



UNIVERSIDAD LA SALLE

FACULTAD DE DERECHO

CON RECONOCIMIENTO DE VALIDEZ OFICIAL DE
ESTUDIOS POR DECRETO PRESIDENCIAL DE
FECHA 29 DE MAYO DE 1987.

**“CULTURA DE CIBERSEGURIDAD, PREVENCIÓN Y
ATENCIÓN PARA LAS EMPRESAS MEXICANAS”**

ESTUDIO DEL CASO

QUE PARA OBTENER EL GRADO DE
MAESTRA EN DERECHO DE EMPRESA

P R E S E N T A

LIC. MARÍA FERNANDA LANDGRAVE SANDOVAL

ASESOR

DR. CARLOS RAMÍREZ CASTAÑEDA

CIUDAD DE MÉXICO, 2023

Ciudad de México, 18 de abril de 2023.

ESP. GABRIEL NUÑEZ GONZÁLEZ
DIRECTOR DE GESTIÓN ESCOLAR
UNIVERSIDAD LA SALLE
P R E S E N T E.

Le informo que la C. MARÍA FERNANDA LANDGRAVE SANDOVAL, Pasante en la Facultad de Derecho de la UNIVERSIDAD LA SALLE, de la Maestría en Derecho de Empresa con reconocimiento de Validez Oficial de Estudios de la Secretaría de Educación Pública, según decreto presidencial publicado el 29 de mayo de 1987, ha elaborado el trabajo titulado "Cultura de ciberseguridad, prevención y atención para las empresas mexicanas", de conformidad con la modalidad de titulación aprobada para esta maestría.

Le comunico, además, que el trabajo que fue elaborado bajo mi conducción tiene la calidad suficiente para ser la base de sustentación de su Examen Recepcional.

ATENTAMENTE



DR. CARLOS RAMÍREZ CASTAÑEDA
ASESOR DE TESIS



MTRO. RAFAEL RICARDO SOLER SUÁSTEGUI
SECRETARIO ACADÉMICO



MTRO. JOSÉ LUIS CÁRDENAS FERNÁNDEZ
DIRECTOR

ÍNDICE

1. Introducción y planteamiento del problema

2. Comprensión de la ciberseguridad empresarial

- a. ¿Qué es la seguridad?
- b. ¿Qué es la ciberseguridad?
- c. Ciberataques existentes hacia empresas
- d. Consideraciones de la ciberseguridad
- e. Problema existente relativo a ciberseguridad en México

3. Contexto de ciberseguridad en empresas internacionales

- a. Tratados internacionales en materia de ciberseguridad
- b. Legislaciones internacionales para empresas en materia de ciberseguridad
- c. Expectativas de la ciberseguridad y su regulación desde una perspectiva internacional

4. Contexto de ciberseguridad en empresas mexicanas

- a. Legislaciones mexicanas en materia de ciberseguridad
- b. Expectativas de ciberseguridad en México

5. Propuesta de solución a la falta de cultura, prevención y atención en temas de ciberseguridad para empresas mexicanas

6. Bibliografía

7. Anexo 1 – Referencias adicionales

Introducción y planteamiento del problema

Actualmente vivimos en un mundo globalizado y tecnológico, lo cual implica que día a día todos estemos conectados a través de una red de internet, donde la mayoría de nuestras actividades se desempeña con ayuda de estas redes y de mismo modo, sean utilizados como forma cotidiana tanto de comunicarnos, como de entretenimiento, para adquirir educación y trabajar.

Derivado de la situación anterior, con el uso de las tecnologías, obtenemos grandes beneficios y facilidades para llevar a cabo nuestra vida diaria, pero a contrario sensu, encontramos que, de mismo modo, la tecnología abre una puerta para que las personas comentan delitos a través del uso de estas herramientas.

Lo anterior es una situación preocupante, toda vez que, si bien, las tecnologías avanzan y se renuevan de manera exponencial, en este mismo ritmo, avanzan los ciberataques y los daños que de estos derivan, por lo que hay que tomar ciertas precauciones para cuidar nuestra integridad digital en todos los ámbitos.

Uno de estos ámbitos que es sumamente afectado y al cual nos enfocaremos en este trabajo, es al ámbito empresarial, donde al manejarse y utilizarse tecnologías en la mayoría de las empresas para llevar a cabo sus actividades diarias, estas se encuentran en un foco rojo dentro de su operación, ya que se vuelven entes vulnerables para ser sujetos a sufrir ciberataques. Esta situación en nuestro país es muy preocupante, debido que México se

encuentra dentro de las economías más grandes del mundo, lo cual implica que, si las empresas establecidas dentro del territorio no cuentan con buena cultura, protección, legislación, entre otras cuestiones, serán objeto de un ciberdelito; lo cual vemos es un problema actual con el que contamos, como se puede ver en las siguientes estadísticas que nos menciona Jerry Low:

“México fue el país más afectado en 2019

Aunque todos los países del mundo experimentan ciberataques, los de México mostraron el mayor grado de compromiso. Más del 93.9% se vio afectado por al menos un incidente en los últimos 12 meses. Le siguió España, seguida de cerca por Italia, Colombia y China.

4 de cada 5 organizaciones experimentaron al menos un ciberataque exitoso

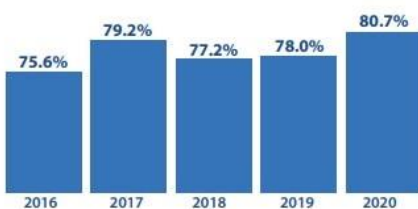


Figure 2: Percentage compromised by at least one successful attack, by year.

Imagen 1

La postura de seguridad actual en nuestro panorama de TI confirma que el 80% de las organizaciones experimentan al menos un ciberataque exitoso a un nivel récord y más de un tercio sufrió seis o mas de tales ataques.” (Low, 2022)

De igual manera, podemos ver que el problema de ciberseguridad en las empresas mexicanas es de gran preocupación desde años pasados, adicional, con la pandemia presentada en 2019 relacionada con Covid – 19 este problema se ha exponenciado como se plasma en las siguientes estadísticas del año 2020:

“México concentró 34 por ciento de los intentos de ciberataques en América Latina con 14 billones de amenazas, de los 41 billones que reportó la región, de acuerdo con FortiGuard Labs, organización de investigación e inteligencia de amenazas de la firma de ciberseguridad Fortinet.

El 25 por ciento de las empresas en México dijo haber sido víctima de un ransomware, es decir, robo de información, debido a que el teletrabajo provocó que las operaciones de las empresas fueran más vulnerables a hackeos, de acuerdo con el reporte “El estado del ransomware 2021” de la firma de ciberseguridad Sophos.

Incluso en el primer trimestre del año, México sufrió más de 800 millones de intentos de ciberataques a equipos personales, de organismos públicos y empresas, de acuerdo con Fortinet.” (Gutiérrez, 2021)

Adicional, si bien con la pandemia aumentaron los ciberataques, podemos ver que estos no se han detenido, ya que, se han vuelto una práctica habitual de los ciberdelincuentes, lo

cual es una situación que todas las empresas deben de tomar como una fuerte preocupación.

“Empresas y organizaciones mexicanas han padecido 80.000 millones de intentos de ciberataques en lo que va del año, aseguró este martes a Efe Agustín Tiburcio Sánchez, director nacional del Comité de Tecnologías de la Información de Index, agrupación industrial.

“Los datos son contundentes: de los 156.000 millones de ataques cibernéticos registrados en el primer semestre de 2022 (en Latinoamérica), unos 80.000 millones corresponden a México”, comentó Tiburcio Sánchez, del Consejo Nacional de la Industria Maquiladora y Manufacturera de Exportación (Index).” (Engelaar, 2022)

Con los ciberataques que suceden en y hacia las empresas mexicanas, se compromete no solo el trabajo e información corporativa de la empresa, sino también datos corporativos y sensibles de clientes y de sus propios trabajadores, adicional a sus activos y capitales lo que provoca que se llegue a dañar la reputación de la empresa, sus ingresos y hasta los derechos de sus propios trabajadores, colaboradores y clientes al vulnerar sus derechos a la intimidad, privacidad, derechos ARCO, propiedad intelectual, acceso a las comunicaciones privadas e internas, entre otros.

Por lo anteriormente mencionado, dentro de este trabajo explicaremos lo que implica un ciberataque, y cómo los países han enfocado lineamientos para prevenir este tipo de problemas, fomentando cultura, legislaciones y tratados que propongan medidas básicas a empresas para prevenir ciberataques y por ende proteger los derechos que pueden y son vulnerados en este tipo de ataques, con la finalidad de poder demostrar que contamos con un problema de legislación y cultura deficiente, y muchas veces inexistente, en materia de ciberseguridad en nuestro país.

Con este trabajo demostraremos que este problema enfocando a nuestro ámbito jurisdiccional, se encuentra en que México cuenta con una legislación deficiente para las empresas en materia de ciberseguridad y de igual manera una poca cultura en dicha materia, lo anterior, sin importar su tamaño y giro, ya que si bien se cuenta con algunos lineamientos, estos no se fomentan, lo cual consideramos una situación de preocupación para todos los ciudadanos y empresarios, ya que deberíamos de contar con un marco jurídico que brinde recomendaciones y exigencias en esta materia, así como un marco que contemple los ciberdelitos que existen y tribunales o autoridades especiales que conozcan y sean especialistas del tema para prevenir, fomentar, investigar y sancionar estos ciberdelitos que se comenten a las empresas segundo a segundo; ya que se comprometen derechos de los ciudadanos involucrados, por lo que el gobierno mexicano debería de fomentar una cultura en esta materia.

Con la finalidad de llegar a comprobar nuestro problema identificado y comentado anteriormente, utilizaremos el método de estudio del caso, el cual, como su definición se conoce, a través de la realización de la investigación completa e informada que realizaremos a lo largo del presente trabajo, sobre el problema grave identificado con el que contamos en nuestra situación actual como mexicanos, en el ámbito de ciberseguridad en las empresas, pondremos como objetivo general comprobar la existencia de dicho problema y sus riesgos que afectan segundo a segundo a cada empresa y específicamente centraremos una fuerte preocupación el problema con el que contamos de una legislación y cultura deficiente, y muchas veces inexistente, en materia de ciberseguridad en México, donde al establecer una posible solución a dicho problema podremos exigir una protección a nuestros derechos como ciudadanos.

Comprensión de la ciberseguridad empresarial

¿Qué es la seguridad?

Con la finalidad de que podamos comprender el significado de lo que abarca la ciberseguridad, es importante conocer y entender qué es la seguridad, la cual, si seguimos una definición coloquial, la entendemos como un acto que nos proporciona protección en cualquier ámbito, sin embargo, de conformidad con la Real Academia Española, la palabra que seguridad se define de las siguientes formas:

- “ 1. Cualidad de seguro.*
- 2. Certeza (conocimiento seguro y claro de algo).*
- 3. Fianza u obligación de indemnidad a favor de alguien.*

Desde un punto de vista jurídica:

- 1. Cualidad del ordenamiento jurídico, que implica la certeza de sus normas y, consiguientemente, la previsibilidad de su aplicación. En España es un principio constitucional.*

Desde un punto de vista social:

- 1. Organización estatal que se ocupa de atender determinadas necesidades económicas y sanitarias de los ciudadanos.*

Desde de un punto de vista de la Administración Pública:

1. *Aquel cuyo fin es el de velar por la seguridad de los ciudadanos.*” (Diccionario de la lengua Española, 2001)

Tomando en cuenta la definición antes mencionada, podemos establecer que la seguridad es aquella materia que debe velar por la protección de aquello que le pertenece con la finalidad de cuidar y mantenerlo en orden y a salvo; llevando esto a un ámbito empresarial, podemos ver que las empresas deben de velar por la seguridad de sus bienes y activos que la conforman, lo cual debe contemplar la propiedad que tienen guardada en sus nubes, computadoras, cámaras, entre todos los demás activos que se conectan a una red, las cuales deben ser cuidadas por una seguridad especializada en el ciberespacio, es decir la ciberseguridad.

Si trasladamos la seguridad que se tiene en las empresas mexicanas, vemos que la mayoría de estas normalmente enfocan la seguridad solo para proteger sus bienes tangibles, como son sus bienes inmuebles y muebles, ejemplo de estos sería su dinero, vehículos, equipo de oficina, sin considerar que es importante establecer una ciberseguridad en los bienes intangibles que utilizan y que les es posible su conexión a una red.

Esto debido que en la mayoría de las empresas establecidas en territorio mexicano que no tienen vínculos o directrices internacionales, o no han sufrido un ciberataque, no cuentan

con una cultura respecto temas digitales, ya que, se considera una ventaja, pero no se concientiza de los riesgos que se encuentran en el ciberespacio y en las acciones que haga o deje de hacer su personal utilizando las herramientas tecnológicas.

Si trasladamos lo anteriormente mencionado, la gran mayoría de las pequeñas empresas mexicanas, invertirán y solo establecerán temas de seguridad en su patrimonio, cuidando sus establecimientos y pertenencias, con el uso de candados en sus locales, cerraduras adicionales, personal asignado para llevar a cabo esta actividad, empleando cámaras, entre otros medios.

Por lo contrario, las grandes empresas establecidas en territorio mexicano, enfocarán su seguridad a sus activos, definiendo sus activos como bienes y derechos de la empresa, ejemplo de estos serían edificios, terrenos, maquinaria, marcas, patentes, inversiones, caja, clientes, mercancías, dinero, información o datos tanto de la empresa, como de sus clientes y trabajadores; en este sentido, una empresa usará diversos métodos para protegerlos como son personal de seguridad, restricción de acceso a sus instalaciones, cámaras y controles de seguridad, celebración de convenios de confidencialidad, selección en su personal, registro ante autoridades correspondientes, entre otros.

Derivado de lo anterior, tanto para empresas pequeñas, medianas o grandes, dentro de la legislación mexicana, se cuenta con diversos medios que contemplan seguridad para las personas y empresarios en la protección de sus bienes tangibles, por lo que si se llega a

cometer algún robo, fraude, o violación a su patrimonio, refiriéndonos a los bienes que no pueden sufrir un ciberataque, estos pueden ejercer algún método de defensa, ya que se contemplan en el Código Nacional de Procedimientos penales, Código Penal Federal y los Códigos Penales correspondientes.

Sin embargo, las empresas, en la mayoría de las ocasiones, no contempla que con el avance de la tecnología en el mundo, muchos de los bienes que tienen, al manejarse y almacenarse en correos electrónicos, nubes o sistemas pertenecientes a la empresa que se almacenan en Internet, corren un gran riesgo, ya que la tecnología ha permitido, si bien, avances tecnológicos que favorecen a las empresas, como es facilidad de comunicación y elaboración del trabajo, trabajo en posibilidad remota, almacenamientos en mayor masas, entre otras, también se ha utilizado para perjudicar y cometer delitos que se realicen de manera virtual, dejando sin protección a las empresas y con ello a sus trabajadores y clientes; por lo que, si una empresa, no cuenta con una seguridad que contemple estos puntos, puede considerarse que corre un gran peligro, esta rama que vigila estos puntos, es lo que actualmente se conoce como ciberseguridad.

¿Qué es la ciberseguridad?

Siguiendo la línea, podemos entender por ciberseguridad, aquella protección que se otorga algún bien intangible ingresado en el ciberespacio con la finalidad de protegerlo, adicional, se debe ver como un conjunto de procedimientos y herramientas que tienen la

finalidad de proteger la información que se ingresa y almacena en computadoras, servidores o cualquier dispositivo que tenga conexión a una red.

Adicional, es importante conocer lo que comprende la ciberseguridad en los distintos ámbitos como son jurídico, social y técnico, con la finalidad de entender en su conjunto las definiciones que se explican en cada ámbito y poder comprender la ciberseguridad en su totalidad, lo cual nos ayudará a entender el problema que se puede originar si no se fomenta en las empresas.

Para comprender la definición desde un ámbito jurídico, podemos tomar como referencia las siguientes definiciones:

“La ciberseguridad es la preservación de la accesibilidad, confidencialidad e integridad de la información y su infraestructura subyacente, a fin de mejorar la seguridad de las personas en línea y fuera de línea.” (humanos, R3D)

“Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.” (DEFENSA, 2013)

“La definición de ciberseguridad por parte de ISACA (Information Systems Audit and Control Association – Asociación de Auditoría y Control sobre los Sistemas de

Información) es la “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

(School., ESIC Business & Marketing School., 2020)

Observándolo desde un punto técnico, podemos tomar como referencia las siguientes definiciones:

“De acuerdo a los expertos de Information Systems Audit and Control Association (ISACA), la ciberseguridad se define como "una capa de protección para los archivos de información. La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos”
(Ciberseguridad, Una guía completa del concepto, tipos, amenazas y estrategias, s.f.)

“La ciberseguridad es el conjunto de acciones y maniobras destinadas a proteger equipos informáticos y conexiones en red ante posibles ataques o intentos de robo de la información o del control del dispositivo.

El significado de la seguridad informática es resultado de la combinación del prefijo Ciber, que se relaciona con todo aspecto vinculado a la Informática. Y Seguridad, que es sinónimo de protección y métodos de apoyo contra algún tipo de ataque.

Su funcionamiento se basa en la implantación de técnicas y herramientas de software y hardware que ejecutan barreras para evitar el acceso desconocido a nuestra información y de protegernos y expulsar al enemigo en caso de vulneración.”

(QUÉ ES CIBERSEGURIDAD. DEFINICIÓN, 2021)

Desde un punto de vista social, podemos entender la ciberseguridad con ayuda de las siguientes definiciones:

“La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.” (Ciberseguridad?, 2020)

“La ciberseguridad es la práctica de proteger los sistemas más importantes y la información confidencial ante ataques digitales. También conocida como seguridad de la tecnología de la información (TI), las medidas de ciberseguridad están diseñadas para combatir las amenazas a sistemas en red y aplicaciones, que se originan tanto desde dentro como desde fuera de una organización.”
(ciberseguridad?)

Tomando en cuenta los conceptos mencionados, al contemplarse la ciberseguridad se debe considerar que esta abarca desde la seguridad en el hardware, entendiéndose como la protección de elementos físicos para proteger las vulnerabilidades de los equipos; seguridad en software, entendiéndose como la protección que debe de proporcionarse a los sistemas; y seguridad en la red, entendiéndose como aquellas actividades que se encargan de proteger las vulnerabilidades que se encuentran en la red para que esta sea segura, y evitar penetraciones a los sistemas en los cuales pueda ocurrir un robo o alteración de información.

Derivado de lo anterior, con la finalidad de que las empresas puedan contar con una ciberseguridad completa, dentro de sus políticas empresariales y la legislación que les sea aplicable en la materia, deben de conocer todos los ámbitos en los cuales se describe la ciberseguridad, para que esta pueda ser entendida, implementada y fomentada.

Podemos observar que la ciberseguridad es importante en la actualidad, ya que sirve como una garantía o protección, no solo para las empresas, sino de igual forma para todos los ciudadanos, para que su información privada permanezca como tal, ya que además de contar con este derecho sobre decidir sobre el manejo de su propia información, en caso de no contar con las medidas necesarias de ciberseguridad, se puede ser acreedor de pasar por robos de identidad, robos de información, fraudes, amenazas, extorsión con la información obtenida de los ciberataques o el manejo de la empresa, entre otros

ciberdelitos ocasionados por motivo de los avances tecnológicos que se dan día a día, segundo a segundo.

Si tomamos en cuenta lo señalado a lo largo del presente trabajo, se puede ver la urgencia e importancia de fomentar la cultura de mantener una buena ciberseguridad, ya que son acciones que están sucediendo exponencialmente en la actualidad, por este motivo es importante que conozcamos los riesgos, delitos y prevenciones que tanto personalmente como empresarialmente debemos fomentar para lograr tener una cultura relativa a la ciberseguridad.

Un punto que consideramos de gran importancia es conocer la diferencia entre seguridad de la información y la ciberseguridad, ya que, si bien son diferentes, de igual manera se complementan:

- La seguridad de la información tiene la finalidad de proteger la confidencialidad, integridad y disponibilidad de la información, donde se identifique qué información se encuentra más vulnerable para sufrir tanto ataques físicos como ciberataques.
- La ciberseguridad, como se definió anteriormente, se enfoca a proteger los dispositivos electrónicos o información y equipo que tenga contacto con tecnologías y contra acciones que sean generados por actos u omisiones del personal; adicional, de igual manera, su finalidad es la prevención de los ciberataques.

Derivado de las definiciones anteriores, podemos ver que la ciberseguridad y la seguridad de la información se complementan, ya que la ciberseguridad se utilizará como el medio, para a su vez, proteger la función de la seguridad de la información.

Con la finalidad que dentro de la empresa se fomente una cultura de ciberseguridad y por ende, se conozca la materia de ciberseguridad, es importante que estas contemplen la gestión de una política empresarial dirigida a la materia de ciberseguridad, ya que estas se definen como:

“Conjunto de lineamientos o principios estructurados, en distintos niveles, que guían la toma de decisiones y la acción de una empresa. Además, dependen de la naturaleza, la filosofía y los objetivos del emprendimiento.” (ESTOS SON LOS TIPOS DE POLÍTICAS QUE PUEDE APLICAR EN SU EMPRESA)

Dentro de la rama seguridad de la información, se menciona que es importante que sus lineamientos se basen de acuerdo con los pilares de confidencialidad, integridad y acceso; ya que, con ayuda de estos, se puede entender de una mejor manera la finalidad de fomentar una cultura de ciberseguridad, lo cual permitirá conservar la confidencialidad de la información de la cual uno es propietario para poder darle acceso solo al personal que se desea dar, garantizar que dicha información sea íntegra y verídica para lo cual fue realizada, y de mismo modo para proteger el acceso a quien el titular o dueño de los datos desea darlo.

Los pilares anteriores, si bien son de seguridad de la información, de igual manera, deben de conocerse y tomarse en cuenta en materia de ciberseguridad, los cuales deben de utilizarse como base en las empresas dentro de su política empresarial enfocada en materia de ciberseguridad, donde su fin sea la protección y que se fomente una cultura de ciberseguridad para todos los integrantes de la empresa, ya que esta política funge como una ley o norma interna y aplicable para su giro y tamaño específico, la cual debe enfocarse de acuerdo a sus necesidades.

Esta política empresarial en materia de ciberseguridad debe de comunicar el objetivo que sigue la empresa, fomentar que se conozca lo que comprende la ciberseguridad, su importancia, los peligros al violar la política, su alcance, vigencia, el contenido, las herramientas que apoyarán a cumplir el objetivo y el contacto para comunicar alguna situación.

Ciberataques existentes hacia empresas

Es importante mencionar que si una empresa, sin importar su giro, tamaño o establecimiento, no toma en cuenta cuestiones de ciberseguridad, puede sufrir diversos ataques, de los cuales es importante comentar en qué pueden consistir alguno de estos, como a continuación se describe:

1. Ransomware, este tipo de ciberataque se da cuando un agente externo ingresa un software malicioso al equipo o sistemas de los usuarios, el cual puede provocar robo, bloqueo, extorsión de información, entre otras acciones.

Este tipo de ciberataque, vemos que es fácilmente que se da en empresas, aun teniendo algunos sistemas de protección, este tipo de ataques provoca prácticamente un secuestro a tu empresa y al control al cual tienes derecho, lo que puede ocasionar perdidas tanto monetarias como de clientes y de mismo modo sanciones ante diversos reguladores y autoridades; un ejemplo de esto se puede dar en la hipótesis de que se roben información almacenada en un sistema, la cual contenga datos personales de clientes, donde dicho cliente sea responsable de los datos de sus propios clientes y esto se convierta en una sanción ante la empresa por el Instituto de Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, lo cual puede provocar desde multas económicas hasta pérdida de clientes y de reputación en proyección de confianza.

- a. Rogue software o falso antivirus, es similar al ransomware pero se utiliza con un enfoque diferente ya que aparenta ser un software de seguridad pero genera alertas falsas para poder cometer el ataque; estableciéndolo dentro de la empresa, la ignorancia de los empleados o del mismo órgano de seguridad de la empresa, se puede establecer un rogueware y poder cometer un ciberataque que dañe fuertemente a la empresa.

2. Phishing, este tipo de ciberataque consiste en realizar una suplantación de identidad para robar información confidencial, lo cual se puede realizar fácilmente a empresas si sus colaboradores no toman algún tipo de capacitación para conocer este tipo de ataques, ya que es muy común que se presenten en forma de correo electrónico.
 - a. Es importante conocer que derivado del phishing podemos encontrar el vishing, el cual tiene el mismo objetivo, pero la diferencia versa en el método en el cual se emplea, donde no se presente en correo electrónico, sino mediante el uso de voz, como puede ser llamadas, las cuales las empresas, utilizan de manera diaria y con todos los empleados, por lo que es un foco rojo que se debe de considerar.
 - b. De igual manera se encuentra el smishing, el cual al igual que vishing es una variante del phishing, pero este se emplea por medio de mensajes de texto para poder engañar al usuario del teléfono; de igual manera en empresas se utilizan los celulares con la finalidad que los empleados realicen sus funciones, por lo que se debe de tomar en consideración este ataque para prevenirlo.
3. Adware, este tipo de ciberataque es a través de un software publicitario, el cual puede establecerse en cualquier página consultada en internet, por tal motivo, al

igual que en phishing, es importante dar capacitaciones a los colaboradores y contar con sistemas de protección que puedan detectar páginas que puedan contener este tipo de ataque, con la finalidad de evitar cualquier robo de información y con esto los problemas que conlleva.

- a. Malvertising o publicidad maliciosa se realiza de la misma manera que el Adware, la diferencia consiste que el segundo es instalado por el usuario y su falta de conocimiento, adicional que no causa daños en el equipo, mientras el malvertising se esconde en la publicidad y no es necesario que el usuario descargue algo, debido que entra si no se cuenta con una solución de seguridad.
4. Spyware, este tipo de ciberataque consiste en ingresar un malware que consigue que se pueda espiar a los dispositivos de otras personas, por lo cual se obtenga un robo de información y confidencialidad, lo cual puede ser motivo de extorsiones o inclusive poder perjudicarse al hacer pública información con competencia de la empresa.
5. Troyanos, este tipo de ataque versa en una especie de virus donde eliminan, bloquean, modifican, copian datos y de mismo modo manejan el equipo, lo cual puede perjudicar gravemente a la empresa y a sus negocios.

6. Exploits, este tipo de ataque versa en mandar programas maliciosos que contienen datos o códigos ejecutables, los cuales se aprovechan de las vulnerabilidades que se encuentren en el software ejecutado en los equipos, por lo que de mismo modo, por falta de capacitación a los colaboradores, o por falta de sistemas de seguridad que implemente la empresa en sus sistemas, se podría llegar a caer en este ciberataque de una manera muy sencilla, logrando sacar información y manejo de sistemas de una empresa.
 - a. Ataque día cero versa en atacar la seguridad de un software que fue encontrado y aún no se cuenta con el desarrollo de protección ya que se descubre el foco de inseguridad una vez que se comete el ataque, por lo que las empresas deben de estar en constante actualización y capacitación para evitar los ataques día cero y tener planes de contingencia para saber identificar y actuar en caso de que suceda.

Dentro de este punto, es importante que conozcamos las diferencia entre vulnerabilidad, amenaza y riesgo como a continuación mencionamos:

Vulnerabilidad	Amenaza	Riesgo
Puntos débiles en la ciberseguridad del usuario por causas propias de este (ejemplo falta de actualización del antivirus).	Aprovechar la vulnerabilidad para atacar el sistema del usuario.	Posibilidad de que suceda cuando se realiza la amenaza y por consecuencia el incidente de seguridad dañando a la empresa.

7. Carding, este ciber ataque va enfocado a la práctica fraudulenta donde se consigue el acceso ilegal al número y dinero de una tarjeta bancaria, el cual en caso de ocurrir en una empresa, pudieran robar sus activos monetarios, logrando hacer grandes daños económicos para la empresa, toda vez que tendrían el control de sus cuentas financieras.

8. Defacement, este ciberataque va a enfocado a desfigurar un sitio web, logrando exponer base de datos que se encuentren dentro de esta, podemos ver que esto es grave para una empresa, toda vez que, al quedar expuesto sus bases de datos, estas podrían tener información confidencial, datos personales y datos personales sensibles tanto de clientes como de su propio personal, por lo que de nueva cuenta se podría hacer responsable de una sanción proveniente de un regulador o una autoridad.

9. DeepFake, este ciberataque versa en la clonación de voz, la cual en otras épocas sería un delito impensable que sucediera, sin embargo, al establecerse mecanismos que utilizan datos biométricos o voz para poder ingresar a nuestra información, como sucede actualmente para acceder a cuentas bancarias, con este ciberdelito, cualquier ciberdelincuente con los conocimientos y mecanismos necesarios, podrían clonar la voz que se utiliza para acudir a las cuentas bancarias tanto privadas como de la empresa, causando un gran daño al patrimonio o suplantando alguna identidad que tenga facultad de tomar decisiones dentro de la empresa, causando un ciber ataque de grande magnitud, por lo cual, es indispensable que conozcamos que estos ataques existen, para fomentar la prevención, con la finalidad de proteger la información de la empresa y de sus empleados.

10. Machine Learning o aprendizaje automático, versa en una rama de la inteligencia artificial, donde la máquina logra realizar algoritmos autónomos donde en ciberataques se enfocan en descubrir o realizar una evasión a los sistemas de seguridad, para lograr tomar el control del equipo.

Consideraciones de la ciberseguridad

Para que exista ciberseguridad en las empresas, estas deberían de fomentar una cultura que implemente y haga consciente a sus colaboradores para llevar a cabo ciertas

acciones que ayuden a prevenir dichos ciberataques, algunas de estas acciones consisten en realizar o evitar realizar actividades muy sencillas como sería:

- Utilizar contraseñas robustas y no reutilizar las mismas
- Tapar cámara de la computadora cuando no se utilice
- No abrir sesiones mientras se encuentre conectado a redes públicas
- Utilizar algún software de seguridad en cada uno de los dispositivos de uso “antivirus”
- No compartir información por medio de formularios en redes sociales
- Cifrar USB
- Cambiar periódicamente las contraseñas
- Formatear 7 veces los dispositivos móviles en caso de que se dejen de utilizar
- No utilizar el equipo empresarial con un uso inadecuado
- No dejar el equipo sin bloquear
- No informar de algún incidente
- Descargar archivos de un correo o página no autorizada o sospechosa
- Actualizar constantemente el software o sistema operativo para tener un mayor nivel de protección

Estos son solo algunos ejemplos de acciones sencillas que podemos realizar, dando una capacitación a los colaboradores para que conozcan todo lo que se puede evitar al realizarlas, con la finalidad de que puedan seguir los lineamientos, es por esto que considero

que uno de los principales requisitos que la autoridad debería de exigir en el ámbito empresarial, es que se brinde una educación y cultura a través de capacitaciones o cursos para su personal en materia de ciberseguridad, ya que existen muchas empresas que no tocan el tema con sus colaboradores o no explican la importancia de que realicen estas acciones.

Adicional de las acciones sencillas antes mencionadas, también las empresas deben de destinar cierta parte de su inversión a conseguir una infraestructura rígida que pueda ayudar a prevenir ciberataques externos, con la finalidad de proteger su información; esto muchas veces no es tan factible en empresas pequeñas o medianas, toda vez que no cuentan con un presupuesto libre para invertir en esta materia, adicional que muchas de estas empresas consideran que por su tamaño no serían acreedoras de un ciberataque por no ser un foco tentativo de ataque, pero es importante mencionar que los ciberdelincuentes han atacado a todo tamaño de empresas, donde si bien no roban la información, pueden llegar a secuestrar los sistemas de las empresas no dando el control a sus dueños hasta que estos paguen cierta cantidad monetaria.

Por tal motivo las empresas deben de tener como prioridad la inversión en medidas de ciberseguridad, las cuales pueden ser la implementación en un control de accesos, así como de instalación de software antimalware, invertir en cursos para sus empleados, contratación de personal que vigile e implemente seguridad en las redes y sistemas, establecer políticas aplicables para todo el personal.

En la siguiente infografía plasmamos los pasos que consideramos son vitales que observen las empresas para evitar en mayor medida un ciberataque, donde logren contar con una ciberseguridad mínima que ayude a evitar que ocurran estos:



Otra consideración que debemos de tomar en cuenta es que la mayoría de las empresas almacena información del negocio, pero dentro de esta información se puede llegar a encontrar datos personales y datos personales sensibles, tanto de su propio personal como de sus clientes.

Este tema considero es de suma importancia, toda vez que actualmente no se le da el valor que merece y por consecuencia un cuidado adecuado, como podemos ver según la Ley Federal para la Protección de Datos Personales en Posesión de Particulares (LFPDPPP), los datos personales se definen como:

***“Datos personales:** Cualquier información concerniente a una persona física identificada o identificable.*

***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.”* (Ley Federal de Protección de Datos Personales en Posesión de Particulares, 2010)

Adicional, actualmente en el ciberespacio, no nos imaginamos ni contamos con la consciencia que el verdadero valor de los activos o bienes de la empresa y por consecuencia el objeto de la mayoría de los ciberataques son nuestros datos e información que se encuentran en nuestros activos o bienes intangibles que se conectan a una red, ya que, a través del uso de sistemas y combinado con la obtención de este tipo de datos lo que genera es una inmensa fortuna, debido que con estos conocen nuestros gustos, estado de salud, intereses, problemas genéticos, filosofías, entre otros puntos, al grado que nos volvemos un producto y a través de las bases de estos datos se vuelven de suma importancia monetaria; por otro lado, la obtención de estos datos como consecuencia puede provocar una fuerte discriminación hacia nuestra persona y nuestra empresa, por tal motivo es de suma importancia que las empresas enfoquen protección al almacenamiento, uso y obtención de nuestros bienes y activos de la empresa en donde al ser vulnerados pueden robar nuestra información confidencial y datos corporativos o personales.

En caso de que una empresa sufra un ciberataque donde esté involucrado el robo, manipulación, secuestro de este tipo de información o datos, puede provocar inmensos daños tanto a la empresa como a sus propios trabajadores y clientes, esto debido que la empresa puede sufrir mala reputación, pérdida de clientes, demandas ante órganos regulatorios que conlleven multas de cantidades importantes de dinero; adicional, los trabajadores podrían sentirse afectados en sus derechos como ciudadanos y trabajadores y de mismo modo los clientes, por lo que se realiza una cadena de afectados en su ámbito

personal, es por esto que las empresas deben de estar conscientes en la importancia de fomentar una ciberseguridad y de mismo modo en la protección de este tipo de datos.

Problema relativo a ciberseguridad empresarial en México

Dentro del contexto mexicano, podemos observar que en el ámbito empresarial, al momento de querer constituir una empresa o emprender algún negocio, no consideramos como algo indispensable contar o tomar en cuenta temas relacionados a la ciberseguridad, ya que al momento de establecer áreas o prioridades para proteger lo que será el ámbito empresarial, solo buscamos el nombre, permisos en secretaría de economía, constituir la sociedad ante notario, entre otras cuestiones legales que la legislación nos marca como obligatorias, así mismo, contamos con la costumbre de establecer áreas primordiales que consideramos esenciales para el funcionamiento de nuestra empresa como sería finanzas, contabilidad, legal, recursos humanos y área comercial; pero en ningún momento la cultura con la que contamos al momento de asesorar o constituir una empresa se designa el tema de la ciberseguridad.

Es importante mencionar que en México, según el censo realizado por el INEGI en 2019, se contaban con 4.9 millones de establecimientos del sector privado y paraestatal, tomando como referencia a micro, pequeñas y medianas (pymes) empresas, ya que conforman la mayor parte de las empresas mexicanas; si bien de 2020 a la fecha muchos negocios cerraron por la pandemia que se presentó, de mismo modo, surgieron muchas

nuevas empresas, como se muestra en las cifras del año 2021 donde podemos mencionar que se duplicaron los nacimientos a comparación del 2020, como podemos mostrar en la siguiente tabla:

Gráfica 3. Proporción de nacimientos y muertes de establecimientos a nivel nacional por sector de actividad económica

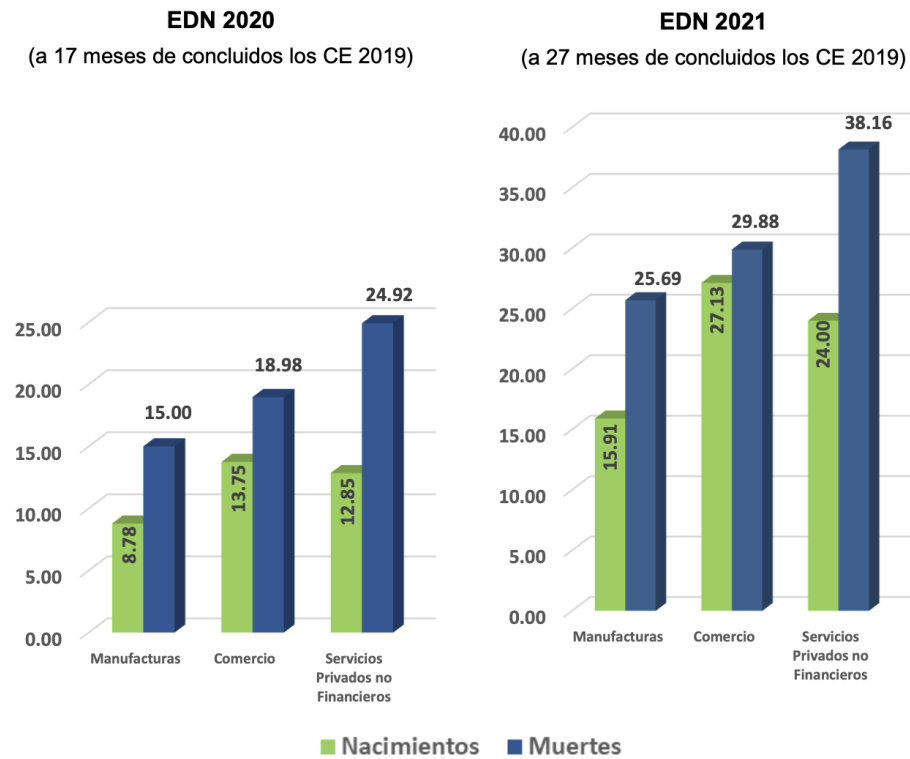


Imagen 2

Si tomamos en cuenta el Directorio Estadístico Nacional de Unidades Económicas proporcionado por el INEGI en mayo del 2022, arrojó que se cuentan con 5,528, 698 empresas existentes que en su mayoría ofrecen actividades de comercio y servicios.

Con las cifras anteriormente mencionadas, podemos dimensionar cuántas empresas se encuentran establecidas dentro del territorio mexicano, donde adicional, debemos de

considerar que la mayoría con la evolución de la tecnología y con motivos de la pandemia que se presentó en 2019, tuvieron que actualizarse para proporcionar sus servicios en línea o plataformas digitales, pero aún con esto, no fomentan una cultura de protección en materia de ciberseguridad, donde de igual manera, el gobierno tampoco realiza este fomento a dicha cultura, es por eso que consideramos que México tiene un gran problema.

En consecuencia, podemos comprender los registros en los cuales se informa que tan solo durante el primer semestre del año 2022, ocurrieron 91,000 millones de intentos de ciberataques en Latinoamérica, de los cuales 60,000 millones ocurrieron en México, ocupando el primer lugar en recibir ciberataques.

Derivado del dato anterior, podemos entender que el problema que se está presentando en las empresas, deriva en que la mayoría de estas no cuenta con una ciberseguridad, o en su caso, esta es muy deficiente, lo cual podemos ver que deberíamos de considerarlo como un tema de suma importancia, ya que, dentro de una empresa, sin importar su giro, es fundamental, toda vez que nos encontramos en un país que va avanzando negativamente en este tema sin contar con protecciones legales que se exijan u orienten a las empresas para poder protegerse, ya que México no cuenta con una legislación robusta y dirigida a empresas que las apoye en este tema en beneficio a los ciudadanos, ya que no solo afecta a los empresarios, sino a sus clientes y a los mismos trabajadores, debido que sus datos e información de mismo modo se puede ver perjudicada.

Haciendo un análisis, actualmente si bien hay muchas empresas que cuentan con protección en materia de ciberseguridad, estas lo realizan por el giro que se encuentra, ya que la mayoría de las empresas que cuenta y pone importancia en esta área, se dedica a la consultoría o implementación de esta práctica, o en su caso son empresas de grandes dimensiones que cuentan con lineamientos ya sea internacionales o con capacidades económicas para fomentar esta área dentro de su empresa.

Sin embargo, las empresas que no se encuentran en lo señalado anteriormente, las cuales son la mayoría, están vulnerables a ciberataques, donde se puede poner en riesgo el patrimonio y la información de las empresas.

Derivado de lo anterior, consideramos fundamental enfocar importancia en el tema de ciberseguridad en empresas y fomentar que se impulse una cultura en ciberseguridad para todos los empleados con ayuda o apoyo de la creación de un manual con medidas básicas dirigido a estas, el cual proteja empresas y ciudadanos, ya que si bien en años anteriores no se contaba con la accesibilidad a las tecnologías como ahora y por ese motivo no se cuenta con la cultura necesaria, es importante tomar en cuenta que la tecnología se incrementa exponencialmente día a día, y si bien ayuda a muchas áreas para su desarrollo, estas igual conllevan la facilidad de caer en malas manos para poder ser usadas negativamente, como está sucediendo actualmente con los ciberataques.

Contexto de ciberseguridad en empresas internacionales

Tratados internacionales que contemplan materia de ciberseguridad

La mayoría de los países reconocen a la ciberseguridad como tema de prioridad, ya que los ciberataques han crecido de manera exponencial y de una manera más sofisticada y peligrosa cada día, tanto para gobiernos como para los estados, al grado que el Foro Económico Mundial ha reconocido lo siguiente:

“El fraude o robo masivo de datos y a los ciberataques cómo dos de los cinco principales riesgos mundiales que perciben los países. Mientras que, a nivel de Norteamérica, el riesgo a los ciberataques ha superado a los ataques terroristas como el número uno de mayor preocupación al hacer negocios.” (Comercio, Scielo, 2019)

Por tal motivo, se han comenzado a establecer estrategias, políticas, leyes y tratados en cada uno de los países, con la finalidad de proteger a sus empresas y a su población de todo lo que conlleva un ciberataque.

“El Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN ha identificado más de 50 países que han publicado una estrategia de ciberseguridad o estrategia

nacional de ciberseguridad, en la que definen “qué significa seguridad para sus futuras iniciativas de seguridad nacional y económica””. (Comercio, Scielo, 2019)

Con relación al comercio electrónico una regulación en materia internacional son los tratados de libre comercio donde se contemplan estipulaciones relacionadas con este tema, dicho punto es importante, toda vez que, cada vez se realizan mayores negocios y transacciones de manera digital, donde si bien es un beneficio enorme tanto para los consumidores como para los productores y la economía de las personas, de mismo modo, aparece serias preocupaciones, toda vez que realizar transacciones en el ciberespacio trae amenazas e incidentes de seguridad tanto para empresas pequeñas, medianas, grandes ya sean privadas o públicas, por lo que como consecuencia, es necesario que se regule dicho tema con la finalidad de proteger a todas las partes involucradas en el comercio electrónico.

Un punto importante de mencionar es que con el avance de la tecnología, el comercio electrónico no se queda dirigido dentro de una nación, sino que ahora se puede comprar con fácil acceso a cualquier portal o comercio electrónico sea donde sea su establecimiento, por tal motivo, debe de considerarse de suma importancia que las naciones cooperen para establecer una cultura de ciberseguridad, un marco normativo, o en su caso un manual de medidas básicas, que contemple protecciones, métodos de defensa y sanciones que sean compatibles con todas las jurisdicciones, toda vez que esta es la manera en que se puede crear un espacio seguro para consumidores y empresas que ofrezcan sus productos de manera electrónica.

Según la organización Mundial del Comercio (OMC) y la Organización para la Cooperación y el desarrollo Económico (OCDE), el ecommerce o comercio electrónico se refiere a lo siguiente respectivamente:

“La producción, distribución, comercialización, venta o entrega de bienes y servicios por medios electrónicos.” (WT/L/274, 2017)

“Venta o compra de bienes o servicios, realizada por computadora redes por métodos diseñados específicamente para recibir o colocar pedidos.” (commerc, 2013)

Ejemplos de ciberataques que se han llevado a cabo en el comercio electrónico son los siguientes:

Año	Empresa atacada	Afectados aproximados
2011	Sony PlayStation Network	77 millones de personas con cuenta de Playstation (nombres, correos electrónicos, datos bancarios).
2011	Citibank	200,000 cuentas bancarias comprometidas en sus usuarios.
2013	Yahoo	Causó daños a 1,000 datos personales de sus usuarios.

2014	eBay	145 millones de usuarios (nombres, datos sensibles, cuentas bancarias).
2014	Sony	Ingresaron y tomaron control sobre equipos de trabajadores, adicional revelaron información confidencial.
2014	Marriott	Datos de 500,000 huéspedes fueron comprometidos.
2015	Ashley Madison	Robaron datos de sus usuarios, las cuales eran de carácter confidencial al ser una plataforma de citas, lo cual ocasionó pago de millones de euros en multas.
2016	Tesco Bank	Vulneraron 40,000 cuentas bancarias, el cual afectó a sus usuarios con pérdidas de 2.65 millones de euros en 2 días.
2017	Uber	57 millones de usuarios (secuestro de información donde se pagó cien mil dólares).
2017	Ransomware WannaCry (malware que entra a un ordenador, cifra datos y pide rescate por dichos datos)	150 países (sector médico, telecomunicaciones).
2018	Cambridge Analytica	50 millones de usuarios en la plataforma de Facebook (robo de datos para ganar elecciones de E.U.A.).
2019	Facebook	419 millones de usuarios (robo de número de teléfonos).
2019	PEMEX	Toma de equipo, el cual afectó el 5% de las computadoras de la empresa.

2020	Zoom	500,000 cuentas de usuarios donde se comprometieron sus datos personales.
2020	SolarWinds	30,000 empresas afectadas, dentro de estas se encontraban empresas gubernamentales (fabricante de software).
2020	Telegram	42 millones de registros de usuarios comprometidos.
2020	Bolsa de Valores de Nueva Zelanda	Provocó una interrupción en el servicio de deuda y accionistas.
2020	Canon	10 Tbytes de datos comprometidos.
2020	Mapfre	Toma de manejo en sus sistemas, evitando que la empresa pudiera dar las respuestas en tiempo y forma.
2020	Dechathlon	36,000 clientes sufrieron pérdida de datos.
2021	MadiaMarkt	3,100 servidores quedaron inoperables tras ataque de ransomware días antes del Black Friday.
2021	Colonial Pipeline	Secuestro de la compañía (oleoducto) causando grandes cortes de gasolina y pánico en los consumidores.
2021	Linkedin	500 millones de perfiles de usuarios en la plataforma sufrieron el robo de sus datos.
2021	Microsoft Exchange Server	250,000 servidores comprometidos.

Algunos tratados internacionales que contemplan puntos relativos a ciberseguridad son los siguientes:

1. La Asociación de Naciones del Sudeste Asiático (ASEAN)

“En 2013, la ASEAN firmó con Japón la “Declaración ministerial conjunta de la reunión de política ministerial de ASEAN y Japón sobre la cooperación en materia de ciberseguridad”, en que además de reconocer la importancia del ciberespacio seguro como uno de los “principales propulsores de la innovación”, éste resulta esencial para “promover las actividades sociales y económicas y fortalecer la conectividad de la ASEAN””. (Comercio, Scielo, 2019)

2. Tratado Integral y Progresista de Asociación Transpacífico (CPTPP)

Los países que conforman el tratado son Australia, Brunéi, Canadá, Chile, Japón, Malasia, México, Nueva Zelanda, Perú, Singapur, República Socialista de Vietnam; el 23 de enero de 2018 se incorporan algunas disposiciones relativas al comercio electrónico, toda vez que se reconoce como un medio de crecimiento a la economía.

Es importante que señalemos para nuestro objeto de estudio que México establece la Estrategia nacional de Ciberseguridad en 2017 donde establece lo siguiente:

“Conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicaciones.” (Comercio, Scielo, 2019)

3. Tratado de México, Estados Unidos y Canadá (T-MEC)

Dentro de este tratado se establece en el punto 19.15 lo relativo a ciberseguridad donde se mencionan los siguientes compromisos por parte de los tres estados con la finalidad de proteger al comercio digital:

“Artículo 19.15: Ciberseguridad

1. Las Partes reconocen que las amenazas a la ciberseguridad menoscaban la confianza en el comercio digital. Por consiguiente, las Partes procurarán:

(a) desarrollar las capacidades de sus respectivas entidades nacionales responsables de la respuesta a incidentes de ciberseguridad; y

(b) fortalecer los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas y utilizar esos mecanismos para tratar rápidamente

los incidentes de ciberseguridad, así como para el intercambio de información para el conocimiento y las mejores prácticas.

2. Dada la naturaleza cambiante de las amenazas a la ciberseguridad, las Partes reconocen que los enfoques basados en riesgos pueden ser mas efectivos que la regulación prescriptiva para tratar aquellas amenazas. En consecuencia, cada Parte procurará emplear y alentar a las empresas dentro de su jurisdicción a utilizar enfoques basados en riesgos que dependan de normas consensuadas y mejores prácticas de gestión de riesgos para identificar y proteger contra los riesgos de ciberseguridad y detectar, responder y recuperarse de eventos de ciberseguridad.”

(Protocolo por el que se sustituye el Tratado de Libre Comercio de América del Norte por el Tratado entre los Estados Unidos de América, 2020)

Referente al T – MEC, podemos ver que el punto antes citado se dirige a la ciberseguridad y respuesta de incidentes donde todas las partes cooperen para evitar y responder de una manera efectiva y eficaz, implementando mecanismos que apoyen a lograr dicho fin. Adicional, un punto importante que se relaciona directamente con el presente estudio de caso, se establece en el punto dos, donde se reconoce que los ciberataques son sumamente cambiantes, toda vez que se realizan con tecnología que día a día avanza exponencialmente, por lo que se propone establecer de igual manera como medida, alentar a las empresas a enfocar su

atención para la prevención, cuidado y medios de solución de este problema, toda vez que se reconoce que conlleva un riesgo.

4. Convenio sobre la ciberdelincuencia (Convenio de Budapest)

La finalidad del Convenio de Budapest es darle prioridad a un tema que es sumamente preocupante, combatir la ciberdelincuencia, donde se establece que una forma de protegerse de la ciberdelincuencia es creando una legislación adecuada donde al ser conscientes que dicho crimen puede realizarse y perjudicar a varios países en un mismo acto, debe de contemplarse una cooperación entre todos los estados para lograr salvaguardar la confidencialidad, integridad, disponibilidad de datos y sistemas informáticos, por lo que legisla delitos relativos a los temas mencionados, con la finalidad proteger los derechos fundamentales y datos de las personas.

Hasta el año 2021, estaba conformado de la siguiente manera: 66 países forman parte del convenio, 2 países lo han firmado y 9 países (dentro de este grupo se encuentra México) participan como observadores, este convenio sirve como base para que los países puedan tomar una directriz para crear sus propias legislaciones con la finalidad de proteger a sus ciudadanos, empresas y gobiernos en temas que son críticos hoy en día.

Legislaciones vigentes en otras jurisdicciones en materia de ciberseguridad

En materia de ciberseguridad, consideramos que la Unión Europea se encuentra avanzada en el ámbito de considerar a la ciberseguridad como una prioridad para todos los países y por ende como una preocupación por el cuidado a los derechos de los ciudadanos, toda vez que, con el avance de las tecnologías que es exponencialmente, todos los ciudadanos al ingresar al ciberespacio en algún momento (redes sociales, consulta de páginas de Internet, consulta de correo personal, usar teléfono con aplicaciones que requieran conexión a Internet, entre otros) se encuentran vulnerables ante posibles ciberdelincuentes que afecten a su persona, su privacidad, sus datos, sus finanzas, su imagen y sus derechos.

Derivado de lo anterior, en la Unión Europea se han establecido diversas regulaciones con la finalidad de proporcionar una ciberseguridad como son:

- Directiva 2016/1148: Se enfoca en establecer medidas para seguridad de redes y sistemas de información.
- Reglamento Europeo de Protección de Datos 2016/679 (GDPR): Establece medidas de seguridad que deben tomar en cuenta todas las empresas establecidas dentro de la Unión Europea que manejen un tratamiento de datos personales y para aquellas

empresas que se encuentren establecidas fuera de la Unión Europea, pero presten servicios a personas de la Unión Europea.

- Ley de Seguridad Cibernética: Se establece una agencia para la ciberseguridad y certificaciones.

Adicional, existen países que cuentan con legislación en materia de ciberseguridad avanzada, donde además de cuidar aspectos relativos a la ciberseguridad nacional, proporcionan directrices enfocadas y dirigidas para entidades privadas, las cuales ayuden a la protección de dichas entidades y por consecuencia la protección de sus empleados, clientes y clientes o empleados de esos clientes.

Un ejemplo de un país establecido en la Unión Europea con una amplia legislación en materia de ciberseguridad es España, donde cuentan con un Código de Derecho de la Ciberseguridad el cual contiene legislaciones para proteger el ciberespacio y por consecuencia la ciberseguridad en los ciudadanos.

Derivado de dicha legislación, las empresas, están obligadas a observar las disposiciones y a cumplirlas en su ámbito de competencia, con la finalidad de establecer y fomentar que los negocios cuenten con un negocio digital libre y seguro.

Una ley española que consideramos importante mencionar, toda vez que, establece obligaciones a ciertas empresas de conformidad con su giro, donde dependiendo este, se

obliga a las empresas a seguir ciertos lineamientos en materia de ciberseguridad, es la Ley de Seguridad de la Información la cual da directrices a las siguientes empresas:

“- Si son servicios fundamentales para la sociedad y la economía

- Si dependen o no de otro sistema de redes*
- Efectos perjudiciales que tendría una incidencia sobre la prestación de esos servicios o la seguridad pública.” (Ayudaley, S/F)*

Derivado de lo anterior dichas empresas deben realizar las siguientes obligaciones:

“1. Mejorar sus sistemas de seguridad contra intrusiones:

- **Prevención:** adoptar las medidas necesarias para prevenir ataques informáticos.*
- **Detección:** si se produce una intrusión, debes detectar el momento en el que se produce y tomar las medidas necesarias para minimizar los daños.*
- **Restauración:** debes restaurar el sistema dañado con las copias de seguridad realizadas anteriormente.*
- **Análisis forense:** con él puedes ver las acciones que el atacante ha realizado en tu sistema.*

2. Comunicar a las autoridades competentes las violaciones de seguridad que sufran:

Se deben notificar las brechas de seguridad tanto a los afectados como a la AEPD en un plazo de 72 horas.” (Ayudaley, S/F)

Otra institución importante de mencionar que se constituye en España es el Instituto Nacional de Ciberseguridad (INCIBE), el cual tiene como función:

“Desde el 28 de octubre de 2014, el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) pasa a llamarse S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE), según el acuerdo adoptado en Junta General del 27 de octubre de 2014. Con dicho cambio de denominación e imagen, INCIBE proyecta una identidad acorde con su orientación estratégica y posicionamiento como centro nacional de referencia en ciberseguridad.

Trabaja para afianzar la confianza digital, elevar la ciberseguridad y la resiliencia y contribuir al mercado digital de manera que se impulse el uso seguro del ciberespacio en España.” (Qué es el INCIBE)

Expectativas de la ciberseguridad y su regulación desde una perspectiva internacional

Desde una perspectiva internacional, existe una grande preocupación por el tema de ciberseguridad, toda vez que, actualmente es un tema alarmante tanto para países como para empresas, debido a que día a día salen nuevas amenazas, delitos y formas para vulnerar la ciberseguridad de las empresas, sin importar su giro o tamaño, de mismo modo, se cuenta con la preocupación que las legislaciones no pueden avanzar o contemplar las situaciones que crecen y se generan exponencialmente, el peligro se contempla en lo vulnerable que nos encontramos frente a ciberdelitos y ciberincidentes porque es un tema prioritario de atender, lo que es importante mencionar, es que países ya están tomando cartas en el asunto, lo cual da pie para que otros países continúen con el fomento de la ciberseguridad y contemplen la importancia del cuidado de la ciberseguridad.

Un ejemplo de lo anteriormente mencionado, es Estados Unidos de América, donde altos funcionarios han expresado su preocupación en el tema de ciberseguridad, por los constantes ciberataques que se realizan a gobierno, empresas y ciudadanos, estableciendo que la estrategia de ciberseguridad voluntaria no se lleva a cabo de la manera que debe llevarse, ya que al no contar con la facultad de obligar a las empresas a cumplir con la normativa que emite la Comisión Federal de las Comunicaciones de Estados Unidos (FCC), se sabe que muchas empresas no invierten en protección de ciberseguridad.

Derivado de lo anterior, Estados Unidos de América ha implementado normas de ciberseguridad para los sectores de bancos, oleoducto, sistemas ferroviarios, aerolíneas y aeropuertos, así como directiva de proveedores al gobierno, sin embargo, saben que cambiar todo el ámbito privado en cuestiones de ciberseguridad es difícil.

"Hay tres cosas importantes que se necesitan para solucionar el lamentable estado actual de la ciberseguridad de EE UU", según Wyden. "Los estándares mínimos obligatorios de ciberseguridad aplicados por los reguladores; las obligatorias auditorías de ciberseguridad, realizadas por auditores independientes que no son elegidos por las empresas que auditan, cuyos resultados se entregarían a los reguladores; y multas elevadas, incluidas condenas de prisión para los altos directivos, cuando la desatención a las ciber-necesidades básicas da como resultado una vulneración".

La nueva regulación de notificación obligatoria de incidentes, que se convirtió en ley el pasado martes, se considera un primer paso. La ley requiere que las empresas privadas compartan rápidamente la información sobre las amenazas comunes que solían mantener en secreto. Esa información exacta a menudo puede ayudar a construir una defensa colectiva más fuerte." (MIT Technology Review, 2022)

Por otro lado, observamos que, en China al contar de igual manera con cierta preocupación en materia de ciberseguridad, a nuestro parecer ha implementado medidas más

restrictivas, como se puede observar en la Ley de Ciberseguridad China que entró en vigor el 1 de junio de 2017:

“Requiere que los operadores de red almacenen datos seleccionados dentro de China y permite a las autoridades chinas realizar controles al azar en las operaciones de red de una empresa. Beijing afirma que la ley tiene la intención de alinear a China con las mejores prácticas mundiales para la seguridad cibernética. La ley ha suscitado preocupación entre algunas compañías extranjeras por mayores controles de datos, así como por un mayor riesgo de robo de propiedad intelectual.

La Ley de Ciberseguridad es aplicable a operadores de red y empresas en sectores críticos.

Los operadores de red se definen como propietarios de red, gerentes y proveedores. Una red se define como cualquier sistema compuesto por ordenadores y equipos relacionados que recopilan, almacenan, transmiten, intercambian o procesan información. Estas definiciones significan que la ley es aplicable a casi todas las empresas en China que administran su propio correo electrónico u otras redes de datos.

Los “sectores críticos” abarcan las empresas involucradas en comunicaciones, servicios de información, energía, transporte, agua, servicios financieros, servicios

públicos y servicios de gobierno electrónico. Cualquier empresa que sea proveedor o socio de firmas en estos sectores también podría estar sujeta a la ley.

La ley exige que los operadores de red cooperen con los investigadores chinos de crímenes o seguridad y permitan el acceso total a los datos y el «soporte técnico» no especificado a las autoridades que lo soliciten.” (China)

Con los dos ejemplos pasados, podemos ver que, sin importar la locación, dos de las más grandes economías mundiales cuentan con preocupaciones relativos al tema de ciberseguridad y se encuentran abordándolo a su manera, por lo que, no debe ser la excepción de nuestro país.

Contexto de ciberseguridad en empresas mexicanas

Contemplaciones dentro de Legislaciones mexicanas en materia de ciberseguridad

Es importante que conozcamos y reconozcamos que México no se encuentra exento de ataques cibernéticos, toda vez que, se conoce que es un tema del cual debe preocuparse, debido que es un territorio que los últimos años se ha visto muy afectado por ciberataques.

“México es el segundo país de América Latina con más ataques cibernéticos. Dado que el 57.4% de la población de México es usuaria de Internet, cerrar las brechas en su entorno de ciberseguridad es una tarea importante.” (Ciberseguridad, s.f.)

Derivado de lo anterior, es importante que mencionemos lo aplicable en el ámbito mexicano respecto de la ciberseguridad, y en su caso, las protecciones o prevenciones que se contemplan en diversas legislaciones, y de mismo modo, conocer si estas existen o en su caso son deficientes, que protejan a las personas en su ámbito laboral, ya sea como trabajador o como cliente o proveedor de las empresas mexicanas, esto con la finalidad de que podamos fomentar medidas de protección que puedan ser tomadas como obligatorias en empresas y por ende protejan a los ciudadanos mexicanos.

Podemos observar que en México contamos con diversas regulaciones en las cuales podemos vincular algunas estipulaciones en materia de ciberseguridad, sin embargo, entre

las que consideramos más importantes, son las siguientes, con las cuales podremos confirmar nuestro problema planteado a lo largo del presente caso y por ende podamos proporcionar una solución viable a dicho problema:

- Constitución Política de los Estados Unidos Mexicanos

Podemos establecer que dentro de nuestra constitución se llega a contemplar de cierto modo el bien que se puede perjudicar en un ciberdelito, el cual puede llegar hacer un derecho humano de las personas, lo cual se contempla en el artículo 1º; por otro lado, el artículo 6º, contempla la facultad del Estado de garantizar a los ciudadanos el acceso a las tecnologías de la información y comunicación, dentro del cual se incluye el Internet; por último, dentro del artículo 73 fracción XVII se establece que el congreso tiene facultades para dictar leyes en materia de tecnología de la información, por lo cual se encontraría facultada de poder generar un ley en materia de ciberseguridad.

- Ley Federal de Protección de Datos Personales en Posesión de Particulares

Esta ley se vincula con los ciberdelitos, ya que protege los datos personales de todos los ciudadanos y en caso de caer en una vulneración, lo que se roba, daña y puede darle un uso distinto al otorgado son de los datos personales, por lo que se podría decir, que un bien que se roba al cometer un ciberdelito son los datos personales.

- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares
- Norma Federal de Transparencia y Acceso a la Información Pública
- Código Penal Federal

Este código es importante que lo mencionemos, toda vez que, se añadieron algunos puntos en los cuales se pueden equiparar ciberdelitos con los delitos ya contemplados en nuestro código penal, sin embargo, no se cuenta con un código de ciberseguridad o ciberdelitos que contemple los casos específicos.

- Plan Nacional de Desarrollo 2013 – 2018

En este documento es importante resaltar que se fundamenta la estrategia Nacional de Ciberseguridad, la cual, como se expondrá a continuación, consideramos se dan fundamentos rígidos para abordar el tema de ciberseguridad para la protección de ciudadanos y empresas mexicanas.

- Estrategia Nacional de Ciberseguridad 2018

Con relación a este documento, nos parece importante resaltar que nace a raíz de un compromiso realizado por México para combatir los delitos cibernéticos, donde se plantea como meta el año 2030 y de mismo modo, se menciona que tiene los siguientes objetivos:

“La Estrategia Nacional de Ciberseguridad plantea cinco objetivos estratégicos: Sociedad y Derechos; Economía e Innovación; Instituciones Públicas; Seguridad Pública y Seguridad Nacional.” (gob.mx, 2017)

Con lo anterior, podemos equiparar los objetivos mencionados “sociedad, derechos y economía”, a las empresas, sus empleados, clientes y proveedores, por lo que una finalidad si bien que no está expresa, deberá proteger a toda la sociedad sin importar su ámbito.

Adicional en México, consideramos que es de los documentos que contienen el punto más enfocado con la ciberseguridad, a comparación de las otras leyes o normativas, ya que se reconoce que debe de fomentarse una cultura a la ciberseguridad, que existe un riesgo inherente de las tecnologías donde día a día, segundo a segundo, aumentan los ciberataques y la importancia y dependencia en los ámbitos laborales y personales de los ciudadanos con las tecnologías de la información y la comunicación.

Por otro lado, se menciona dentro de esta estrategia un punto que consideramos de suma importancia, ya que reconoce que los ciberataques perjudicarán a las personas y por ende a las empresas privadas:

“Los riesgos y amenazas en el ciberespacio pueden constituir un posible ataque a la dignidad humana, a la integridad de las personas, a la credibilidad, reputación y patrimonio de las empresas y las instituciones públicas; así como afectaciones a la seguridad pública o incluso la seguridad nacional.” (gob.mx, 2017)

Dentro de esta estrategia, se mencionan los siguientes 8 ejes con los que se conseguirá cumplir la meta y la elaboración de un plan para actuar y poder mejorar en este tema:

- “1. Cultura de ciberseguridad.*
- 2. Desarrollo de capacidades.*
- 3. Coordinación y colaboración.*
- 4. Investigación, desarrollo e innovación TIC.*
- 5. Estándares y criterios técnicos.*
- 6. Infraestructuras críticas.*
- 7. Marco jurídico y autorregulación.*
- 8. Medición y seguimiento.” (gob.mx, 2017)*

- Programa Nacional de Seguridad Pública 2014-2018

Dentro de este programa, se establece como una estrategia (1.6) promover una normatividad en seguridad pública, la cual proporcione herramientas para los delitos cibernéticos.

- Plan Nacional de Desarrollo 2019 - 2024

Es importante mencionar que no se establece un apartado específico en ciberseguridad, lo cual consideramos un tema preocupante, ya que no se contempla un fomento a esta materia, la cual es de suma importancia en la actualidad y de igual manera al dejar a un lado lo establecido en esta materia en el año 2018, estos lineamientos se vuelven desactualizados ya que no van a la par de los ataques nuevos que salen día a día.

Analizando cada uno de los textos legislativos mencionados, podemos ver que ninguno contempla lineamientos que sean exigibles para empresas privadas o incluso públicas (exceptuando el sector financiero, toda vez que se cuenta con su propia legislación, por el giro del negocio), por lo que existe un amplio vacío legal donde queda a la deriva el intento de fomentar una cultura donde se exija requerimientos mínimos a empresas para tener medidas de ciberseguridad y por ende cuidar los derechos que pueden ser vulnerados, los cuales se reconoce que es una urgencia.

Por otro lado, consideramos importante mencionar que México cuenta con algunos organismos que se encuentran capacitados para sancionar ciertos actos que se encuentran vinculados con la ciberseguridad, los cuales son los siguientes:

- Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX), donde la página del Gobierno de México menciona que cuenta con la siguiente misión:

“Brindar los servicios de apoyo en la respuesta a incidentes cibernéticos que afectan a las instituciones en el país que cuentan con infraestructura crítica de información, que incluye la identificación de amenazas y modus operandi de la ciberdelincuencia para el alertamiento a la ciudadanía, mediante la gestión de incidentes de seguridad informática, fungiendo como el único punto de contacto y coordinación dentro y fuera del territorio nacional y actuando en la investigación forense digital y el análisis técnico policial en apoyo al Ministerio Público.” (Gobierno de México, s.f.)

En la página del CERT-MX se puede reportar los siguientes incidentes cibernéticos, con la finalidad de solicitar su apoyo: agravio contra personas, fraude y extorsión, eventos de seguridad informática, denuncia de ilícitos a través de la web, delitos contra menores.

- CSIRT

Los cuales son centros de respuesta ante incidentes informáticos particulares y enfocados en distintas áreas como puede ser gobierno, académicos, empresas privadas o públicas.

- Policía Cibernética, la cual ayuda con la coordinación de delitos electrónicos y colabora con el CERT-MX.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el cual es un organismo que está encargado de velar por la protección de los datos personales de todos los ciudadanos y de mismo modo, se encuentra facultado para sancionar a los responsables en caso de que el derecho de protección de datos personales sea violado, por lo que uniendo el INAI en materia de ciberseguridad, se puede equiparar como un organismo sancionador de una consecuencia que puede derivar de un ciberdelito.

Expectativas de ciberseguridad en México

Analizando el marco jurídico y los organismos involucrados en temas de ciberseguridad antes mencionados, podemos ver que la expectativa de México que se proyectó en el año 2018 en materia de ciberseguridad con la Estrategia Nacional de Ciberseguridad 2018 es fomentar que se realice una cultura en esta materia, ya que se

plasma que es un tema preocupante para el país y sus ciudadanos en todos los ámbitos por los daños que han causado los ciberdelitos tanto en el patrimonio y reputación de los ciudadanos como en el patrimonio y reputación de empresas públicas y privadas; dentro de este documento, se menciona que el eje inicial para poder elaborar un plan de acción es establecer una cultura de la ciberseguridad que se genere a la población:

“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.” (Gobierno de México , 2017)

Lo anterior, nos ayuda a comprender que para que se desarrolle un ambiente armónico y funcional, la población y por lo tanto las empresas, deben de contar con una cultura en ciberseguridad, donde se fomente su gestión, el conocimiento de los derechos involucrados y de igual manera una colaboración entre todos para mejorar, realizando la Estrategia Nacional de Ciberseguridad 2018, se cumpliría con los tratados a los que se ha comprometido México.

Adicional, podemos ver que dentro del Plan Nacional de Desarrollo 2019 – 2024 se dejó de lado o no se estableció como objetivo primordial la continuidad en tema de ciberseguridad,

por lo que no se ha realizado algún esfuerzo por crear una legislación específica en materia de ciberdelitos y por ende el fomento de una cultura en dicha materia, donde se comuniquen lineamientos básicos para empresas privadas o públicas y sociedades con la finalidad de que impulsen medidas de prevención y se sancione a quien realice ciberdelitos.

La omisión de estas acciones por parte de México, provoca que los ciberdelitos se sigan cometiendo y estos cambien día a día, segundo a segundo, estableciendo nuevos retos a las empresas sin contar con orientación por parte del gobierno, en un tema que es prioritario para toda la sociedad; por consecuencia podemos observar que esta omisión es sumamente preocupante para nuestro país, toda vez que, no va avanzando en temas que globalmente se ha comprometido trabajar y adicional, se fomenta que la sociedad se ponga en un estado vulnerable al no contar con la cultura y conocimientos adecuados y actualizados que apoyen a fomentar la ciberseguridad y que esta adquiera la importancia que tiene en estos tiempos donde la tecnología cuenta un papel importante.

Ejemplo de lo anteriormente mencionado, es el supuesto ocurrido en nuestro país el mes de septiembre del presente año a la Secretaría de la Defensa Nacional (SEDENA), donde un grupo de hacker llamados "Guacamaya" reveló 6 Tb de información confidencial y sensible de la SEDENA, la cual es nuestra institución máxima de seguridad, lo cual es sumamente alarmante para todos los mexicanos, ya que como menciona el Doctor Carlos Ramírez Castañeda *"Si a los cuerpos de defensa encargados de la seguridad nacional los han vulnerado, ¿qué se espera de un usuario común, una empresa, una institución bancaria?"*

(Castañeda, 2022); por tal motivo es iluso pensar que la estrategia que está planteando y fomentando actualmente nuestro país sea correcta, ya que se está atrasando en fomentar, legislar y combatir ciberataques, ya que como se mencionó anteriormente, estos cambian día a día.

Por otro lado, con el ejemplo anteriormente señalado, vemos que en México no existe una cultura de prevención, detección y que se conozcan medidas que combatan los ciberataques, ya que, en primera instancia, los mismos empleados de la SEDENA no supieron actuar para evitar este ataque, donde esto comprueba que los empleados de la mayor institución de seguridad no se encuentra preparado, y por otro lado, muchos ciudadanos observando el incidente no encuentran alarmante dicha situación, es por ese motivo la importancia de fomentar una cultura de ciberseguridad en nuestro país.

Propuesta de solución a la falta de cultura, prevención y atención en temas de ciberseguridad para empresas mexicanas

Como mencionamos a lo largo del trabajo, el problema que identificamos para las empresas en materia de ciberseguridad, es una falta de legislación, directrices, recomendaciones, manuales proporcionadas por parte del gobierno, que proporcionen requisitos mínimos a empresas tanto micro, pequeñas, medianas y grandes, con la finalidad de protegerlos, lo cual provoca que se protejan a su vez sus servicios, bienes, reputación y lo más importante a clientes y a su propio personal que labora dentro de sus instalaciones. Por lo que podemos concluir que es la falta de una cultura que fomente una conciencia en los riesgos que se cuentan al no darle la importancia que se merece la ciberseguridad.

Entendemos lo difícil que puede resultar para empresas micro, pequeñas o medianas, llevar a cabo lineamientos en materia de ciberseguridad voluntarias, por los costos que podrían tener al realizar implementaciones en esta materia para su protección; adicional, las empresas de grande tamaño, de igual manera cuentan con este problema, por lo que podemos ver que todas las empresas sin importar su tamaño, no importando su tamaño o giro, se encuentran vulnerables a un ciberataque ya que los ciberdelincuentes no discriminan y ven una oportunidad en cualquiera de estas.

Derivado de lo anterior, nuestra propuesta de solución a este problema planteado a lo largo del presente estudio del caso, es comunicar y fomentar una cultura en materia de ciberseguridad, la cual desarrolle que la sociedad considere establecer acciones básicas para la prevención y atención en temas de ciberseguridad, donde se pueda entender que al contar con cultura en esta materia, se pueden contener diversos ciberataques a las empresas por las acciones que ya se tenga de una manera consciente por parte de los ciudadanos, que al ser trabajadores, influyen en los actos de la empresa que ayuden a prevenir, detectar y actuar en caso de un ciberincidente.

Proponer una legislación, regulación o normatividad, donde se establezcan requisitos mínimos que exijan a las empresas establecer y tener en cuenta temas para contar con una ciberseguridad, es muy complejo y sería una solución que tardaría su debido tiempo, como se propuso en la Estrategia Nacional de Ciberseguridad 2018, en caso de no perder continuidad en el presente tema, se estaría realizando en 2030, lo cual dejaría desprotegido todo el ámbito de la ciberseguridad durante este periodo, causando daños a las empresas exponencialmente, sin mencionar que, actualmente como se mencionó, no se está dando la continuidad correspondiente.

Debido de lo anterior, consideramos que un apoyo para fomentar la cultura en materia de ciberseguridad es elaborar una especie de manual que se comunique a los ciudadanos, donde se logre que se establezca una ciber cultura con puntos básicos para la prevención,

detección y acción a ciberataques; algunos de estos puntos que ayudan a fomentar dicha cultura son los siguientes:

1. Que la autoridad proporcione un curso gratuito en materia de datos personales, el cual sea requisito para todos los trabajadores de una empresa tomar y acreditar, y este a su vez, proporcione conocimientos básicos de protección de datos personales con un lenguaje accesible, el cual fomente una cultura de protección, se concientice la importancia y el valor de los datos personales y los derechos de los cuales cada titular tiene.
2. Que cada empresa cuente con un aviso de privacidad, en el cual se cumplan con los requisitos establecidos en la ley, este punto puede establecerse que se encuentra contemplado en la Ley Federal de Protección de Datos Personales en Posesión de Particulares, sin embargo, se podrían realizar cursos forzosos a los trabajadores, de conocerlo e implementarlo.
3. Culturalizar la importancia que genera instalar y contar con un antivirus en cada equipo que tenga conexión a una red, lo ideal sería exigir al gobierno que fomente proporcionar antivirus gratuitos, en caso de que las empresas no puedan pagar por uno.
4. Fomentar la importancia que los equipos electrónicos cuenten con contraseñas y estas deban de ser modificadas cada periodo de tiempo.

5. Que la autoridad proporcione un curso gratuito, en materia de ciberseguridad, con lenguaje y terminología accesible el cual sea requisito acreditar para todos los trabajadores de las empresas, donde se establezca una cultura de ciberseguridad, recomendaciones, concientización de los peligros y puntos a seguir, de tal forma que cada trabajador tenga certificado del cumplimiento del curso.
6. Recomendaciones a empresas que acrediten que cuentan con capital, que inviertan en infraestructura dentro de sus sistemas (VPM) con la finalidad de proteger sus sistemas ante posibles ciberataques.
7. Implementar dentro de cada empresa, un curso de civismo digital que sea forzoso para cada empleado, lo cual proporcione conocimiento de cómo comportarse y proteger los derechos de todos en los medios digitales y se aprendan técnicas de seguridad para el negocio en línea.
8. Dentro de la empresa contar con un puesto o equipo de ciberseguridad, cuyas funciones sean la vigilancia e implementación de protecciones en materia de ciberseguridad.
9. Se establezca un proceso de denuncias de ciberataques en empresas, el cual sea otorgado por un equipo especializado en la materia para prevenir y sancionar, de mismo modo otorgar recomendaciones a empresas para mejorar en cuestiones de ciberseguridad.

Otro punto importante es conocer cuáles son los ciberdelitos existentes, con la finalidad de que las empresas y ciudadanos conozcan qué clases de delitos existen, sus métodos de defensa y protecciones, de mismo modo, al contar con este conocimiento se puede exigir al gobierno que se generen y fomenten autoridades que conozcan del tema y vayan actualizándose día a día como pasa en los ciberdelitos, ya que, estos se actualizan cada día.

Implementando un manual que comunique los puntos anteriormente mencionados, lograríamos ir desarrollando una cultura en la sociedad que haga que las empresas presten atención en el tema de ciberseguridad y se pueda reducir de forma significativa los ciberataques, donde lo antes propuesto implica exigir que se fomente en el país una cultura y educación de prevenir, detectar y actuar.

Bibliografía

Ayudaley. (S/F). Recuperado el febrero de 2022, de Normativa de ciberseguridad. Todo lo que debes saber: <https://ayudaleyprotecciondatos.es/2018/09/18/normativa-ciberseguridad/>

Ayudaley. (S/F). Recuperado el febrero de 2022, de Normativa de ciberseguridad. Todo lo que debes saber: <https://ayudaleyprotecciondatos.es/2018/09/18/normativa-ciberseguridad/>

Ayudaley. (S/F). Recuperado el febrero de 2022, de Normativa de ciberseguridad. Todo lo que debes saber: <https://ayudaleyprotecciondatos.es/2018/09/18/normativa-ciberseguridad/>

Ayudaley. (S/F). Recuperado el febrero de 2022, de Normativa de ciberseguridad. Todo lo que debes saber: <https://ayudaleyprotecciondatos.es/2018/09/18/normativa-ciberseguridad/>

Castañeda, C. R. (1 de octubre de 2022). *Expansión*. Obtenido de Las lecciones que comienzan con el hackeo a la Sedena: <https://expansion.mx/opinion/2022/09/30/lecciones-hackeo-sedena>

China. (s.f.). Recuperado el agosto de 2022, de CIBERSEGURIDAD Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas: <https://ciberseguridad.com/normativa/china/#:~:text=Unidos%20y%20China-Ley%20de%20Ciberseguridad%20China,de%20red%20de%20una%20empresa.>

Ciberseguridad. (s.f.). Recuperado el marzo de 2022, de Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas: <https://ciberseguridad.com/normativa/latinoamerica/mexico/#:~:text=M%C3%A9xico%20no%20ha%20promulgado%20una,como%20terrorismo%2C%20secuestro%20y%20narcotr%C3%A1fico.>

Ciberseguridad, Una guía completa del concepto, tipos, amenazas y estrategias. (s.f.). Recuperado el febrero de 2022, de Infosecurity Mexico: <https://www.infosecuritymexico.com/es/ciberseguridad.html>

Ciberseguridad?, ¿. e. (2020). Recuperado el julio de 2022, de Kaspersky: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>

Ciberseguridad?, ¿. e. (s.f.). *IBM*. Recuperado el agosto de 2022, de IBM: <https://www.ibm.com/es-es/topics/cybersecurity>

Comercio, L. c. (2019). *Scielo*. Recuperado el febrero de 2022, de Revista chilena de derecho y tecnología: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000200111

Comercio, L. c. (2019). *Scielo*. Recuperado el marzo de 2022, de Revista chilena de derecho y tecnología: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000200111

Comercio, L. c. (2019). *Scielo*. Recuperado el marzo de 2022, de Revista chilena de derecho y tecnología: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000200111

Comercio, L. c. (2019). *Scielo*. Recuperado el marzo de 2022, de Revista chilena de derecho y tecnología: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000200111#t1

Commerc, G. o. (2013). *OCDE*. Recuperado el marzo de 2022, de <http://bit.ly/2M8PrcG>

DEFENSA, B. O. (19 de febrero de 2013). Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas. España, Madrid.

Diccionario de la lengua Española. (2001). Recuperado el febrero de 2021, de Real Academia Española: <https://www.rae.es/drae2001/seguridad>

Engelaar, R. (2 de julio de 2022). *México Registra 80.000 Millones de Intentos de Ciberataques en 2022*. Recuperado el julio de 2022, de Confederación de Cámaras Nacionales de Comercio, Servicios y Turismo: <https://www.concanaco.com.mx/prensa/tepuedeinteresar/mexico-registra-80-000-millones-de-intentos-de-ciberataques-en-2022>

ESTOS SON LOS TIPOS DE POLÍTICAS QUE PUEDE APLICAR EN SU EMPRESA. (s.f.). Recuperado el julio de 2022, de py+: <https://www.pymas.com.co/ideas-para-crecer/recursos-humanos/tipos-de-politicas-de-una-empresa>

gob.mx. (13 de noviembre de 2017). *Gobierno de México*. Recuperado el marzo de 2022, de Estrategia Nacional de Ciberseguridad: <https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad>

gob.mx. (13 de noviembre de 2017). *Gobierno de México*. Recuperado el marzo de 2022, de Estrategia Nacional de Ciberseguridad: <https://www.gob.mx/gobmx/documentos/estrategia-nacional-de-ciberseguridad>

gob.mx. (13 de noviembre de 2017). *Gobierno de México*. Recuperado el marzo de 2022, de Estrategia Nacional de Ciberseguridad:

https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

Gobierno de México. (2017). Recuperado el agosto de 2022, de Estrategia Nacional de Ciberseguridad:

https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf

Gobierno de México. (s.f.). *Gobierno de México*. Recuperado el marzo de 2022, de Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional:

<https://www.gob.mx/gncertmx?tab=%C2%BFQu%C3%A9%20es%20CERT-MX?>

Gutiérrez, A. L. (29 de junio de 2021). *México está en la mira de los hackers: concentra 34% de ciberataques de AL*. Recuperado el julio de 2022, de El Financiero: <https://www.elfinanciero.com.mx/empresas/2021/06/29/acechan-hackers-a-empresas-mexico-concentra-el-34-de-ciberataques-de-al/>

Humanos, 1. p. (s.f.). *R3D*. Recuperado el agosto de 2022, de <https://r3d.mx/ciberseguridad/>

Humanos, 1. p. (s.f.). *R3D*. Recuperado el agosto de 2022, de *R3D*: <https://r3d.mx/ciberseguridad/>

INEGI. (21 de diciembre de 2021). *EL INEGI PRESENTA LOS RESULTADOS DEL ESTUDIO SOBRE LA DEMOGRAFÍA DE LOS NEGOCIOS 2021*. Recuperado el agosto de 2022, de COMUNICADO DE PRENSA NÚM. 790/21: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EDN/EDN_2021.pdf

Ley Federal de Protección de Datos Personales en Posesión de Particulares. (5 de 07 de 2010). Recuperado el febrero de 2022, de <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>

Low, J. (21 de marzo de 2022). Recuperado el julio de 2022, de 24 estadísticas alarmantes de ciberseguridad que necesita saber: <https://www.webhostingsecretrevealed.net/es/blog/security/cybersecurity-statistics/>

Microsoft. (2022). Recuperado el febrero de 2022, de ¿Qué es la ciberseguridad?: <https://support.microsoft.com/es-es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390>

MIT Technology Review. (13 de junio de 2022). Recuperado el agosto de 2022, de La situación de la ciberseguridad en EE UU es insostenible, pero hay un plan:

<https://www.technologyreview.es/s/14080/la-situacion-de-la-ciberseguridad-en-ee-uu-es-insostenible-pero-hay-un-plan#:~:text=Computaci%C3%B3n-,La%20situaci%C3%B3n%20de%20la%20ciberseguridad%20en%20EE,insostenible%2C%20pero%20hay%20un%20plan&text=El%20hack>

Protocolo por el que se sustituye el Tratado de Libre Comercio de América del Norte por el Tratado entre los Estados Unidos de América, I. E. (2020). *Tratado entre México, Estados Unidos y Canadá (T-MEC)*. Recuperado el febrero de 2022, de Gobierno de México: <https://www.gob.mx/t-mec/acciones-y-programas/textos-finales-del-tratado-entre-mexico-estados-unidos-y-canada-t-mec-202730?state=published>

QUÉ ES CIBERSEGURIDAD. DEFINICIÓN, T. Y. (2021). Recuperado el julio de 2022, de Avansis : <https://www.avansis.es/ciberseguridad/que-es-ciberseguridad/>

Qué es el INCIBE. (s.f.). Recuperado el agosto de 2022, de INCIBE: <https://www.incibe.es/que-es-incibe>

Revista Seguridad 260. (3 de febrero de 2022). Recuperado el 2022 de febrero, de Novedades en ciberseguridad y delitos informáticos para 2022: <https://revistaseguridad360.com/noticias/ciberseguridad-y-delitos-informaticos/>

Revista seguridad 360. (4 de febrero de 2022). Recuperado el febrero de 2022, de ¿Qué es la ciberseguridad y su importancia?: <https://revistaseguridad360.com/destacados/que-es-la-ciberseguridad/>

School., E. B. (2020). *ESIC*. Obtenido de Definicion de la ciberseguridad y su riesgo.

School., E. B. (2020). *ESIC Business & Marketing School*. Recuperado el agosto de 2022, de Definición de Ciberseguridad y su riesgo: esic.edu/rethink/tecnologia/definicion-ciberseguridad-riesgo

WT/L/274, W. p. (2017). Recuperado el marzo de 2022, de Organización Mundial de Comerci: <http://bit.ly/2Sb0B4A>

ANEXO 1

REFERENCIAS ADICIONALES

1. Imagen 1

Low, J. (21 de marzo de 2022). Recuperado el julio de 2022, de 24 estadísticas alarmantes de ciberseguridad que necesita saber:
<https://www.webhostingsecretrevealed.net/es/blog/security/cybersecurity-statistics/>

2. Imagen 2

INEGI. (21 de diciembre de 2021). *EL INEGI PRESENTA LOS RESULTADOS DEL ESTUDIO SOBRE LA DEMOGRAFÍA DE LOS NEGOCIOS 2021*. Recuperado el agosto de 2022, de COMUNICADO DE PRENSA NÚM. 790/21:
https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/EDN/EDN_2021.pdf