implementar seguridad.

Jurídico: se refiere al cumplimiento de la legislación en materia de ciberseguridad, que afecta a las empresas, en función, por ejemplo, de su actividad, del sector al que pertenecen o de los datos que utilizan en sus procesos de negocio. Principalmente podemos encontrarnos con la LOPD, entre otras.

Organizativo: se refiere al cumplimiento de normativas relativas a seguridad, como normas ISO, políticas de seguridad, buenas prácticas, etc.[29]

Existe una gran interrelación entre estos ámbitos, en especial, entre el ámbito jurídico y organizativo, puesto que son muy similares y se complementan y a su vez se apoyan en el ámbito técnico.

El escenario de la seguridad informática se ve vulnerable al momento de efectuar operaciones electrónicas conectadas a la red, Marc Goddman un especialista en temas de seguridad informática nos menciona que “Los sistemas para prevenir el lavado de dinero y su falsificación no funciona en el mundo cibernético; por ejemplo, si yo quiero salir de Estados Unidos de América con más de diez dólares hay que firmar algo y hacer un reporte. En otros países hay que verificar quienes tienen el dinero. La policía y el gobierno debe cambiar porque los delincuentes están más adelante cada día”[30]

[29] López, Jorge Chinea, “Tipos de herramientas básicas para garantizar la ciberseguridad en la empresa”, INCIBE, 2014, https://www.incibe.es/protege-tu-empresa/blog/herramientas-basicas-ciberseguridad-empresa Consulta 24 de Abril del 2019

[30] Goodman Marc, “Cibercriminalidad”, Edit. Impresos Chávez, 2003, Pág. 14

1.3.3 Principios de Seguridad Informática y Paradigma del etiquetamiento.

Para el fortalecimiento de la Ciberseguridad fue necesario implementar estrategias en combate a los ciberataques dentro del sector financiero:

"A. Perspectiva de derechos humanos. Contemplar en las diferentes acciones en materia de ciberseguridad la promoción, respeto y cumplimiento de los derechos humanos; entre otros, la libertad de expresión, el acceso a la información, el respeto a la vida privada, la protección de datos personales, la salud, educación y trabajo.

B. Enfoque basado en gestión de riesgos. Contar con la capacidad de manejar escenarios de incertidumbre por medio de enfoques preventivos y correctivos, con la intención de minimizar el impacto de las cambiantes amenazas y riesgos del ciberespacio.

C. Colaboración multidisciplinaria y de múltiples actores. Enfoque basado en la colaboración multidisciplinaria de las diferentes partes (actores y sectores): con un enfoque de gobernanza de internet en materia de ciberseguridad, que permita el desarrollo integral, transversal y holístico de la Estrategia y facilite la participación abierta y transparente de los mismos"[31]

Antes de la Estrategia Nacional de Ciberseguridad se habló mucho de otros principios más técnicos apegados a uso preventivo de una terminal, es decir de una computadora. Pero enfocándonos a la estrategia podemos mencionar que el primero es unos de los más importantes; los Derechos humanos hoy en día juegan un papel muy importante para poder enfrentarse a las normas jurídicas establecidas,

[31] SEGOB, "Estrategia de Ciberseguridad", 2018
https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf
Consulta 25 de Abril del 2019

sobre todo cuando la norma se aplica y se está afectando la integridad de la persona, en este caso se afecta a la persona pero en la nube; es decir que se puede afectar a una persona en diferentes plataformas, como redes sociales, plataformas bancarias, perfiles profesionales, juegos de azar o videojuegos en línea. Estos sitios pueden tener una serie de estafas las cuales pueden afectar la integridad humana de las personas.

El otro principio nos habla respecto a la usabilidad es decir usar lo preventivo y lo correctivo, este punto es muy importante para este trabajo de investigación debido a que se trabajará con Blockchain, esta plataforma brinda seguridad informática con base al uso de bloques y llaves digitales. La prevención y protección de datos es uno de los más importantes proyectos en materia de Ciberseguridad, no obstante, faltan muchas personas especializadas que quieran dedicarse a esta área.

Algo muy importante desde la perspectiva de la Política criminal y la criminología nos menciona que "Hay tres niveles de prevención: el primario, cuando se actúa sobre los contextos sociales y situaciones para evitar que se favorezca la delincuencia y para procurar condiciones favorables a comportamientos legales; el secundario, dirigido específicamente a evitar que se cometan infracciones e incivilites; el tercero nivel, cuando la prevención se encuentra orientada a evitar la reincidencia". [32]

Si lo ponemos en plano de la seguridad Informática nos podemos quedar con el segundo porque ofrece prevención directa y evita que se puedan consumar delitos en materia de robo de la información o extracción de datos.

Por último, la colaboración multidisciplinaria se refiere a la cooperación entre instituciones, foros, organizaciones que combaten a los ciberataques. Hay muchas dependencias que ya están combatiendo los ciberataques, no obstante, aún no es suficiente.

[32] Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 164

1.3.4 Política de Seguridad Informática

En otro apartado se revisó lo referente a la Estrategia Nacional de Ciberseguridad la cual: “Es el documento que establece la visión del Estado mexicano en la materia, a partir del reconocimiento de:

A. La importancia de las tecnologías de la información y comunicación (TIC) como un factor de desarrollo político, social y económico de México; en el entendido de que cada vez más individuos están conectados a Internet y que tanto organizaciones privadas como públicas desarrollan sus actividades en el ciberespacio.

B. Los riesgos asociados al uso de las tecnologías y el creciente número de ciberdelitos.

C. Las necesidades de una cultura general de ciberseguridad”.[33]

Desde la creación de esta estrategia se ha atendido el problema de los ciber ataques, no obstante, el criminal intenta una forma nueva de poder operar en la clandestinidad y sin saber su identidad, cada día crea nuevas conductas, las cuales son nuevas y difíciles de identificar. Muchas veces por los cambios tecnológicos, los cibercriminales lo que hacen es cambiar de tecnología y si la legislación mencionaba que ya no se podía perseguir un delito bajo el uso de esa tecnología, al final ya no puede por que el sujeto cambio completamente la forma de operar.

A pesar de que son estadísticas del 2009 estas son alarmantes, la OEA hizo un estudio referente a los delitos en internet a gran escala:

“Panorama de los crímenes cibernéticos mundiales -2009

[33] SEGOB, “Estrategia de Ciberseguridad”, 2018 https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf Consulta 26 de Abril del 2019

- Botnets*

1) à 6.8 millones de computadoras infectadas con bots
2) à 47,000 activos cada día
3) à 17,000 nuevos servidores de control y comando”[34]

Distribución geográfica de computadoras infectadas con sólo un botnet Zeus.

[35] Delitos en Internet a gran escala.

[34] Anthony V. Teelucksingh, “Delitos en Internet a gran escala”, Edit. OEA, 2010, Pág. 6 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 27 de Abril del 2019
[35] Anthony V. Teelucksingh, “Delitos en Internet a gran escala”, Edit. OEA, 2010, Pág. 7 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 27 de Abril del 2019

Overall Rank LAM	Overall Rank Global	Country	Percentage LAM	Percentage Global
1	3	Brazil	54%	7%
2	12	Argentina	18%	3%
3	21	Chile	7%	1%
4	22	Peru	6%	1%
5	25	Mexico	5%	1%
6	29	Colombia	4%	<1%
7	37	Dominican Republic	2%	<1%
8	50	Puerto Rico	1%	<1%
9	62	Bolivia	<1%	<1%
10	63	Venezuela	<1%	<1%

Table 3. Bot-infected computers by country, LAM
Source: Symantec

[36]

Panorama de los crímenes cibernéticos

Mundiales -2009

1. 2.9 millones de nuevas amenazas de código malicioso*
2. Filtración de datos debido al hackeo; ejemplos**
3. à 160,000 registros de seguros médicos e historiales clínicos - universidad
4. à 530,000 números de seguridad social – agencia gubernamental
5. à 570,000 historiales de tarjetas de crédito – negocios
6. à 750,000 listados de clientes – proveedor de telefonía móvil
7. à 130,000,000 números de tarjetas de crédito – gestores de tarjetas de crédito[37]

[36] Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 8 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 28 de Abril del 2019
[37] Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 9 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 28 de Abril del 2019

LAM Rank 2009	LAM Rank 2008	Country	Percentage 2009 LAM	Percentage 2008 LAM	Percentage 2009 Global
1	1	United States	40%	58%	23%
2	5	Brazil	13%	3%	4%
3	16	Mexico	5%	<1%	1%
4	4	Argentina	5%	3%	1%
5	2	China	4%	8%	12%
6	18	Costa Rica	3%	<1%	<1%
7	3	Chile	3%	3%	1%
8	7	Canada	2%	2%	2%
9	6	Spain	2%	2%	3%
10	10	Colombia	2%	1%	1%

Table 2. Top countries of attack origin targeting LAM
Source: Symantec

38

1.4 Seguridad Informática y Derechos Humanos

2.4.1 Protección de datos personales como un derecho humano

El acceso a internet últimamente se está considerando como un derecho humano, es así que tantas organizaciones internacionales y los gobiernos nacionales han comenzado a reconocer formalmente su importancia para la libertad de expresión e intercambio de información.[39]

La protección de datos es un tema de Política Criminal muy amplio Iñiaki nos menciona que “En sus niveles más altos de elaboración de la política criminal, en

[38] Anthony V. Teelucksingh, “Delitos en Internet a gran escala”, Edit. OEA, 2010, Pág. 10 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 29 de Abril del 2019
[39] Expok https://www.expoknews.com/ciberseguridad-derecho-humano/ Consulta 30 de Abril del 2019

cuanto a género, es como un universo mucho más complejo de la especie “Política penal”[40]

Este es un derecho que tenemos como ciudadanía, la protección de datos es algo que ya está estipulado en la Constitución Política de los Estados Unidos Mexicanos en el artículo 16

Los derechos humanos se basan en una postura jusnaturalista; hoy en día en que se está ejerciendo este tipo de acciones, también entra dentro de la nube, cuando alguien crea un perfil y tiene información personal, se convierte en un/una usuario/a activo/a de la red y los derechos humanos velan también por alguien que esté en situación de vulnerabilidad; alguien que se robe su identidad, sus datos, sus contraseñas, sus fotos o algún dato que esté en el ciberespacio.

Es casi imposible poder combatir esta situación, debido que siempre extraen fotos de perfiles, por lo general realizan publicidad y los llamados “memes” que es “Elemento cultural o de comportamiento que se transmite de persona a persona o de generación a generación”[41]. En la actualidad hay muchas formas de vulnerar los derechos humanos en la red; Ferrajoli nos decía que dentro de las garantías y derechos sociales “«derechos sociales»: entendiendo por tal expresión, como se ha dicho, los derechos a prestaciones públicas positivas”[42] por ejemplo, en el caso del ámbito bancario, muchos hackers se roban la información, principalmente contraseñas y usuarios, para poder acceder a las cuentas y poder extraer el dinero, se hacen transferencias.

Zafaroni nos habla de algo muy interesante en su “Tratado de Derecho Penal” en la sección de victimizaste y el ejercicio del poder. Constantemente son violentados los derechos a la protección de datos personales; es decir que cada vez que se desarrolla un Ciberataque hay un colectivo de víctimas, se ejerce la violencia al momento de verse una lógica represora y se pide el reconocimiento del derecho, no obstante, tan sólo un ataque cibernético se arrojan muchas víctimas, las cuales es

[40] Iñiaki Rivera Raúl, “Criminología y Ciencias Penales” Edit. Anthropos, España, 2005, Pág. 153
[41] Lexico Oxford, “Diccionario de Inglés y Español https://es.oxforddictionaries.com/definicion/meme Consulta 30 de Abril del 2019
[42] Ferrajoli Luigi “Derechos y Garantías”, Edit. Trotta, 2004, Pág. 108

complicado poder llevar un procedimiento por cada persona. Supongamos que se hace un robo bancario de ciertas personas por vía plataforma informática; la victimización puede ser masiva ya que se afectan a muchas personas, en diferente posición geográfica.

Raúl Zafaroni nos propone que "Las agencias políticas pueden resolver esos conflictos mediante la habilitación de una coacción estatal que impida el ejercicio de ese poder arbitrario (coacción administrativa directa) o que obligue a quien lo ejerza a reparar o restituir (coacción reparadora civil)".[43] Al momento que se da el conflicto hay un reconocimiento del derecho, hay una habilitación de una acción estatal, es decir que hay una coacción reparadora civil, se ejerce la reparación, hay una homogenización y se puede detectar la criminalización primaria, en el cual se reconoce el status de la víctima.

El ejercicio de poder se da cuando hay violencia confirmada, es decir estamos hablado de la victimización secundaria, la víctima puede hacer uso de la privatización de la justicia, se apoya de las agencias, hay una orden particular.

Después las agencias policiales -"Policía Cibernética"- en el caso de los delitos informáticos ¿Existe una polarización de la seguridad? Si la respuesta es cierta hay una estratificación social de la vulnerabilidad victimizaste, que esta puede ir orientada a la niñez, jóvenes, personas de la tercera edad, mujeres muy probablemente de zonas carenciadas; aunque en internet todas las personas pueden ser víctimas, la mayoría de las víctimas son personas carentes de recursos y sin educación ¿Cuántas jóvenes son engañadas por las redes sociales y jamás vuelven a casa? ¿Cuántos personas son vulnerables al dar fechas de nacimiento o algún tipo de dato y con eso intentar vulnerar la identidad de las personas? Al hablar de la polarización de la sociedad, estamos hablando de que si no la hay no se puede hablar de un "Desarrollo Humano", es decir que hay una polarización de la riqueza y por lo tanto se orienta a la criminalización. Zafaroni no decía que la polarización de la seguridad crea una estratificación social de la vulnerabilidad victimizante, cuyo

[43] Zaffaroni, Raul, "Derecho Penal", Buenos Aires, Edit. Ediar, 1973 Pág. 14

efecto es dejar más expuestas a las zonas urbanas con menor rentabilidad".[44] Al no tener una polarización de la seguridad definida, y no tener identificado a las victimas estas caen en la criminalización, es decir que para el "Estado de Derecho" esto causa un efecto político peligroso.

¿El acceso a Internet es un derecho?

Para Vinton Cerf, conocido como el "padre del Internet", la tecnología en sí misma no es un derecho, **sino un medio a través del cual se pueden ejercer los derechos.[45]**

¿Qué relación puede tener el Derecho Informático con los Derechos humanos?

La relación que"existe a través del Derecho Informático es la regulación jurídica que apoya el buen funcionamiento de los órganos jurisdiccionales"

2.4.2 Primer Principio de la Estrategia de ciberseguridad

Por la necesidad de poder atender este problema de la inseguridad en el ciber espacio, se tuvo que generar principios, basados en la protección de las personas:

"Perspectiva de derechos humanos. Contemplar en las diferentes acciones en materia de ciberseguridad la promoción, respeto y cumplimiento de los derechos humanos; entre otros, la libertad de expresión, el acceso a la información, el respeto a la vida privada, la protección de datos personales, la salud, educación y trabajo"[46]

En el Artículo 19 de la Declaración Universal de los Derechos Humanos incluye protecciones a la libertad de expresión, comunicación y acceso a la información.

---

[44] Zaffaroni, Raul, "Derecho Penal", Buenos Aires, Edit. Ediar, 1973 Pág. 15

[45] Expok, "Comunicaciones de Sustentabilidad", https://www.expoknews.com/ciberseguridad-derecho-humano/ Consulta 20 de Mayo del 2019

[46] SEGOB, "Estrategia de Ciberseguridad", 2018 https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf Consulta 29 de Mayo del 2019

En el Artículo 3 establece que “Toda persona tiene derecho a la vida, a la libertad y a su seguridad.

En 2013, la propia Asamblea General de la ONU, el organismo rector general de la organización, integrado por representantes de todos los países miembros, votó para confirmar el “derecho a la privacidad en la era digital” de las personas. A raíz de revelaciones sobre el espionaje electrónico estadounidense en todo el mundo, el documento también respaldó la importancia de proteger la privacidad y la libertad de expresión en línea. Finalmente, en noviembre del 2015, el G-20, un grupo de naciones en la cual se encuentran las economías más grandes del mundo también respaldó esta idea de privacidad, “incluso en el contexto de las comunicaciones digitales”.

CAPÍTULO II

2.1 Derecho Informático

2.1.1 Formas de Información y Comunicación

La Tecnología cambia el escenario de la vida cotidiana de las personas, es muy frecuente que los ciudadanos se adapten a las innovaciones, el Derecho y la Política Criminal van de la mano de estos cambios, modificando su modo de aplicación.

Hoy en día el sistema judicial opera bajo la innovación, los procedimientos son llevados a cabo de forma regular con la finalidad de prestar un buen servicio a los defensores y las partes las cuales persiguen un interés en común.

Hay instancias judiciales las cuales ya están operando de forma puntual, funcionan con base a plataformas electrónicas, páginas web, uso de datos por la red, firmas digitales, correo electrónico, juicios en línea y video conferencias. La indagación manejada está cambiando de forma contaste y requiere de un control que le permita poder tener seguridad y confiabilidad.

La información y la comunicación no pueden ser violadas ni mucho menos manipuladas. Los índices de seguridad informática han tenido la necesidad de crear diferentes formas para poder proteger los “datos”, por ello se ha creado figuras que protejan estos intereses. Se ha implementado una Estrategia de Política Criminal, representada en una Estrategia de ciberseguridad para mantener a salvo las bases de datos en la nube.

México está todavía en vías de crear una cultura de las Tecnologías de la Información y es muy complicado en ocasiones poder interpretar y adaptarse al nuevo concepto de la nube; las instituciones mexicanas tendrán que enfocarse en acoplarse a la nueva industria debido a que el manejo de los procesos será mejor operados.

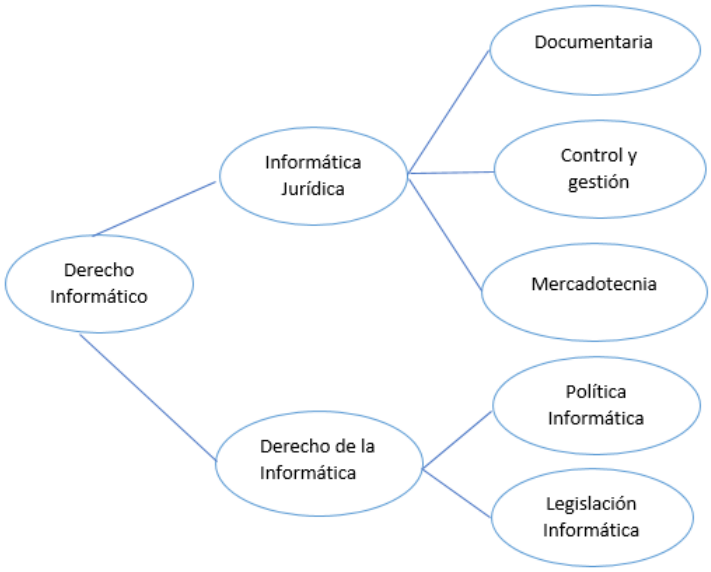
2.1.2 Concepto y Clasificación del Derecho Informático

Dentro del escenario jurídico es muy importante en tiempos de la era tecnológica, hacer una clasificación de todas las ramas que tiene que ver con el derecho y la información en la nube.

El escenario informático que ayuda a la mejora de los procesos sociales influye mucho en la rama jurídica, su identidad se deba ver en el momento que se aplican procedimientos en los que se involucra mucho la protección de datos personales.

La dogmática jurídica permite que el positivismo científico se generalice y se pueda involucrar en casi todas las ramas de conocimiento, por lo tanto, el modo de ver la realidad es distinta; antes los documentos para los procedimientos se manejaban sólo en papel y ahora se puede ver que se puede hacer uso de datos digitales los cuales ahorran tiempo, espacio y sobre todo se aumenta la efectividad.

Julio Téllez nos propone un esquema respecto a la clasificación de Derecho Informático.[47]



[47] Téllez Valdés Julio, Derecho Informático, Edit. MC Graw Hill, Edición 2018, Pág. 20

2.1.3 Concepto y Clasificación de la Informática Jurídica

Según Julio Téllez menciona que el Derecho Informático es: "es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".[48]

En la era de la informática jurídica los escenarios cambian y se establecen nuevas normas que van de la mano de la era digital. La digitalización de documento y el manejo de datos en la red, compromete al sistema jurídico a manejarse de forma más eficiente y por ello se establecen clasificaciones importantes que contribuyen a argumentar su contenido.

En el séptimo arte a menudo vemos que hay un futuro en dónde las máquinas ayudan al ser humano a completar tareas, el escenario positivista del derecho nos dice que la norma es eficiente cuando se cumple y que se aplica para el orden, en esta época moderna la informática jurídica "es la última instancia, del empleo de las computadoras en el ámbito jurídico"[49]

Otra definición de Informática jurídica nos la dice Téllez "cómo la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la informática general, aplicables a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dice recuperación"[50]

[48] Téllez Valdés Julio, Derecho Informático, México, MC Graw Hill, 2018, Pág. 13 Ibid
[49] Téllez Valdés Julio, Derecho Informático, México, MC Graw Hill, 2018, Pág. 19 Ibidem
[50] Téllez Valdés Julio, Derecho Informático, México, MC Graw Hill, 2018, Pág. 19 Idem

2.2 Legislación Nacional

2.1.4 Constitución Política de los Estados Unidos Mexicanos y relación con el Derecho Informático

Para partir este análisis es importante mencionar que el Artículo 6 nos habla del ataque a la vida moral, la vida privada y los derechos de los terceros, por ello cabe mencionar que la tecnología se ha caracterizado por arrojar víctimas del robo y extracción de datos personales. Un ejemplo claro es cuando se afecta la moral de alguien al momento de que se difama por redes sociales a partir de sus imágenes, un caso es cuando alguien de fama internacional tiene muchos problemas con su figura pública y contantemente es víctima de insultos y morbo ante la sociedad. El artículo constitucional nos dice que sólo se puede consumar una inquisición judicial cuando se perturbe el orden público, por ellos podemos argumentar que definitivamente la imagen de esta persona fue dañada, igual que la de su familia.

Hoy en día por el ciberespacio nos da muchos beneficios, no obstante, se crean nuevos perfiles de criminalidad y la ley apenas está revisando como poder atender este problema.

Hay otro artículo de nuestra carta magna que habla con respecto a la libertad de expresión. El artículo 7 nos dice que es inviolable la libertad de difundir opiniones, información e ideas, a través de cualquier medio. Este artículo es un punto a favor para los que actúan de forma inadecuada en el ciberespacio. Por ejemplo, las redes sociales se hace la difusión muchas veces de información confidencial, a través de foros de discusión se hace preguntas a los propios usuarios, logrando que terceros puedan conocer la vida pública.

Tomando en cuenta esto de la libertad de expresión, se puede ver que aplicado al sector financiero es muy violado, según el SAT “unos 490 mexicanos tienen adeudos fiscales por datos robados”

En una investigación del periódico “Capital” “Una cuenta bancaria abierta en nombre de una estudiante originaria de Nayarit recibió en 2009 una serie de depósitos que

sumaron 800 millones de pesos. La cifra no correspondía al monto de una herencia, tampoco a un premio, la verdad es que se trata del mayor robo de identidad registrado en México"[51]

La nota menciona que "La joven, quien no puede ser identificada debido a que así lo prescribe el Código Fiscal de la Federación, empezó a vivir una pesadilla. Debido a las multimillonarias cantidades depositadas, la cuenta llamó la atención del Servicio de Administración Tributaria (SAT), toda vez que la titular ni siquiera estaba dada de alta en el Registro Federal de Contribuyentes" [52]

Es evidente que cualquier civil puede ser vulnerable, cada vez que revisa un correo electrónico uno puede ser víctima al recibir mensaje los cuales pueden comprometer-por error- a brindar datos personales. Los datos de las personas son completamente un foco para la ciberdelincuencia organizada.

2.2.2 Código Penal Federal

El Código nos especifica respecto al acceso ilícito de sistemas y equipos de informática, por lo general todos los individuos de la sociedad tienen acceso a muchos dispositivos, equipos informáticos con diferentes especificaciones, la vulnerabilidad de que las personas tengan equipos es una realidad que no se puede detener. El articulo 211 bis1 nos habla respecto al uso indebido de equipos informáticos, que estén protegidos bajo un mecanismo de seguridad, no obstante, tomando en cuenta de que en México no se tiene una cultura de seguridad informática, dentro de la esta ley existen lagunas, si en México y en las organizaciones muchas veces no hay "seguridad informática" ¿Si no hay un

[51] Palacios Surya, "Capital" Casos más graves del robo de identidad" Edit. Capital, 19 de Julio del 2017 https://www.capitalmexico.com.mx/especial/casos-mas-graves-del-robo-de-identidad-sat-adeudos-fiscales/ Consulta 1 de agosto del 2019
[52] Palacios Surya, "Capital" Casos más graves del robo de identidad" Edit. Capital, 19 de Julio del 2017 https://www.capitalmexico.com.mx/especial/casos-mas-graves-del-robo-de-identidad-sat-adeudos-fiscales/ Consulta 5 de agosto del 2019

mecanismo de control que pueda ser violado, como se espera que se pueda configurar un delito?

Por otro lado, el Artículo 211 bis 2 nos habla respecto a la violación de un mecanismo de seguridad, con la diferencia de que es equipos informáticos del Estado.

El artículo ya se concentra en bienes del Estado y nos habla respecto a la penalización de la modificación de datos, obstrucción y pérdidas de información. Esta última tiene una penalización de uno a cuatro años de prisión y de doscientos a seiscientos días de multa. Mientras que por el copiado de información se impondrá de seis meses a dos años de prisión y de cien trescientos días de multa.

2.2.3 Código Penal de Sinaloa

Hay varios Estados que evolucionan y atienden a las necesidades, por ello Sinaloa ha asumido una postura enérgica en materia de delitos informáticos. En el artículo 217 se refleja al momento de indicar que comete un delito, aquella persona que entre a una base de datos, sistemas de computadoras o red de computadoras o a cualquier parte de la misma, con el propósito de diseñar, ejecutar o alterar un esquema o artificio, con el fin de defraudar, obtener dinero, bienes o información.

De la misma forma nos menciona que comete un delito aquel que Intercepte, interfiera, reciba, use, altere, dañe o destruya un soporte lógico o programa de computadora o los datos contenidos en la misma, en la base, sistema o red. Al responsable de delito informático se le impondrá una pena de seis meses a dos años de prisión y de noventa a trescientos días multa.

Debido a que en el Estado mencionado se cometen delitos relacionados con el robo de identidad se han adoptado estas medidas y su Código Penal es diferente. Según una investigación del periódico “Debate” del Estado de Sinaloa “Se ejerce una nueva

modalidad de fraude que ha tomado auge en los últimos años debido a que empresas no registradas instalan módulos en lugares públicos y ofrecen servicios financieros para obtener los datos personales de los usuarios, reveló la subdelegada de la Comisión Nacional para la Protección y la Defensa de los Usuarios de Servicios Financieros (Condusef), María Guadalupe Espinoza"[53]

El escenario es muy claro al momento de señalar este foco de la república mexicana como uno de los más difíciles en materias de delincuencia organizada. Es claro que la Ciberdelincuencia Organizada está también rebasando y generando una problemática que ha obligado-como ya hemos mencionado- a adoptar medidas que den frente.

2.2.4 Código Civil

El artículo 1916 del Código Civil para el Distrito Federal nos menciona que "por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien, en la consideración que de sí misma tienen los demás y que se presume el daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas."[54] Para tratar el asunto del robo de datos personales y la vulneración de la libertad de poder tener un perfil en la red, en dónde se publican fotos y datos específicos. El código civil también nos habla de "preservar los derechos de la personalidad, es decir, garantizar a la persona el goce de sus facultades y el respeto al desenvolvimiento de su personalidad física y moral, mediante la protección de los valores intrínsecos del ser humano, esto es, aquellos bienes propios de él (la paz, la tranquilidad del espíritu, la libertad individual, la integridad física, el honor, la reputación, etcétera) que tienen un valor notable en la

[53] Andrade Edith, "Detectan nueva modalidad de fraude en Sinaloa" Edit. Debate, 2 de Octubre del 2018 https://www.debate.com.mx/sinaloa/nuevo-fraude-sinaloa-robo-de-datos-empresas-falsas-modulos-publicos-20181002-0023.html Consulta 8 de agosto del 2019
[54] Código Civil del Distrito Federal http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/180/180163.pdf Consulta 10 de agosto del 2019

vida del hombre. Por tanto, no es posible considerar que se puede causar daño moral a las personas jurídicas, que por ser entes creados por ficción de la ley para la realización de fines colectivos no son titulares del derecho subjetivo tutelado por el citado precepto, esto es, como carecen de los citados valores intrínsecos, que sólo las personas físicas poseen en atención a su individualidad o intimidad, tampoco son titulares de la acción para reclamar la reparación de su afectación."[55]

2.2.5 Ley Federal de Derechos de Autor

Esta ley da protección de los derechos de los autores, de los artistas intérpretes o ejecutantes, así como de los editores, de los productores y de los organismos de radiodifusión, en relación con sus obras literarias o artísticas en todas sus manifestaciones, sus interpretaciones o ejecuciones, sus ediciones, sus fonogramas o videogramas, sus emisiones, así como de los otros derechos de propiedad intelectual, esto se fundamenta en el artículo 1.

Mientras tanto en el Artículo 13 se menciona que:

> "Los derechos de autor a que se refiere esta ley se reconocen respecto de las obras [56]de las siguientes ramas:
>
> a) Literaria, esta se refiere a cualquier creación escrita, por ejemplo, una obra poética, muchos autores se quejan por las copias desmedidas que se hacen de las obras literarias, sobre todo las imitaciones.
> b) Musical, con o sin letra, este problema es atendido
> c) Dramática;
> d) Danza;
> e) Pictórica o de dibujo;

[55] Código Civil del Distrito Federal http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/180/180163.pdf 13 de agosto del 2019
[56] Ley Federal del Derecho de Autor. http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf 15 de agosto del 2019

f) Escultórica y de carácter plástico

> Por otro lado, tenemos al artículo 112, el cual nos menciona que "queda prohibida la importación, fabricación, distribución y utilización de aparatos o la prestación de servicios destinados a eliminar la protección técnica de los programas de cómputo, de las transmisiones a través del espectro electromagnético y de redes de telecomunicaciones y de los programas de elementos electrónicos señalados en el artículo anterior."[57]
>
> El artículo 105 nos menciona que "el usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:
>
> I. Sea indispensable para la utilización del programa, o
>
> II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación."[58]

Por último, tenemos al Artículo 6 el cual nos habla del derecho patrimonial en el que se prohíbe la reproducción permanente o provisional del programa en todo o en parte, por cualquier medio y forma; esto significa que la piratería no ha respetado esta ley, claramente podemos ver que hay muchas discos compactos en el mercado en dónde se graba música y películas, evidentemente violentado los derechos del autor, ente otros delitos esta la traducción, la adaptación, el arreglo o cualquier otra modificación de un programa y la reproducción del programa resultante; muchas veces son alterados los materiales musicales, se adaptan para poder lucrar. Por otro lado, la forma de distribución del programa o de una copia del mismo, incluido

[57] http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf 16 de agosto del 2019
[58] http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf 16 de agosto del 2019

el alquiler, y la de compilación, los procesos para revertir la ingeniería de un programa de computación y el desembalaje.

2.2.5 Ley federal de Protección de Datos Personales

Esta ley entró en vigencia en el año 2007 y se hizo ante la demanda de la vulnerabilidad de datos sensibles para la ciudadanía, esta nos habla respecto a la protección de datos personales en manos de particulares, de la misma forma nos habla de su regulación del tratamiento legítimo para garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. La privacidad es lo que siempre se ha buscado, por ello las empresas sobre todo las privadas, hace políticas de privacidad de datos personales. A pesar de la ley se ha detectado extrañas anomalías en materia de robo de datos, muchos usuarios se quejan por los correos y llamadas que hacen personas desconocidas que aseguran ser parte de alguna institución bancaria. Según Paul Lara "Pocos Bancos detectan ciberataques con sistemas propios", "Los ataques exitosos en el país ya costaron 107 millones de dólares en recuperación ante incidentes a todas las instituciones, y se han afectado a 14.3 millones de usuarios, 31 por ciento del total.[59] Es claro con lo anterior de que se tiene cifras alarmantes las cuales se pueden combatir, siempre y cuando se pueda detectar el uso indebido de datos personales.

Por otro lado, el Artículo 2 también nos menciona lo referente a que son sujetos regulados los particulares sean personas físicas o morales de carácter privado que lleven a cabo el tratamiento de datos personales, con excepción de las sociedades de información crediticia en los supuestos de la Ley para Regular las Sociedades de Información Crediticia y demás disposiciones aplicables, y las personas que lleven a cabo la recolección y almacenamiento de datos persona. Si lo pensamos

[59] Paul Lara, "1 e cada 3 cliente, víctimas de hackers", Edit. Excélsior, 12 de Julio del 2009 Consulta 18 de agosto del 2019

este artículo por lo general es vulnerado, ya que hay varias instituciones bancarias que filtran información a terceros, por ejemplo según Ricardo Riquelme “Casi dos de cada 10 instituciones financieras que han sido víctimas de un ataque cibernético al menos una vez han vuelto a serlo por segunda ocasión en 2018, según consta en el informe de tendencias de ciberseguridad de Mandiant, M-Trends 2019, que además destaca que esta industria es la más investigada por ataques en los que los perpetradores permanecen por mucho tiempo en los sistemas de las compañías”[60] Esto significa que las instituciones Bancarias son más vulnerables al robo de datos personales.

También tenemos un el artículo 3 en la fracción VI, donde nos dice que los “datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquellos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual”[61]

2.3 Legislación Internacional (Organismos Internacionales)

2.3.1 Convenio de Budapest

El convenio fue celebrado en el 2001, “es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la

[60] Riquelme Rodrigo, “18% de instituciones financieras recibió ataques cibernéticos por segunda vez en 2018: Mandiant”, Edit. El Economista, 26 de Marzo del 2019. https://www.eleconomista.com.mx/tecnologia/18-de-instituciones-financieras-recibio-ataques-ciberneticos-por-segunda-vez-en-2018-Mandiant-20190326-0018.html Consulta 19 de agosto del 2019

[61] Ley Federal de Protección de datos personales en posesión de los particulares, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf Consulta 20 de agosto del 2019

armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones firmantes"[62]

Este convenio fue celebrado por el Consejo de Europa en Estrasburgo, con la participación activa de Canadá, Japón y China como estados observadores.

2.3.2 Protocolo Adicional a la Convención sobre el delito cibernético

El Protocolo exige a los Estados participantes penalizar la difusión de material racista y xenófobo por medio de sistemas informáticos, así como de las amenazas e insultos racistas y motivados por la xenofobia.

Su principal objetivo, que figura en el preámbulo, es aplicar una política penal común encaminada a la protección de la sociedad contra el cibercrimen, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

Los principales objetivos de este tratado son los siguientes:

1. La armonización de los elementos nacionales de derecho penal de fondo de infracciones y las disposiciones conectados al área de los delitos informáticos.
2. La prevención de los poderes procesales del derecho penal interno es necesaria para la investigación y el enjuiciamiento de esos delitos, así como otros delitos cometidos por medio de un sistema informático o pruebas en formato electrónico.
3. Establecimiento de un régimen rápido y eficaz de la cooperación internacional.

[62] Convenio de Budapest, 2001, https://www.oas.org/juridico/english/cyb_pry_convenio.pdf Consulta 20 de agosto del 2019

2.3.3 Pronunciamiento de la ONU de los crímenes por Internet

Por primera vez se habló del tema de crímenes en internet en el Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010. En este se habló respecto a que "los delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, el narcotráfico, la trata de niños con fines pornográficos y el acecho"[63]

El apartado anterior nos menciona sobre los delitos que son reconocidos por dichos organismos y que tiene que ver sobre todo con las conductas que se presentan en la Red para poder cometer acciones de cibercriminaliad.

Por otro lado, en el congreso se habló referente a "Los delincuentes cibernéticos que pueden pasar desapercibidos a través de las fronteras, ocultarse tras incontables «enlaces» o simplemente desvanecerse sin dejar ningún documento de rastro. Pueden despachar directamente las comunicaciones o esconder pruebas delictivas en «paraísos informáticos» -o sea, en países que carecen de leyes o experiencia para seguirles la pista"[64]

El problema es que los actos ilícitos se pueden llevar a cabo desde cualquier lugar, esto afecta mucho, debido a que el acto no se puede detectar, afectando los negocios sobre todo de los bancos, según la ONU ""El delito cibernético se ha convertido en un negocio que supera el billón de dólares anual producto del fraude cibernético, el robo de identidad y la pérdida de propiedad intelectual. Afecta

[63] Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010. https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml Consulta 22 de agosto del 2019

[64] Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010. https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml Consulta 22 de agosto del 2019

millones de personas alrededor del mundo, a innumerables empresas y a las empresas y a gobiernos de todas las naciones"[65]

2.3.4 Organización de Estados Americanos (OEA)

En el año 2017 México convocó a una comisión de expertos internacionales para compartir las mejores prácticas con las principales entidades mexicanas para mejorar las capacidades nacionales de seguridad cibernética en el país. La OEA respondió al llamado y se hicieron mesas de discusión en las que se discutieron "el estado actual de la seguridad cibernética en México y avanzar en la construcción y definición de un Marco Nacional de Seguridad Cibernética"[66]

Según la OEA "México está teniendo muchos incidentes de seguridad digital financiera, el costo es de 107 millones de dólares en recuperación y respuesta a ciberataques". [67]

La OEA en conjunto con la CNBV se centran en monitorear los ciberataques, "Los eventos de seguridad más comunes identificados en el 2018 fueron el código malicioso o malware, afectando a 56% de las entidades financieras mexicanas, seguido por *phishing* dirigido para tener accesos a sistemas, con impacto de 47% de total de los jugadores del sistema financiero. [68]

---

[65] Seguridad Cibernética, 12 de diciembre 2011, Nueva York, https://www.un.org/development/desa/es/news/intergovernmental-coordination/seguridad-cibernetica.html

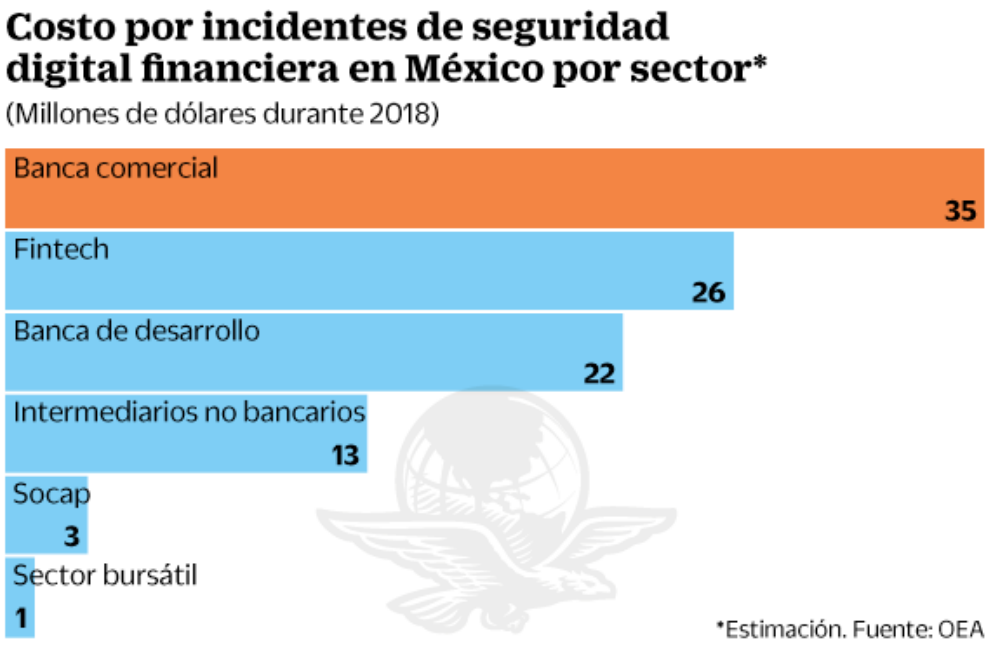
[66] http://www.oas.org/documents/spa/press/Recomendaciones-para-el-Desarrollo-de-la-Estrategia-Nacional-de-Ciberseguridad.pdf Consulta 23 de agosto del 2019

[67] Antonio Hernández "Costó 107 mmd recuperación por ciberataques, dice la OEA", Edit. El Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 23 de agosto del 2019

[68] Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 24 de agosto del 2019

En la misma nota se ofrece una estadística interesante de la OEA respecto a los incidentes:

Gráfica 1[69]



2.4. Marco Normativo Comparado en materia de Seguridad Informática

2.4.1 Ciberseguridad en la Unión Europea

La era digital es como "El lejano oeste", el ambiente es bárbaro, vulnerable a ataques, el campo es temeroso, se carece de seguridad, no hay muchas estrategias implementadas, las plataformas están vulnerables sin seguridad, varias bases de

[69] Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 25 de agosto del 2019

datos están cargadas en la red, el tener una computadora hoy en día es como tener un revolver en 1888.

La globalización ha obligado a que se acelere la búsqueda de soluciones a este problema, no obstante falta mucho por hacer. La UE ha logrado poner el tema sobre la mesa, gracias a esto, cuenta con la creación de la Agencia Europea de Seguridad de las redes y de la información (ENISA), la elaboración de una "Estrategia para una sociedad de la información segura" o el "Plan de Ciberseguridad de la Unión Europea".

El objetivo principal de la Agencia es el de reforzar las capacidades de la Unión Europea, sus Estados Miembros y las empresas en relación a la prevención, la reacción y la gestión de los problemas vinculados con la seguridad de las redes y la información. La ENISA también presta asistencia y asesoramiento a la Comisión y a los Estados de la UE cuando lo necesita, y se puede recurrir a ella para ayudar a la Comisión en los trabajos preparatorios de carácter técnico de actualización y desarrollo de la normativa comunitaria. La Agencia desarrolla una serie de tareas para poder llevar a cabo los objetivos anteriormente mencionados.[70]

¿Cuál es el Plan Nacional de Ciberseguridad de la Unión Europea? antecedentes Según cifras recientes, las amenazas digitales evolucionan con rapidez y los ciudadanos perciben la ciberdelincuencia como un grave peligro: los ataques con programas de secuestro de archivos han aumentado un 300 % desde 2015 y el impacto económico de la ciberdelincuencia se ha multiplicado por cinco entre 2013 y 2017, y todavía podría cuadruplicarse de aquí a 2019, según los estudios. El 87 % de los europeos consideran la ciberdelincuencia como un importante desafío para la seguridad interior de la UE. La Agenda Europea de Seguridad y la revisión intermedia de la Estrategia para el Mercado Único Digital guían la actividad de la Comisión en este ámbito, ya que exponen las principales medidas de refuerzo de la ciberseguridad. Las medidas que hoy se proponen complementan las normas en vigor y colman los resquicios que la evolución de la amenaza ha abierto desde la

[70] Estado de la Unión 2017 – Ciberseguridad: la Comisión intensifica la respuesta de la UE a los ciberataques, Edit. Comisión Europea 19 de septiembre del 2017

adopción de la Estrategia de Ciberseguridad de la UE de 2013, atendiendo con ello la prioridad esencial de garantizar la seguridad interior con arreglo a la Declaración y la Hoja de Ruta de Bratislava la cual fue una reunión informal de los veintisiete jefes de Estado o de gobierno el 16 de septiembre de 2016 presidido por Donald Tusk.

Existe un Plan Nacional de Ciberseguridad, se denomina “Un ciberespacio abierto, protegido y seguro”, y se encarga de dar una visión de conjunto sobre cómo la UE debe prevenir y resolver mejor las perturbaciones en la red y los ciberataques. El Plan tiene como finalidad promover e impulsar los valores europeos de libertad y democracia y velar por un crecimiento seguro de la economía digital. La meta es que, a partir del Plan, se de libertad y apertura promoviendo sus valores esenciales y los derechos fundamentales en el ciberespacio.

Según la ENISA nos menciona que:

> “Los incidentes de seguridad cibernética en un país pueden tener un impacto a través de las fronteras nacionales. El incidente de Diginotar muestra cómo los incidentes nacionales pueden tener un impacto transfronterizo. Esto significa que, para mejorar la seguridad en toda la UE, todos los países deben acordar principios comunes. Además, los proveedores de servicios a menudo operan en todos los países de la UE, especialmente las empresas de telecomunicaciones y los proveedores de servicios de Internet. Es engorroso para estos proveedores tener que adaptar sus sistemas a diferentes requisitos nacionales. Una legislación armonizada en toda la UE evita las fronteras digitales y permite un campo de juego nivelado para los proveedores en todo el mercado de la UE.”[71]

[71]Agencia de la Unión Europea para la Seguridad Cibernética, https://www.enisa.europa.eu/topics/incident-reporting Consulta 30 de agosto del 2019

2.4.1.1 España

En Europa se tiene un avance muy interesante en delitos, su impacto en las instituciones ha logrado de varios organismos atiendan el problema, elaborando protocolos de alta seriedad. España tiene un importante papel ya que su catálogo de delitos es muy amplio y se sanciona la destrucción, espionaje y divulgación.

Según el Departamento de Seguridad Nacional de España nos dice que "Un ciberespacio seguro es posiblemente el mayor desafío al que se enfrenta España desde el punto de vista de la seguridad por lo que los riesgos y las amenazas que se ciernen en él requieren una respuesta oportuna, proporcionada, eficaz y coordinada que garantice la libre y segura utilización del mismo por el conjunto de la sociedad española"[72]

El Gobierno español implemento en el 2013 una Estrategia de Ciber Seguridad Nacional la cual tiene los siguientes puntos específicos:

a) para las Administraciones Públicas, garantizar que los Sistemas de Información y Telecomunicaciones utilizadas por estas poseen el adecuado nivel de seguridad y resiliencia;
b) para las empresas y las infraestructuras críticas, impulsar la seguridad y la resiliencia de las redes y los sistemas de información usados por el sector empresarial en general y los operadores de infraestructuras críticas en particular;
c) en el ámbito judicial y policial, potenciar las capacidades de prevención, detección, respuesta, investigación y coordinación
d) frente a las actividades del terrorismo y la delincuencia en el ciberespacio;

[72] Ciberseguridad https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad Consulta 1 de Septiembre del 2019

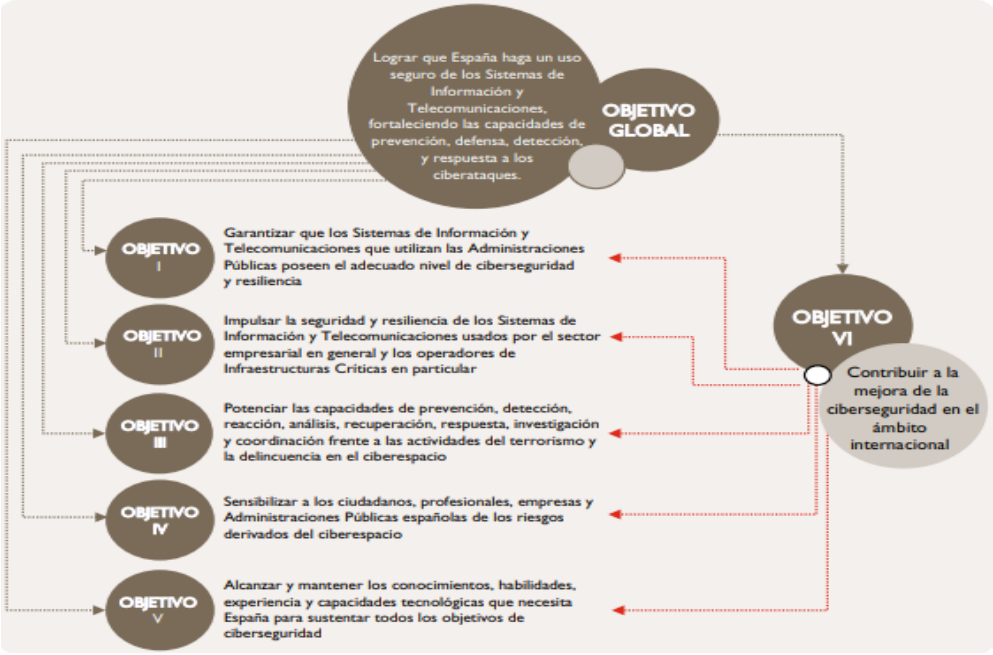
e) en materia de sensibilización, concienciar a los ciudadanos, profesionales, empresas y Administraciones Públicas españolas de los riesgos derivados del ciberespacio;

f) en capacitación, alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de la ciberseguridad;

g) en lo que se refiere a la colaboración internacional, contribuir en la mejora de la ciberseguridad, apoyando el desarrollo de una política de ciberseguridad coordinada en la Unión Europea y en las organizaciones internacionales, así como colaborar en la capacitación de Estados que lo necesiten a través de la política de cooperación al desarrollo.[73]

Esta estrategia española tiene las siguientes líneas de acción

Figura 2[74] Objetivo Global de la Ciberseguridad.



[73] Sistema Nacional de Seguridad, https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad Consulta 3 de Septiembre del 2019

[74] Estrategia Nacional de Ciberseguridad https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf Consulta 3 de Septiembre del 2019

2.4.2 Estados Unidos

La Unión Americana cuenta con un sistema de defensa de nueva generación su particular liderazgo en tecnologías de la información ha logrado que sus aspectos, sociales, políticos y económicos cambien de forma importante para poder orientar la mayoría de sus gestiones por vía de “Ciencia de Datos”. Desde 1986 este país cuenta con un Marco Legal referente a la defensa de delitos informáticos, esta era denominada a Federal Abuse FraudAct.

En 1994 se realizó otra ley, esta vez haciendo referencia a los ataques informáticos los cuales se orientaba a quienes creaban virus haciendo una clasificación:

a) Los que intencionalmente causan daño por la transmisión de un virus
b) Los que transmiten de manera imprudencial y la sanción es de una multa y hasta un año de prisión.
   Ley de Fraude y abuso Informático en EUA

   Sanciones Penales:

   (1) haber accedido a sabiendas a una computadora sin autorización o exceder el acceso autorizado, y mediante dicha conducta haber obtenido información que ha sido determinada por el Gobierno de los Estados Unidos de conformidad con una orden ejecutiva o estatuto para exigir protección contra la divulgación no autorizada por razones nacionales defensa o relaciones exteriores, o cualquier información restringida, como se define en el párrafo y. de la sección 11 de la Ley de Energía Atómica de 1954, con razones para creer que dicha información así obtenida podría usarse para perjudicar a los Estados Unidos, o en beneficio de cualquier nación extranjera que comunique, entregue, transmita o haga que comunicado, entregado o transmitido, o intentos de comunicarse, entregar, transmitir o hacer que se comunique, entregue o transmita lo mismo a cualquier persona que no tenga derecho a recibirlo,

(2) accede intencionalmente a una computadora sin autorización o excede el acceso autorizado, y de ese modo obtiene:

a) información contenida en un registro financiero de una institución financiera, o de un emisor de tarjeta como se define en la sección 1602 (n) [1] del título 15, o contenida en un archivo de una agencia de informes del consumidor sobre un consumidor, como tal los términos se definen en la Ley de Informes de Crédito Justos (15 USC 1681 et seq.);
b) información de cualquier departamento o agencia de los Estados Unidos; o
c) información de cualquier computadora protegida;

(3) intencionalmente, sin autorización para acceder a cualquier computadora no pública de un departamento o agencia de los Estados Unidos, accede a dicha computadora de ese departamento o agencia que es exclusivamente para uso del Gobierno de los Estados Unidos o, en el caso de una computadora no exclusiva para dicho uso, es utilizada por o para el Gobierno de los Estados Unidos y dicha conducta afecta ese uso por o para el Gobierno de los Estados Unidos;

(4) a sabiendas y con la intención de defraudar, accede a una computadora protegida sin autorización, o excede el acceso autorizado, y por medio de tal conducta fomenta el fraude previsto y obtiene algo de valor, a menos que el objeto del fraude y lo obtenido consista solo del uso de la computadora y el valor de dicho uso no es más de $ 5,000 en un período de 1 año;

(5)a sabiendas causa la transmisión de un programa, información, código o comando, y como resultado de tal conducta, intencionalmente causa daños sin autorización a una computadora protegida;

a) accede intencionalmente a una computadora protegida sin autorización y, como resultado de dicha conducta, causa daños de manera imprudente; o

b) accede intencionalmente a una computadora protegida sin autorización, y como resultado de tal conducta, causa daños y pérdidas.

(6) a sabiendas y con la intención de defraudar el tráfico (como se define en la sección 1029) en cualquier contraseña o información similar a través de la cual se pueda acceder a una computadora sin autorización, si:

a) dicho tráfico afecta el comercio interestatal o extranjero; o
b) dicha computadora es utilizada por o para el Gobierno de los Estados Unidos;

(7) con la intención de extorsionar a cualquier persona cualquier dinero u otra cosa de valor, transmite en el comercio interestatal o extranjero cualquier comunicación que contenga:

a) amenaza de causar daños a una computadora protegida;
b) amenaza de obtener información de una computadora protegida sin autorización o en exceso de autorización o de perjudicar la confidencialidad de la información obtenida de una computadora protegida sin autorización o al exceder el acceso autorizado; o
c) exigir o solicitar dinero u otra cosa de valor en relación con el daño a una computadora protegida, donde dicho daño fue causado para facilitar la extorsión[75]

Estados Unidos en la actualidad es vulnerable a ataques cibernéticos a pesar de esto sigue siendo el líder en la cibernética, cuenta con el mayor frente de ciberseguridad del mundo. Su poder cibernético es tan potente que ha prevenido ataques y elaborando ataques en contra de sus enemigos. La Unión Americana ha tenido Oportunidades y Debilidades. Dentro de sus ***Oportunidades*** fue el ataque que realizó a Irán en el 2010 en el que las instalaciones nucleares persas fueron vulneradas que por su peligrosidad fue el ataque más grande de la historia. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias,

[75] Legal Information Institute, 18 U.S. Code § 1030.Fraud and related activity in connection with computers https://www.law.cornell.edu/uscode/text/18/1030 Consulta 8 de Octubre del 2019

se vieron afectados por un virus de una potencia sin precedentes, denominado Stuxnet.

El objetivo de EUA era retrasar los procesos de elaboración de armas nucleares.

Se dieron cuenta hasta que “los inspectores de la Agencia Internacional de Energía Atómica que visitaban una planta nuclear en Natanz, Irán, notaron con desconcierto que las centrifugadoras usadas para enriquecer uranio estaban fallando. Curiosamente, los técnicos iraníes que reemplazaban las máquinas también parecían asombrados”. [76]

Las autoridades iraníes estaban completamente en estado de alerta al ver esta situación, su seguridad estaba comprometida. “El fenómeno se repitió cinco meses después en el país, pero esta vez los expertos pudieron detectar la causa: un malicioso virus informático. El "gusano" - ahora conocido como Stuxnet - tomó el control de 1.000 máquinas que participaban en la producción de materiales nucleares y les dio instrucciones de autodestruirse.”[77]

Fue la primera vez que un ataque cibernético logró dañar la infraestructura del "mundo real".

Tras el nivel de efectividad de los Hakcers estadounidenses la respuesta fue inmediata y varios “Estados enemigos respondieron de la misma forma, Irán, Rusia, Corea del Norte y varios países. Esto provocó que desde el 2015 EUA elaborara una ley de ciberseguridad destinada a luchar contra ataques en el ciberespacio mediante la compartición de datos entre empresas privadas y el Gobierno Federal, después de que durante los últimos meses se produjese una oleada de ataques cibernéticos.

[76] Wonder. Edit. BBC, 2010
https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
Consulta 10 de Octubre del 2019
[77] Wonder. Edit. BBC, 2010
https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet
Consulta 10 de Octubre del 2019

“La Ley de Compartición de Información de Ciberseguridad (CISA por sus siglas en inglés) aumenta la protección gubernamental a aquellas empresas que voluntariamente decidan compartir con el Gobierno federal aquellos datos que consideren que podrían constituir ciber amenazas”. [78]

“El Senado aprobó la medida con apoyo bipartidista (74 votos a favor y 21 en contra), y ahora el texto deberá conciliarse con otros dos proyectos de ley similares que aprobó la Cámara de Representantes a principios de año para que la ley pueda ser promulgada”[79]

Por otro lado, haciendo una clasificación de las ***debilidades***, recientemente en nuestros días Estados Unidos sufrió una serie de ataques informáticos debido a la revelación de los documentos Wiki Leas, “los cuales son una organización mediática internacional sin ánimo de lucro que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes.”[80]

Este sitio fue fundado en el 2006 por Julian Assange y se revelaron documentos secretos que hicieron vulnerables a EUA.

Los ciberataques se pueden dar de diferentes formas e incluso con un apoyo físico. “La soldado Manning, entonces Bradley Manning antes de su operación de cambio de sexo, llegó a filtrar al portal del 'hacker' y activista Julian Assange más de 700.000 archivos confidenciales. Su acción puso en jaque al Gobierno de EEUU y convirtió

[78] “El senado de Estados Unidos aprueba una Ley de Ciberseguridad” Edit. El Mundo. https://www.elmundo.es/internacional/2015/10/28/5630219e46163f29348b4595.html Consulta 11 de Noviembre del 2019

[79] El senado de Estados Unidos aprueba una Ley de Ciberseguridad” Edit. El Mundo. https://www.elmundo.es/internacional/2015/10/28/5630219e46163f29348b4595.html Consulta 17 de Noviembre del 2019

[80] Navarro Fernando, Wikileaks: cómo destapar escándalos en Internet, Edit. El país, https://elpais.com/internacional/2010/07/26/actualidad/1280095206_850215.html Consulta 22 de Noviembre del 2019

en relevantes a Assange y Wikileaks, que pasó de ser una web minoritaria a convertirse en uno de los mayores temores de la inteligencia estadounidense"[81]

Este evento ocasionó mucho caos en el gobierno y muchas cosas cambiaron, tanto en el ámbito político, económico y social; su impacto fue de grandes proporciones debido a la cantidad de datos subidos, aproximadamente 470.000 registros de las guerras de Irak y Afganistán, 250.000 cables diplomáticos del Departamento de Estado y otros documentos clasificados que dejaron en evidencia a la diplomacia estadounidense.

CAPÍTULO III

3.1 Ciberataques a Bancos Internacionales

Las instituciones crediticias han tenido problemas con respecto a la violación de sus sistemas, a medida que avanza la tecnología la vulnerabilidad en la red aumenta. Las empresas necesitan con urgencia un nuevo modelo el cual pueda ayudar a soportar la cantidad de accesos ilícitos a sus datos, mejor conocidos como ciberataques.

Una forma de poder hacer ciber ataques es esconderse "en los rincones oscuros de internet, ahora también aprovechan las redes sociales. Los investigadores de Talos, el grupo de investigación y seguridad de Cisco descubrió a varios grupos criminales que operan en Facebook con nombres bastante obvio como "spam profesional" o "spam y piratas informáticos". Usan la red social para contactar a otros piratas

[81] Reynolds Michel, Así fue el 'caso Wikileaks', Edit. P Internacional, https://www.elperiodico.com/es/internacional/20170118/asi-fue-el-caso-wikileaks-5750289 Consulta 23 de Noviembre del 2019

informáticos, compartir y vender herramientas o datos robados y, en algunos casos, estafarse entre ellos"[82]

A nivel internacional se han buscado soluciones, no obstante, se ha convertido en una guerra en internet. Principalmente las instituciones más afectadas son el sector bancario, con pérdidas millonarias.

Muchas instituciones públicas y privadas se han visto vulneradas, es decir que son constantemente atacadas bajo personalidades que en realidad no se pueden detectar ni ver.

Más adelante veremos algunas de las características de los ataques cibernéticos a nivel internacional, no obstante, es importante mencionar que esto le compete a una Política Criminal ya que se perfila como un problema de gran envergadura.

3.1.1 Estonia y su Banca Electrónica

La guerra fría arrojó muchas batallas entre las diferentes naciones; y hasta nuestros tiempos se lidia una guerra de ideas y resentimientos.

Es el ejemplo entre las naciones el báltico y Rusia, las cuales todavía tienen una lucha ideológica. Tomando como perfil a los bancos, se puede mencionar que hubo un caso muy sonado en Europa del Este. Después de la caída de la Unión Soviética varias repúblicas se convirtieron en países, uno de ellos es Estonia, el cual se alineo con la OTAN y permitió que un nuevo modelo entrara en sus fronteras. Las políticas estadounidenses se introdujeron en países bálticos e implementaron una era de progreso.

[82] Ciber Ataques en el 2020 se materializan; expertos advierten auge en hackeos, Aura Hernández, Excelsior, 11 de abril del 2020 https://www.excelsior.com.mx/hacker/ciberataques-en-2020-se-materializaran-expertos-advierten-auge-en- Consulta 12 de Febrero del 2020 hackeos/1355817?fbclid=IwAR1Ks_7qewpVBM2JG4Es4PWUnxfiMFrios69yCLFLpFzg3ODo0u1iLHx0hE Consulta 12 de Febrero del 2020

Estonia en la actualidad es un país de primera línea debido a que cuenta con una industria moderna y aplica un proyecto sectorial muy avanzado en materia tecnológica; no obstante, fue víctima de un ataque cibernético directo a su banca electrónica.

Los intereses culturales siempre son la base de todos los pueblos, principalmente cuando se toca el sentimiento ideológico y la imagen que representa. Fue el caso de un "soldado de Bronce, que fue instalado por las autoridades soviéticas en 1947, originalmente se llamó "Monumento para los libertadores de Tallin". En el 2007 el gobierno estonio tomo la decisión de llevar la estatua a un cementerio, lo que represento algo muy significativo para la minoría rusa. "Las Manifestaciones se intensificaron debido a noticas falsas en medios rusos que aseguraban que las estatuas y cercanas tumbas militares soviéticos estaban siendo destruidas"[83]

A partir de estas acciones la población rusa tomo resentimiento y el 27 de abril – después de muchos disturbios de 156 heridos y más de 1000 detenidos-Estonia fue víctima de un ciberataque en sus principales instituciones gubernamentales.

Los ciberataques se concentraron principalmente en sitios web de Bancos, medios de prensa y organismos gubernamentales. Estas estancias fueron dañadas debido al exagerado tráfico de información que se enviaban en datos, los servicios colapsaron la Banca electrónica- la cual los estonios hacían pagos- fue neutralizada y prácticamente Hackeada.

"Redes de Robots informáticos-conocidos como botnets- enviaron cantidades masivas de mensajes (spam) y pedidos automáticos online para saturar los servidores."

[83] Demien Mc Guinness, "Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país" Edit BCC de Londre, https://www.bbc.com/mundo/noticias-39800133?fbclid=IwAR3MxHaP2NUHwUbXTtWNBRabUXftDbV0qTnZi6ZAhjZ7ZvqrmC_zXZ2tGwg Consulta 22 de Febrero del 2020

Al acontecer esta acción la economía se colapsó y dejaron de dar servicio los cajeros automáticos y los servicios de la banca electrónica.

Para la sociedad fue un caos ya que no había liquidez de dinero debido a un hackeo masivo de los sistemas, no se podía hacer pagos y por lo tanto las operaciones se pararon de varias organizaciones.

3.1.2 Ataque DDOS a plataforma online de filial del HSBC en Reino Unido

Este ataque fue efectuado en el 2016 los servicios en línea fueron vulnerados por un ataque DDos, que se caracteriza por denegar servicios, este ataque inutiliza los equipos de cómputo y no se puede acceder a las redes, se niega cualquier actividad dentro de la red y es inaccesible para los usuarios legítimos.

"Un ataque DDoS tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. Existen diversas formas de ataque DDoS: por saturación del ancho de banda del servidor para dejarlo inaccesible, o por agotamiento de los recursos del sistema de la máquina, impidiendo así que esta responda al tráfico legítimo."[84]

Al saturarse el ancho de banda de un "sistema de Pagos electrónicos Interbancario (SPEI)" se empiezan a generar una serie de problemas en cumplimiento de operaciones físicas y morales.

El verdadero Desarrollo de un ataque DDoS

- "El servidor está operativo enviando y recibiendo paquetes normalmente.
- El ataque DDoS se produce por la sobrecarga del ancho de banda o por el agotamiento de los recursos del sistema.

[84] OVH CLOUD, "Anti DDos" https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml?fbclid=IwAR0xBFfrLvqD4qJvZESGA2Le4Mr6V4TMUYpN0g8xoLrbsOL6n0FwHkN7_Ok
ídem Consulta 21 de Febrero del 2020

- La red se satura, por lo que el servidor no puede procesar los paquetes legítimos entre la masa de información entrante" [85]
- Gracias a que Londres cuenta con ayuda de un Centro de ciberseguridad pudo repeler el ataque con éxito, pero por algunas horas dejaron de operar los servicio.

3.1.3 Banco Griego

Otro banco que fue vulnerado casi con las mismas características al de Londres fue el griego, en el 2015 se lanzó un ciberataque distribuido de degeneración de servicio y un grupo de cibercriminales demandaron un rescate de bitcoins. Recordemos que los bitcoins es la nueva moneda digital, basada en un protocolo de código abierto y red peer-to que se utiliza como criptomoneda y que se usa como sistema de pago para mercancías.

La banda de cibercriminales se denominada como "Armada Collective hasta la fecha siguen operando de forma clandestina y no han sido detenidos, han Hackeado instituciones de Suiza y Taiwán.

3.1.4 Banco de Bangladesh

Los ciberdelincuentes operan en muchas partes del mundo y siempre detectan debilidades dentro de los sistemas informáticos. Las operaciones bancarias en Asia siempre operan con mucho dinamismo y no cuentan con un sistema protector a ataques, en otro termino un sistema de respuesta ante incidentes.

El robo cibernético del Banco de Bangladesh, el cual se caracterizó por el uso de un código malicioso detectado por ESET como una variable de Win32/Agent.XZH. El código tiene la característica de que es altamente sofisticado, es decir que utiliza

[85] OVH CLOUD, "Anti DDos" https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml?fbclid=IwAR0xBFfrLvqD4qJvZESGA2Le4Mr6V4TMUYpN0g8xoLrbsOL6n0FwHkN7_Ok ibídem Consulta 22 de Febrero del 2020

lenguaje de alto nivel y moderno. Con esto se permitió internarse al software de mensajería de nominado como SWIT Alliance Acces, el cual era utilizado por más de 11 mil bancos e instituciones financieras de 200 países. El robo efectuado accedió a más de 81 millones de dólares dinero ubicado en cuentas de la Reserva Federal de Nueva York. De estas actividades jamás se encontró a los responsables.

3.1.5 Banco Ruso

De la misma forma que pasó en Bangladesh en este "atraco digital" se utilizó un sistema de mensajería denominado SWIFT que fue hecho desde la computadora de un empleado y se robaron muchas cuentas bancarias, se transfirieron fondo de su propia cuenta con un valor de 6 millones de dólares.

Este ataque ruso demostró que Rusia también es vulnerable y que hay bandas cibercriminales a veces con identidad y sin identidad operando de forma arbitraria por la red.

Rusia por lo general no es débil en una guerra cibernética, no obstante, es uno de los más afectados en los últimos tiempos por ciber ataques por diferentes enemigos principalmente por EUA.

Del mismo modo este país realiza ataques de alta escala a naciones pobres para poder cambiar el rumbo de sus operaciones, principalmente a sus exrepúblicas.

3.2 Ciberataques a Bancos Mexicanos

En la actualidad se está gestando un problema dentro de las instituciones bancarias; su principal debilidad se gesta en sus sistemas informáticos y no se tiene un oponente para poder hacer frente.

Todas las instituciones financieras en México han sido objetivos de intentos de ciberataques en el último año. "Éste fue el principal hallazgo del reporte Estado de la Ciberseguridad en el Sistema Financiero Mexicano, elaborado por la Organización de Estados Americanos (OEA) en colaboración con la Comisión Nacional Bancaria y de Valores (CNBV). Del total de intentos de ciberataques en contra de bancos, socaps, sofipos y fintechs, más de 40% tuvo éxito"[86]

Las organizaciones no cuentan con sistemas que repelan ataques cibernéticos y son vulnerables a que se pueda robar datos y dinero electrónico. "De acuerdo con un informe realizado por la Organización de los Estados Americanos (OEA) y la Comisión Nacional Bancaria y de Valores (CNBV), si se suman los ataques, también exitosos, en el resto de la banca mexicana, la cifra de usuarios víctimas del cibercrimen es de 14.3 millones, 31% del total de clientes"[87]

México está siendo víctima de ciberataques, los bancos se están quejando frente a este modus operandi, no obstante**,** a pesar de que se cuente con una Estrategia de Ciberseguridad del PND, no se toma en cuenta frente al no apoyo institucional.

Aunque la estrategia se haya creado para la prevención de la violación de datos personales y brindar seguridad en la red, un ciberataque es muy peligroso y los bancos están siendo los principales afectados.

---

[86] Riquelme Rodrigo, 5 sectores más expuestos en ciberataques en México, Edit. El Economista, https://www.eleconomista.com.mx/tecnologia/5-sectores-mas-expuestos-a-ciberataques-en-Mexico-20191112-0058.html Consulta 25 de Febrero del 2020

[87] Hernández Aura "Ciberataques, reto en el 2019", Excélsior, 4 de Diciembre del 2018. https://www.excelsior.com.mx/hacker/bajo-ciberataques-la-mitad-de-la-banca/1324085 Consulta 28 de Febrero del 2020

“El mayor riesgo para los especialistas en ciberseguridad es la vulneración de dependencias como el SAT o la Secretaría de Defensa Nacional, de las cuales se asegura ya están en miras de este grupo de hackers.”[88]

Si bien se tiene un contacto con la policía cibernética, no existe infraestructura para poder repeler la cantidad de ataques que se dan por día; “los ataques cibernéticos contra las instituciones financieras pasaron de 1 a cuatro por trimestre, lo que representó afectaciones por 784.7 millones de pesos, reveló el Reporte de Estabilidad Financiera del Banco de México (Banxico) a diciembre del 2019”[89]

La ciberdelincuencia aumenta, estas bandas tienen conocimientos de informática y que, por lo regular, cuentan con una amplia experiencia en el manejo del lenguaje de código. Conocen varias plataformas electrónicas, las cuales se muestran vulnerables para ellos.

La OEA en conjunto con la CNBV se centran en monitorear los ciberataques, “Los eventos de seguridad más comunes identificados en el 2018 fueron el código malicioso o malware, afectando a 56% de las entidades financieras mexicanas, seguido por *phishing* dirigido para tener accesos a sistemas, con impacto de 47% de total de los jugadores del sistema financiero. [90]

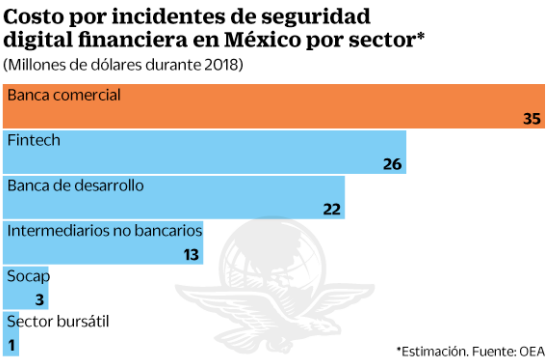
En la misma nota se ofrece una estadística interesante de la OEA respecto a los incidentes:

[88] Lara Paula, “Hackers endurecen chantaje a Pemex; suben a la red documentos de la empresa”, Edit. Excélsior, 27 de Febrero del 2020 https://www.excelsior.com.mx/nacional/hackers-endurecen-chantaje-a-pemex-suben-a-la-red-documentos-de-la-empresa/1366588 Consulta 29 de Febrero del 2020

[89] Martínez Carla, “Ciberataques contra los bancos se incrementan”https://www.eluniversal.com.mx/cartera/se-disparan-ciberataques-contra-bancos-cuestan-784-mdp Consulta 30 de Febrero del 2020

[90] Hernández Antonio, “Costó 107 mdd recuperación por ciberataques” Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 1 de Marzo del 2020

Gráfica 1[91]



3.2.1 Sistema de pagos Electrónico Interbancario (SPEI)

Cuando un Hacker lanza un código malicioso y las instituciones bancarias no cuentan con la suficiente seguridad informática, con todo asertividad se puede preparar un ataque que incluso puede tardar meses. Por otro lado, la desventaja de esta forma de robar y secuestrar datos personales es como se infiltra poco a poco a los sistemas, muchas veces son indetectables. En medio de todo este problema el Sistema de Pagos Electrónicos Interbancarios sufre de ataques diarios. La capacidad de respuesta de cada institución con este sistema de pagos no está siendo eficiente debido a que son vulnerados sus escudos, es decir que a pesar de una respuesta a incidentes -los Hackers- planean un ataque cada vez más eficiente. Abundando más a las propiedades del sistema este se caracteriza "por alineado a las finalidades que la Ley del banco central señala, entre las que se encuentran promover el sano desarrollo del sistema financiero y propiciar el buen funcionamiento de los sistemas de pagos"[92]

[91] Hernández Antonio, "Costó 107 mdd recuperación por ciberataques" Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 3 de Marzo del 2020

[92] Banco de México, "Sistema de Pagos Electrónicos Interbancarios (SPEI)" https://www.banxico.org.mx/sistemas-de-pago/d/%7B89B6CCF0-6070-7389-3DD5-B27AC4ECD9D1%7D.pdf Consulta 4 de Marzo del 2020

En fechas resientes “los piratas informáticos que atacaron a algunos bancos en México en abril y mayo de 2018 estuvieron hasta año y medio antes dentro de las redes…sin ser detectados, de acuerdo con la consultora de seguridad informática Tekium”[93]

Asimismo, las bandas de ciberdelincuentes aumentan más y los ataques a la banca aumentan. Por lo tanto, ya no es rentable robo a mano armada o asalto a bancos de forma física, simplemente con saber de programación es más que suficiente para poder robar dinero electrónico.

El dinero electrónico es una modalidad que hoy en día se utiliza, cada vez más usuarios se conectan a diferentes sitios y aplicaciones para comprar objetos de distinta naturaleza. Hoy en día el SPEI nos ayuda a agilizar los procesos electrónicos, contribuye a buen uso de la Banca electrónica. La cibercriminalidad es muy eficaz cada día y se enfrenta a un nuevo reto informático, afortunadamente existen llaves potentes que sellan lo datos en la nueve y no permiten que entren personas ajenas a las cuentas. En este caso lo que se manejan son cuentas las cuales tienen cantidades considerables de dinero.

Algo importante señalar y que se debe conocer para poder entender el contexto del ataque cibernético hacia este sistema “es que las funciones relativas a los sistemas de pagos, que incluyen las relacionadas con el SPEI, están encomendadas principalmente a la Dirección General de Sistemas de Pagos y Servicios Corporativos, y, en particular, a la Dirección de Sistemas de Pagos, quien tiene entre sus principales atribuciones diseñar, elaborar e implementar las políticas para el desarrollo y buen funcionamiento de los sistemas de pagos”[94]

---

[93] Notimex, El Economistas, 7 de abril del 2019, https://www.eleconomista.com.mx/sectorfinanciero/Hackers-detras-de-ataques-al-SPEI-estuvieron-dentro-de-las-redes-de-los-bancos-por-ano-y-medio-20190407-0018.html Consulta 7 de Marzo del 2020

[94] Banco de México, “Sistema de Pagos Electrónicos Interbancarios (SPEI)” https://www.banxico.org.mx/sistemas-de-pago/d/%7B89B6CCF0-6070-7389-3DD5-B27AC4ECD9D1%7D.pdf Consulta 8 de Marzo del 2020

Desafortunadamente todos los usuarios entran a plataformas y aplicaciones a través de los diferentes buscadores y el problema “el navegador Chrome, de Google, el más popular entre los cibernautas, en su versión 68, que emite una notificación de ‘No seguro’ cuando encuentra un sitio sin el protocolo de encriptación de seguridad HTTPS”

ES un reto para el escenario nacional e internacional el poder blindar a SPEI a partir de otros programas de seguridad como Blockchain, que blinda datos y protege claves a un alto nivel.

3.2.1.1 Banxico

Recientes reportes de Banxico, ofrece que el SPEI fue vulnerado ya muchas veces. Este banco ha puesto caso a los ciberataques y ha realizado investigaciones sobre los principales acontecimientos de amenazas. “Cuenta con metodologías y criterios más uniformes para evaluar el riesgo ambiental, así como promover instrumentos de inversión sustentable”[95]

Para poder actuar en esto Banxico tiene alguna disposición en materia de pago, las cuales los cibercriminales conocen:

- Establece el sano desarrollo del sistema financiero y el buen funcionamiento de los sistemas de pagos como dos de las finalidades del Banco de México (Artículo 2).
- Establece como una de las funciones del Banco de México regular los sistemas de pagos (Artículo 3).
- Faculta al Banco de México a expedir disposiciones que tengan por propósitos, entre otros, el sano desarrollo del sistema financiero, el buen

[95] Flores León, “Banxico, preocupado por los ciberataques”, El universal, 25 de marzo de 2019, https://www.eluniversal.com.mx/cartera/banxico-preocupado-por-los-ciberataques Consulta 16 de Marzo del 2020

funcionamiento del sistema de pagos y la protección de los intereses del público (Artículo 24).

- Faculta al Banco de México para regular el servicio de transferencias de fondos a través de instituciones de crédito (Artículo 31).
- Faculta al Banco de México para realizar supervisión de los intermediarios y entidades financieras sujetos a la regulación que este expida, para proveer a la observancia de la regulación que lleve a cabo (Artículo 35 Bis).

Todas estas disposiciones se inclinan desde luego para una mejor seguridad informática, no obstante, no es suficiente. Banxico recientemente lleva un control de incidentes, utilizan plataformas de alta seguridad informática así como protocolos de seguridad; mencionan que "la materialización de riesgos cibernéticos puede causar a las instituciones financieras daños de tres tipos: i) disrupciones de las tecnologías de la información que utilizan y la consecuente indisponibilidad de sus servicios; ii) afectación a la integridad, confidencialidad y disponibilidad de la información que gestiona la institución, incluida la de sus clientes; iii) pérdidas económicas a las propias instituciones o a sus clientes"[96]

3.2.1.2 Banorte

Otro caso más sonado es el del Banco del Norte el cual ha sido víctima de ataques cibernéticos. Era el 26 de abril cuando se suscitó el siniestro "al pasar a operar al sistema alterno del SPEI, las operaciones se volvieron lentas detonando las alertas

[96] Jeannete Leyva "Así fue el ciberataque a la banca en 2018"El Financiero, 29 de Abril del 2019, https://www.elfinanciero.com.mx/economia/asi-fue-el-ciberataque-a-la-banca-en-2018 Consulta 20 de Marzo del 2020

en todo el sistema, aunque en ese momento se negaba por parte de todas las autoridades un ataque"[97]

Cuando se realizaron los ataques "Las transferencias interbancarias comenzaron a sufrir retrasos desde finales de abril, lo que alimentó las preocupaciones de que la segunda mayor economía de América Latina podría ser la última víctima en una ola global de ataques cibernéticos.

Del mismo modo el ataque de Banorte fue similar a que aconteció al Banco HSBC en Reino Unido en el que fueron vulnerados por un ataque DDos, que se caracteriza por denegar servicios, este ataque inutiliza los equipos de cómputo y no se puede acceder a las redes, se niega cualquier actividad dentro de la red y es inaccesible para los usuarios legítimos.

Tomando como dato importante en una entrevista que se le hizo al director de Grupo Financiero Marcos Ramírez menciona que "el número de ataques cibernéticos que sufre el sistema financiero mexicano está creciendo ante lo cual se han reforzado las medidas de seguridad para evitar daños a las instituciones y usuarios"[98]

La cantidad de ataques a esta institución son constantes y reciben a diario afortunadamente los firewalls han logrado repeler las amenazas, no obstante, siempre se mejora una nueva estrategia de atacar. Es decir que los servicios de Banca móvil y Banca Digital están sustentados en sistemas de alta seguridad informática.

Banorte ha tenido muchos problemas con su SPEI esto debido al rezago de sus sistemas de defensa los cuales están basados en tecnología de la generación 3 y se necesita tener componentes de sexta generación.

---

[97] Jeannete Leyva "Así fue el ciberataque a la banca en 2018" El Financiero", 29 de Abril del 2019, https://www.elfinanciero.com.mx/economia/asi-fue-el-ciberataque-a-la-banca-en-2018 Consulta 20 de Marzo del 2020

[98] El universal, 21 de Abril 2018 https://www.eluniversal.com.mx/articulo/cartera/finanzas/2016/10/21/incrementan-ciberataques-financieros-banorte Consulta 25 de Marzo del 2020

De acuerdo con la FGR “Los ataques cibernéticos han deja pérdidas por más de 500 millones de pesos y que hay una cifra negra de daños económicos sólo que no se conocen públicamente, dado que distintas instituciones financieras prefieres no precisar dicha información para no generar publicidad adversa”[99]

3.2.2 Interacción con otras organizaciones

Aunque los bancos tienen siempre relación con miles de instituciones públicas y privadas, los datos no son del todo cuidados, mientras que en Europa se cuenta con una política en materia de ciberseguridad, en México apenas se está atendiendo este problema a pasos muy lentos.

En medio del caos de los ataques a los sistemas de pagos varios bancos mexicanos han sido víctimas de ciberataques, por ejemplo, después del 17 de abril del 2018 “se detectaron cuatro eventos adicionales del ciberataque: dos el 24 de abril, uno el 26 de abril y uno más el 8 de mayo. Los vulnerados fueron Kuspit Casa de Bolsa, Banjército, Banorte, Inbursa y una caja de ahorro”[100]

Este problema cada vez tiene mucha ventaja, debido a que los cibercriminales se actualizan en materia de programación con la finalidad de afinar ataques de alta bandera.

Los diferentes organismos internacionales han puesto atención, se han celebrado foros internacionales y varios eventos relacionados a este tema.

La primera intervención de la ONU respecto a este tema se habló de crímenes en internet en el Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010. En este se habló

[99] Arturo Rangel, Animal Político, 17 de marzo del 2019, https://www.animalpolitico.com/2019/03/fiscalia-responsables-ciberataques-bancos/?fbclid=IwAR3c-2lROoKgjtnAb1vY1nmNGXnY8Htd7vF-ALqpjZHyC_GtdN9-utULJug Consulta 26 de Marzo del 2020

[100] Jeannete Leyva “Así fue el ciberataque a la banca en 2018” Edit. El Financiero, 29 de Abril del 2019, https://www.elfinanciero.com.mx/economia/asi-fue-el-ciberataque-a-la-banca-en-2018 Consulta 27 de Marzo del 2020

respecto a que “los delincuentes cibernéticos se pasean a su aire por el mundo virtual, incurriendo en delitos tales como el acceso sin autorización o «piratería informática», el fraude, el sabotaje informático, el narcotráfico, la trata de niños con fines pornográficos y el acecho”[101]

De la misma forma la postura de la ONU es que debido a que el índice de delitos informático ha aumentado, “El delito cibernético se ha convertido en un negocio que supera el billón de dólares anual producto del fraude cibernético, el robo de identidad y la pérdida de propiedad intelectual. Afecta a millones de personas alrededor del mundo, a innumerables empresas y a los gobiernos de todas las naciones”[102]

La ONU, la OEA, el Fondo Monetario Internacional celebran reuniones regularmente, por ejemplo “La Semana Nacional de la Ciberseguridad” que consiste en llevar diferentes talleres, foros, conferencias y discusiones que fomenten el diálogo interdisciplinario en materia de Tecnologías de la Información y Comunicación, infraestructuras críticas y gobernanza del ciberespacio

El Sector bancario será contantemente atacado por estos ciberdelincuentes y se debilitará más en cuanto a seguridad “al comparar la Banca Comercial o Múltiple de México con el promedio de la región de América Latina y el Caribe, se observa que, en dicho sector, en 85% de las entidades bancarias la junta directiva recibe reportes periódicos acerca de riesgos de seguridad de la información (incluyendo

[101] Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010.
http://www.onu.org.mx/la-unodc-presenta-su-programa-global-de-ciberdelito-durante-la-5a-semana-nacional-de-la-ciberseguridad-en-mexico/ Consulta 30 de Marzo del 2020

[102] ONU, “Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010”.
[102] http://www.onu.org.mx/la-unodc-presenta-su-programa-global-de-ciberdelito-durante-la-5a-semana-nacional-de-la-ciberseguridad-en-mexico/ Consulta 30 de Marzo del 2020

ciberseguridad) y fraudes ocurridos a través de medios digitales, cifra superior a la reportada en la región (72%)".[103]

3.3 Sujeto en la figura de robo informático en Instituciones Bancarias

La figura en la actualidad todavía es desconocida por muchas instituciones, mientras que los Bancos son atacados de forma desmedida, las autoridades ignoran los que pasa. La Estrategia de ciberseguridad propuesta por el sector público y privado ha tenido un efecto lento, debido a que no cumple con una prevención integral.

Desafortunadamente los Bancos siguen siendo vulnerables y la figura de "robo informático es muy ambigua; las operaciones bancarias son por lo regular desencriptadas por grupos de ciberdelincuentes que son en la mayoría de las veces indetectables.

Por lo general para poder tener acceso a las líneas bancarias se pueden presentar por estos ataques cibernéticos más comunes son:

- Extorsión mediante Ramsomware del cifrado de la información.
- Pirateo de la información
- Fallos de seguridad/Accesos no autorizados
- Infecciones con Malware
- Suplantación de Identidad
- Ataques de denegación de servicio
- Pérdida o robo de activos informáticos

[103] Paul Lara, Bajo ciberataque la mitad de la banca, Edit. Excélsior, https://www.excelsior.com.mx/hacker/bajo-ciberataques-la-mitad-de-la-banca/1324085 Consulta 5 de Abril del 2020

- Otras ciber extorsiones[104]

3.3.1 Sujeto activo y pasivo

Sujeto Activo: Es toda persona que infrinja la ley penal por propia voluntad o sin ella. Por lo general este tipo de delitos son cometidos "con conocimiento de la acción que va a realizar, esperando el resultado de ése o en caso contrario, sin voluntad de ese sujeto, cuando la acción que da origen al delito no es deseada y se comete por imprudencia o sucede por un accidente, este sujeto será el que realice la acción de la conducta o la omisión de la misma que están previstas y sancionadas por la ley penal".[105]

Sujeto Pasivo: "Es toda persona que resienta el daño que ocasiona la comisión del delito, la consecuencia de la conducta delictiva ya se trate de su persona en sus derechos o en sus bienes, persona a quien se le afecta en su esfera personal de derechos e intereses"[106]

Ejemplos de sujeto Pasivo aplicado a el robo de información: Individuos, Instituciones crediticias, órganos estatales que utilices sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos.

[104] Globalkfinanz, "¿Sabes qué es un ataque cibernético y cuáles son los más comunes?" https://www.responsabilidadconsejerosydirectivos.com/que-son-los-ataques-ciberneticos/ Consulta 9 de Abril del 2020

[105] Armando Benítez Molina, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.26

[106] Armando Benítez Molina, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.26

3.3.2 Objeto del delito

Esta figura se obliga a inclinar a la naturaleza y el tipo de delito a la calidad, tipo y número de los sujetos activos y las consecuencias de eso son los pasivos. “el objeto jurídico del delito es el bien protegido por el derecho y que precisamente por esa razón se denomina bien jurídico, es decir el quid de la norma, con la amenaza de la sanción, trata de proteger contra posibles agresiones”[107]

La aplicación del robo informático se puede clasificar como un hecho jurídico, es decir que este puede tener consecuencias jurídicas. Si un individuo violenta un sistema electrónico, un objeto tecnológico se le puede clasificar como delito.

“Cómo el delito es un hecho jurídico voluntario, supone que él es ante todo un hecho humano y no un hecho natural”[108]

3.3.3 Otros sujetos

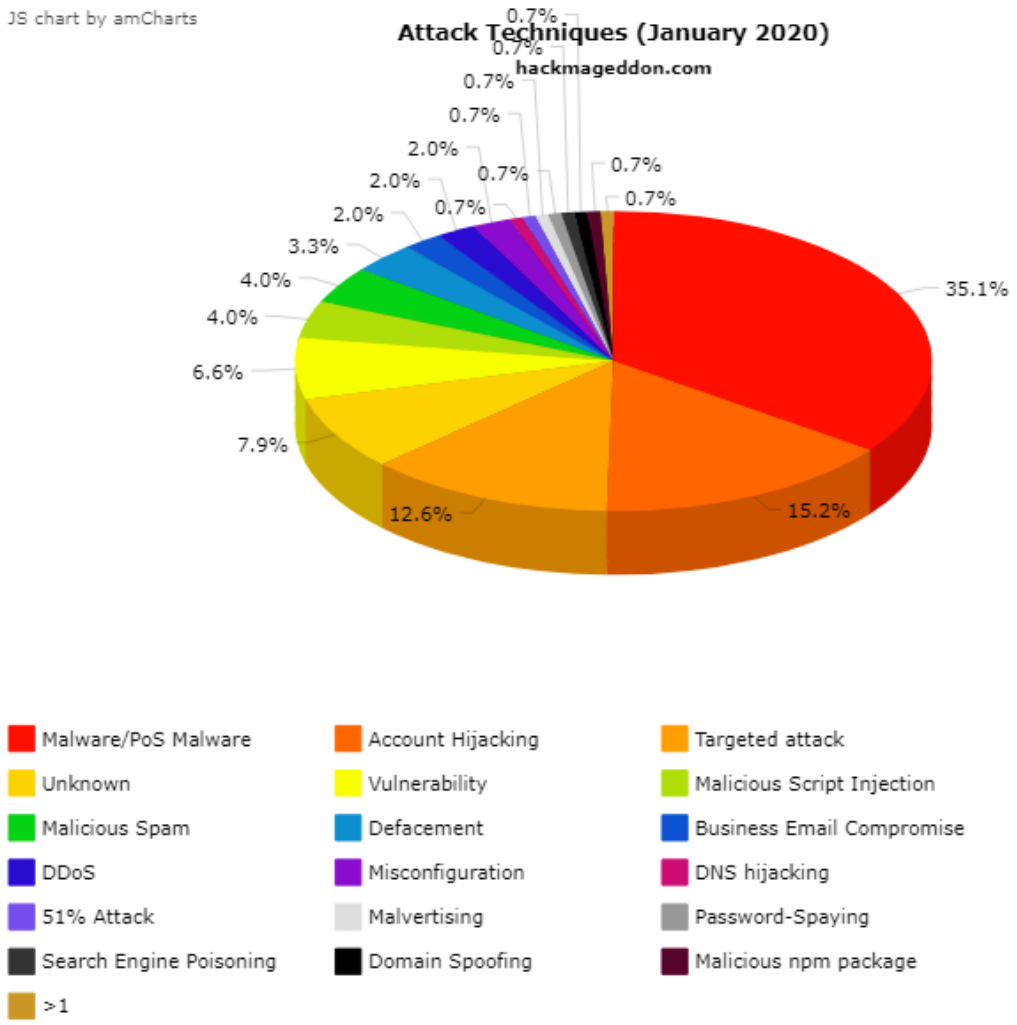
La ley nos ofrece una estricta configuración del delito, no obstante, la actividad delictiva registra otro tipo de conductas que deberían ser y clasificarse de orden penal. Este tipo de figuras han surgido a partir del nuevo escenario global de las tecnologías, las cuales avanzan más rápido que las investigaciones sociales. Cada una de estas conductas se visualiza como un peligro debido a que no existe tipicidad del delito, es decir no se le puede hacer una buena configuración del delito.

En la siguiente gráfica se puede apreciar la cantidad de ciberataques:[109]

[107] Armando Benítez Molina, “Propuesta del delito informático”, Edit. UNAM, Edición diciembre de 2009, Pág.27

[108] Armando Benítez Molina, “Propuesta del delito informático”, Edit. UNAM, Edición diciembre de 2009, Pág.29

[109] https://www.hackmageddon.com/2020/03/03/january-2020-cyber-attacks-statistics/ Consulta 16 de Abril del 2020



3.3.3.1 Hacker

Esta persona es un profesional de la informática y realiza intervenciones grandes, se dedica a husmear y conocer el funcionamiento de diferentes sistemas informáticos, tiene un alto conocimiento en software y se caracteriza por un ser un delincuente discreto y silencioso.

Esta personalidad es responsable de realizar ataques masivos a diferentes instituciones, por lo general se dedica al robo de información por lo que a primera vista se le podría configurar el delito, no obstante, de la cadena de custodia este es capaz de evadir a la justicia y puede desaparecer en las redes a pesar de haber dejado un rastro.

Esta figura suele ser divertirse es decir “generalmente se traducen por paseos por el sistema haciendo alarde de su intromisión, es lo que se llama joyriding o paseos de diversión, caracterizado a esta clase de hacking: el Hacker es una persona experta en materias informáticas y con edad fluctuante entre los 15 y 25 años de edad es por ello que esta delincuencia se ha denominado, pantalones cortos, su motivación no es la de causar daños sino de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad”[110]

“El uso de códigos maliciosos para secuestrar un equipo y pedir un rescate para que éste vuelva a funcionar afectó en 2019 al menos a 174 instituciones municipales con más de tres mil subdivisiones, 60% más respecto a lo registrado en 2018, de acuerdo con expertos de Kaspersky Lab”.[111]

Esta figura es más conocida que las demás y su reputación tiene más auge que las otras figuras, debido a que es más mencionado en los medios masivos de comunicación. Es muy conocido en la vida social, cibernética, en los medios electrónicos y se le tiene pavor.

En la actualidad hay Hackers en las penitenciarías y se les aplica penas severas por hacer sistemas informáticos que afectan a las instituciones, principalmente esto se ve en EUA, Canadá y Reino Unido. En México la configuración de delitos es muy ambigua y sobre todo para este tipo de figuras.

Recientemente se atrapó a una banda de Hackers los cuales se hicieron ricos por la cantidad de ataques cibernéticos a los bancos.

---

[110] Molina Benítez Armando, “Propuesta del delito informático”, Edit. UNAM, Edición diciembre de 2009, Pág. 30

[111] Aura Hernández “Ciber Ataques en el 2020 se materializan; expertos advierten auge en hackeos”, Aura Hernández, Excélsior, 11 de abril del 2020 https://www.excelsior.com.mx/hacker/ciberataques-en-2020-se-materializaran-expertos-advierten-auge-en-hackeos/1355817?fbclid=IwAR1Ks_7qewpVBM2JG4Es4PWUnxfiMFrios69yCLFLpFzg3ODo0u1iLHx0hE Consulta 19 de Abril del 2020

La banda “, obtuvo hasta mil millones de pesos por robos a los bancos, a través del hackeo realizado en cajeros electrónicos, mediante un software lograban entrar al Sistema de Pagos Electrónicos Interbancarios (SPEI) con el que habrían sido sustraídos en forma ilegal entre 200 millones y 400 millones de pesos de las arcas de Banorte, Inbursa, entre otros”[112]

Desgraciadamente estos grupos ya son utilizados por la delincuencia organizada del narcotráfico para poder obtener dinero de forma ilícita “Con los recursos obtenidos de manera ilegal, eran utilizados para comprar inmuebles de alta plusvalía, en los principales destinos turísticos de México y el extranjero, además de que el dinero era invertido en paraísos fiscales en el país de Panamá y otros países”[113]

3.3.3.2 Craker

Esta persona se caracteriza por ser experta en programación de alto nivel e introducir sistemas informáticos con el objetivo de destruir, robar datos, denegar servicios a usuarios legítimos. Dentro del ámbito informático es conocido como “Pirata Informático”.

Con el arte de la programación pueden ocasionar bloqueos de los sistemas, desencriptar llaves y desproteger todo tipo de programas. Al bajar los escudos de los sistemas estos penetran haciéndolos plenamente operativos, “como de programas completamente comerciales que presentan protecciones anticopia”[114].

---

[112] INFOBAE, 22 de mayo del 2019, https://www.infobae.com/america/mexico/2019/05/22/como-atraparon-a-la-mayor-banda-de-hackers-mexicanos-que-orquesto-robos-millonarios-al-sistema-bancario/ Consulta 20 de Abril del 2020

[113] OBAE, 22 de mayo del 2019, https://www.infobae.com/america/mexico/2019/05/22/como-atraparon-a-la-mayor-banda-de-hackers-mexicanos-que-orquesto-robos-millonarios-al-sistema-bancario/ Consulta 22 de Abril del 2020

[114] Molina Benítez Armando, “Propuesta del delito informático”, Edit. UNAM, Edición diciembre de 2009, Pág.32

El bloqueo de los sistemas se realiza por medio de programas muchas veces creados por el mismo Pirata informático, otra vez se pude hacer uso de un producto y emplearlo para comerte el ultraje.

El perfil de estos cibercriminales desgraciadamente son jóvenes que estudian o son egresados de la universidad de Ingeniera en Sistemas Computaciones o en su caso matemáticas aplicadas a la computación.

3.3.3.3 Phreaker

Una forma de operar ilícitamente es desde el ámbito de la telemática, se caracteriza por usar los sistemas de telefonía, tanto terrestres como móviles. Esta figura se encarga de violentar las líneas telefónicas y sabotear el control centralista.

Atacan a redes públicas y privadas, tratan de hacer fraudes con "reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos obtienen al lograr el acceso mediante técnicas de hacking a sus servidores".[115]

Este tipo de figura se ve mucho en Bancos, se implementa una operación, se neutralizan los sistemas. Un Phreaker puede acceder a la computadora central a través de las líneas telefónicas, se puede implementar un virus Trojano y se accede al sistema.

Hay tres tipos de phreaking:

1) Shoulder-surfing: Esta figura se caracteriza por la identificación del código secreto de la línea telefónica, esto se maneja mucho

[115] Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.33

en espionaje. Esto sucede a menudo en el ámbito gubernamental, por ejemplo, cuando se realizan elecciones por lo general se interviene teléfonos con la finalidad de extraer información. Las victimas muchas veces "no pueden percatarse de que están siendo observadas"[116] o escuchadas.

2) Call-sell: esta conducta se caracteriza por robar un código de usuario que no le pertenece y cargar el costo de llamada a la cuenta de la víctima. Esto se da cuando llegan cuentas cargas a nuestros recibos telefónicos y en realidad no sabemos de su procedencia.
3) Diverting: Esta conducta se realiza en empresas con alto tráfico en llamadas telefónicas, el sujeto entra a las líneas, se adhiere de forma clandestina y las utiliza para hacer llamadas a distancia, su éxito se da debido a que es muy difícil de detectar.

3.3.3.4 Lammers Bucanas

Esta figura es más usuaria de lo que las otras figuras hacen, es decir que se dedican a traficar datos, venden productos de los crackers, utilizan sus conocimientos y herramientas. Este navega por la red y busca oportunidades, venden tarjetas de control de acceso de canales de pago, exploran hadwares, no saben de informática y no saben de programación. Su principal actividad es poner a la venta productos bajo un nombre comercial, esto se ve y es la "realidad que es un empresario con mucha afición a ganar dinero rápido y de forma sucia"[117]

[116] Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.34
[117] Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág. 35

Un ejemplo de venta de información por internet han sido los “datos, planos de infraestructura y trabajos corporativos de varias empresas, entre ellas Petróleos Mexicanos, así como información de proveedores, clientes y datos personales de los trabajadores están siendo ofrecidos en el portal Dopple Leaks en la Deep Web, como represalia a que compañías no pagaron a hackers que usaron el DoppelPaymer Ransomware para vulnerar servidores”[118]

Las instancias gubernamentales tienen mucha fuga de datos, los cuales son -como ya sabemos- son utilizados para fines de extorsión y para obtener un beneficio económico, en este caso también se puede hacer venta de productos lo cuales también son robados y vendidos en las redes; los productos se pueden entender también como paquetes de datos.

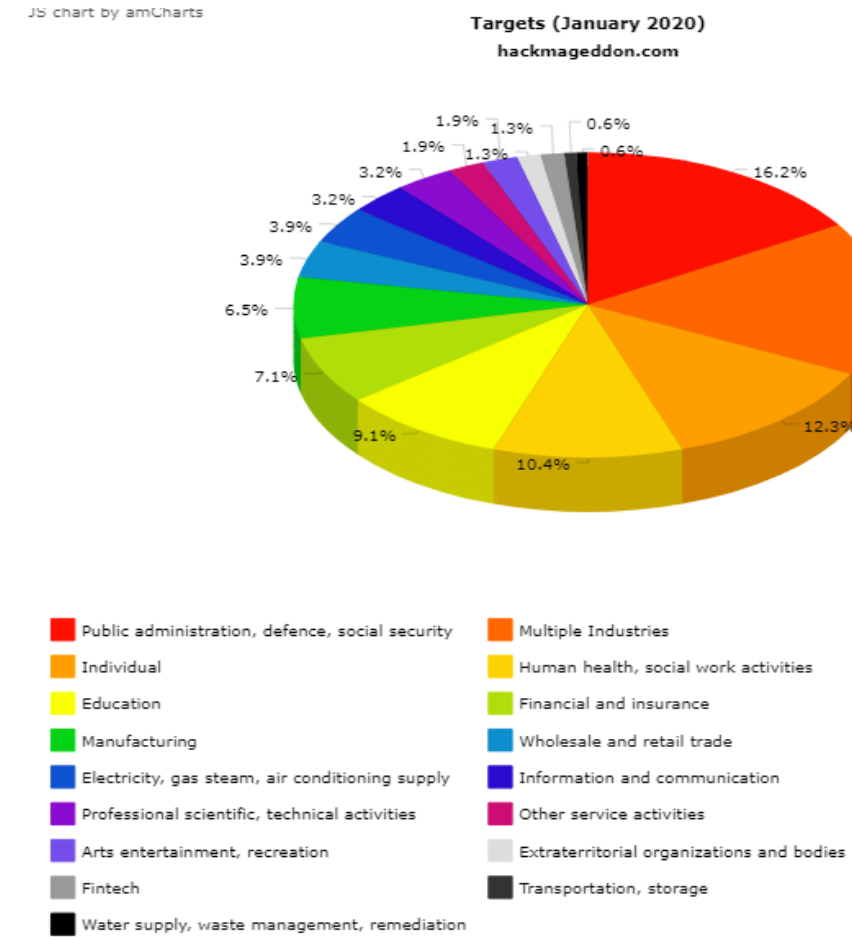
3.3.3.5 Gurus Newbie

Existe la elite de la elite y estas personas por lo general lo saben todo, es muy difícil detectar su ubicación, debido a que se esconden y pueden pasar desapercibidos debido a su nivel de confidencialidad. Por lo general se dedican a decodificar información de alto nivel, pueden acceder a información secreta o privada. Utilizan todo medio informático que este a la mano para cometer actos delictivos, principalmente el “delitos informáticos”.

Su capacidad se puede visualizar al ser capaces de realizar espionaje de alto nivel “coerción o simplemente el lucro mediante el uso ilegitimo de códigos de ingreso a

[118] Lara Paula “Hackers endurecen chantaje a Pemex; suben a la red documentos de la empresa, Paula Lara, Excélsior, 27 de febrero del 2020 https://www.excelsior.com.mx/nacional/hackers-endurecen-chantaje-a-pemex-suben-a-la-red-documentos-de-la-empresa/1366588
Consulta 15 de Abril del 2020

sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada"[119] En la siguiente gráfica se puede ver como esta conducta afecta a los sectores:[120]



[119] Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.44

[120] Passeri Paolo, "HACKMAGEDDON2 3 de marzo del 2020 https://www.hackmageddon.com/2020/03/03/january-2020-cyber-attacks-statistics/ Consulta 15 de Mayo del 2020

CAPÍTULO IV

4.1 Blockchain para protección de datos Bancarios

Debido a la cantidad de incidentes que se registran en las plataformas informáticas, se han hecho muchas propuestas para poder combatir la extracción de datos personales que han derivado en algunos casos en el robo de dinero a Bancos, sobre todo para evitar el roba de dinero digital.

Por los tanto, las plataformas, programas y diferentes creaciones de software para combatir a la Ciberdelincuencia se han caracterizado para brindar una mejor seguridad a los usuarios, no obstante y a pesar de su creación, no es suficiente debido a que los ciberdelincuentes mejoran sus tecnicas de ataque.

Según el El Reporte Global de Riesgos "**El sector financiero es el más afectado** por las ventajas directas que obtienen los ciberdelincuentes de estafar a instituciones y usuarios de esos servicios. También es el sector con más experiencia en la adopción de tecnologías y soluciones de ciberseguridad"[121] Esto nos indica que hay una seria debilidad en los Bancos, se necesita urgentemente líneas de acción.

Mi propuesta es usar Blockchain una herramienta tecnológica que es útil para las criptomonedas pero que, debido a su blindaje en el ciberespacio en materia de datos, se puede usar e implementar en cualquier industria, se puede aplicar en Instituciones Públicas y privadas, y dependencias de gobierno.

Esta cadena de datos es confiable debido a que "las principales ventajas que aporta esta nueva tecnología es la seguridad de almacenamiento de las transacciones por medio de los elementos que componen esta red, los cuales permiten registrar las

[121] Bravo Jorge, " Estrategia Nacional de Ciberseguridad" 30 de Julio del 2020 https://www.proceso.com.mx/640722/estrategia-nacional-ciberseguridad-mexico-columna-jorge-bravo Consulta 5 de Agosto del 2020

transacciones, almacenarlas, compartirlas públicamente, además de verificar dicha transacción, por medio de un ordenador que está incluido a la red"[122]

A sí mismo esta herramienta tecnológica evidentemente trae mucha ventaja para poder prevenir robo de datos personales aplicado al sector bancario, es decir que el criminal tendrá una barrera tecnológica para poder acceder a los datos. La forma preventiva se puede ayudar con las líneas de acción de la "Estrategia de Ciberseguridad"

4.1.1 Concepto de Blockchain

"Tecnología basada en la teoría de juegos, criptografía e ingeniería de software para que una red de computadoras anónimas pueda llegar a un consenso sobre un registro compartido"[123]

El concepto es nuevo puede tener un significado diferente al poder orientarse a las diferentes industrias. En este caso lo hemos estado enfocando al sector Bancario. En la primera definición se nos menciona que es una teoría de juegos; evidentemente se inclina a las materias de carácter abstracto, lo cual le da un valor agregado. La tecnología tiene utilidad en la nube, principalmente en operaciones del sector financiero.

Por lo mismo en plena edad moderna, en dónde las tecnologías tienen su punto más alto, la industria 4 .0 se ve muy relacionado con los campos de la ingeniería social.

---

[122] Ortega Uribe Daniel, "La Tecnología Blockchain en el sector Bancario" http://vitela.javerianacali.edu.co/bitstream/handle/11522/11602/Tecnologia_blockchain_sector_bancario.pdf?sequence=1&isAllowed=y Consulta 7 de Agosto del 2020

[123] González Becerreil Mabel Luna, "La tecnología de Blockchain y su impacto en el Sector Público en México. Análisis del caso Blockchain HACKMX"

Es el momento histórico en el cual la ciencia de datos es utilizada para poder resolver problemas como el robo de datos en el sector bancario a partir de la inteligencia artificial.

El escenario internacional sufre de constantes ataques cibernéticos, precisando que esto se genera por el uso constante de las redes informáticas; el Blockchain resolvería muchos problemas, previniendo las amenazas y eliminando la necesidad de arriesgar los datos personales en el ámbito bancario.

4.1.2 Antecedentes

"La transformación de la tecnología, a lo largo de la historia, ha sido un aliado importante para el sector bancario, que hoy, enfocado a los servicios en línea y transacciones bancarias, tiene como objetivo lograr un mejor control de las principales sistematizaciones, que a su vez permitan cuidar la seguridad de las operaciones, confidencialidad de los datos y agilidad de los procesos"[124]

Por lo tanto, a lo largo de la mejora continua de las tecnologías de la información se presenta el blockchain como plataforma que encripta la información para su protección. Funciona como cadena de datos en donde se escriben transacciones en criptomonedas que hacen usuarios anónimos. El uso del Blockchain su antecedente son las plataformas electrónicas en materia de seguridad informática que cuidan y garantizan la protección de datos.

Por el contrario, debido a su alto impacto que está causando en los mercados las instituciones bancarias se han estado reunido con frecuencia para construir una línea de defensa "El objetivo es convertir la tecnología blockchain en un sistema

[124] Ortega Uribe Daniel " La Tecnología Blockchain en el sector Bancario"http://vitela.javerianacali.edu.co/bitstream/handle/11522/11602/Tecnologia_blockchain_sector_bancario.pdf?sequence=1&isAllowed=y Consulta 9 de Agosto del 2020

eficiente para compensar deudas, reducir costes y tiempo en las operaciones y programar el dinero de manera eficaz"[125]

Agilizar estos movimientos ayuda a que se pueda repeler amenazas como las antes mencionadas en otros capítulos.

4.1.3 Elementos de Blockchain

Descentralización

Al ser una Tecnología sin intermediarios, no existe una autoridad central que valide las operaciones, entonces la confianza se construye con base en programas de software que validan, verifican y hacen un consenso de las operaciones, es por eso que se llamada red descentralizada.

La intención "es crear una comunidad a nivel mundial que sirva en el funcionamiento de la blockchain.

Fuente: (Buterin, 2017)

"Los datos se distribuyen a través de diferentes servidores y su gestión no depende de una "entidad" central (están descentralizados)"[126]

[125] Burgueño Fernández Pablo "Apunes sobre el uso de Blockchain en el Sector Financiero, https://www.pablofb.com/2019/08/apuntes-sobre-el-uso-de-blockchain-en-el-sector-financiero/ Consulta 14 de Agosto del 2020

[126] García Moreno Carlos "Descentralización, inmutabilidad y seguridad de los datos, las claves de Blockchain"https://www.indracompany.com/es/blogneo/descentralizacion-inmutabilidad-seguridad-datos-claves-blockchain Consulta 19 de Agosto del 2020

Inmutabilidad

Esta se caracteriza en información que almacenan “Es decir, la incapacidad de realizar cambios en el historial o libro mayor de la blockchain”[127]

Con esto la información no se puede editar, se queda exactamente desde el último acceso a la terminal, es decir que “cuando emitimos una transacción en una blockchain, la información que enviamos ya va marcada con un hash (el TXID o ID de transacción) y una firma digital. El TXID nos ayuda a rastrear la transacción en todo momento, asignándole un identificador único para toda su existencia”[128]

Es decir que el uso de este elemento se caracteriza por principalmente porque “son a priori modificables (son inmutables) y están protegidos criptográficamente (son seguros)”

4.1.4 Usabilidad de Blockchain y la prevención en robo y extracción de datos Bancarios

El escenario del uso de los dispositivos para las instituciones bancarias ha provocado un robo excesivo de datos personales. Debido al uso inevitable de dispositivos para entrar a la Red se debe de adoptar medidas de seguridad, principalmente cuando se tiene información delicada y de alto valor. Una solución es usar plataformas seguras blindadas con un sistema de encriptación eficaz y nuevo. El mercado nos ofrece Blokchain como tecnología que puede usar para la seguridad bancaria. Lo que hace es hacer una clave pública y una privada y es la forma es que la información no puede ser manipulada ya que varios serán los usuarios.

[127] Investing, “Seguridad en la blockchain, conoce los elementos que la conforman” 20 de abril del 2020 https://es.investing.com/news/cryptocurrency-news/seguridad-en-la-blockchain-conoce-los-elementos-que-la-conforman-1990973 Consulta 22 de Agosto del 2020

[128] Investing, “Seguridad en la blockchain, conoce los elementos que la conforman” 20 de abril del 2020 https://es.investing.com/news/cryptocurrency-news/seguridad-en-la-blockchain-conoce-los-elementos-que-la-conforman-1990973 Consulta 1 de Septiembre del 2020

El uso excesivo de las plataformas obliga a que se creen mecanismos y el uso de tecnologías para poder prevenir el robo de información. Los bancos –como sector más afectado- se beneficiarían mucho y aumentaría la calidad de su servicio, se protegería el dinero de las personas y sobre todo se aprovecharía de forma correcta los espacios virtuales, realizando pagos confiables, transacciones con un alto grado de confianza.

La Usabilidad mezclada con el concepto de blockchain ayudaría definitivamente a la Política Criminal porque brindaría datos con respecto a la ubicación de ciberdelincuentes. Se podría rastrear a las personas que quieran ingresar por número de veces a claves privadas.

La Tecnología de Blockchain se aprovecharía para que las instituciones dedicadas a la práctica forense se establezcan para poder brindar atención a usuarios en línea. Por ejemplo, la policía cibernética tiene la "finalidad de prevenir, por medio del monitoreo y patrullaje en la red pública, cualquier situación constitutiva de un delito que pudiera poner en riesgo la integridad física y patrimonial de los habitantes de la Ciudad de México." [129] Está ayudándose de tecnologías de blockchain podría prevenir e investigar de forma puntual actos informáticos acontecidos en otros momentos de los hechos.

4.2 Planeación para enfrentar al tipo de delincuente Bancario

4.2.1 Delincuentes comunes

Cómo hemos visto en el capítulo anterior la ciberdelincuencia se desarrolla en ámbito digital, no obstante, la clasificación dentro de la política criminal se puede dirigir hacia delincuentes que sólo lo que quieren es sacar un provecho económico.

[129] Policía Cibernética https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica Consulta 9 de septiembre del 2020

Un delincuente común en la informática es aquél que viola los protocolos de seguridad de sitios informáticos para poder obtener información y efectuar ataques principalmente al sistema Bancario. Se utiliza programación de alto nivel como herramienta de desencriptación y violación de las plataformas electrónicas.

Este tipo de delincuentes se dedican a lucrar robando información para un posterior ataque. Su forma de operar de clandestina muchas veces no es detectada por las autoridades oficiales, debido a que operan en la clandestinidad con seudónimos o alias.

Para poder neutralizar a este tipo de delincuentes se les restringe directamente con una protección de datos usando Blockchain, cadenas de datos encriptadas que tienen varios usuarios en diferentes partes del mundo.

4.2.2 Delincuentes políticos

Son aquellos que por alguna razón ideológica se atreven a violentar sitios para que estas acciones puedan surtir efecto ante las decisiones políticas.

Un ejemplo fue lo que mencione en un capítulo anterior respecto a Estonia que fue víctima de un ataque cibernético debido a un problema con la política estonia que a Rusia no le convenía, el resultado inmediato fue un ataque a la Banca Electrónica de Estonia, nulificando operaciones bancarias y sobre todo negación de servicios. El problema duro días hasta que se pudo resolver el incidente.

Muchas veces estos tipos de sujetos actúan en instituciones públicas y privadas, operan para personalidades que tienen fines políticos. Por lo general trabajan para personalidades que quieren dar guerra asimétrica.

4.2.3 Elementos principales

La Banca Electrónica es atacada por la ciberdelincuencia y como elemento principal es la violación de cierta plataforma. Se debe distinguir entre la causa del problema

y la consecuencia, que ya se ha trabajado en los capítulos anteriores. Ahora lo que se debe de reunir una serie de elementos que generen mecanismos de defensa.

Un sistema de control es el “computo Forense” el cual es una disciplina que se ayuda de las ciencias de la computación y la criminología para poder identificar hallazgos en materia de ciberdelincuencia organizada.

Se implementa una cadena de custodia en materia de cómputo forense. En la actualidad los laboratorios de ciberseguridad hablan muy seriamente de poder abrir una investigación ante la cantidad de ataques cibernéticos.

La complejidad de poder obtener datos cuando se cometen robos a partir de la violación de plataformas bancarias de muy complicado ya que en muchas ocasiones es difícil detectar y rastrar indicios que lleven al hallazgo principal. Cuando se tiene evidencia física se puede tener un trabajo amplio, son embargo cuando el crimen se cometió directamente en “La nube” este se transforma en un caso muy especial. A pesar de esto con técnicas de desencriptación es posible rastrar las señales, esto es a partir del filtrado y modulación. Si se utiliza la tecnología blockchain las investigaciones van a poder ser más productivas debido a que se va registrar con facilidad el usuario que haya querido entrar en este caso al “Sistema de Pagos Electrónicos”.

4.2.4 Estrategias de información en materia de encriptación.

Se debe implementar de la mano de la estrategia de ciberseguridad una propuesta en materia de encriptación en los Bancos que han sufrido ataques cibernéticos. La estrategia de ciberseguridad debe de acompañarse de esta encriptación.

Si analizamos los puntos de la “Estrategia de Ciberseguridad” podemos empezar a realizar un vínculo.

La estrategia tiene objetivos marcados como son: Sociedad y sus derechos en el Ciberespacio, economía e innovación en el ciberespacio,

Para lograr una protección adecuada a cada uno de los cinco objetivos estratégicos, la ENCS plantea ocho ejes transversales:

1) “Cultura de la ciberseguridad”, referente al conjunto de valores, principios y acciones en materia de concientización, educación y formación, los cuales inciden en la forma de interactuar en el ciberespacio de una manera armónica, confiable y como factor de desarrollo sostenible. [130] En este punto el blokchain permitirá que se pueda garantizar la armonización. Será muy difícil que alguien pueda vulnerar las plataformas, esto se puede implementar brindándoles la cultura de blockchain para proteger los datos.

2) “Desarrollo de capacidades”, busca la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad.[131] La cadena de datos que encriptará cualquier clase de información, puede generar la competitividad del capital humano, es decir que ayudará para poder fijar mejor el perfil de las personas dentro de la red y que no sean extraídos sus datos personales de la red. Blockchain es una nueva visión para las empresas las cuales adoptaran patrones de vigilancia digital.

3) “Coordinación y colaboración”, encaminadas a la generación y fortalecimiento de las capacidades organizacionales, de capital humano y recursos tecnológicos en materia de ciberseguridad. [132] Si le damos un enfoque a el ámbito bancario nos vamos a encontrar que varios bancos nacionales se han estado poniendo de acuerdo para poder combatir a la cibercriminalidad, un ejemplo de banco es

[130] “Estrategia Nacional de Ciberseguridad”
https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
Consulta 10 de septiembre del 2020

[131] “Estrategia Nacional de Ciberseguridad”
https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
Consulta 11 de septiembre del 2020

[132] “Estrategia Nacional de Ciberseguridad”
https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf
Consulta 12 de septiembre del 2020

Santander el cual ha estado diseñando la posible implementación de blockchain "no solo funciona para realizar transacciones económicas. Con esta tecnología se pueden almacenar y transferir documentos e información importante de empresas sin la posibilidad de que alguien pueda acceder a ella sin su consentimiento."[133] Es decir que la tecnología tendrá impacto en otras industrias importantes que se deriven de la industria 4.0.

4) "Investigación, desarrollo e innovación en TIC" refiere al fomento de la investigación, desarrollo e innovación en el uso y aprovechamiento de las tecnologías en materia de ciberseguridad. [134] En los laboratorios de ciberseguridad de los institutos de nuestro país se ha incrementado la investigación sobre todo se han concentrado en materia de blockchian, la UNAM está trabajando respecto a esto. Como institución sería la máxima casa de estudios está implementado proyectos de gran trascendencia con esta tecnología y la define como" una base de datos distribuida y segura, gracias al cifrado, que aplica para distintos tipos de transacciones, ya sea de valores o datos, con la seguridad de que la identidad de los usuarios y el contenido de la transferencia serán desconocidos por terceras personas, lo que evitará robo de información"[135]

5) "Estándares y criterios técnicos", refiere al desarrollo, adopción y fortalecimiento de los estándares, criterios técnicos, mejores prácticas y de normalización en materia de ciberseguridad. [136] Enfocado al ámbito bancario esta puede funcionar debido a que se analizarán estándares en materia de ciberataques y se podrá

[133] Santander, "Blockchain: seguridad y transparencia al servicio de la Banca" https://www.santander.com/es/stories/blockchain-seguridad-y-transparencia-al-servicio-de-la-banca Consulta 20 de septiembre del 2020

[134] Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 21 de septiembre del 2020

[135]Espinoza Magali, "La revolución tecnológica llamada blockchain" Global UNAM, 12 de Agosto del 2019http://www.unamglobal.unam.mx/?p=70831 Consulta 22 de septiembre del 2020

[136] Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 23 de septiembre del 2020

aplicar criterio en materia de repeler incidentes cibernéticos. Las buenas prácticas se verán reflejada en una educación digital obteniendo datos óptimos que refleje la usabilidad de Blockchain.

6) “Infraestructuras Críticas, para minimizar la probabilidad de riesgos y vulnerabilidades en el uso de las TIC para la identificación, monitoreo y gestión de infraestructuras críticas”. [137] Esto se ve reflejado en la recopilación de datos que apenas se está realizando en materia de ciberataques. Para crear una infraestructura en materia de Blockchain se debe de adoptar “Un árbol de Ataque” ” Estructura de datos en forma de árbol donde a partir de un objetivo final (representado como la raíz) se identifican (como ramificaciones) objetivos secundarios que nos permitirían alcanzar el objetivo final. Los árboles de ataque se utilizan para modelar las posibles vías por las que puede perpetrarse un ataque” [138] en otros términos, se crea un software en este caso que tenga base blockchain para poder proteger los nodos, debido a que el hackeo se da precisamente en este lugar. Un nodo se caracteriza principalmente por un punto de intersección en la nube que está conectado a redes de interconectividad. Al ser vulnerado este se deduce que tiene una debilidad, por ello se debe de atender el problema para minimizar la probabilidad de riesgos.

7) “Marco jurídico y autorregulación”, busca adecuar el marco jurídico nacional vinculado a la ciberseguridad y promover mejores prácticas de autorregulación. [139] Este punto que no da la ENCS es muy importante porque se deberá flexibilizar las

[137] Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 24 de septiembre del 2020

[138] Glosario, Arboles de Ataque https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=72.html Consulta 27 de septiembre del 2020

[139] Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 28 de septiembre del 2020

leyes mexicanas para poder implementar la protección necesaria y urgente de los datos bancarios. El Marco jurídico tendrá que ser discutido por los legisladores.

8) “Medición y seguimiento, encaminado al fomento y desarrollo de mecanismos homologados de medición que permitan dar seguimiento a los resultados obtenidos de la implementación de la ENCS, así como proporcionar métricas de uso general. Cómo se comentaba en el punto 6 respecto al diseño de una estrategia basada en blockchain para poder evitar y prevenir el robo de información bancaria, se debe culminar es la protección de la red de interconectividad, la cual puede ser vulnerada con la violación de un nodo. El nodo puede violarse y el ciberataque puede actuar de forma lenta, denegando poco a poco servicios. La encriptación que ofrece blokchain tiene muchas alternativas el principal “reto consiste en prevenir el mal uso de esta forma de transferencia electrónica” [140]

Todas las acciones de la ENCS se han de desarrollar sobre tres principios rectores: 1. Perspectiva de derechos humanos; 2. Enfoque basado en gestión de riesgos, y 3. Colaboración multidisciplinaria y de múltiples actores.

4.3 Estrategia preventiva de Política Criminal para el tratamiento del robo de extracción de datos Bancarios.

4.3.1 Planilla de Investigación de cómputo forense en Bancos

Ante la implementación de Blockchain se debe de contar con instalaciones en materia de seguridad informática, ante una investigación inicial se debe de identificar primera un hecho, encontrar un indicio, este puede ser un espacio físico, pero también un espacio la red el cual es rastreado y puesto en cadena de custodia. “Para realizar investigaciones sobre delitos relacionados con las TI se utilizan

[140] Espinosa Magali, “La revolución tecnológica llamada blockchain” Global UNAM 12 de agosto del 20|9 http://www.unamglobal.unam.mx/?p=70831 Consulta 29 de septiembre del 2020

técnicas de cómputo forense con el objetivo de preservar y analizar adecuadamente la evidencia digital. Asimismo, se encuentra ligado a aspectos legales que deben considerarse para presentar adecuadamente los resultados arrojados por la investigación de la evidencia digital" [141] Este tipo de evidencia debe ser tratada por" técnicas de ingeniería forense aplicadas al análisis de dispositivos móviles"[142]

Una rama muy importante que le compete al cómputo forense para poder realizar una investigación respecto al indicio es la geolocalización, la cual "consiste en obtener la ubicación geográfica de un objeto como puede ser un teléfono móvil, un coche o una calle. Para ello se puede utilizar diferentes métodos como por ejemplo comprobar el código postal de una carta, la dirección IP de un equipo o el sistema GPS de nuestro teléfono móvil." [143]

Esta disciplina ayuda a la cadena de custodia agiliza el proceso de investigación porque ofrece una instrumentación efectividad.

La Geolocalización ofrece las siguientes ventajas:

- Obtener resultados de una búsqueda basados en la ubicación.
- Publicidad personalizada en función de tu ubicación.
- Pedir ayuda en caso de emergencia, como por ejemplo un accidente
- Conocer la posición de una flota de vehículos.
- Dar a conocer en redes sociales la ubicación de una foto o un video.
- Analizar el comportamiento de los usuarios para mejorar la "experiencia de uso".

[141] Congreso Seguridad en Computo 2018, UNAM, https://congreso.seguridad.unam.mx/2017/L1 Consulta 30 de septiembre del 2020

[142] Centro Especializado para el aprendizaje " Computo Forense Digital", https://cea-fdm.mx/computo-forense-digital Consulta 30 de septiembre del 2020

[143] Accesos Corporativos " Geolocalización: virtudes y riesgos", 20 de Septiembre del 2016 https://www.osi.es/es/actualidad/blog/2016/09/20/geolocalizacion-virtudes-y-riesgos Consulta 8 de Octubre del 2020

- Realizar estudios con los que mejorar una tecnología existente o crear una nueva[144]

Por otro lado, tenemos al hacking ético el cual contribuye a la investigación y ayuda a desencriptar todo aquel indicio que se encuentre que sea de carácter digital. En México contamos con una línea cibernética la cual participa en las cadenas de custodia, todo apegado al procedimiento indicado al "Acuerdo 009" en sus disposiciones preliminares capítulo 1 en dónde se nos indica que es un "Sistema de control y registro que se aplica al indicio o elemento material probatorio, desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión" con esto estamos hablando de dispositivos físicos que contengan información de carácter digital, la otra es encontrar el dispositivo dónde se inició el hackeo el cual es asegurado y sometido al procedimiento.

El blockchain tendrá una participación importante porque ayudará a generar un dictamen que será la "opinión científico técnica que emite por escrito un perito o experto en cualquier ciencia, arte, técnica u oficio, como resultado del examen de personas, hechos, objetos o circunstancias sometidos a su consideración"[145]

La persona que realice este tipo de dictámenes deberá de conocer de Ciberseguridad especialmente de Ingeniería forense, experta en blockchain para poder desencriptar información e identificar problemas relacionado con el ataque de nodos y su vulnerabilidad.

---

[144] Accesos Corporativos " Geolocalización: virtudes y riesgos", 20 de Septiembre del 2016 https://www.osi.es/es/actualidad/blog/2016/09/20/geolocalizacion-virtudes-y-riesgos Consulta 11 de Octubre del 2020

[145]Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 18 de Octubre del 2020

Cómo lo sustenta el acuerdo A009 en cuanto a que "**Elemento material probatorio.** Evidencia física, objeto, instrumento o producto relacionado con un hecho delictivo y que puede constituirse como prueba" debe de ponerse en práctica."[146] Esto quiere decir cómo preservar las evidencias electrónicas, y obtener los conocimientos teórico-prácticos suficientes para realizar informes periciales en la materia.

Hablar de cómputo forense nos indica que no existe todavía una solución, es decir si se realizara una denuncia ante el ministerio público se debió de indicar de robo de identidad y extracción de datos persónales, la tipificación se haría elementalmente por extorción.

Al aumentar las denuncias en los últimos años los bancos se blindaron y antes de poder confiar en las autoridades las instituciones obedecieron a realizar estrategias de ciberseguridad para evitar todo este escenario de denuncias, ya que les estaba costando mucho dinero y como no se encontraba por lo general al responsable se caía en un vacío jurídico, debido a la falta de interpretación de la ley en materia sobre todo de daño patrimonial.

Un ejemplo de aplicación de la ciberseguridad en materia de protección de datos personales es la "Estrategia de Ciberseguridad que en el 2017 realizó el Banxico el cual se basó en los siguientes criterios:

I) Proteger la información y sus procesos, no sólo los sistemas y aplicaciones informáticas. La ciberseguridad en Banco de México abarcará aspectos adicionales a los tecnológicos, como seguridad de la información. [147] Este punto importante nos refleja el interés de la protección de los sistemas informáticos, esto usando

[146] Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 20 de Octubre del 2020

[147]"Estrategia de Ciberseguridad del Banco de México" 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 21 de Octubre del 2020

estrategias de protección de encriptación para blindar las plataformas y evitar la vulnerabilidad. Esto algo similar como lo está haciendo Santander aplicando Blockchain y brindar seguridad y transparencia al servicio de la banca.

II) Abordar el tema desde una perspectiva proactiva y dinámica que permita salir en busca de indicadores de compromiso o prevención de riesgos, en lugar de sólo reaccionar a incidentes informáticos; [148] En este caso se da el tratamiento de los incidentes, es decir crear una fuerza cibernética para poder repeler ataques directamente al sistema de pagos electrónicos y sobre todo tener una planilla de cómputo forense para poder combatir estos incidentes con tecnología blokchain.

III) Enfocar la seguridad de la información a todo el ecosistema, extendiendo requerimientos hacia las instituciones financieras que interactúan con Banco de México;[149] Por lo general la atención a víctimas en materia de robo de datos personales es un problema hoy en día que deja estadísticas enormes de robo de dinero digital las cuales son atendidas a partir de un requerimiento exigido a la institución bancaria. El Blockchain ayudará a poder identificar el origen del robo de datos, a partir de un análisis de encriptación en nodos de un sistema. Se identifica el nodo vulnerado y se informa de los resultados, estableciendo hora, lugar y fecha del ataque.

IV) Reforzar la gobernabilidad de la seguridad de la información, reorganizando áreas, dotando de recursos humanos, y diseñando políticas institucionales de ciberseguridad.[150] Este punto que se toca ayuda mucho a que se pueda atender el

[148] "Estrategia de Ciberseguridad del Banco de México" 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 23 de Octubre del 2020

[149] "Estrategia de Ciberseguridad del Banco de México" 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 26 de Octubre del 2020

[150] "Estrategia de Ciberseguridad del Banco de México" 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 28 de Octubre del 2020

problema, es decir que a partir de las estadísticas de los incidentes y el resultado de los dictámenes periciales en cómputo forense basados en Blockchain se pueda determinar que se necesita atender un problema, el cual debe tener una mediación inmediata para atenderse como un problema público y se pueda diseñar una política pública que pueda atender esta disyuntiva.

La política deberá de estar diseñada a partir de “Fromework de seguridad” termino que se utiliza para hacer una propuesta ante las organizaciones para ayudarlas a afrontar de mejor manera los riesgos en materia de ciberseguridad.

Dentro de esta propuesta de Política Criminal se debe de hacer mención de la falta de tipificación de ciertas conductas que afectan la integridad de los DH en datos personales en la nube. Los datos bancarios son violentados por delincuentes políticos y comunes, teniendo un fin diferente que por lo tanto se debe de considerar como nuevas conductas de orden penal.

4.3.2 Cadena de Custodia y la participación de Blockchain

La propuesta de esta figura se puede interpretar de diferente forma, no obstante, se tiene que aterrizar el concepto de forma objetivo y enfocado a la evidencia digital. Dentro de mi investigación con la finalidad de poder establecer una solución preventiva para el robo de datos personales en el ámbito bancario en México, me di a la tarea además de la planilla forense de poder establecer pasos para la “Cadena de Custodia” en el ámbito digital. Cada segundo, minuto, hora y día se ejecutan acciones en la red desde entrar a sitios lícitos y revisar información, hasta internarse en la red y entrar a sitios de dudosa construcción.

La cadena de custodia en el ámbito digital se ve representado por la evidencia física en donde se descargaron datos digítales y los datos que están en la nube que son investigados bajo instrumentación especializada en materia de seguridad informática.

La cadena de custodia ayuda a que la evidencia digital pueda archivarse para que a través de la investigación forense en cómputo, se pueda prevenir delitos cibernéticos.

La cadena de custodia tiene una inclinación muy importante en materia de Blockchain, se refuerza y "permite crear bases de datos que son prácticamente inalterables"[151]

No obstante, para poder llegar a un entorno digital se pasa por una cadena de custodia tradicional ejemplo si tenemos un caso en un Banco, desde dónde se realizó el hecho lo que se tiene que hacer es lo siguiente:

4.3.2.1 Detección, Identificación y registro

Se hace la identificación de elementos informáticos "debitados, –computadoras, red de computadoras, netbook, notebook, celular, ipad, gps, etc.-.**- Inventario de Hardware en la Inspección y Reconocimiento Judicial - Formulario Registro de Evidencia"**[152]

"

a. Colocarse guantes

b. Fotografiar el lugar del hecho o filmar todos los elementos que se encuentran en el área de inspección, desde la periferia hacia el área dubitada.

[151] Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019 https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 4 de Noviembre del 2020

[152] Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011 http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 9 de Noviembre del 2020

c. Fotografiar los elementos informáticos, determinando en cuál de ellos efectuar macro fotografía:
    i. Pantallas del monitor del equipo dubitado.
    ii. Vistas frontal, lateral y posterior, según corresponda
    iii. Números de series de los elementos informáticos, etiquetas de garantías.
    iv. Periféricos, (teclados, mouse, monitor, impresoras, agendas PDA, videocámaras, video grabadora, Pendrive, dispositivos de almacenamiento en red, Unidades de Zip o Jazz, celulares, ipod, entre otros)
    v. Material impreso en la bandeja de la impresora o circundante
    vi. Cableados
    vii. Dispositivos de conectividad, alámbricos e inalámbricos
    viii. Diagramas de la red y topologías"[153]

En esta primera etapa se puede apreciar que se hace la recopilación de todo objeto que pudiera haber sido vulnerado por los cibercriminales. Después nos quedaría la investigación de todos estos objetos para poder llevar a cabo una investigación más robusta en el área digital.
Se procede a lo siguiente:

d. "Inventariar todos los elementos utilizando una planilla de registro del hardware, identificando: Tipo, Marca, Número de serie, Registro de garantía, Estado (normal, dañado), Observaciones Particulares. consultar **Inventario del hardware de la Inspección Judicial y Reconocimiento Judicial – Formulario de Registro de evidencia de la computadora**

[153] Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011, http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 14 de Noviembre del 2020

e. Efectuar un croquis del lugar del hecho, especificando el acceso al lugar, la ubicación del o los equipos informáticos y de cualquier otro elemento, mobiliario, racks, cableado, existentes en el área a inspeccionar, para luego representarlo con cualquier herramienta de diseño."[154]

El procedimiento inicial es esencial y pertenece a lo que se hace referencia en el Acuerdo A009/15 en su segunda disposición preliminar en donde se dice que "Elemento material probatorio. Evidencia física, objeto, instrumento o producto relacionado con un hecho delictivo y que puede constituirse como prueba"[155]

Evidentemente el acuerdo nos menciona más respecto a la cadena de custodia, no obstante, quisiera hacer énfasis sobre todo en lo que se dice en la disposición preliminar V dónde nos menciona que "La cadena de custodia deberá comprender las siguientes etapas y en todas ellas se debe llevar a cabo el registro correspondiente"[156] en dónde se hace hincapié en lo referente a Procesamiento de los indicios, traslado, análisis, almacenamiento y disposición final.

En el ámbito cibernético el procesamiento y sobre todo el análisis forense se llevan a cabo de la siguiente forma:

[154] Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011 http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 17 de Noviembre del 2020

[155] Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 19 de Noviembre del 2020

[156] Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 26 de Noviembre del 2020

4.3.2.2 "Recolección de los elementos informáticos dubitados –Físicos o Virtuales-

El Perito Informático Forense deberá recolectar la evidencia procediendo acorde al origen del requerimiento de la pericia informático forense, a saber:"[157]

PROCEDIMIENTO

1. "Por orden judicial, cuyo texto indica:

    a. Secuestrar la evidencia para su posterior análisis en el laboratorio, el Perito Informático Forense procederá a:
        i. Certificar matemáticamente la evidencia
        ii. Identificar y registrar la evidencia
        iii. Elaborar un acta ante testigos
        iv. Iniciar la cadena de custodia
        v. Transportar la evidencia al laboratorio

    b. Efectuar la copia de la evidencia para su posterior análisis en el laboratorio, el Perito Informático Forense procederá a:
        i. Certificar matemáticamente la evidencia
        ii. Duplicar la evidencia
        iii. Identificar y registrar la evidencia y la copia
        iv. Elaborar un acta ante testigos
        v. Transportar la copia o duplicación de la evidencia al laboratorio"[158]

[157] Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011,http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 30 de Noviembre del 2020

[158] Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011 http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 17 de Noviembre del 2020

En esta fase de la cadena de custodia se puede introducir el Blokchain el cual trabaja el análisis digital de los “nodos”, es decir que se analiza “el gigantesco libro de cuentas donde los bloques están enlazados y cifrados”[159] En la siguiente imagen se ve un árbol el cual se puede implementar para el análisis de la información encontrada.

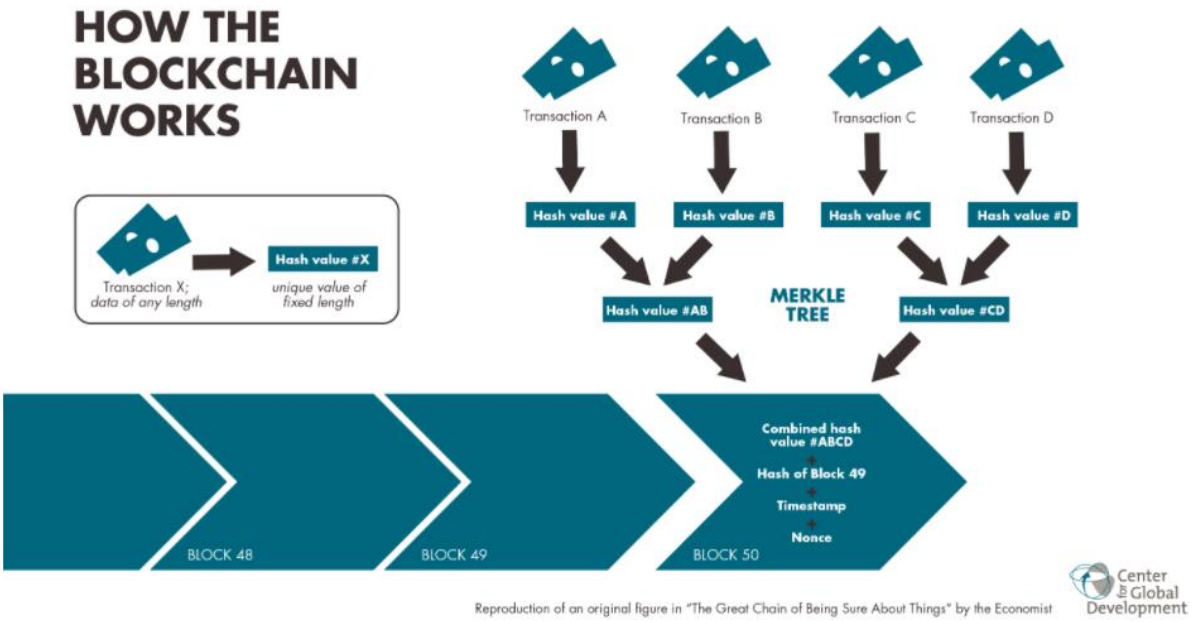
---

[158] Diario Oficial de la Federación “**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA” 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 19 de Noviembre del 2020

[158] Diario Oficial de la Federación “**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA” 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 26 de Noviembre del 2020

[158] Darahuge María Elena, El Investigador “ La cadena de Custodia informático Forense” 3 de Noviembre del 2011,http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 30 de Noviembre del 2020 http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 14 de Diciembre del 2020

[159] Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 19 de Diciembre del 2020



Como podemos ver en este diagrama de árbol se puede visualizar la forma de trabajar de Blochkchain en la cadena de custodia la cual "Cada bloque de la cadena contiene unos metadatos característicos, donde existe un hash criptográfico dependiente del bloque anterior. De este modo, para la modificación de un único bloque, es necesario modificar la cadena al completo, lo que requiere el consenso del resto de nodos participantes en la cadena"[160]

El Blokchain refuerza la cadena de custodia en el ámbito digital es decir que "esta propiedad se usa para crear registros de información con prueba de movimientos y trazabilidad. Estos registros forman una identidad digital de cada elemento que se registra, que tiene a partir de ese momento un historial propio y trazable"[161]

[160] Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019 https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 7 de Enero del 2020

[161] Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019 https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 14 de Enero del 2020

Los registros en la red tienen hoy en día el mismo valor, lo vemos principalmente en la gestoría de procesos que se llevan de modo digital. La evidencia digital se puede trabajar a través de lo que se genere de la:

1. Servicio de registro: Almacenar registros digitales en un libro distribuido inmutable y auditable.

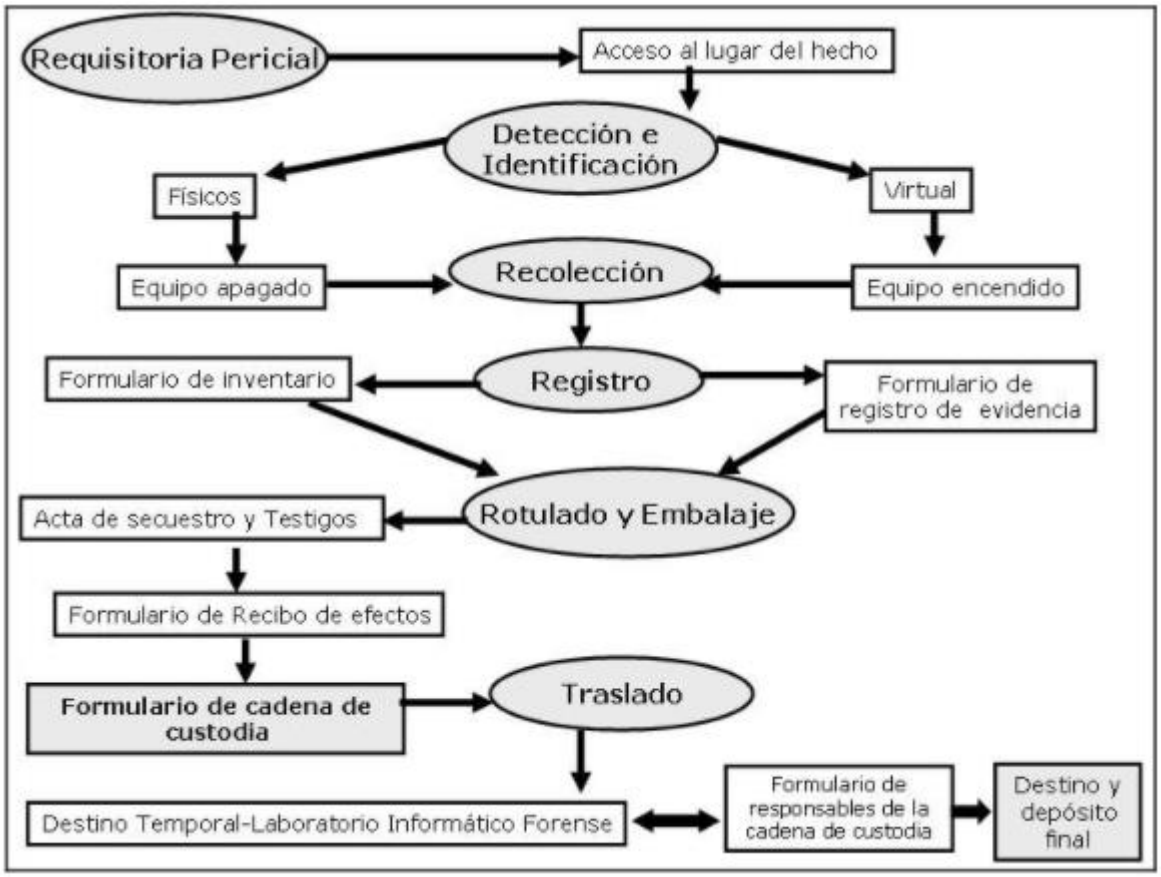
2. Intercambio de activos: Creación de activos y transferencia de la propiedad.

3. Ejecución de contratos inteligentes: Automatizar procesos comerciales ejecutando un código.[162]

Esto último se somete al ámbito de los "bienes materiales, estos registros se presentan como especialmente útiles para la identificación y el seguimiento del origen de los bienes y de su cadena de custodia"[163]

[162] Yvonne-Anne Pignolet "Blockchain: elementos básicos y avanzados" https://search.abb.com/library/Download.aspx?DocumentID=9AKK107046A1240&LanguageCode=es&DocumentPartId=&Action=Launch Consulta 14 de Enero del 2020

[163] Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 15 de Enero del 2020



164

Después de poder analizar ciertos registros se puede hacer análisis con "**un sistema de trazabilidad específico en redes blockchain** según las necesidades de un particular sector, como por ejemplo sistemas de trazabilidad de alimentos o de bienes de gran valor"[165]

Esto último depende mucho de una persona preparada un "perito forense en materia de Blockchain"

[164] Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011, http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 15 de Enero del 2020

[165] Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 16 de Enero del 2020

> “La trazabilidad en la red de blockchain también ha alcanzado el campo de los bienes inmateriales. Se ha descrito en la utilidad de un registro de estas características para la trazabilidad de la explotación de las obras en soporte digital. Una vez creada la identidad digital de la obra, sería posible acreditar su autenticidad, identificar al autor, registrar sus sucesivas transmisiones, sus actos de explotación, conocer el alcance y asegurar la validez de las licencias obtenidas, etc.”[166]

4.3.3 Prevención

Las instituciones Bancarias son atacadas y desgraciadamente no se cuenta con una línea de avanzada de defensa. El índice Global de ciberseguridad encuentra que **México falla precisamente en estrategia, coordinación, acuerdos internacionales y alianzas público-privadas**. Tampoco ha desarrollado un ecosistema de emprendimiento de *startups* y el talento en ciberseguridad es muy escaso”[167]

Como se mencionó con anterioridad es fundamental que se pueda elevar a nivel de política pública la disyuntiva para el problema de los robos de datos personales, para poder lidiar en lo que se hace el diseño, se debe de establecer líneas de prevención para hacer frente al problema. Cómo se ha consultado en el capítulo 3 respecto a la línea cibernética que cuenta la UE se puede analizar su modelo de prevención y también su conjunto de líneas de acción.

---

[166] Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 16 de Enero del 2020

[167] Bravo Jorge “Estrategia Nacional de Ciberseguridad” 30 de Julio del 2020 https://www.proceso.com.mx/640722/estrategia-nacional-ciberseguridad-mexico-columna-jorge-bravo Consulta 16 de Enero del 2020

4.3.4 Aplicación de una estrategia de ciberseguridad, encriptación de Datos Bancarios.

Una de las soluciones que se ha presentado últimamente es la de la existencia de "una iniciativa de la senadora Lucía Trasviña Waldenrath (Morena) de una Ley de Seguridad Informática que daría paso a una Agencia Nacional de Seguridad Informática, la cual pertenecería a la Secretaría de Seguridad y Protección Ciudadana federal"[168]

Hasta la fecha se ha elaborado la denominada "ley Olimpia" la cual se caracteriza por atender el problema de "violencia digital y mediática"[169]

Esta ley se encarga principalmente de atender principalmente la violencia sexual en el ámbito digital, no obstante es un punto a favor para que se pueda fortalecer la idea de "elevar a nivel de política pública la ciberseguridad en México.

La aplicación de una estrategia de ciberseguridad basada en Blockchain para protección de datos bancarios debe tener un enfoque netamente en acciones de carácter público como: a) una transacción monetaria, b) un registro de transacciones monetarias y c) un sistema que verifica y almacena las transacciones monetarias.

Su implementación tiene un alto beneficio debido a que "ofrece beneficios potenciales para la prevención del fraude e incluso para la eliminación de algunos errores propios de los humanos."[170]

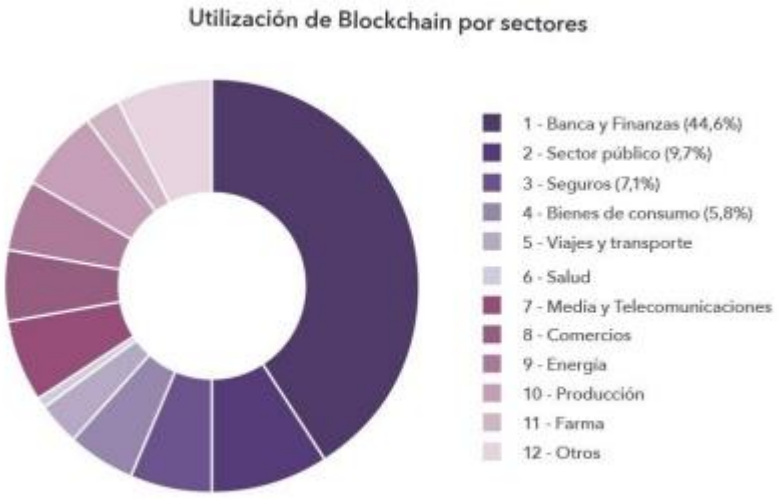
---

[168] Bravo Jorge "Estrategia Nacional de Ciberseguridad" 30 de Julio del 2020 https://www.proceso.com.mx/640722/estrategia-nacional-ciberseguridad-mexico-columna-jorge-bravo Consulta 18 de Enero del 2020

[169] Senado de la República "Aprueban la Ley Olimpia; hasta seis años de cárcel a quien viole la intimidad sexual" 5 de Noviembre del 2020 http://comunicacion.senado.gob.mx/index.php/informacion/boletines/49590-aprueban-la-ley-olimpia-hasta-seis-anos-de-carcel-a-quien-viole-la-intimidad-sexual.html Consulta 18 de Enero del 2020

[170] Zúñiga Díaz Elizabeth "La tecnología Blockchain en las instituciones financieras" 27 de Diciembre del 2018 https://www.ig.com/es/estrategias-de-trading/la-tecnologia-blockchain-en-las-instituciones-financieras-181224 Consulta 18 de Enero del 2020

La necesidad de usar esta tecnología para bajar los índices de criminalidad en el ámbito digital ha tenido buena respuesta debido a que desde el 2018 ya es usado en diferentes industrias como:



Fuente datos: Microsoft

La seguridad industrial obliga al uso de esta tecnología debido a que según

> "investigaciones en el 2018 Global Blockchain Survey de PwC, aproximadamente un 84% de los ejecutivos encuestados están buscando calcular el impacto que esta tecnología podría tener en sus negocios. Paralelamente, compañías globales como Amazon, Microsoft, IBM y Facebook evalúan posibles aplicaciones para el blockchain, al igual que otras instituciones financieras, como JP Morgan

> y HSBC, y otras multinacionales líderes en consultoría y auditorías, como Accenture y Deloitte (respectivamente).”[171]

En este tenor se tiene que seguir la línea de acción de la Estrategia de Ciberseguridad, la cual plantea diferentes puntos preventivos, uno de ellos es el uso de una “Plataforma más deficiente en materia de seguridad” es aquí donde se va a utilizar el Blockchain como herramienta de seguridad informática que va encriptar la información bancaria.

No cabe duda que los miedos globales propuestos por Urlich Beck como producto de la mundialización y la expansión industrial, traen como consecuencia la creación de figuras como “El Blockchain” el cual promete ser una solución para problemas futuros en diferentes industrias ya mencionadas. En el caso del ámbito bancario la realización de miles de operaciones bancarias conlleva al mundo a tener riesgos de carácter informático y digital. . “Desafortunadamente estas herramientas también son objeto e instrumento de conductas ilícitas que causan afectación a otras personas físicas o morales, y a sus patrimonios”[172]

Los riesgos directos son precisamente la generación de conductas en el ámbito digital que deben ser prevenidas y también sancionadas.

Según el fuentes del banco BBVA

> ““el mayor impacto potencial de una contabilidad pública podría ir más allá del sistema de pagos. Dado que la mayoría de los activos financieros, como bonos, valores, derivados y préstamos ya son electrónicos, sería posible que algún día todo el sistema se reemplazara por una estructura descentralizada. De hecho, las últimas

[171] Zúñiga Díaz Elizabeth “La tecnología Blockchain en las instituciones financieras” 27 de Diciembre del 2018 https://www.ig.com/es/estrategias-de-trading/la-tecnologia-blockchain-en-las-instituciones-financieras-181224 Consulta 18 de Enero del 2020

[172] Justicia México, “Delitos Informáticos” https://mexico.justia.com/derecho-penal/delitos-informaticos/ Consulta 18 de Enero del 2020

> innovaciones utilizan tokens para almacenar y comercializar activos como valores, bonos, automóviles, casas y productos básicos"[173]

El uso de blockchain podría prevenir conductas en materias de: robo y extracción de datos personales en el ámbito bancario, robo de identidad partir del uso de "programas de cómputo (software) y el hardware; los teléfonos inteligentes; tabletas; redes como Internet; sistemas informáticos y otros"[174]

CONCLUSIÓN

El miedo al cambio global siempre va acompañado de caos y problemas, no obstante la humanidad sale adelante y cumple sus cometidos a partir de nuevas propuestas. Las ideas mueven al mundo y lo llevan a la vanguardia, la sociedad adopta "nuevos escenarios de usabilidad", de conocimiento y aplicación de la tecnología.

El escenario de la era digital lo estamos viviendo y se necesitan nuevas alternativas para poder enfrentar a los males públicos globales, y sobre todo, los peligros asociados que conllevan los referentes digitales que se presentan, cada vez con mayor frecuencia.

La era de las máquinas y la cibernética involucran a muchas disciplinas, principalmente las de orden forense, en dónde lo que se busca es principalmente encontrar los procedimientos pertinentes de investigación de resultados con transcendencia jurídicas y nuevas líneas de investigación que hagan frente a los problemas de la delincuencia organizada.

---

[173] BBVA, "Bitcoin: luces y sombras"BBVA, https://www.bbva.com/es/bitcoin-luces-sombras/ Consulta 18 de Enero del 2020

[174] Justicia México, "Delitos Informáticos", https://mexico.justia.com/derecho-penal/delitos-informaticos/ Consulta 18 de Enero del 2020

La prevención de delitos a partir de la tecnología blockchain se ha convertido en una nueva necesidad, ante las actuales formas de operar del crimen organizado que han afectado principalmente a las instituciones bancarias, entre otras instancias.

No cabe duda que en los próximos años se tendrá que apoyar mucho a la "Estrategia Nacional de Ciberseguridad" para poder elevarlo a nivel de política pública el problema del robo de datos personales en el ámbito bancario.

Cada vez más las instituciones van a implementar una estrategia en materia de ciberseguridad que ayude a blindar principalmente los datos que están albergados en la nube y principalmente la información de sus servidores de base. Las tecnologías de último nivel pueden frenar el robo de información en instituciones bancarias, obteniendo como resultado, plataformas confiables, sitios web confiables, mejores aplicaciones con alto grado de seguridad, mejor confianza por parte de las personas, mejor usabilidad, mayor responsabilidad por parte de los usuarios, una ambiente de libertad en materia de derechos el humanos en el Ciberespacio.

El ambiente de la vulnerabilidad se puede cambiar significativamente implementado una estrategia de ciberseguridad basado en la información de encriptación de datos para poder proteger las terminales del ciberespacio.

La Informática forense es una rama joven que está ayudando a combatir este tipo de conducta delictiva, a partir de técnicas y metodologías enfocadas a criptografía con la que se puede detectar a partir de la geolocalización cualquier terminal que pretenda ser vulnerada.

La presente tesis se realizó con la finalidad de resolver una problemática que nos aqueja día con día y que merece poner atención debido a que hay muchas víctimas las cuales buscan justicia y merecen ser atendidas.

He llegado a la conclusión de que las nuevas tecnología implican un nuevo uso de medidas jurídicas para poder regular la conducta de un sujeto que opera en plataformas electrónicas, el blockchain ayudará a poder blindar la información y

sobre todo a poder custodiar la información. La conducta de los nuevos perfiles criminales debe ser atendida porque los mayores problemas ahora ya no sólo están en la vida pública sin en la vida virtual de los individuos.

En lo personal me siento satisfecho de poder haber concluido esta tesis y el haber expuesto un problema que sin lugar a duda en el futuro tendrá un amplio campo de ocupación tanto para la Política Criminal, el Computo Forense y el Derecho.

La ingeniería social que se presenta en la actualidad nos ofrece una nueva oportunidad para mejorar en nuestros hábitos y costumbres. Las Tecnologías de la Información nos facilitarán una mejor calidad de vida y para asegurarla se necesita un buen cuidado de nuestros datos personales.

Ante este joven conocimiento el nivel de compromisos se incrementará y se buscará un nuevo campo de investigación para la vigilancia digital.

“Los frutos del blockchain serán dulces en el futuro por el nivel se seguridad que se brindará” [175]

[175] Calles Meléndez José Román “cita propia” Octubre del 2021

FUENTES

BIBLIOGRAFÍA

1. A. de Sola, "El pensamiento Criminológico", Edit. Temis, Colombia, 1983, Pág. 247
2. Barry Buzan, People, States and Fear, 1983, Inglaterra, Pág. 16
3. Beck, Ulrich, "La Sociedad del Riesgo", Barcelona, Edit. Paidos, Iberica, 1986, Pág. 40
4. Beck, Ulrich (1998), "*La sociedad del riesgo. Hacia una nueva modernidad"*, Barcelona, Paidós. Pág. 70
5. Beck Ulrich, "La Sociedad del Riesgo", Barcelona, Edit. Paidos,Iberica, 1986, Pág. 144
6. Calles Meléndez José Román "cita propia" Octubre del 2021
7. Diccionario de la Real Academia Española, "Diccionario de la Lengua Española", Edit. Vox, España, 2002, Pág. 70
8. Elizondo Elisa Rosa, "Informática I", Edit. Mc. Graw. Hill, 2006, México Pág. 25
9. Ferrajoli Luigi "Derechos y Garantías", Edit. Trotta, 2004, Pág. 108
10. Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 15
11. González Becerreil Mabel Luna, "La tecnología de Blockchain y su impacto en el Sector Público en México. Análisis del caso Blockchain HACKMX"
12. Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 14
13. Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 14
14. Goodman Marc, "Cibercriminalidad", Edit. Impresos Chávez, 2003, Pág. 14
15. López, Jorge Chinea, "Tipos de herramientas básicas para garantizar la ciberseguridad en la empresa",
16. Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 164
17. Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 153
18. Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 153
19. Iñiaki Rivera Raúl, "Criminología y Ciencias Penales" Edit. Anthropos, España, 2005, Pág. 153

20. Martínez Echeverría A. Miguel, "Informática y Derechos Humanos", Pág. 99

21. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.26
22. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.26
23. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.27
24. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág. 30

25. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.32
26. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.33

27. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.34
28. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág. 35

29. Molina Benítez Armando, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.44

30. Téllez Valdés Julio, "Derecho Informático", Edit Mc Graw Hill, 2009, México, Pág. 21

31. Téllez Valdés Julio, Derecho Informático, Edit. MC Graw Hill, Edición 2018, Pág. 20

32. Téllez Valdés Julio, Derecho Informático, México, MC Graw Hill, 2018, Pág. 13 Ibid

33. Téllez Valdés Julio, Derecho Informático, México, MC Graw Hill, 2018, Pág. 19 Ibidem

34. Téllez Valdés Julio, Derecho Informático, México, MC Graw Hill, 2018, Pág. 19 Idem

35. Paul Lara, "1 e cada 3 cliente, víctimas de hackers", Edit. Excélsior, 12 de Julio del 2009 Consulta 18 de agosto del 2019

36. Vasconcelos Santillana Jorge, "Informática II Sistemas de Información", Publicaciones culturales, México 2002, Pág. 30

37. Zaffaroni, Raul, "Derecho Penal", Buenos Aires, Edit. Ediar, 1973 Pág. 14

38. Zaffaroni, Raul, "Derecho Penal", Buenos Aires, Edit. Ediar, 1973 Pág. 15

39. Armando Benítez Molina, "Propuesta del delito informático", Edit. UNAM, Edición diciembre de 2009, Pág.29

CIBERGRAFÍA

40. Accesos Corporativos " Geolocalización: virtudes y riesgos", 20 de Septiembre del 2016 https://www.osi.es/es/actualidad/blog/2016/09/20/geolocalizacion-virtudes-y-riesgos Consulta 8 de Octubre del 2020

41. Accesos Corporativos " Geolocalización: virtudes y riesgos", 20 de Septiembre del 2016 https://www.osi.es/es/actualidad/blog/2016/09/20/geolocalizacion-virtudes-y-riesgos Consulta 11 de Octubre del 2020

42. Agencia de la Unión Europea para la Seguridad Cibernética, https://www.enisa.europa.eu/topics/incident-reporting Consulta 30 de agosto del 2019

43. Andrade Edith, "Detectan nueva modalidad de fraude en Sinaloa" Edit. Debate, 2 de Octubre del 2018 https://www.debate.com.mx/sinaloa/nuevo-fraude-sinaloa-robo-de-datos-empresas-falsas-modulos-publicos-20181002-0023.html Consulta 8 de agosto del 2019

44. Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 6 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 27 de Abril del 2019

45. Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 7 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 27 de Abril del 2019

46. Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 8 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 28 de Abril del 2019

47. Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 9 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 28 de Abril del 2019

48. Anthony V. Teelucksingh, "Delitos en Internet a gran escala", Edit. OEA, 2010, Pág. 10 https://www.oas.org/juridico/spanish/cyber/cyb_per_escala.pdf Consulta 29 de Abril del 2019
49. Expok https://www.expoknews.com/ciberseguridad-derecho-humano/ Consulta 30 de Abril del 2019

50. Antonio Hernández "Costó 107 mmd recuperación por ciberataques, dice la OEA", Edit. El Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 23 de agosto del 2019

51. Aura Hernández "Ciber Ataques en el 2020 se materializan; expertos advierten auge en hackeos" , Excelsior, 11 de abril del 2020 https://www.excelsior.com.mx/hacker/ciberataques-en-2020-se-materializaran-expertos-advierten-auge-en-hackeos/1355817?fbclid=IwAR1Ks_7qewpVBM2JG4Es4PWUnxfiMFrios69yCLFLpFzg3ODo0u1iLHx0hE Consulta 19 de Abril del 2020
52. Banco de México, "Sistema de Pagos Electrónicos Interbancarios (SPEI)" https://www.banxico.org.mx/sistemas-de-pago/d/%7B89B6CCF0-6070-7389-3DD5-B27AC4ECD9D1%7D.pdf Consulta 4 de Marzo del 2020

53. Banco de México, “Sistema de Pagos Electrónicos Interbancarios (SPEI)” https://www.banxico.org.mx/sistemas-de-pago/d/%7B89B6CCF0-6070-7389-3DD5-B27AC4ECD9D1%7D.pdf Consulta 8 de Marzo del 2020

54. Banxico, “Estrategia de Ciberseguridad del Banco de México” 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 21 de Octubre del 2020

55. Banxico, “Estrategia de Ciberseguridad del Banco de México” 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 23 de Octubre del 2020

56. Banxico, “Estrategia de Ciberseguridad del Banco de México” 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 26 de Octubre del 2020

57. Banxico, “Estrategia de Ciberseguridad del Banco de México” 2019 https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf Consulta 28 de Octubre del 2020

58. Bravo Jorge “Estrategia Nacional de Ciberseguridad” 30 de Julio del 2020 https://www.proceso.com.mx/640722/estrategia-nacional-ciberseguridad-mexico-columna-jorge-bravo Consulta 16 de Enero del 2020

59. Bravo Jorge “Estrategia Nacional de Ciberseguridad” 30 de Julio del 2020 https://www.proceso.com.mx/640722/estrategia-nacional-ciberseguridad-mexico-columna-jorge-bravo Consulta 18 de Enero del 2020

60. BBVA “Bitcoin: luces y sombras”BBVA, https://www.bbva.com/es/bitcoin-luces-sombras/ Consulta 18 de Enero del 2020

61. Bravo Jorge, “Estrategia Nacional de Ciberseguridad” 30 de Julio del 2020 https://www.proceso.com.mx/640722/estrategia-nacional-ciberseguridad-mexico-columna-jorge-bravo Consulta 5 de Agosto del 2020

62. Burgueño Fernández Pablo “Apunes sobre el uso de Blockchain en el Sector Financiero, https://www.pablofb.com/2019/08/apuntes-sobre-el-uso-de-blockchain-en-el-sector-financiero/ Consulta 14 de Agosto del 2020

63. Centro Especializado para el aprendizaje “Computo Forense Digital”, https://cea-fdm.mx/computo-forense-digital Consulta 30 de septiembre del 2020

64. Cámara de Diputados http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf 16 de agosto del 2019

65. Cámara de Diputados http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf 16 de agosto del 2019

66. Ciberseguridad https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad Consulta 1 de Septiembre del 2019

67. Código Civil del Del Distrito Federal http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/180/180163.pdf Consulta 10 de agosto del 2019

68. Código Civil del Del Distrito Federal http://sjf.scjn.gob.mx/SJFSist/Documentos/Tesis/180/180163.pdf 13 de agosto del 2019

69. Convenio de Budapest, 2001, https://www.oas.org/juridico/english/cyb_pry_convenio.pdf Consulta 20 de agosto del 2019

70. Congreso Seguridad en Computo 2018, UNAM, https://congreso.seguridad.unam.mx/2017/L1 Consulta 30 de septiembre del 2020

71. Darahuge María Elena, El Investigador "La cadena de Custodia informático Forense" 3 de Noviembre del 2011, http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 14 de Noviembre del 2020

72. Darahuge María Elena, El Investigador "La cadena de Custodia informático Forense" 3 de Noviembre del 2011 http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 17 de Noviembre del 2020

73. Darahuge María Elena, El Investigador "La cadena de Custodia informático Forense" 3 de Noviembre del 2011, http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 15 de Enero del 2020

74. Darahuge María Elena, El Investigador "La cadena de Custodia informático Forense" 3 de Noviembre del 2011 http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 9 de Noviembre del 2020

75. Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011,http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 30 de Noviembre del 2020

76. Darahuge María Elena, El Investigador " La cadena de Custodia informático Forense" 3 de Noviembre del 2011,http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 30 de Noviembre del 2020

77. Demien Mc Guinness, "Cómo uno de los primeros ciberataques de origen ruso de la historia transformó a un país" Edit BCC de Londre, https://www.bbc.com/mundo/noticias-39800133?fbclid=IwAR3MxHaP2NUHwUbXTtWNBRabUXftDbV0qTnZi6ZAhjZ7ZvqrmC_zXZ2tGwg Consulta 22 de Febrero del 2020

78. Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 19 de Noviembre del 2020

79. Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 26 de Noviembre del 2020

80. Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 18 de Octubre del 2020

81. Diario Oficial de la Federación "**ACUERDO POR EL QUE SE ESTABLECEN LAS DIRECTRICES QUE DEBERÁN OBSERVAR LOS SERVIDORES PÚBLICOS QUE INTERVENGAN EN MATERIA DE CADENA DE CUSTODIA" 2015** https://www.dof.gob.mx/nota_detalle.php?codigo=5381699&fecha=12/02/2015 Consulta 20 de Octubre del 2020

82. Economía simple .net https://www.economiasimple.net/glosario/ciberseguridad Consulta : 3 de Marzo del 2019

83. Estrategia Nacional de Ciberseguridad http://www.oas.org/documents/spa/press/Recomendaciones-para-el-Desarrollo-de-la-Estrategia-Nacional-de-Ciberseguridad.pdf Consulta 23 de agosto del 2019

84. Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 21 de septiembre del 2020

85. Espinoza Magali, "La revolución tecnológica llamada blockchain" 12 de Agosto del 2019http://www.unamglobal.unam.mx/?p=70831 Consulta 22 de septiembre del 2020

86. Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 23 de septiembre del 2020

87. Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 24 de septiembre del 2020

88. Estrategia Nacional de Ciberseguridad https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 28 de septiembre del 2020

89. "Estrategia Nacional de Ciberseguridad" https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 10 de septiembre del 2020

90. Estrategia Nacional de Ciberseguridad https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf Consulta 3 de Septiembre del 2019

91. Espinosa Magali, "La revolución tecnológica llamada blockchain" Global UNAM 12 de agosto del 20|9 http://www.unamglobal.unam.mx/?p=70831 Consulta 29 de septiembre del 2020

92. El senado de Estados Unidos aprueba una Ley de Ciberseguridad" Edit. El Mundo. https://www.elmundo.es/internacional/2015/10/28/5630219e46163f29348b4595.html Consulta 11 de Noviembre del 2019

93. El senado de Estados Unidos aprueba una Ley de Ciberseguridad" Edit. El Mundo. https://www.elmundo.es/internacional/2015/10/28/5630219e46163f29348b4595.html Consulta 17 de Noviembre del 2019

94. Expok, "Comunicaciones de Sustentabilidad", https://www.expoknews.com/ciberseguridad-derecho-humano/ Consulta 20 de Mayo del 2019

95. Flores León, "Banxico, preocupado por los ciberataques" El universal, 25 de marzo de 2019, https://www.eluniversal.com.mx/cartera/banxico-preocupado-por-los-ciberataques Consulta 16 de Marzo del 2020

96. García Moreno Carlos "Descentralización, inmutabilidad y seguridad de los datos, las claves de Blockchain"https://www.indracompany.com/es/blogneo/descentralizacion-inmutabilidad-seguridad-datos-claves-blockchain Consulta 19 de Agosto del 2020

97. Globalkfinanz, "¿Sabes qué es un ataque cibernético y cuáles son los más comunes?" https://www.responsabilidadconsejerosydirectivos.com/que-son-los-ataques-ciberneticos/ Consulta 9 de Abril del 2020
98. Glosario, Arboles de Ataque https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=72.html Consulta 27 de septiembre del 2020

99. Guadarrama José de Jesús, "Nada detiene el robo de Identidad", Edit. Excelsior, 2019, México, Pág.14 https://www.excelsior.com.mx/periodico/flip-dinero/17-03-2019/portada.pdf Consulta: 20 de Abril del 2019

100. Harán, Manuel, Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 6 de Abril del 2019

101. Harán Manuel Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 10 de Abril del 2019

102. Harán Manuel Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 11 de Abril del 2019

103. Harán Manuel Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 21 de Abril del 2019

104. Harán Manuel Juan, "Los ciberataques dirigidos a bancos más importantes de los últimos tiempo", Wilive security, 2018 https://www.welivesecurity.com/la-es/2018/06/01/ciberataques-dirigidos-bancos/ Consulta: 21 de Abril del 2019

105. Hernández Antonio, “Costó 107 mdd recuperación por ciberataques, dice OEA” Edit. Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 1 de Marzo del 2020

106. Hernández Antonio, “Costó 107 mdd recuperación por ciberataques, dice OEA” Edit. Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 3 de Marzo del 2020

107. Hernández Antonio, “Incrementan ciberataques financieros: Banorte” El universal, 21 de Abril 2018 https://www.eluniversal.com.mx/articulo/cartera/finanzas/2016/10/21/incrementan-ciberataques-financieros-banorte Consulta 25 de Marzo del 2020

108. Hernández Aura, “Ciber Ataques en el 2020 se materializan; expertos advierten auge en hackeos”, Excelsior, 11 de abril del 2020 https://www.excelsior.com.mx/hacker/ciberataques-en-2020-se-materializaran-expertos-advierten-auge-en- Consulta 12 de Febrero del 2020 hackeos/1355817?fbclid=IwAR1Ks_7qewpVBM2JG4Es4PWUnxfiMFrios69yCLFLpFzg3ODo0u1iLHx0hE Consulta 12 de Febrero del 2020

109. Hernández Aura, “Ciberataques, reto en el 2019”, Excélsior, 4 de Diciembre del 2018. https://www.excelsior.com.mx/hacker/bajo-ciberataques-la-mitad-de-la-banca/1324085 Consulta 28 de Febrero del 2020

110. Investing, “Seguridad en la blockchain, conoce los elementos que la conforman” 20 de abril del 2020 https://es.investing.com/news/cryptocurrency-news/seguridad-en-la-blockchain-conoce-los-elementos-que-la-conforman-1990973 Consulta 22 de Agosto del 2020

111. Investing, “Seguridad en la blockchain, conoce los elementos que la conforman” 20 de abril del 2020 https://es.investing.com/news/cryptocurrency-news/seguridad-en-la-blockchain-conoce-los-elementos-que-la-conforman-1990973 Consulta 1 de Septiembre del 2020

112. INCIBE, 2014, https://www.incibe.es/protege-tu-empresa/blog/herramientas-basicas-ciberseguridad-empresa Consulta 24 de Abril del 2019

113. INFOBAE, 22 de mayo del 2019, https://www.infobae.com/america/mexico/2019/05/22/como-atraparon-a-la-mayor-banda-de-hackers-mexicanos-que-orquesto-robos-millonarios-al-sistema-bancario/ Consulta 20 de Abril del 2020

114. Jeannete Leyva “Así fue el ciberataque a la banca en 2018” El Financiero, 29 de Abril del 2019, https://www.elfinanciero.com.mx/economia/asi-fue-el-ciberataque-a-la-banca-en-2018 Consulta 20 de Marzo del 2020

115. Jeannete Leyva “Así fue el ciberataque a la banca en 2018” El Financiero, 29 de Abril del 2019, https://www.elfinanciero.com.mx/economia/asi-fue-el-ciberataque-a-la-banca-en-2018 Consulta 20 de Marzo del 2020

116. Jeannete Leyva “Así fue el ciberataque a la banca en 2018” El Financiero, 29 de Abril del 2019, https://www.elfinanciero.com.mx/economia/asi-fue-el-ciberataque-a-la-banca-en-2018 Consulta 27 de Marzo del 2020

117. Justicia México, “Delitos Informáticos”, https://mexico.justia.com/derecho-penal/delitos-informaticos/ Consulta 18 de Enero del 2020

118. Lexico Oxford, “Diccionario de Inglés y Español, https://es.oxforddictionaries.com/definicion/meme Consulta 30 de Abril del 2019

119. Ley Federal del Derecho de Autor. http://www.diputados.gob.mx/LeyesBiblio/pdf/122_150618.pdf 15 de agosto del 2019

120. Ley Federal de Protección de datos personales en posesión de los particulares, http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf Consulta 20 de agosto del 2019

121. Legal Information Institute, 18 U.S. Code § 1030.Fraud and related activity in connection with computers https://www.law.cornell.edu/uscode/text/18/1030 Consulta 8 de Octubre del 2019

122. Laura Paula, “Hackers endurecen chantaje a Pemex; suben a la red documentos de la empresa”, Excélsior, 27 de Febrero del 2020 https://www.excelsior.com.mx/nacional/hackers-endurecen-chantaje-a-pemex-suben-a-la-red-documentos-de-la-empresa/1366588 Consulta 29 de Febrero del 2020

123. Martínez Carla, “Ciberataques contra los bancos se incrementan”https://www.eluniversal.com.mx/cartera/se-disparan-ciberataques-contra-bancos-cuestan-784-mdp Consulta 30 de Febrero del 2020

124. Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019 https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 4 de Noviembre del 2020

125. Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 19 de Diciembre del 2020

126. Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019 https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 7 de Enero del 2020

127. Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019 https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 14 de Enero del 2020

128. Martínez Asier “Usos del blockchain para reforzar la cadena de custodia” 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cade

na%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 15 de Enero del 2020

129. Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 16 de Enero del 2020

130. Martínez Asier "Usos del blockchain para reforzar la cadena de custodia" 25 de abril del 2019, https://solidgeargroup.com/blockchain-custodia-forense/?lang=es#:~:text=Usos%20del%20blockchain%20para%20reforzar%20la%20cadena%20de%20custodia.&text=Esta%20propiedad%20se%20usa%20para,un%20historial%20propio%20y%20trazable. Consulta 16 de Enero del 2020

131. Navarro Fernando, Wikileaks: cómo destapar escándalos en Internet, Edit. El país, https://elpais.com/internacional/2010/07/26/actualidad/1280095206_850215.html Consulta 22 de Noviembre del 2019

132. Notimex, "Hackers detrás de ataques al SPEI, estuvieron dentro de las redes de los bancos por año y medio" El Economistas, 7 de abril del 2019, https://www.eleconomista.com.mx/sectorfinanciero/Hackers-detras-de-ataques-al-SPEI-estuvieron-dentro-de-las-redes-de-los-bancos-por-ano-y-medio-20190407-0018.html Consulta 7 de Marzo del 2020

133. OBAE, 22 de mayo del 2019, https://www.infobae.com/america/mexico/2019/05/22/como-atraparon-a-la-mayor-banda-de-hackers-mexicanos-que-orquesto-robos-millonarios-al-sistema-bancario/ Consulta 22 de Abril del 2020

134. ONU, Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010. http://www.onu.org.mx/la-unodc-presenta-su-programa-global-de-ciberdelito-durante-la-5a-semana-nacional-de-la-ciberseguridad-en-mexico/ Consulta 30 de Marzo del 2020

135. ONU, "Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil", del 12 al 19 de abril de 2010". https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml Consulta 22 de agosto del 2019

136. ONU, "Xº Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador, Brasil, del 12 al 19 de abril de 2010". https://www.un.org/es/conf/xcongreso/prensa/2088hs.shtml Consulta 22 de agosto del 2019

137. OVH CLOUD, "Anti DDos" https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml?fbclid=IwAR0xBFfrLvqD4qJvZESGA2Le4Mr6V4TMUYpN0g8xoLrbsOL6n0FwHkN7_Ok ídem Consulta 21 de Febrero del 2020

138. OVH CLOUD, "Anti DDos" https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml?fbclid=IwAR0xBFfrLvqD4qJvZESGA2Le4Mr6V4TMUYpN0g8xoLrbsOL6n0FwHkN7_Ok ibídem Consulta 22 de Febrero del 2020

139. Ortega Uribe Daniel, “La Tecnología Blockchain en el sector Bancario” http://vitela.javerianacali.edu.co/bitstream/handle/11522/11602/Tecnologia_blockchain_sector_bancario.pdf?sequence=1&isAllowed=y Consulta 7 de Agosto del 2020

140. Ortega Uribe Daniel “ La Tecnología Blockchain en el sector Bancario”http://vitela.javerianacali.edu.co/bitstream/handle/11522/11602/Tecnologia_blockchain_sector_bancario.pdf?sequence=1&isAllowed=y Consulta 9 de Agosto del 2020

141. Palacios Surya, “Capital” Casos más graves del robo de identidad” Edit. Capital, 19 de Julio del 2017 https://www.capitalmexico.com.mx/especial/casos-mas-graves-del-robo-de-identidad-sat-adeudos-fiscales/ Consulta 1 de agosto del 2019

142. Palacios Surya, “Capital” Casos más graves del robo de identidad” Edit. Capital, 19 de Julio del 2017 https://www.capitalmexico.com.mx/especial/casos-mas-graves-del-robo-de-identidad-sat-adeudos-fiscales/ Consulta 5 de agosto del 2019

143. Paul Lara, “Bajo ciberataque la mitad de la banca”, Edit. Excélsior, https://www.excelsior.com.mx/hacker/bajo-ciberataques-la-mitad-de-la-banca/1324085 Consulta 5 de Abril del 2020

144. Passeri Paolo “Hackmageddon” https://www.hackmageddon.com/2020/03/03/january-2020-cyber-attacks-statistics/ Consulta 16 de Abril del 2020

145. Paula Lara “Hackers endurecen chantaje a Pemex; suben a la red documentos de la empresa” , Excélsior, 27 de febrero del 2020 https://www.excelsior.com.mx/nacional/hackers-endurecen-chantaje-a-pemex-suben-a-la-red-documentos-de-la-empresa/1366588Consulta 15 de Abril del 2020

146. Passeri Paolo, “HACKMAGEDDON2 3 de marzo del 2020 https://www.hackmageddon.com/2020/03/03/january-2020-cyber-attacks-statistics/ Consulta 15 de Mayo del 2020

147. Policía Cibernética https://www.ssc.cdmx.gob.mx/organizacion-policial/subsecretaria-de-inteligencia-e-investigacion-policial/policia-cibernetica Consulta 9 de septiembre del 2020

148. Ramírez Castro Alexandra, “Riesgo Tecnológico y su impacto para las organizaciones parte 1”Seguridad, cultura de prevención para TI” UNAM, https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i Consulta: 7 de Abril del 2019

149. Rangel Arturo, Animal Político, 17 de marzo del 2019, https://www.animalpolitico.com/2019/03/fiscalia-responsables-ciberataques-bancos/?fbclid=IwAR3c-2lROoKgjtnAb1vY1nmNGXnY8Htd7vF-ALqpjZHyC_GtdN9-utULJug Consulta 26 de Marzo del 2020

150. Real Academia Española http://lema.rae.es/dpd/srv/search?key=software Marzo del 2019

151. Real Academia Española https://dle.rae.es/?id=QgpwJRv Marzo del 2019

152. Reynolds Michel, Así fue el 'caso Wikileaks', Edit. P Internacional, https://www.elperiodico.com/es/internacional/20170118/asi-fue-el-caso-wikileaks-5750289 Consulta 23 de Noviembre del 2019

153. Riquelme Rodrigo, "5 sectores más expuestos en ciberataques en México", Edit. El Economista, https://www.eleconomista.com.mx/tecnologia/5-sectores-mas-expuestos-a-ciberataques-en-Mexico-20191112-0058.html Consulta 25 de Febrero del 2020

154. Riquelme Rodrigo, "18% de instituciones financieras recibió ataques cibernéticos por segunda vez en 2018: Mandiant", Edit. El Economista, 26 de Marzo del 2019. https://www.eleconomista.com.mx/tecnologia/18-de-instituciones-financieras-recibio-ataques-ciberneticos-por-segunda-vez-en-2018-Mandiant-20190326-0018.html Consulta 19 de agosto del 2019

155. Santander, "Blockchain: seguridad y transparencia al servicio de la Banca" https://www.santander.com/es/stories/blockchain-seguridad-y-transparencia-al-servicio-de-la-banca

156. Consulta 20 de septiembre del 2020

157. Senado de la República "Aprueban la Ley Olimpia; hasta seis años de cárcel a quien viole la intimidad sexual" 5 de Noviembre del 2020 http://comunicacion.senado.gob.mx/index.php/informacion/boletines/49590-aprueban-la-ley-olimpia-hasta-seis-anos-de-carcel-a-quien-viole-la-intimidad-sexual.html Consulta 18 de Enero del 2020

158. SEGOB, "Estrategia de Ciberseguridad", 2018 https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf Consulta 29 de Mayo del 2019

159. SEGOB, "Estrategia de Ciberseguridad", 2018 https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf Consulta 23 de Abril del 2019

160. SEGOB, "Estrategia de Ciberseguridad", 2018 https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf Consulta 25 de Abril del 2019

161. SEGOB, "Estrategia de Ciberseguridad", 2018 https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf
Consulta 26 de Abril del 2019

162. SEGOB, "Estrategia Nacional de Ciberseguridad" https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 11 de septiembre del 2020

163. SEGOB, "Estrategia Nacional de Ciberseguridad" https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf Consulta 12 de septiembre del 2020

164. Seguridad Cibernética, 12 de diciembre 2011, Nueva York, https://www.un.org/development/desa/es/news/intergovernmental-coordination/seguridad-cibernetica.html Consulta 22 de Agosto.

165. Sistema de Seguridad Nacional https://www.dsn.gob.es/es/sistema-seguridad-nacional/qu%C3%A9-es-seguridad-nacional/%C3%A1mbitos-seguridad-nacional/ciberseguridad Consulta 3 de Septiembre del 2019

166. Tony Roing, "El Investigador"http://policiasenlared.blogspot.com/2011/11/la-cadena-de-custodia-informatico.html Consulta 14 de Diciembre del 2020

167. Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 24 de agosto del 2019

168. Universal, 12 de julio del 2019, https://www.eluniversal.com.mx/cartera/costo-107-mdd-recuperacion-por-ciberataques-dice-oea Consulta 25 de agosto del 2019

169. Villa y Caña Pedro, "Ciberataques, una amenaza exterior contra organismos", El Universal, 14 de Octubre del 2018 https://www.eluniversal.com.mx/nacion/ciberataques-una-amenaza-exterior-contra-organismos Consulta 2 de Abril del 2019

170. Wonder. Edit. BBC, 2010 https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet Consulta 10 de Octubre del 2019

171. Wonder. Edit. BBC, 2010 https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet Consulta 10 de Octubre del 2019

172. Yvonne-Anne Pignolet "Blockchain: elementos básicos y avanzados" https://search.abb.com/library/Download.aspx?DocumentID=9AKK107046A1240&LanguageCode=es&DocumentPartId=&Action=Launch Consulta 14 de Enero del 2020

173. Zuñiga Díaz Elizabeth "La tecnología Blockchain en las instituciones financieras" 27 de Diciembre del 2018 https://www.ig.com/es/estrategias-de-trading/la-tecnologia-blockchain-en-las-instituciones-financieras-181224 Consulta 18 de Enero del 2020