Microsoft

El Libro Blanco DE SEGURIDAD CIBERNÉTICA

The Software Alliance

BSA

RESUMEN EJECUTIVO

Hoy en día la interconexión de los individuos ha ido más allá de las relaciones interpersonales, lo que ha generado ciertos beneficios, pero también riesgos y amenazas tanto para el ciudadano común, como para entidades gubernamentales que tienen la obligación velar por la seguridad de los gobernados. De este nuevo desafío, surge la inminente necesidad de redoblar esfuerzos a nivel público y privado con el fin de lograr un espacio digital más seguro.

¿Qué es un ciberdelito?

De acuerdo con la Enciclopedia Británica de Michael Aaron Dennis, lo define como: El uso de una computadora o dispositivo electrónico con internet para cometer actividades ilícitas tales como fraude, trata de personas, distribución y producción de pornografía infantil, tráfico de sustancias ilícitas, piratería, entre otras. La naturaleza transnacional del ciberdelito ha causado pérdidas que ascienden a los 600,000 millones de dólares en la economía mundial. Con el fin de combatir este tema y en general regular la seguridad cibernética, el gobierno mexicano ha emprendido ciertas acciones las cuales se describirán en el presente documento.

¿Qué es un delito informático?

Delito informático: El Convenio de Ciberdelincuencia del Consejo de Europa los define como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos. Existen acciones que México ha implementado para la prevención y regulación de este tema que serán explicados más adelante.

¿Qué soluciones prácticas México puede ejercer para hacer frente a los desafíos en materia de seguridad cibernética?

1. Creación de una Estrategia Nacional de Seguridad Cibernética y una Agencia Nacional de Seguridad Cibernética (ANSC).
   El tener una ENSC es un primer paso para garantizar y dar certeza a la sociedad en materia de seguridad cibernética y, para la implementación de esta Estrategia, se sugiere la creación de la ANSC única.
2. Establecimiento y cumplimiento de medidas de seguridad cibernética apegadas a estándares internacionales.
   En el caso de los productos de seguridad cibernética es importante contar con certificaciones que brinden claridad de la información y transparencia en el proceso de certificación de la revisión de esta y análisis de la tecnología, con el fin de generar mayor confianza.
3. Adopción de prácticas resilientes.
   La creación de productos, procesos y sistemas de tecnologías de la información que sean resilientes hoy en día es esencial, ya que la resiliencia genera que los productos, procesos o sistemas puedan reinventarse más fácilmente para actualizar sus funciones al mismo ritmo que avanza la tecnología y seguir operando a pesar de sufrir un ataque.
4. Impulsar una cultura de seguridad cibernética.
   El actor clave para la mejora de la seguridad cibernética en el país es el mismo ciudadano. Es él el usuario común quien puede funcionar como facilitador para un ataque cibernético, incluso sin saberlo. Una alianza entre el gobierno, la iniciativa privada y la sociedad para la capacitación y educación en esta materia puede ayudar a generar una cultura de protección y prevención de los ciberdelitos y delitos informáticos en el país.

INTRODUCCIÓN

INTRODUCCIÓN

La Industria 4.0 ha transformado nuestro estilo de vida a un ritmo vertiginoso y sin precedentes, obligándonos a adaptar nuestra realidad y actividades cotidianas al exponencial paso que marcan los continuos avances tecnológicos, como lo es el fenómeno de la hiperconectividad. Hoy en día la interconexión de los individuos no se limita a relaciones interpersonales, sino que se extiende a otros aspectos de la vida común, que van desde transacciones bancarias, hasta compras de productos de la canasta básica o servicios esenciales del hogar y de entretenimiento. Además de la generación de eficiencias y mejoras en bienestar y calidad de vida, estos cambios vienen también acompañados de riesgos y amenazas, no sólo para el ciudadano común sino para las entidades gubernamentales que tienen la obligación de velar por la seguridad de los gobernados y salvaguardarlos de los peligros que se presentan en la red.

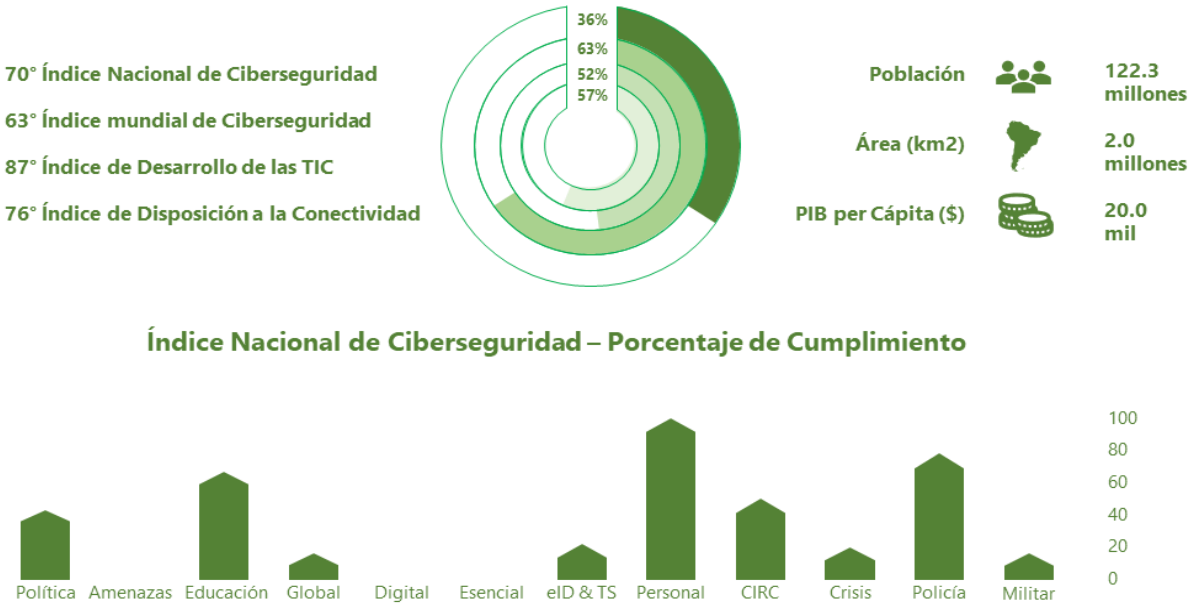
De este nuevo desafío surge la inminente necesidad de redoblar esfuerzos a nivel público y privado para lograr un espacio digital más seguro. El reto no se limita a la creación de productos innovadores de seguridad cibernética, sino que también se deben acompañar con la creación de productos, procesos y sistemas de Tecnologías de la Información (TI) que sean resilientes. En este contexto, la resiliencia tecnológica significa que un sistema está preparado para enfrentar una crisis, que cuente con una alta capacidad de respuesta ante un ataque cibernético y, lo que es más importante, que dicho sistema tenga la capacidad para adaptarse y reinventar su estructura aun cuando la seguridad cibernética haya sido vulnerada.

Ante tal situación, la seguridad cibernética se ha convertido en una disciplina que desafía las estructuras de gobernanza y que alienta a la elaboración de políticas públicas transformadoras e inusuales. Si bien México ha implementado diversas medidas a nivel nacional e internacional con el objetivo de prepararse y hacer frente a los retos en materia de seguridad cibernética, aún hay algunas medidas con las que puede beneficiarse, por ejemplo, formar grupos de trabajo con expertos y empresas del sector tecnológico, a fin de poder diseñar un marco de política pública que permita enfrentar los riesgos que presentan las amenazas cibernéticas globales y nacionales.

En virtud de lo anterior, resulta evidente que México tiene una gran oportunidad de seguir creciendo en materia de seguridad cibernética. De acuerdo con el *National Cyber Security Index* (NCSI), que desarrolla la *e-Governance Academy Foundation* de Estonia, México ocupa el puesto 70 de 100 países estudiados.[1] Este índice analiza cinco principales indicadores: medidas legales, técnicas, orgánicas, de capacitación y de cooperación tanto nacionales como internacionales. La calificación otorgada por el NCSI señala que México presenta un bajo nivel de preparación para enfrentar amenazas en el ciberespacio (diagrama 1 traducido).

[1] "National Cyber Security Index, México", *NCSI*, 7 de abril de 2018, https://ncsi.ega.ee/country/mx/

Diagrama 1[2]



En relación con Latinoamérica, México se encuentra por encima de países como Paraguay y Venezuela, pero muy por debajo de otros como Brasil, Uruguay, Argentina, Costa Rica, Chile y Colombia. Los costos que generan los ciberdelitos en México ascienden a $3,000 millones de dólares afectando al sector público, privado y en mayor medida a la sociedad mexicana.[3] Estos costos incluyen el capital perdido a causa del ataque y los recursos que se gastan en preparar la defensa del ataque y la reparación de los daños ocasionados. Las amenazas más comunes incluyen: *malware, phishing, hackeos*, fraude, extorsión, difamación, amenazas, robo de contraseñas, suplantación de identidad, acoso cibernético, intrusión no autorizada en sistemas, *ransomware,* entre otros.

Tomando en cuenta lo anterior, el mayor desafío que han traído las tecnologías emergentes a las autoridades mexicanas es el de evitar que los delincuentes utilicen estas herramientas para realizar operaciones ilícitas y aprovechen el anonimato que les brinda el internet para perpetrar actos ilícitos en perjuicio de ciudadanos y del propio gobierno. La capacitación constante, así como el uso de nuevas herramientas, puede ser de gran utilidad para que las autoridades mexicanas eviten que la incidencia y sofisticación actual de los delitos cibernéticos rebasen la capacidad de respuesta, acción y prevención. Por ello, en este documento se propone la creación e implementación de soluciones que permitan a México estar mejor preparado en este ámbito considerando la situación actual y las necesidades del país.

---

[2] *Ibid*.

[3] Expansión, "México foco de ciberdelitos en América Latina," *Expansión,* 20 de abril del 2016, https://expansion.mx/empresas/2016/04/20/mexico-foco-de-ciberdelitos-en-america-latina

En primer lugar, se presentará brevemente un panorama general e histórico sobre los avances en el país en temas de seguridad cibernética. Posteriormente, se hará distinción entre dos vertientes de la seguridad cibernética: los ciberdelitos, y delitos informáticos que es la protección de datos e infraestructuras críticas, explicando en cada sección cuáles son los recursos con los que cuenta México para el combate de estos delitos en el contexto nacional e internacional. Después, se expondrán algunas soluciones prácticas que hemos identificado para ayudar a México hacer frente a los desafíos del país en la era digital:

1. Creación de una Estrategia Nacional de Seguridad Cibernética y una Agencia Nacional de Seguridad Cibernética.
2. Establecimiento y cumplimiento de medidas de seguridad cibernética apegadas a estándares internacionales.
3. Adopción de prácticas resilientes.
4. Impulsar una cultura de seguridad cibernética.

Finalmente, el documento recomendará una guía plausible para la implementación de dichas medidas que a largo plazo podrán posicionar a México en un mejor nivel en la protección y prevención de las amenazas en el ciberespacio.

ANTECEDENTES

ANTECEDENTES

En junio de 2013 se promulgó la reforma constitucional en materia de telecomunicaciones mediante la cual se reconoció el acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet como un derecho fundamental. Se creó el Instituto Federal de Telecomunicaciones (IFT) como órgano constitucional autónomo el cual tiene como objetivo principal el desarrollo eficiente de las telecomunicaciones y la radiodifusión en el país y promover la competencia.[4] De acuerdo con el reporte emitido en 2018 por el Instituto Federal de Telecomunicaciones llamado "Comportamiento de los indicadores de los mercados regulados," esta reforma ha logrado grandes cambios en las telecomunicaciones, por ejemplo, se ha promovido la competitividad entre los proveedores de servicios de internet, así como también ha mejorado la calidad y el costo de los servicios tecnológicos en México.[5]

Derivado de estos cambios normativos e institucionales, y en la consecuente regulación de los agentes económicos que intervienen en las telecomunicaciones, en 2018 se registró un incremento del 4.3% en la cantidad de mexicanos con acceso a internet en comparación con el 2017, alcanzando un total de 82.7 millones de mexicanos como usuarios de internet, lo que significa una penetración de 71% entre la población de personas de 6 años en adelante y en 2019 los usuarios de internet en México pasan diariamente 8 horas con 20 minutos, 8 minutos más que en 2018.[6]

Este incremento ha sido posible gracias al aumento de planes tarifarios accesibles de internet y la proliferación de redes inalámbricas gratuitas disponibles en espacios públicos, las cuales han logrado que la brecha digital en el país se reduzca, pero también han generado dos principales problemas:

1. **La aparición e incremento de ciberdelitos:** los ciberdelincuentes aprovechan el fácil acceso a internet a través de planes tarifarios de bajo costo y la falta de cultura de protección cibernética en el país para operar más fácilmente, también frecuentemente utilizan las redes de internet gratuitas lo que dificulta a las autoridades identificarles y en consecuencia limita su capacidad de investigación, persecución y proceso de delitos cibernéticos. De acuerdo a un estudio elaborado por la Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes en colaboración con la Organización de Estados Americanos y recursos del

[4] Los organismos autónomos son creados directamente en la Constitución e independientes de los poderes públicos tradicionales (Ejecutivo, Legislativo y Judicial), esto es, existen por fuera de la jerarquía política y jurídica de los tres poderes, aunque están sujetos a ciertos mecanismos de rendición de cuentas frente al Legislativo. Con frecuencia tienen atribuciones exclusivas para desempeñar funciones cruciales del Estado, están facultados para expedir las normas que los rigen y pueden definir su presupuesto y administrarlo.

[5] Instituto Federal de Telecomunicaciones, "Comportamiento de los Indicadores de los Mercados Regulados 2018," *IFT*, 2018. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/indicadores2018vacc.pdf

[6] Asociación de Internet.mx, "15 Estudio sobre los Hábitos de los Usuarios de Internet en México 2019 versión pública,", 01 agosto 2019. https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/15-Estudio-sobre-los-Habitos-de-los-Usuarios-de-Internet-en-Mexico-2019-version-publica/lang,es-es/?Itemid=

Gobierno del Reino Unido, menciona que respecto a las conexiones a redes públicas, en muchas ocasiones los usuarios no se detienen a pensar sobre los lugares a los que se conectan y las consecuencias que esto puede tener, existe un exceso de confianza por parte de los usuarios manteniendo el riesgo de que su información pueda ser robada.[7]

2. **La vulnerabilidad de datos:** al hacer uso de redes públicas de manera frecuente, los usuarios están sobre expuestos a ataques cibernéticos como el robo de datos personales sensibles y financieros, extorsión, fraude, *malware*, robo de identidad, entre otros.

Es importante señalar que el nuevo Plan Nacional de Desarrollo 2019-2024 no hace referencia sobre el rumbo que debe tomar el país en materia de seguridad cibernética. Esto evidencia la necesidad de proponer e implementar recomendaciones y mejores prácticas que ayuden a fomentar la materia.

El gobierno, la academia, el sector privado y la sociedad civil se han organizado con el objetivo de compartir prácticas y recomendaciones en foros de cooperación en el tema. Por ejemplo, el Instituto Tecnológico de Estudios Superiores de Monterrey, que, en conjunto con Cisco, Deloitte, Thales, IBM y la Universidad de Texas, han creado un centro donde se comparte conocimiento y experiencia mediante la capacitación, investigación y servicios brindados por el denominado "*Tec Cybersecurity Hub*". Ambas iniciativas se apegan a los aspectos principales de seguridad cibernética y tienen un enfoque multidisciplinario y de colaboración para mejorar el nivel en el que se encuentra México en esta materia, otro ejemplo de que se ha llevado a cabo, son las mesas temáticas de ciberseguridad de la Secretaría de Comunicaciones y Transportes y su documento base de "Habilidades de Ciberseguridad para Telecomunicaciones y Radiodifusión" del 28 mayo 2019.

Asimismo, la Asociación Mexicana de la Industria de Tecnologías de Información (AMITI) actualmente colabora con el Gobierno mexicano mediante foros en materia de ciberseguridad con el objetivo de impulsar la digitalización de México. La AMITI, la Cámara Nacional de la Industria Electrónica, de Telecomunicaciones y Tecnologías de la Información (CANIETI) y la Asociación de Internet MX han presentado también al gobierno federal un reporte denominado "Evaluación de la Ciberseguridad en México: Brechas y Recomendaciones en un Mundo Hiper-Conectado," mediante el cual a través de un enfoque multidisciplinario y de cooperación se tiene el objetivo de mejorar el nivel en el que se encuentra México en materia de seguridad cibernética.

En resumen, México cuenta con valiosas herramientas para combatir los delitos cibernéticos y cuenta con instituciones encargadas de salvaguardar la seguridad en línea, sin embargo, hace falta que estas instituciones se robustezcan y sean capaces de la implementación de los protocolos e instrumentos internacionales, y la posibilidad de elaborar nuevas legislaciones nacionales, así como la creación de otras instituciones relacionadas a la seguridad cibernética.

---

[7] Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes en colaboración con la Organización de Estados Americanos y recursos del Gobierno del Reino Unido "Estudio Hábitos de los usuarios en ciberseguridad en México 2019" México 08 de marzo 2019. https://www.gob.mx/cms/uploads/attachment/file/444447/Estudio_Ciberseguridad.pdf

La *Sysem Audit and Control Association* estimó que en el año 2019 habrá un déficit mundial de 2 millones de profesionistas en seguridad cibernética. En México se pronostica que casi 148 mil puestos en el rubro de tecnologías de la información no podrán ocuparse en el 2019; de estos cerca de 36 mil estarán relacionados con temas de seguridad cibernética.[8] Por ello, es necesario el desarrollo de profesionales, la creación y ejecución de programas de capacitación y de certificación de habilidades en materia de seguridad cibernética (públicas y privadas); y promover la acreditación de instituciones académicas que ofrezcan carreras en esta materia.

Para efectos de lograr una mejor claridad al exponer los recursos con los que dispone México para combatir la ciberdelincuencia actualmente, en este documento se hará una división de dos categorías, las cuales serán definidas a continuación **1) Ciberdelito y; 2) Delitos en materia de protección de datos e infraestructuras críticas o delitos informáticos**. Esta distinción es relevante para enfatizar el alcance de las recomendaciones que se exponen en este documento, así como para brindar al lector una clara diferenciación entre las variedades de crímenes cibernéticos de los que los ciudadanos podemos ser objeto en la era digital.

1. **Ciberdelito:** El uso de una computadora o dispositivo electrónico con internet para cometer actividades ilícitas tales como fraude, trata de personas, distribución y producción de pornografía infantil, tráfico de sustancias ilícitas, piratería, entre otras.[9] Este tipo de delito normalmente persigue una remuneración monetaria.
2. **Delito informático:** El Convenio de Ciberdelincuencia del Consejo de Europa los define como "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos".[10] En general son aquellos que tienen como común denominador el ataque a activos de información; en esta categoría incluiremos aquellos actos que estén dirigidos a infraestructuras críticas no sólo a nivel público sino también en el sector privado.[11]

A continuación, se expondrá el contexto nacional e internacional actual en cada una de estas categorías, así como una serie de medidas y recomendaciones para posicionar a México en un mejor nivel en materia de seguridad cibernética.

---

[8] Consejo Mexicano de Asuntos Internacionales, "Perspectiva de Ciberseguridad en México," *COMEXI,* junio 2018, https://consejomexicano.org/multimedia/1528987628-817.pdf

[9] Michael Aaron Dennis, "Cybercrime," *Encyclopedia Britannica*" última revisión 17 de marzo de 2005, https://www.britannica.com/topic/cybercrime.

[10] Convenio sobre la Ciberdelincuencia (Estados Unidos: Organización de Estados Americanos, 2001).

[11] Por infraestructuras críticas nos referiremos a "aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de la administración pública." (Manuel Sánchez, "Infraestructuras Críticas y Ciberseguridad," *Manuel Sánchez Gómez-Merelo)*.

CIBERDELITO

CIBERDELITO

Contexto Nacional

El Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal define a la ciberseguridad como: la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada.[12]

La Asociación Mexicana de Instituciones de Seguros, más de 33 millones de personas fueron víctimas de un ataque cibernético en 2017, es decir, uno de cada cuatro mexicanos sufrió las consecuencias de ataques cibernéticos.[13] De acuerdo con la consultora de información estratégica *Lexis Nexis Risk Solutions*, México ocupa el segundo lugar de los países más afectados por el cibercrimen en Latinoamérica.[14]

El principal delito cibernético en el país es fraude, y los constantes ataques cibernéticos a las instituciones financieras en el país facilitan la proliferación de este delito. Existen además otros delitos cibernéticos de alta frecuencia, por ejemplo, la venta de droga por internet, el robo de identidad, extorsión, abuso sexual infantil, *cybergrooming* (contacto con menores), pornografía infantil, *revenge porn* y *cyberbulling,* son sólo algunos de los delitos más recurrentes encontrados por la policía cibernética.

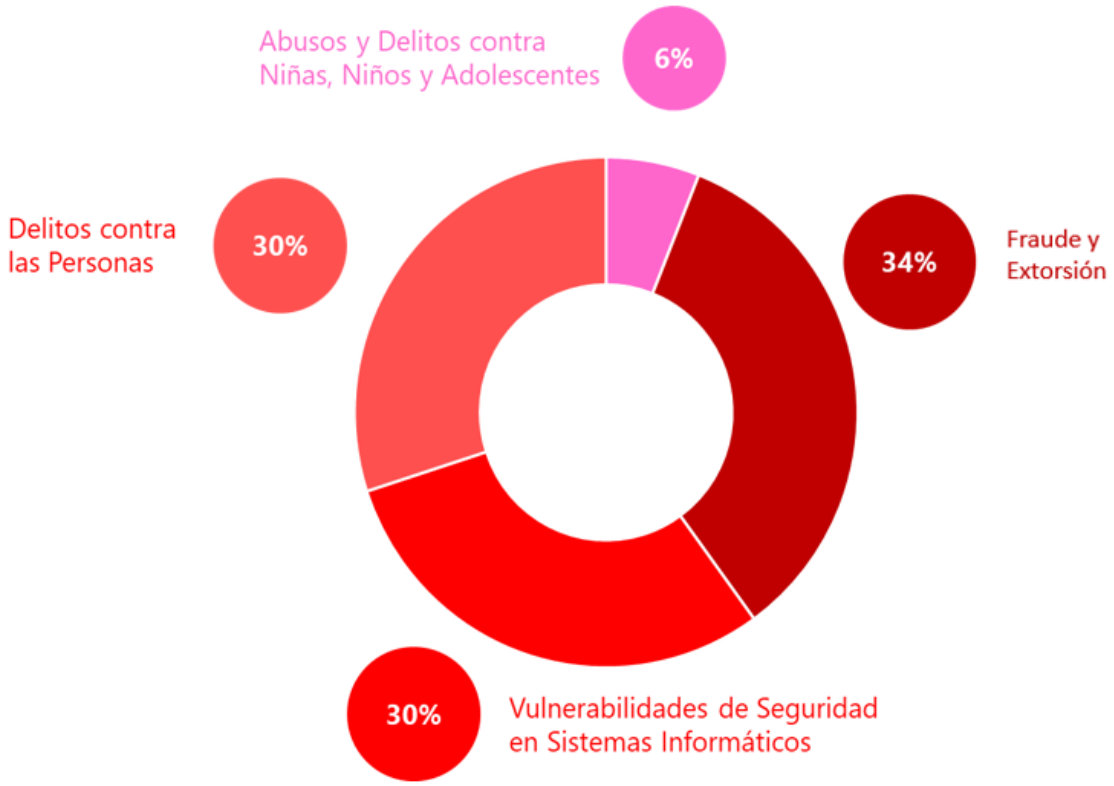
El diagrama a continuación expone los delitos cibernéticos mayormente reportados por la División Científica de la Policía Federal. (*Diagrama 2)*[15]

[12] Secretaría de la Función Pública, "Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal." *Diario Oficial de la Federación* 06 de septiembre de 2011. http://dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/09/2011

[13] Consejo Mexicano de Asuntos Internacionales, "Perspectiva de Ciberseguridad en México," *COMEXI,* junio 2018, p. [6] https://consejomexicano.org/multimedia/1528987628-817.pdf

[14] Notimex. "México, segundo país más vulnerable a ciberataques," *Excélsior,* 27 de noviembre de 2018, https://www.excelsior.com.mx/trending/mexico-segundo-pais-mas-vulnerable-a-ciberataques/1281130

[15]División Científica de la Policía Federal, "Prevención del Delito Cibernético," *PF División Científica*, 2018. https://www.infosecuritymexico.com/content/dam/sitebuilder/rxmx/intra-logistics/PDF/presentacione_2018/infosecurity2018_ArturoGome_PF.pdf.



Ante este contexto, la preocupación de los mexicanos de ser víctimas de un ataque cibernético ha incrementado. Por ejemplo, el 90% de los mexicanos dice estar seriamente preocupado por la obtención y uso de sus datos bancarios por criminales cibernéticos.[16] Dicha preocupación ha aumentado un 216.6% en comparación a las cifras registradas en encuestas del 2014, México se colocó como el segundo país con el mayor nivel de preocupación de un fraude financiero entre los 13 encuestados desde 2014.[17]

Amenazas como virus cibernéticos o el hacking son también inquietudes que la población mexicana expresó en las mismas encuestas registrándose un incremento al 77% con respecto al 62% de la población del 2014.[18] Por otro lado, el robo de identidad y el acceso no autorizado o uso indebido de información personal mantuvo el mismo nivel de inquietud con 86% de la muestra respondiendo sobre esta preocupación.[19] Sin embargo, se debe de tener en cuenta que un gran porcentaje de los

---

[16] Ricardo Meléndez, "El 90% de los mexicanos está preocupado por la obtención y uso de sus datos bancarios,"Qore, 24 de junio del 2017, https://www.qore.com/noticias/56515/El-90-de-los-mexicanos-esta-preocupado-por-la-obtencion-y-uso-de-sus-datos-bancarios .

[17] Ricardo Meléndez, "El 90% de los mexicanos está preocupado por la obtención y uso de sus datos bancarios,"Qore, 24 de junio del 2017, https://www.qore.com/noticias/56515/El-90-de-los-mexicanos-esta-preocupado-por-la-obtencion-y-uso-de-sus-datos-bancarios

[18] *Ibid.*

[19] *Ibid.*

ciberdelitos se pueden prevenir, fomentando la conciencia de la importancia de la ciberseguridad y creando instituciones que ayuden a la prevención y combate de estos delitos cibernéticos.

Es por eso, que es urgente el fortalecer las medidas de seguridad digital para mitigar los riesgos y amenazas en el ciberespacio.

Debido al incremento de amenazas cibernéticas el gobierno mexicano ha emprendido algunas acciones para prepararse y combatir de manera eficaz el ciberdelito apoyándose de las siguientes normativas y recursos:

Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico y Subcomisión de Ciberseguridad (CIDGE)

La CIDGE tiene como objetivo promover y consolidar el uso y aprovechamiento de las tecnologías de la información y comunicaciones (TIC) en la Administración Pública Federal, y mejorar la entrega de servicios al ciudadano, facilitarle el acceso a la información del gobierno y facilitar la interoperabilidad entre las dependencias y entidades.[20]

La CIDGE ha trabajado en coordinación con la Secretaría de la Función Pública y la Coordinación de Estrategia Digital Nacional para implementar un sistema que simplifique al menos cinco mil servicios ofrecidos a la ciudadanía[21] y que con esto se logre ahorrar recursos públicos, tiempo y evitar actos de corrupción.[22] Su misión es la democratización de los servicios públicos y para ello la digitalización e innovación en sus sistemas es imprescindible.

Ley de la Guardia Nacional y su Reglamento

La Ley de Guardia Nacional establece que ésta tendrá por objeto realizar la función de seguridad pública a cargo de la Federación y, en su caso, conforme a los convenios que para tal efecto se celebren, colaborar temporalmente en las tareas de seguridad pública que corresponden a las entidades federativas o municipios. De conformidad con su Reglamento y con la publicación del Diario Oficial de la Federación de fecha 30 de septiembre 2019, se establece que dentro de la estructura de la Guardia Nacional, estará la Unidad de Órganos Especializados por Competencia, la cual contempla a la Dirección General Científica (esta última Dirección, será la equivalencia a la División Científica de la Policía Federal) y dentro de sus atribuciones será el vigilar, identificar, monitorear y rastrear la red pública de Internet, para prevenir conductas delictivas.

---

[20] Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (México, 2005).

[21] El ejemplo más reciente de esto es la digitalización del acta de nacimiento, hasta abril de 2019 se tramitaron un millón cuatrocientos mil actas digitales.

[22] Secretaria de la Función Pública, "Crea SFP Subcomisión de Inteligencia Artificial y Deep Learning de la CIDGE," Comunicado 063, *Gobierno de México,* 30 de abril del 2018. https://www.gob.mx/sfp/prensa/crea-sfp-subcomision-de-inteligencia-artificial-y-deep-learning-de-la-cidge

Código Penal Federal

El Capítulo II del Código Penal Federal tipifica el acceso ilícito a sistemas y equipos de informática. En los artículos correspondientes a dicho capítulo se establecen las penas que serán imputadas a aquellas personas, física o moral, que atenten contra los sistemas y equipos de informática pertenecientes al Estado e instituciones del sistema financiero.[23]

Código Nacional de Procedimientos Penales

Establece los lineamientos para operaciones de intervención de sistemas de telecomunicaciones y obliga a los concesionarios de telecomunicaciones, los autorizados o proveedores de servicios de aplicaciones y contenidos a cooperar con las autoridades y proporcionar la información solicitada para la investigación de hechos delictivos.[24]

Contexto Internacional

El crimen cibernético es también una preocupación creciente a nivel global. La naturaleza transnacional del ciberdelito ha causado pérdidas que ascienden a los 600,000 millones de dólares en la economía mundial. Esto representa el 0.8% del Producto Interno bruto global.[25] Es un problema que lejos de disminuir, los avances tecnológicos facilitan su expansión y permanencia. La creciente sofisticación del delito cibernético y lo relativamente fácil que es ocultar la identidad del criminal mediante el internet suponen los retos más grandes para las instituciones a nivel mundial.

El informe "*Economic Impact of Cybercrime -No Slowing Down*" reveló el impacto que tiene el cibercrimen en las economías internacionales, y también puso de manifiesto que el robo de propiedad intelectual representa al menos el 25% del crimen en línea. Asimismo, el informe señaló la peligrosidad de este acto cuando estas conductas involucran tecnología militar. [26] El informe concluyó que este delito es el primero en número de víctimas afectadas, rebasando el narcotráfico.[27]
Usualmente el delito cibernético trasciende fronteras y esto genera problemas de jurisdicción. El ataque de *ransomware* WannaCry (mayo de 2017) que infectó a más de 230,000 computadoras en 150 países, o el llamado Dyn attack (octubre de 2016) que ocasionó disturbios en centros de acopio de datos de sitios de noticias y comerciales causando un efecto dominó en toda la unión americana y

[23] Código Penal Federal (México, 2019).
[24] Código Nacional de Procedimientos Penales (México, 2016).
[25] El apetitoso negocio del cibercrimen, Dinero , 2 de febrero del 2017, https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593
[26] J.M. Sánchez, "El cibercrimen es incesante: provoca un agujero de 600.000 millones de dólares a las, empresas," *ABC Redes*, 7 de marzo del 2018 https://www.abc.es/tecnologia/redes/abci-cibercrimen-incesante-provoca-agujero-600000-millones-dolares-empresas-201803050122_noticia.html.
[27] *Ibid.*

Europa son sólo algunos ejemplos de este tipo de ataque.[28] En respuesta a estos incidentes, los países han buscado foros y espacios de cooperación que los ayuden a combatir el delito cibernético más eficaz y eficientemente. A continuación, se mencionan aquellos recursos internacionales de los que México puede hacer uso en el combate del crimen cibernético:

Convenio de Budapest

El Convenio de Budapest o Convenio sobre la Ciberdelincuencia, fue elaborado en 2001 por el Consejo de Europa y sus miembros activos, con el fin de combatir los delitos informáticos.[29] México ha fungido como observador del Convenio de Budapest desde 1999, sin embargo, a la fecha no ha ratificado ni implementado su adhesión.
Este es el único tratado internacional en materia de ciberdelincuencia y se presenta como guía para que los Estados que formen parte se comprometan a realizar lo siguiente:

1) Implementar dentro de su ordenamiento jurídico nacional la legislación pertinente para investigar y perseguir penalmente aquellos delitos cometidos en contra de sistemas o medios informáticos o mediante el uso de estos.
2) Facilitar la asistencia jurídica mutua y extradición.

El Convenio tiene tres ejes u objetivos esenciales, los cuales son:

1) Armonización de los delitos informáticos, establecer un catálogo de tipos penales.
2) Establecer las normas procesales que establezcan los procedimientos para salvaguardar la evidencia digital,
3) Establecer un régimen de cooperación internacional en la investigación de un delito.

La eficiencia de este instrumento depende de la plena adaptación de la legislación nacional de los Estados que lo han ratificado y debe quedar constancia de esto para verdaderamente adherirse al Convenio. Al ser un documento especializado en temas de ciberseguridad internacional y protección informática, es importante que México logre homologarse a los estándares internacionales.

Foro para la Gobernanza de Internet

El Foro de Gobernanza de Internet (FGI), celebrado cada año, es el principal centro de discusión sobre políticas públicas relacionadas con Internet en un esquema abierto donde participan las diversas partes interesadas del ecosistema de internet, que incluyen a la academia, la comunidad técnica, los gobiernos, la iniciativa privada, la sociedad civil e interesados en la gobernanza de Internet. el FGI los

[28] Kaspersky daily, "Top 5 de los ciberataques más memorables," *Kaspersky Daily,* 6 de noviembre del 2018, https://latam.kaspersky.com/blog/five-most-notorious-cyberattacks/13613/
[29] Convenio sobre la Ciberdelincuencia (Budapest: Organización de Estados Americanos, 2001).

reúne en igualdad de condiciones y la toma de decisiones se realiza mediante un proceso abierto e inclusivo.

El Foro para la Gobernanza de Internet ahora también incluye Foros de Mejores Prácticas en temas de seguridad cibernética. México fue anfitrión de la reunión del FGI en 2016, en la cual se abordó la seguridad cibernética como un fenómeno multifactorial que es y será una pieza clave para el desarrollo sostenible. Esto demuestra el compromiso que México ha mostrado por promover y aprovechar las ventajas del uso de las TIC.

Tratado de Asistencia Jurídica Mutua (MLAT) en los Delitos Informáticos

El MLAT es el sistema de acuerdos bilaterales y multilaterales mediante los cuales los Estados se comprometen a ayudarse mutuamente en investigaciones criminales y procedimientos penales. Actualmente, México colabora con agencias de varios países bajo estos acuerdos de cooperación; sin embargo, siempre es posible ampliar y estrechar las relaciones de cooperación y amistad con sus aliados, de tal manera que se ayuden a expedir de manera más eficaz y segura las solicitudes de información, operativos conjuntos o mera cooperación entre fuerzas policiacas con el objetivo de combatir los delitos cibernéticos que por naturaleza trascienden fronteras.

DELITO INFORMÁTICO

DELITO INFORMÁTICO. PROTECCIÓN DE DATOS E INFRAESTRUCTURAS CRÍTICAS

Como se mencionó anteriormente, en esta sección se expondrán el contexto nacional e internacional de aquellos delitos cibernéticos en **materia de protección de datos e infraestructuras críticas,** es decir, aquellos que sólo pueden cometerse a través de una computadora, una red o redes de computadoras u otras formas de tecnología de comunicación de la información y tienen como objetivo limitar o incapacitar las operaciones de una compañía, industria o un gobierno.

Contexto Nacional

Los recientes ciberataques al sector financiero han hecho evidente la necesidad de crear nuevas y mejores estrategias para evitar el acceso no autorizado a los sistemas de información. Algunos de los casos que evidenciaron la debilidad del sistema de seguridad cibernético en México son: el sucedido en abril de 2018 cuando el sistema de pagos electrónicos interbancarios del Banco de México fue el blanco de delincuentes cibernéticos, quienes lograron sustraer más de 300 millones de pesos de distintas instituciones bancarias y las transfirieron a cuentas falsas para vaciarlas finalmente en distintas sucursales en todo el país. Otro ejemplo también sucedido en 2018 es aquel ataque que Pemex recibió en el cual ciberdelincuentes intentaron secuestrar la información contenida en 60 mil equipos de cómputo de la paraestatal, así como robar la identidad de funcionarios e infiltrarse en sus 160 portales de internet.[30]

De acuerdo con Finccom, una firma especializada en prevención y detección de delitos financieros, México es el segundo país donde se producen más robos de datos personales en América Latina, únicamente por debajo de Brasil.[31] En México, una empresa sufre ataques cibernéticos cada siete minutos, por lo que se estima que 1.5 millones de personas son afectadas por ciberataques a diario.[32] Los criminales cibernéticos o hackers han ido actualizando sus modos de operación con la evolución de las diversas tecnologías, por lo que día a día se vuelven más sofisticados los ataques. Mer Group, una empresa de tecnología reveló recientemente que el robo de información sensible se ha transformado en una industria millonaria, pues estos datos se comercializan principalmente en la *deep*

[30] Dinero en Imagen, "¿Existen delincuentes cibernéticos en el robo de combustible?," *Dinero en Imagen,* 20 de enero de 2019. https://www.dineroenimagen.com/hacker/existen-delincuentes-ciberneticos-en-el-robo-de-combustible/106381

[31] Ángel Ortiz, "México es el segundo país con mayor robo de datos personales: Finccom," *El Economista,* 29 de noviembre del 2018. https://www.eleconomista.com.mx/empresas/Mexico-es-el-segundo-pais-con-mayor-robo-de-datos-personales-Finccom-20181129-0069.html

[32] Forbes, "Mexicanos reciben 1.5 millones de ataques cibernéticos al día", Forbes Magazine, 16 de abril de 2018, https://www.forbes.com.mx/mexicanos-reciben-1-5-millones-de-ataques-ciberneticos-al-dia/

web. Mer Group también expuso que un ataque cibernético le cuesta a las empresas mexicanas alrededor de 500,000 dólares; y a nivel mundial, estos delitos generan costos de hasta 445,000 millones de dólares.[33]

Según la encuesta global de Software publicada por *BSA* | The Software Alliance realizada en mayo de 2016, aproximadamente 430 millones de nuevas unidades de software malicioso fueron descubiertas en el 2015. La misma encuesta reveló que el costo total de una filtración incrementó 23% en el periodo de 2013-2015, esto debido a que solo dos de cada tres empresas de entre 250 y 1,000 integrantes que forman parte de la Asociación de Internet MX han declarado estar "medianamente preparadas para enfrentar amenazas cibernéticas."[34]

El sector público también enfrenta riesgos cibernéticos de este tipo como el robo o alteración a la información que resguarda de los ciudadanos, la intrusión a los sistemas que permiten la prestación de servicios públicos, o la interrupción de operaciones de entidades gubernamentales. Todos estos riesgos pueden causar potencial daño a la confianza en instituciones por parte de los ciudadanos, por lo que es importante contar con instituciones y recursos legales para hacer frente a estas amenazas.

A continuación, se describen algunas de las regulaciones que son relevantes en la materia desde la perspectiva nacional:

Ley General de Transparencia y Acceso a la Información Pública

Esta ley tiene como objetivo establecer los principios, bases generales y procedimientos para garantizar el derecho de acceso a la información. Se entiende por información todos aquellos datos que se encuentren en posesión de cualquier autoridad, entidad, órgano u organismo de los poderes Legislativo, Ejecutivo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos; así como en posesión de cualquier persona física, moral y sindicato que reciba y ejerza recursos públicos o realice actos de autoridad a nivel federal, estatal y municipal. Dicha legislación es relevante porque garantiza el acceso a la información a todo ciudadano mexicano y además prevé la protección de datos del solicitante y de la información solicitada.

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

Tiene como objetivo regular el uso y posesión de los datos que los ciudadanos proveen de manera voluntaria a los particulares. La regulación en el manejo de estos datos tiene la finalidad de garantizar la privacidad y el derecho a la autodeterminación informativa a todas las personas. Toda persona física o moral de carácter privado están obligados al cumplimiento de esta ley, con excepción de sociedades

[33] *Ibid.*
[34] Rodrigo Riquelme, "6 datos sobre la ciberseguridad en México y el mundo," *El Economista,* 9 de septiembre de 2017, https://www.eleconomista.com.mx/tecnologia/6-datos-sobre-la-ciberseguridad-en-Mexico-y-el-mundo-20170909-0003.html

de información crediticia o aquellas personas que recolecten y/o almacenen datos para uso personal y que no comercialicen de manera directa o indirecta los datos.[35]

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados

Esta ley tiene como objetivo establecer los lineamientos para la protección de datos que los individuos entregan a sujetos obligados. Por sujetos obligados se refiere a cualquier autoridad, entidad, órgano y organismo sin importar el ámbito ya sea federal, estatal o municipal y que pertenezca a alguno de los tres poderes de gobierno (Ejecutivo, Legislativo y Judicial). También se considera sujetos obligados a los partidos políticos, fideicomisos, sindicatos y fondos públicos; y cualquier otra persona física o moral que haga uso recursos públicos o realice actos de autoridad en los tres niveles de gobierno.[36]

Ley Federal de Telecomunicaciones y Radiodifusión

La Ley Federal de Telecomunicaciones y Radiodifusión tiene como finalidad regular el uso aprovechamiento, explotación y convergencia entre el espectro radio eléctrico, las redes públicas de telecomunicaciones, el acceso a la infraestructura activa y pasiva, los recursos orbitales, la comunicación vía satélite, la prestación de los servicios públicos de interés general de telecomunicaciones y radiodifusión. En esta legislación también se prevén los derechos de los usuarios y las audiencias, y el proceso de competencia entre los actores de los sectores antes mencionados.[37]

Grupo de Respuesta a Incidentes de Seguridad de la Información

El Grupo de Respuesta a Incidentes de Seguridad de la Información (GRI) se establece en 2018 tras el ataque cibernético que sufrió el sistema financiero mexicano. El grupo es conformado por funcionarios públicos y de las instituciones financieras, así como sus equipos internos de identificación y respuesta a incidentes sensibles. La Secretaría de Hacienda y Crédito Público, el Banco de México; las Comisiones Nacionales Bancaria y de Valores, de Seguros y Fianzas, del Sistema de Ahorro para el Retiro, para la Protección y Defensa de los Usuarios de Servicios Financieros, y la Fiscalía General de la República (FGR) son algunos ejemplos de los miembros de este grupo. Además, se sumaron las asociaciones de bancos, de instituciones bursátiles, de fondos para el retiro; los sectores de ahorro y crédito popular, y las llamadas *fintech*, entre otros intermediarios financieros.

El documento señala las bases establecidas para emprender acciones para atender los incidentes de seguridad de la información que pudieran presentarse en contra de entidades del sector financiero. Se exponen medidas como: conocer, clasificar y evaluar los sucesos que se puedan considerar como

[35] Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México, 2010).
[36] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (México, 2017).
[37] Ley Federal de Telecomunicaciones y Radio Difusión (México, 2018).

incidentes; analizar las causas, consecuencias y efectos de éstos; contar con información oportuna y relevante que permita a los sujetos clave resolverlos; asegurar que esta sea precisa y completa, y coordinar la comunicación entre autoridades.

Disposiciones Generales aplicables a las Instituciones de Tecnología Financiera.

En marzo pasado, la Comisión Nacional Bancaria y de Valores "CNVB" publicó una resolución por la que se modifican las Disposiciones Generales para las *Fintechs*, en virtud de estas reformas, se añadió un capítulo denominado "De la Seguridad de la Información" que se refiere a la seguridad de la información con respecto a las disposiciones generales de notificación de incidentes de seguridad y establece las responsabilidades y la obligación de tener un Director de Seguridad de la Información conocido como "CISO" por sus siglas en inglés (*Chief Information Security Officer*).

Contexto Internacional

En el ámbito internacional la protección y privacidad de datos es un tema que recibe constante atención debido a la gravedad que representa un ataque cibernético a sistemas de información. Cisco indicó que alrededor del 49% de las empresas en el mundo fueron afectadas por al menos un ataque cibernético en 2016, de los cuales 39% son del tipo *ransomware*.[38] En este tipo de ataque, el atacante hace uso de un código malicioso para infectar una máquina y encriptar su contenido con la intención de pedir un rescate. La motivación y propósito para efectuar un ataque de este tipo varían enormemente. Algunos de los ejemplos más famosos y recientes que evidenciaron la necesidad de robustecer los sistemas de protección de información fueron:

- **WannaCry (12 de mayo, 2017).** Ataque masivo de *ransomware* que afectó a organismos públicos, empresas y particulares a nivel mundial. El ataque golpeó seriamente al Servicio de Salud Británico, a la multinacional francesa Renault, al sistema bancario ruso, al grupo de mensajería estadounidense FedEx, así como al servicio de ferrocarriles alemán y a universidades en Grecia e Italia. El ataque tenía un objetivo económico. México fue el quinto país más afectado por este ataque a nivel mundial y el primero a nivel Latinoamérica. Aproximadamente 50 empresas fueron expuestas a esta vulnerabilidad en el país.[39] Wannacry es el mayor ataque de un virus informático en la historia, y se considera un crimen cibernético trasnacional al haber afectado a más de 150 países.[40]

---

[38] Aura Hernández, "Ciberataques se sofistican; México no está a salvo," *Excélsior,* 11 de noviembre del 2017, https://www.excelsior.com.mx/hacker/2017/11/11/1200545

[39] Gabriela Chávez, "Este es el país más afectado por el ciberataque wannacry," *CNN Español,* 15 de mayo de 2017, https://cnnespanol.cnn.com/2017/05/15/este-es-el-pais-de-latinoamerica-mas-afectado-por-el-ciberataque-wannacry/

[40] Alexandra Perlof-Giles, "Transnational Cyber Offenses: Overcoming Jurisdictional Challenges," *Yale Journal of International Law*, 43, 2018, https://digitalcommons.law.yale.edu/yjil/vol43/iss1/4

➔ **Petya (junio, 2017).** Afectó especialmente a la infraestructura de Ucrania, incluyendo a compañías eléctricas, aeropuertos, transporte público y el banco central y ha sido el último de una serie de ataques cibernéticos contra este estado. Petya afectó a grandes empresas en Europa y Estados Unidos, entre los que destacan la firma de publicidad WPP, la empresa francesa de materiales de construcción Saint-Gobain, y Mondelez, Danish shipping, entre otros. [41]Expertos clasifican a Petya como un ataque más sofisticado que WannaCry y basado en el mismo principio de propagación masiva a través de redes locales.[42]

A pesar de su sofisticación, el propósito de este ataque no era económico sino destruir la reputación de la empresa que afectó.

Algunos de los recursos que México puede consultar y utilizar como guía en este tema son:

Reglamento General de Protección de Datos de la Unión Europea (RGDP)

El RGPD establece los requisitos específicos para empresas y organizaciones sobre recolección, almacenamiento y gestión de datos personales. Se aplica tanto a las organizaciones europeas que manejan datos personales de ciudadanos en la Unión Europea (UE) como a las organizaciones que tienen su sede fuera de la UE y cuya actividad se dirige a personas que viven en la UE.[43]

Tratado de Asistencia Jurídica Mutua (MLAT) en los Delitos Informáticos – véase Contexto Internacional de ciberdelito.

[41] Olivia Solon and Alex Hern, "'Petya' ransomware attack: what is it and how can it be stopped?", *The Guardian,* 28 de junio de 2017, https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

[42] Félix Palazuelos, "Petya un virus más peligroso y sofisticado que WannaCry," *El País,* 29 de junio del 2017, https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html

[43] Reglamento general de protección de datos del Parlamento Europeo (Bruselas, 2016)

SOLUCIONES PRÁCTICAS E IMPLEMENTACIÓN

SOLUCIONES PRÁCTICAS E IMPLEMENTACIÓN

1. La creación de una Estrategia Nacional de Seguridad Cibernética (ENSC) y una Agencia Nacional de Seguridad Cibernética.

Después de los ataques cibernéticos en Estonia (2007), por primera vez se habló de la seguridad cibernética como un problema que necesitaba atención y recursos económicos para su fortalecimiento. Desde entonces, más de 80 países a nivel mundial han creado estrategias de seguridad cibernética nacional y han iniciado el camino a su implementación.

El tener una ENSC es un primer paso para garantizar y dar certeza a la sociedad en materia de seguridad cibernética ya que, en este tipo de estrategias, se puede abarcar temas de seguridad nacional, protección de datos, marco jurídico, colaboración entre las diferentes autoridades hasta temas de conciencia en la ciberseguridad ciudadana e investigación.

En adición, se propone que para que la implementación de la ENSC sea efectiva es necesario crear simultáneamente una institución especializada que funja como autoridad o agencia central. Esta agencia reguladora debiera ser un ente a nivel federal con operaciones descentralizadas y que además coordine la cooperación entre diversos actores de la seguridad cibernética en el país.

Ventajas

La creación de una agencia dedicada exclusivamente a la seguridad cibernética a nivel nacional sería una manera efectiva de administrar la seguridad de las agencias civiles, la protección de la infraestructura crítica y la respuesta nacional a incidentes de nivel desde una misma entidad. Reduciría los gastos de operación de diversas entidades si se consolidara todo en un mismo lugar. Esta institución coordinaría más eficientemente el establecimiento de estándares y la cooperación entre los diversos actores que se involucran con la protección de la seguridad cibernética en el país.

Destinar un fondo específico para esta institución se podría invertir en investigación y equipo especializado que ayuden al combate del crimen cibernético de manera más eficiente. Esta agencia permitiría a los gobiernos priorizar sus limitados recursos y enfocarlos en objetivos específicos delineados en la ENSC.

Retos

Establecer mecanismos de evaluación y monitoreo que brinden transparencia y un sistema de rendición de cuentas para la ciudadanía. De esta manera, se promueve y fortalece mayor confianza en la institución y la buena gobernanza. Para esto la participación ciudadana y de organismos no

gubernamentales son de vital importancia, su contribución puede ayudar a crear mejores prácticas sobre la protección de las libertades civiles y privacidad de los ciudadanos.

Implementación

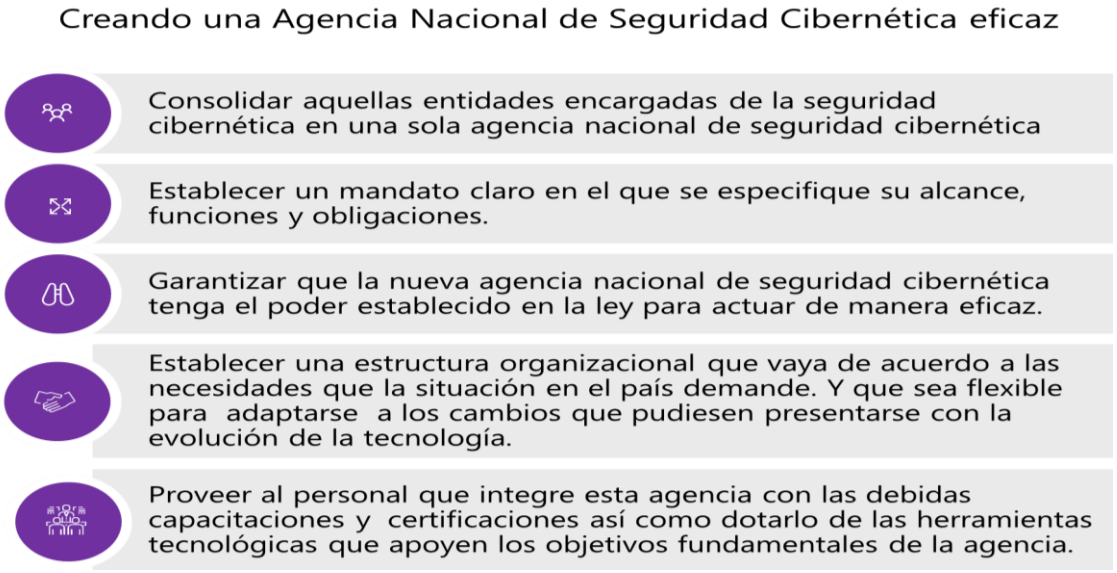
1. Designar una agencia nacional de seguridad informática única. Consolidar aquellas entidades encargadas de la seguridad cibernética nacional en una sola agencia, puede ser un medio eficaz para dirigir la seguridad de agencias civiles, proteger la infraestructura crítica y responder a incidentes a nivel nacional, creando mejores prácticas en ciberseguridad.

2. Establecer un mandato claro a la agencia. Especificar su alcance, funciones y obligaciones, con el fin de tener una certeza de cómo podrá colaborar tanto con el sector público como con el privado.

3. Garantizar que la nueva agencia nacional de seguridad cibernética tenga el poder establecido en la ley para actuar de manera eficaz y se le otorguen todas las facultades que requiere, para cumplir con eficiencia sus nuevas funciones.

4. Implementar una estructura organizacional. La cual vaya de acuerdo con las necesidades que la situación en el país demande. Y que sea flexible para adaptarse a los cambios que pudiesen presentarse con la evolución de la tecnología.

5. Expectativa de evolución y adaptación. Derivado a la transformación digital, se recomienda proveer al personal que integre esta agencia con las debidas capacitaciones y certificaciones y que se establezcan procesos regulares para evaluar el desempeño de la agencia con el fin de poder rectificar o modificar sus objetivos y generar mejores prácticas para el sector público y privado.



2. Establecimiento y cumplimiento de medidas de seguridad cibernética apegadas a estándares internacionales

Las certificaciones internacionales son mecanismos que ayudan a establecer confianza en los productos y servicios. Si dichos productos cumplen con marcos de referencia nacionales o internacionales, se demuestra claramente que el producto o servicio satisfará o excederá los requerimientos mínimos, y en consecuencia ofrecerá beneficios significativos de eficiencia. En el caso de productos de seguridad cibernética es importante contar con certificaciones que brinden claridad de la información, y que el proceso de certificación sea transparente en la revisión y análisis de la tecnología.

Este documento recomienda que México emita medidas de seguridad cibernética que estén apegadas a estándares internacionales como la serie de normas ISO 27000. La norma ISO 27001 es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información.[44] Esta serie clasifica a la información como un activo vital para el éxito de cualquier organización, por ello se crearon una serie de estándares que delimitan un marco de gestión y establecen objetivos claros de seguridad que pueden ser utilizados en cualquier tipo de organización, ya sea pública o privada, pequeña o de mayor tamaño. Aunque no es obligatoria la implementación de todos los estándares enumerados en la serie, es recomendable que toda organización se adhiera a la mayoría de los controles mencionados en la norma y de no hacerlo debe argumentar eficazmente el no cumplimiento de estas. Algunos de los ejemplos de la serie que ayudan a comprender la importancia de su establecimiento y apego son:

- **ISO 27002:** es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.[45]
- **ISO 27005:** establece las pautas para la gestión del riesgo en la seguridad de la información. Recalca y afirma los conceptos generales especificados en la norma ISO/IEC 27001 y tiene el objetivo de ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. [46]
- **ISO 27018:** Este documento establece objetivos de control, controles y directrices para implementar medidas para proteger la información de identificación personal (IIP) acuerdo con los principios de privacidad en ISO/IEC 29100 para el entorno de computación en la nube pública. Y, especifica directrices basadas en ISO/IEC 27002, para la protección de la IIP que pueden ser aplicables en el contexto de los entornos de riesgo de seguridad de la información de un proveedor de servicios de nube pública.

[44] International Organization for Standardization, "ISO 27000," *ISO,* 1 de julio del 2007, http://www.iso27000.es/download/doc_iso27000_all.pdf
[45] *Ibid.*
[46] *Ibid.*

- ➔ **ISO 27032:** Guía de Buenas Prácticas en Ciberseguridad, considerando todo el Ciberespacio: Equipamiento de red, Software, Interconexión de redes, Personas y Servicios de Internet. [47]
- ➔ **ISO 27103:** este estándar es uno de los más relevantes de la serie pues dicta una guía para aprovechar los estándares anteriormente implementados. Es decir, mientras los estándares antes mencionados explican el actuar para establecer inicialmente un marco de seguridad cibernética, este estándar corresponde a un segundo nivel de protección y administración de las TIC. Es un estándar que tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información y además se basa en un análisis de riesgo que es perfectamente adaptable a diferentes tecnologías, sectores, o etapas del ciclo.[48] Asimismo está enfocado para obtener resultados de seguridad organizados en torno a cinco funciones: identificar, proteger, detectar, responder y recuperar.

Ventajas

Este enfoque ofrece beneficios para los gobiernos y ecosistema de seguridad cibernética, porque las normas brindan un punto de partida y garantizan que de cumplir con ellas los productos ofrecen resultados inmediatos. De esta manera los gobiernos tienen la posibilidad de compartir información sobre sus productos y colaborar para mejorar el ecosistema cibernético.

Las normas internacionales también permiten a los gobiernos determinar sus necesidades, pues se elabora una evaluación exhaustiva y se implementan cambios necesarios de manera más precisa al prepararse para participar en la certificación de dichas normas. Además, el contar con certificaciones internacionales brinda un nivel de seguridad comparable a otros gobiernos que también cumplen con dichos estándares, lo que incentiva a proveedores de tecnología en el país a innovar y competir con los productos y servicios de seguridad cibernética del extranjero. Esto permite un mayor acceso a nuevas y mejores tecnologías, el gobierno debe permanecer neutral al evaluar dichas tecnologías si es que quiere optimizar sus resultados.

Retos

Las certificaciones de seguridad cibernética no garantizan que el cliente estará libre de ataques. Todos los productos o servicios pueden ser susceptibles a infiltraciones, sin embargo, es ahí donde

---

[47] *Ibid.*
[48] International Organization for Standardization, "ISO/IEC TR 27103:2018
Information technology — Security techniques — Cybersecurity and ISO and IEC Standards," *ISO*, 2018.
https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:27103:ed-1:v1:en

la resiliencia de los productos entra en juego para funcionar incluso aunque se encuentren bajo amenaza o en estrés continuo.

Por otro lado, las certificaciones de seguridad cibernética también pueden generar desafíos para la adopción de la tecnología cuando la certificación está diseñada de manera deficiente o el proceso de certificación no se ejecuta bien. Por ejemplo, uno de los problemas frecuentes es que algunas certificaciones de seguridad cibernética pudiesen ser discriminatorias por naturaleza cuando se basan en consideraciones como el país de origen. Esto puede ocasionar que determinada función no aplique al país receptor y se distorsione o limite su propósito. Adicionalmente, las certificaciones de seguridad cibernética pueden no estar a día con la complejidad tecnológica de los productos y servicios de TCI, estos contienen nuevas características y funcionalidades que son actualizadas constantemente y la certificación puede no abordarlas en su creación.

Implementación

3. Adopción de prácticas resilientes

La resiliencia cibernética es la alta capacidad de respuesta ante un ataque y contar con la capacidad para reinventar la estructura de un sistema de TI para que aun cuando ha sido vulnerado este continúe funcionando como se pretende. En otras palabras, podríamos decir que es la "capacidad para continuar operando y proporcionar los mismos resultados esperados a pesar de haber sido víctima de un ciberataque. [49]

La importancia de implementar un sistema de ciber-resiliencia recae en que no siempre es posible evitar un ataque cibernético; sin embargo, sí es posible prepararse para limitar el impacto de dicho evento. De este modo, este documento propone a cualquier organización la creación de un área que sea la responsable de desarrollar las capacidades digitales que den continuidad al negocio y que protejan el valor de los activos de información que cada organismo posee. Un sistema de alerta temprana que sea resiliente y con vasta capacidad de respuesta ante ataques cibernéticos requiere de la coordinación entre las distintas áreas de una organización y/o gobierno, donde exista un trabajo conjunto y sobre todo el compromiso de lograr un objetivo mayor, es decir, ofrecer un sistema y/o infraestructura más segura para todos los usuarios. Algunas de las mejores prácticas para lograr la ciber resiliencia organizacional son:

1. Establecer lineamientos básicos de seguridad, es decir, implementar políticas, actividades prácticas y controles que sirvan de base para el manejo y gestión de la seguridad cibernética en una organización. Estas políticas deben ser adoptadas por todos los miembros de dicho organismo y deben ser actualizadas para evitar que se vuelvan obsoletas debido a la rápida evolución de la tecnología. Para la creación de estos lineamientos es importante estudiar y conocer la estructura organizacional de la compañía o gobierno donde se implementarán los mismos, también es importante desarrollar un plan efectivo para la pronta adopción de las nuevas o mejoradas normas y políticas, tomando en cuenta las características específicas del sector.

2. Adopción del modelo de computación en la nube. La computación en la nube permite que un administrador pueda controlar y gestionar los servicios informáticos de manera remota. Esto agiliza la capacidad de respuesta ante una eventualidad y propicia el uso eficiente de los recursos de hardware y software, ya que los usuarios comparten plataformas, licencias, almacenamiento y

[49] Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham, https://doi.org/10.1007/978-3-319-16486-1_31

servicios lo que permite una alta disponibilidad y flexibilidad por parte del área que supervisa los sistemas informáticos.

3. Establecer un mecanismo para reportar y gestionar incidentes cibernéticos. Todo organismo debe establecer un mecanismo que permita que los usuarios de los sistemas de información reporten a los administradores cualquier falla o irregularidad que hayan observado en el sistema. Dicho mecanismo debe estar preparado para detectar, evaluar, analizar y responder a dicho incidente. Se debe establecer una cadena de comunicación en donde el usuario tenga la facilidad de reportar el incidente rápidamente y que dicho reporte sea dirigido específicamente al personal que pueda resolverlo inmediatamente. Dentro de las políticas de seguridad se debe incluir la cultura del reporte para hacer la labor de los primeros respondientes más sencilla y sobre todo proteger los activos eficientemente.

Es importante recalcar, que todos los organismos son diferentes y deben basar su sistema de resiliencia cibernética en un análisis de sus características individuales y de los riesgos que enfrentan específicamente sus símiles en el sector en el que se desenvuelven.

Ventajas

Al diseñar productos y servicios resilientes el Estado se encontrará preparado para enfrentar los retos y amenazas en el ciberespacio. Si se crean este tipo de productos adaptables a las condiciones que se demanden cuando los sistemas se encuentran bajo estrés, el costo de respuesta se disminuirá y el organismo que cuenta con este sistema, llámese entidad pública o privada, podrá hacer frente de manera más eficaz a los ataques recibidos.

Cuando un producto es resiliente puede reinventarse más fácilmente para actualizar sus funciones al mismo ritmo que avanza la tecnología. Esto también promueve que las empresas de tecnología estén en constante evolución para crear productos funcionales y de mejor calidad. Contar con la nube como una herramienta de resiliencia cibernética permite aumentar la capacidad de recuperación de la información perdida en un ataque y mejorar la respuesta.

Retos

Para lograr resiliencia en los productos el diseño de estos debe estar basado en un análisis de riesgos y pruebas de vulnerabilidad complejas que reten el funcionamiento de los sistemas y den mejores resultados bajo estrés. Para que esta recomendación sea exitosa debe cumplirse con las anteriores, pues los productos requeridos dependerán de los objetivos planteados en la nueva Estrategia Nacional de Seguridad Cibernética que se sugiere y su funcionamiento será mejor si al momento de su diseño se considera el cumplimiento de las normas internacionales.

Un sistema de seguridad cibernética resiliente no sólo depende del área que maneja las tecnologías de la información, debido a que la mayoría de las vulnerabilidades son en muchos

casos causadas por los propios usuarios. Por ello se debe considerar aumentar la capacitación del personal para que haga uso de un sistema resiliente, promover entrenamientos, talleres y constantes capacitaciones para así mantener los sistemas fuera de peligro y menos susceptibles a un ataque.

Otro gran reto es el de incrementar la seguridad en las operaciones que se lleven a cabo dentro de la nube a través de ciertos datos o configuraciones a los usuarios, establecer cambios periódicos de contraseñas, establecer el sistema de reporte, entre otros.

Implementación

4. Impulsar la mejora de la educación sobre seguridad cibernética en el país

El actor clave para la mejora de la seguridad cibernética en el país es el mismo ciudadano. Es él el usuario común, quien puede funcionar como facilitador para un ataque cibernético, incluso sin saberlo, al abrir un correo electrónico o visitar algún hipervínculo que contenga código malicioso.

Es importante elaborar un plan para brindar apoyo económico a instituciones que puedan ofrecer talleres, campañas, entrenamientos y conferencias que traten temas de seguridad cibernética sencillos para que el ciudadano común sepa cómo protegerse y proteger a los demás de posibles ataques cibernéticos.

Otra manera de promover la cultura de seguridad cibernética en México es incentivar la educación y entrenamiento de personal especializado para satisfacer la demanda profesional en el país, especialmente en el sector financiero. Según el reporte emitido en julio de 2019 por la Organización de Estados Americanos y la Comisión Nacional Bancaria y de Valores denominado "Estado de la Ciberseguridad en el Sistema Financiero Mexicano" las instituciones financieras hicieron hincapié en que tienen insuficiencia de personal especializado para responder a las amenazas cibernéticas en este sector.[50] En este reporte también se expuso que sólo el 57% de las entidades financieras en México cuentan con planes de preparación, respuesta y capacitación en materia de seguridad de la información y seguridad cibernética para sus empleados.[51] Sin embargo, estos talleres de concientización y entrenamiento se elaboran anualmente, siendo insuficiente este esfuerzo ante la rápida evolución de la tecnología y el ciberdelito. Al menos el 68% de las entidades e instituciones financieras en México considera necesario que el equipo de respuesta a incidentes cibernéticos crezca en el corto plazo.[52]

Ventajas

Una alianza entre el gobierno de México y la iniciativa privada puede ayudar a generar una cultura de protección y prevención del delito informático en la sociedad. Mediante talleres, conferencias y/o entrenamientos los ciudadanos pueden aprender a reconocer actividades sospechosas y de esta manera evitar ser víctimas de un ataque cibernético. Si los individuos aprenden habilidades básicas de protección cibernética, se pueden mitigar los riesgos de un ataque masivo. Los ciberdelincuentes aprovechan la falta de conocimientos informáticos de la población para explotar vulnerabilidades. Si se promueven campañas de concientización e información de delitos en el ciberespacio los efectos de los ataques cibernéticos se disminuirían.

---

[50] Organización de Estados Americanos y Comisión Nacional Bancaria y de Valores, "Estado de la Ciberseguridad en el Sistema Financiero Mexicano," *OEA y CNBV*, Julio 2019. p.31
[51] *Ibid.*
[52] *Ibid.*

Retos

Es importante que la población tenga la voluntad de aprender nuevas habilidades, pero también es imprescindible el destinar fondos públicos y privados para llevar a cabo estos esfuerzos. El presupuesto de los gobiernos para la educación es limitado en algunas poblaciones de la República Mexicana y los niños no pueden recibir educación computacional por falta de equipos o incluso educadores expertos en la materia. El gobierno Federal debe estar convencido del valor de incluir dentro del currículum obligatorio temas sobre el uso y manejo de tecnologías de la información y la seguridad en línea.

Implementación

Mejorando la conciencia sobre seguridad cibernética

- Identificar una dependencia que pueda brindar educación y ofrecer campañas de concientización
- Brindar recursos para conducir investigación que ayude a mejorar la seguridad en internet
- Incrementar el acceso a la educación computacional
- Incluir seguridad en línea en el currículum obligatorio de las escuelas
- Brindar soporte a las asociaciones publicas y privadas que promueven la seguridad cibernética
- Continuar con campañas de conciencia cibernética para la población

CONCLUSIÓN

CONCLUSIÓN

La transformación digital y el uso creciente de las TIC es inevitable. El número de ciudadanos y empresas digitales incrementa día con día, lo que ha generado beneficios en todos los sectores (público, privado y social), por ejemplo, la productividad aumenta y la vida diaria de las personas se facilita, sin embargo, esto también incrementa la exposición de datos, amenazas digitales y los delitos cibernéticos, es por eso que, como ya se mencionó, México debe de estar comprometido en alcanzar los más altos estándares de seguridad, protección de datos, cumplimiento y transparencia tanto nacionales como internacionales, con el fin de generar confianza en sus ciudadanos y empresas, teniendo presente a la confianza como premisa principal de cada proceso de transformación digital y uso de nuevas tecnologías.

Como se describió, México cuenta con instituciones, estrategias para fortalecer a la seguridad cibernética y recursos internacionales en la materia, pero a pesar de eso, aún quedan grandes opciones para seguir impulsándola. Un ejemplo sería el trabajar en la adhesión al Convenio de Ciberdelincuencia de Budapest, lo que sería un gran logro para coadyuvar internacionalmente en la lucha contra los delitos cibernéticos e informáticos.

Estando en el panorama de una sociedad interconectada, surgen las soluciones prácticas ya explicadas que son, la creación de una Estrategia Nacional de Seguridad Cibernética y una Agencia Nacional de Seguridad Cibernética, el establecimiento y cumplimiento de medidas de seguridad cibernética apegadas a estándares internacionales, la adopción de prácticas resilientes y el impulso una cultura de seguridad cibernética en la sociedad, que se proponen junto con su implementación, son solo algunas de las ideas que funcionarían como una guía para impulsar, fortalecer y mejorar tanto nacional como internacionalmente en los índices de ciberseguridad.

Es de suma importancia la creación de una Estrategia Nacional de Seguridad Cibernética y que para su implementación se determine la creación de una Agencia. Al crear esta Estrategia, se debe tomar en cuenta que nos encontramos en una constante transformación digital, que los ciudadanos digitales cada vez son más y que será necesario el establecimiento y cumplimiento de medidas de seguridad cibernética apegadas a estándares internacionales como ISO 27000 ya que esto traería beneficios al país, garantizando la eficacia de los productos y servicios que desemboquen de estos esfuerzos en mantener la seguridad cibernética de todos.

Es importante recalcar que el diseño y creación de productos tecnológicos resilientes son la clave para que México se encuentre preparado ante eventualidades que pongan en riesgo la funcionalidad de sus sistemas e infraestructuras críticas, porque esta capacidad de respuesta ante un ataque y la capacidad de reinventar la estructura de un sistema de tecnologías de la información, será indispensable para la actual y futura transformación digital de los países.

Debe también impulsarse la mejora de la educación y conciencia sobre seguridad cibernética en el país, pues son las personas el eslabón más débil en la cadena de los ciberataques y son quienes directamente pueden evitar la propagación de un ataque y por consecuencia disminuir el impacto que pueda generar, porque lamentablemente la mayoría de la gente no sabe cuáles son los peligros en línea y la magnitud de ellos hasta que les sucede algo inesperado y negativo, desafortunadamente hasta ese punto, es cuando suelen adoptar hábitos, prácticas resilientes y más seguras en línea, es por eso que dentro de todos los sectores (público, privado y social) existe un deber de ayudar a los individuos a entender cómo las decisiones que tomen en línea les afectan a sí mismos y al ecosistema cibernético general.

Es esencial que para cualquier gobierno cuyo fin sea el fortalecimiento de la seguridad cibernética por medio del desarrollo de políticas, modelos sostenibles de gobernanza y demás prácticas, tenga un proceso de colaboración para involucrar a los creadores de políticas y a los interesados en su aplicación y funcionamiento, porque la seguridad cibernética es una tarea de todos y el trabajo en conjunto puede ayudar a crear mejores prácticas sobre la protección y conciencia ante los constantes ataques cibernéticos que se generan todos los días y a los que todos estamos expuestos, dando como resultado un México más seguro en el mundo digital.

REFERENCIAS

REFERENCIAS

Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico (México: Secretaría de la Función Pública, 2005).

Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) Cyber Resilience – Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham, https://doi.org/10.1007/978-3-319-16486-1_31

Chávez, Gabriela. "Este es el país más afectado por el ciberataque WannaCry." *CNN Español*. 15 de mayo de 2017. https://cnnespanol.cnn.com/2017/05/15/este-es-el-pais-de-latinoamerica-mas-afectado-por-el-ciberataque-wannacry/

Código Nacional de Procedimientos Penales (México, 2016).

Código Penal Federal (México,2019).

Convenio sobre la Ciberdelincuencia (Budapest: Organización de Estados Americanos, 2001).

Dinero en Imagen. "¿Existen delincuentes cibernéticos en el robo de combustible?." *Dinero en Imagen*. 20 de enero de 2019. https://www.dineroenimagen.com/hacker/existen-delincuentes-ciberneticos-en-el-robo-de-combustible/106381

Dinero. "El apetitoso negocio del cibercrimen." *Dinero*. 2 de febrero del 2017. https://www.dinero.com/edicion-impresa/tecnologia/articulo/las-cifras-que-mueven-el-cibercrimen-a-nivel-global/241593

Expansión. "México foco de ciberdelitos en América Latina." *Expansión*. 20 de abril del 2016. https://expansion.mx/empresas/2016/04/20/mexico-foco-de-ciberdelitos-en-america-latina

Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal. (México, 2011)

Habilidades de Ciberseguridad para Telecomunicaciones y Radiodifusión, SCT (México, 2019)

Hern Alex and Solon Olivia. "Petya ransomware attack: What is it and how can it be stopped?" *The Guardian*. 28 de junio de 2017. https://www.theguardian.com/technology/2017/jun/27/petya-ransomware-cyber-attack-who-what-why-how

Hernández, Aura. "Ciberataques se sofistican; México no está a salvo." *Excélsior*. 11 de noviembre del 2017. https://www.excelsior.com.mx/hacker/2017/11/11/1200545

Instituto Federal de Telecomunicaciones. "Comportamiento de los Indicadores de los Mercados Regulados 2018." *IFT*, 2018. http://www.ift.org.mx/sites/default/files/contenidogeneral/transparencia/indicadores2018vacc.pdf

International Organization for Standardization. "ISO 27000." *ISO*. 1 de julio del 2007. http://www.iso27000.es/download/doc_iso27000_all.pdf

Kaspersky daily. "Top 5 de los ciberataques más memorables." Kaspersky Daily. 6 de noviembre del 2018. https://latam.kaspersky.com/blog/five-most-notorious-cyberattacks/13613/

Ley de la Guardia Nacional(México, 2019)

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (México, 2010).

Ley Federal de Telecomunicaciones y Radio Difusión (México, 2018). Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (México, 2017).

Meléndez, Ricardo. "El 90% de los mexicanos está preocupado por la obtención y uso de sus datos bancarios." *Qore*. 24 de junio del 2017. https://www.qore.com/noticias/56515/El-90-de-los-mexicanos-esta-preocupado-por-la-obtencion-y-uso-de-sus-datos-bancarios

Martínez, León A. "7 gráficos sobre los usuarios de internet en México en 2018." *El Economista*. 17 de mayo del 2018. https://www.eleconomista.com.mx/tecnologia/7-graficos-sobre-los-usuarios-de-internet-en-Mexico-en-2018-20180517-0077.html

National Cyber Security Index, "México," *NCSI*, 7 de abril de 2018, https://ncsi.ega.ee/country/mx/

Notimex. "México, segundo país más vulnerable a ciberataques." *Excélsior*. 27 de noviembre de 2018, https://www.excelsior.com.mx/trending/mexico-segundo-pais-mas-vulnerable-a-ciberataques/1281130

Organización de Estados Americanos y Comisión Nacional Bancaria y de Valores. "Estado de la Seguridad cibernética en el Sistema Financiero Mexicano." *OEA y CNBV*. Julio 2019.

Palazuelos, Félix. "Petya un virus más peligroso y sofisticado que WannaCry." *El País*. 29 de junio del 2017. https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html

Perlof-Giles, Alexandra. "Transnational Cyber Offenses: Overcoming Jurisidictional Challenges." *Yale Journal of International Law*, no 43 (2018): 191-226. https://digitalcommons.law.yale.edu/yjil/vol43/iss1/4 .

Reglamento general de protección de datos del Parlamento Europeo (Bruselas: Parlamento Europeo, 2016).

Sánchez, J.M. "El cibercrimen es incesante: provoca un agujero de 600.000 millones de dólares a las, empresas." *ABC Redes*. 7 de marzo del 2018. https://www.abc.es/tecnologia/redes/abci-cibercrimen-incesante-provoca-agujero-600000-millones-dolares-empresas-201803050122_noticia.html

Secretaria de la Función Pública. "Crea SFP Subcomisión de Inteligencia Artificial y Deep Learning de la CIDGE." Comunicado 063. *Gobierno de México*. 30 de abril del 2018. https://www.gob.mx/sfp/prensa/crea-sfp-subcomision-de-inteligencia-artificial-y-deep-learning-de-la-cidge


Microsoft


The
Software
Alliance
BSA