El Estado de la Ciberseguridad en México

// Estudio realizado por Metabase Q

// Better Base, Better Future

metabaseq.com

METABASE Q

Tabla de contenido

Metabase Q

En Metabase Q contamos con un equipo de profesionales que, además de administrar soluciones en ciberseguridad, fomentamos la consolidación de una comunidad consciente en ciberseguridad que incida en la agenda pública, incluyendo el desarrollo de un marco regulatorio sólido e innovador en Latinoamérica para garantizar un espacio de confianza digital.

A través de nuestra área de Vinculación Institucional buscamos promover herramientas y perspectivas que le permitan a gobiernos, corporaciones y el público general de toda Latinoamérica superar a ciberamenazas emergentes.

La construcción de un espacio digital seguro y confiable es un asunto de ética que nos concierne a todos y no es exclusivo de las autoridades.

El presente estudio proporciona información sobre: ataques sistémicos y una lista de los ataques dirigidos a instituciones públicas mexicanas más importantes; los esfuerzos del gobierno de México en materia de ciberseguridad; adhesión de México a tratados internacionales en ciberseguridad como el Convenio de Budapest y el Tratado de Ciberseguridad de la ONU; México en la agenda internacional y en comparación con otros países; incorporación de estándares de ciberseguridad mínimos; y finalmente, algunas apreciaciones finales y recomendaciones generales.

El objetivo del documento es visibilizar el estado de la ciberseguridad en México, en aras de fomentar el debate sobre la urgencia de contar con un marco regulatorio sólido e innovador, así como con una comunidad consciente de la ciberseguridad a la altura de los retos de la digitalización.

Colaboradores

Louise Ireland

Mauricio Benavides

Diana Tadeo

Liliana Jiménez

Maite Soto

Mariana Gómez

Mariana Marín

Monserrat Peña

El Estado de la Ciberseguridad en México

Los efectos de la pandemia han favorecido el aumento de riesgos en las tecnologías de la Información y Comunicación (TICs) debido al incremento en su uso; el cual no siempre se hace de manera responsable. Así, para las compañías, instituciones y para las personas la información se han convertido en un activo fundamental. Por citar un ejemplo, el censo 2020[1] del Instituto Nacional de Estadística y Geografía (INEGI) indica que 70% de la población mexicana tiene acceso a Internet y que 94.7% se conecta a través su teléfono móvil, por lo que el cibercrimen se ha convertido en un riesgo considerable.

La mayoría de las personas han sido víctimas de un ciberdelito, el cual tiene un costo en la economía global de $11.4 millones de dólares por minuto (RiskIQ, 2020).[2] El Banco Interamericano de Desarrollo (BID) ha estimado que, a nivel agregado, los daños económicos de los ataques cibernéticos podrían sobrepasar 1% del Producto Interno Bruto (PIB) en algunos países y la cifra de ataques a la infraestructura crítica podría alcanzar hasta 6% del PIB.[3]Las compañías se están viendo forzadas a adaptarse, con gran velocidad, a un nuevo tipo de mercado. Como ejemplo, destaca el crecimiento del comercio electrónico en el país; el cual, según un estudio de la consultora Kantar aumentó más de 500% contra 2019 y en 2020, una muestra de esto es que 10 millones de personas hicieron por primera vez una compra en línea.[4]

Asimismo, de acuerdo con el Índice de Ciberseguridad Global (ICG)[11] de la Unión Internacional de Telecomunicaciones (UIT) en su última edición en 2018, México ocupa el lugar 63 de 175 países que son analizados en materia de preparación de seguridad cibernética. Entre 2017 y 2018, México pasó del lugar 28 al 63 en la lista de países que integran este índice. Dicho índice destaca a México en materia legal y técnica, específicamente en la protección de activos digitales —considerando la Ley Federal de Protección de Datos Personales— y, los esfuerzos del Congreso de la Unión para desarrollar e implementar mayores regulaciones.

Estos números muestran claramente que el mercado está cambiando a un paso vertiginoso hacia la economía digital con los riesgos que esto conlleva en materia de ciberseguridad.

Según datos de la Asociación de Certificadores de Fraude (ACFE, por sus siglas en inglés), se estima que a lo largo del 2021 incrementaron los fraudes a nivel mundial. En especial, se espera que el ciberfraude en todas sus formas continúe creciendo.[5] Desde esta perspectiva no es aventurado decir que la carrera armamentista por la ciberseguridad es más importante que

nunca, y solo fue acelerada como consecuencia de la migración hacia el mundo digital que provocó la pandemia.

También se debe considerar que uno de los principales problemas del país radica en la falta de cultura y concientización de las personas usuarias mexicanas en materia de ciberseguridad. La Corporación Universitaria para el Desarrollo del Internet (2020) señala que el abordaje de la educación 4.0 en ciberseguridad se debe hacer desde una línea transversal. De acuerdo con la responsable del Comité de Ciberseguridad de la Red LaTe, la Dra. Gina Gallegos-García, la educación básica y media superior no contempla temas relacionados con la seguridad de la información. Así como se enseña sobre prevención de sismos, también se debería educar sobre el uso responsable de las tecnologías de información.

Imagen: Uno de los principales problemas del país radica en la falta de cultura y concientización en materia de ciberseguridad.

Amenazas a la interconexión digital

El Internet de las Cosas (IoT, por sus siglas en inglés) es un concepto que se refiere a una interconexión digital de objetos cotidianos con Internet, así como a la interacción entre productos de consumo, bienes y servicios y objetos cotidianos. Si bien estos nuevos canales de comunicación son una realidad intensificándose día a día, también los riesgos cibernéticos han evolucionado.

Un solo punto vulnerable puede ser todo lo que el cibercrimen necesita para perjudicar la seguridad nacional de un país entero. Este punto vulnerable puede ser desde un aire acondicionado, hasta el termómetro de una pecera.

Ninguna compañía, institución o persona que use Internet es inmune a los ataques cibernéticos. De acuerdo con el reporte de riesgos por COVID-19 del Foro Económico Mundial (2021), los ataques cibernéticos y fraudes, debido a la adopción de nuevos patrones de trabajo en línea, son la tercera preocupación para las empresas en este 2021.[6]

La situación en América Latina y el Caribe es particularmente inquietante, ya que actualmente es una de las regiones con mayor expansión en el uso de las Tecnologías de la Información y Comunicación (TICs).[7] En 2020, a partir del inicio de la pandemia, las detecciones de ataques de ingeniería social se duplicaron en la región. Además, México ocupa el tercer lugar regional con 16.94% de los ciberataques en América Latina [8] ataques cibernéticos que han aumentado en un 11% en los primeros ocho meses del 2021 con respecto al año anterior, según Kaspersky.

Lo que hace a México un blanco para los ataques cibernéticos es:

- Falta de un marco regulatorio sólido e innovador.
- Falta de programas en ciberseguridad efectivos (defensa y resiliencia cibernética).
- Baja cultura de concientización sobre la importancia de la ciberseguridad.

México representa un mercado enorme con gran potencial de ganancias económicas para cibercriminales. Algunos ejemplos de los ataques más recientes a instituciones públicas en México:

1. Condusef, SAT y Banxico (ataque coordinado) sufrieron en julio de 2020 afectaciones en sus páginas de internet. La técnica de *hacking* utilizada fue *defacement*, en la cual se modifica la apariencia de los portales electrónicos. Este ataque duró una semana.
2. Secretaría de la Función Pública (incidente de seguridad) expuso en julio de 2020 la información sobre declaraciones patrimoniales de 830,000 funcionarios públicos.
3. Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE). (incidente de seguridad) se expuso en agosto de 2020 en internet durante un lapso indeterminado de tiempo la información de 551 asegurados del ISSSTE sin protección.
4. Comisión Nacional de Seguros y Finanzas (ataque anunciado) en diciembre 2020 a través de un *ransomware* Lockbit se secuestró información de los equipos de la institución y se amenazó con hacerla pública.
5. Secretaría de Economía (amenaza de ataque cibernético) en febrero 2020 afectaciones en algunos servidores de la Secretaría. Los servicios impactados fueron principalmente los de correo electrónico y servidores de archivos.
6. Petróleos Mexicanos (ciberataque dirigido) en noviembre de 2019 sufrió un ciberataque a determinadas aplicaciones de *software* informático. En el último año este caso se ha estado comentando nuevamente debido al ataque al oleoducto perteneciente a Colonial Pipeline en Estados Unidos, por las repercusiones de estos a la infraestructura crítica energética.
7. Lotería Nacional (ataque de *ransomware*). Es el ataque más reciente a una institución pública, por medio del cual, en junio de 2021, se encriptó información crítica, financiera, interna y de empleados. Como rescate se pidió casi un millón de pesos a cambio de las claves para descifrar esta información y que no se publicara.

Por otro lado, un ataque sistémico es aquel que simultáneamente afecta a compañías alrededor de diferentes industrias y que pueden derivar en otras consecuencias. Dos ejemplos de este tipo de ciberataques y que representan los dos más devastadores en la historia por costo y afectación de dispositivos respectivamente, fueron NotPeya, este ataque cibernético tuvo un costo de más de $10 billones de dólares estadounidenses y el *ransomware* WannaCry, el cual infectó a más de 360,000 equipos en 150 países y se calcula que el costo fue de más de 4,000 millones de euros, ambos perpetrados en 2017.

En el caso de México, un ataque sistémico relevante fue la infiltración al Sistema de Pagos Electrónicos Interbancarios (SPEI) en 2018, cuando redes que se conectaban al SPEI fueron atacadas. Los bancos tuvieron pérdidas calculadas entre los 400 a 800 millones de pesos y como respuesta, el Banco de México (Banxico) creó su Departamento de Ciberseguridad ese

mismo año y a partir del 2019 comenzó a implementar el Programa de Reforzamiento de Seguridad de la Información en la prevención, contención y recuperación ante incidentes de ciberseguridad en el sistema financiero.[9]

La mayoría de la prevención cibernética que las compañías han llevado a cabo ha sido después de los ataques y de haber incurrido en daños financieros, así como en su reputación.

Esfuerzos de México en materia de ciberseguridad

De acuerdo con el monitoreo 2020 del Cybersecurity Defense Center (CDC) de Minsait[10], los mayores riesgos para México en materia de ciberseguridad son: la pérdida de datos y la filtración de información.

Existen algunos esfuerzos por parte del gobierno mexicano para contar con un marco normativo que propicie la seguridad y confianza digital, muestra de esto es la importancia otorgada a entidades como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) dada la necesidad de proteger los datos de amenazas cibernéticas, de concientizar a la población sobre las implicaciones de compartirlos con terceros, y promover el crecimiento económico inclusivo frente a revolución digital.

Imagen: En septiembre de 2021 entró en vigor la Estrategia Nacional Digital, promueve la implementación del Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre Instituciones.

En septiembre de 2021 entró en vigor la Estrategia Nacional Digital, la cual promueve la implementación del Protocolo Homologado para la Gestión de Incidentes Cibernéticos entre Instituciones, y de esta manera también busca fortalecer la coordinación entre autoridades para mejorar la prevención de incidencias cibernéticas. Además, en la misma fecha se publicó el acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

Estrategia Nacional de Ciberseguridad

Tomando conciencia del aumento de riesgos y amenazas en el ciberespacio, el gobierno en México lanzó en 2017 la Estrategia Nacional de Ciberseguridad (ENC), la cual precisa los objetivos, ejes transversales y actores involucrados para definir las acciones encaminadas al uso, aprovechamiento y seguridad de las TIC.

En los años 2017 y 2018 se realizaron diversas acciones multidisciplinarias encaminadas a la implementación de la Estrategia (mesas de trabajo, foros, creación de entidades a cargo) y, como ya se mencionó, recientemente fue publicado en el Diario Oficial de la Federación la Estrategia Digital Nacional 2021-2024 (EDN) la cual tiene como propósito orientar el uso y el desarrollo de las TIC al bienestar social y lograr independencia tecnológica, así como evitar monopolios. Mientras que sus objetivos particulares son establecer la política digital de la APF y la política social digital del país.

Pese a lo anterior, sigue siendo necesario que se revise y adecué la END para que se articulen las acciones que en materia de ciberseguridad son necesarias para la transformación digital del país. Es por eso qué la ENC debe salir del papel e implementarse a través de una real política de Estado.

México en comparación con otros países

La ciberseguridad es un asunto que compete a todas y todos tanto en el ámbito local como en el global. Es por ello por lo que, la cooperación internacional y el intercambio de mejores prácticas en la materia es clave para el fortalecimiento de las capacidades nacionales.

Es alarmante el rezago que tiene México en cuanto a regulación sobre ciberseguridad, no solo respecto al resto de los países sino respecto a los desafíos en la materia. Según el Reporte de Ciberseguridad 2020 del BID, un tercio de los países en América Latina no cuenta con un marco legal sobre delitos informáticos y México es parte de ellos.

Sin embargo, contar con legislación no es suficiente, se recomienda observar la infraestructura institucional necesaria para implementar dicha legislación. Podemos ver el caso de la Oficina de Administración y Oficina de Gobierno Electrónico (EE. UU), el Centro Nacional de Respuesta a Incidentes de Seguridad Informática (Uruguay), Consejo de Ciberseguridad público-privado (Dinamarca) estas son entidades específicas cuyo objetivo es la adopción de medidas de seguridad cibernética que garanticen y promuevan el uso seguro y confiable de las TIC.

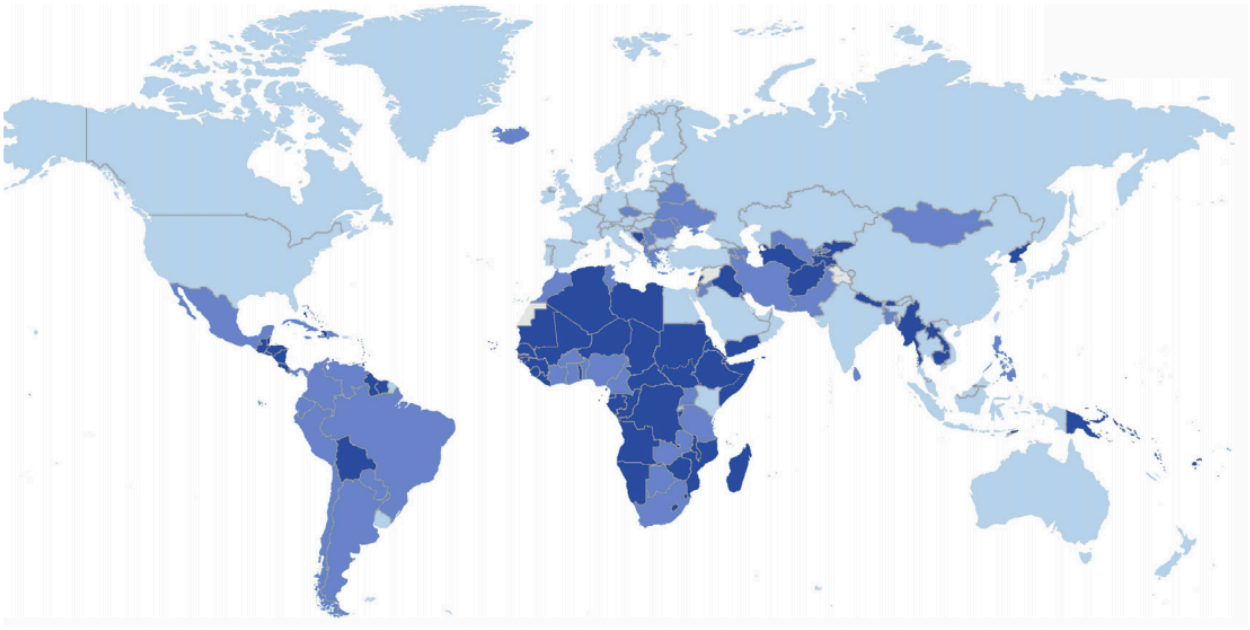

Imagen: Mapa de calor del Global Cybersecurity Index 2018, pg. 15. México se encuentra en el nivel medio de compromiso en materia de ciberseguridad.

Asimismo, poner atención a mejores prácticas internacionales y fomentar el intercambio de información, conocimientos y experiencias nos permitirá no solo contar con un marco regulatorio sólido e innovador, sino que podremos contribuir para tener un espacio digital seguro y confiable a nivel global. Por ejemplo, las recomendaciones de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) que pueden apoyar al diseño de políticas públicas. Esto es visible en el informe Perspectivas Económicas de América Latina 2020: Transformación Digital para una Mejor Reconstrucción (2020), en el que se analiza cómo la transformación digital puede ayudar a hacer frente a la situación socioeconómica actual, impulsar la productividad, fortalecer las instituciones y lograr niveles más altos de inclusión y bienestar.

Otro ejemplo es la recomendación que la Organización de los Estados Americanos dio a México para el Desarrollo de la Estrategia Nacional de Ciberseguridad. Entre las recomendaciones destacan que la Estrategia debería establecer un marco institucional que garantice que las responsabilidades y las modalidades de implementación sean claras y que las instituciones tengan la autoridad y los recursos para actuar, la estrategia debe contar con el apoyo al más alto nivel del gobierno y que la Estrategia debe abarcar la aplicación de la legislación federal y estatal en materia de delincuencia cibernética.

Asimismo, el reporte Ciberseguridad “2020: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe de la OEA y el BID”, expone que México es de los 10 países en América Latina que han presentado su primer avance en materia de ciberseguridad, y se encuentran dentro de los únicos cinco países en un nivel establecido con base en los requisitos mínimos de la Agenda Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones (UIT).

Imagen: Indicadores de Política y Estrategia de Seguridad Cibernética de México de acuerdo a la Organización de Estados Americanos y el Banco Interamericano de Desarrollo en su documento Ciberseguridad: Riesgos, Avances y el Camino a seguir en América Latina y el Caribe.

Compromisos internacionales en ciberseguridad

// Convenio de Budapest 2001

El Convenio de Budapest, del Consejo de Europa, es considerado el tratado internacional más avanzado en cuanto a los países que se han adherido y con objetivos en materia de ciberseguridad. Su principal objetivo es perseguir una política criminal común enfocada en proteger a la sociedad contra el cibercrimen. De esta manera, se ofrece un marco internacional integral, considerado referente global, para la armonización de los esfuerzos de los Estados y para fomentar la cooperación internacional. El Convenio ha sido adoptado por 65 países. Entre los países no miembros del Consejo de Europa, pertenecientes a nuestro continente se encuentran: Argentina, Canadá, Chile, Colombia, Costa Rica, República Dominicana, Panamá, Paraguay, Perú y los Estados Unidos.

México no es parte del convenio y existe un debate polarizado sobre las ventajas y desventajas de adhesión, dentro de las ventajas está la cooperación internacional, toda vez que el ciberdelito trasciende fronteras. Existen diversos promotores para que México se adhiera al Convenio, como por ejemplo los exhortos presentados al congreso el 29 de octubre de 2019, el 10 de septiembre de 2019 e incluso este mes de septiembre en el que el Senado exhortó al gobierno federal a concluir la etapa de evaluación y que considerara la adhesión.

Además de lo anterior, el pasado mes de marzo, la Comisión de Relaciones Exteriores de la Cámara de Diputados aprobó un dictamen para exhortar al Ejecutivo Federal que suscriba a acuerdos internacionales en materia de ciberseguridad y para solicitar al Canciller que impulse un convenio latinoamericano de ciberseguridad ante la Organización de Estados Americanos (OEA), infraestructura institucional necesaria para implementar adecuadamente las estrategias en materia de ciberseguridad.

En la oposición se menciona que no solo es cuestión de firmar, sino que también el país debe ser capaz de cumplir con los compromisos que conlleva, además se expresa preocupación por la incompatibilidad entre los principios del derecho penal mexicano y el Convenio, como la imprecisión en la definición de algunos delitos.

Otro aspecto que considerar es que el grupo que se conforma a través del Convenio da paso a una integración a través de dos posibilidades: por un lado, la tipificación de actos de cibercriminalidad y de renovación del marco jurídico que permitiría que México (y otros países suscritos) renueven la definición de aquellos delitos existentes que se han transformado con el uso de tecnologías. Mientras que, por otro lado, se trata de una colaboración transnacional que habilita la estandarización en métodos de investigación y respuesta ante la cibercriminalidad.

// Agenda de ciberseguridad de la ONU 2019

En 2013 la Asamblea General de Naciones Unidas a través del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional llegó a un acuerdo en torno a la aplicabilidad al ciberespacio del Derecho Internacional, como lo es la Carta de las Naciones Unidas, los Derechos Humanos y las reglas básicas sobre responsabilidad internacional.

En diciembre de 2019, se aprobó una resolución impulsada por Rusia para establecer un comité de expertos para considerar un nuevo tratado internacional en ciberseguridad. El 26 de mayo de 2021, la Asamblea General de Naciones Unidas aprobó por unanimidad la resolución titulada "Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos", la cual establece los términos para la negociación del Tratado sobre delitos cibernéticos. El principal objetivo es contrarrestar el uso de las tecnologías de la información y comunicación con fines delictivos. Además, en la resolución 73/187, la Asamblea General solicitó al secretario general que recabara las opiniones de los Estados Miembros sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, México no envió respuesta a esta invitación.

El Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos deberá presentar un borrador de la convención sobre la lucha contra el ciberdelito a la Asamblea General en su septuagésima octava sesión en 2023.A partir de la pandemia por COVID-19, el Secretario General de la ONU António Guterres, ha propuesto superar la brecha digital como una de las 10 prioridades para el 2021 en el mundo. Entre los objetivos para alcanzar esto están reforzar la ciberseguridad y promover un comportamiento responsable en esta esfera, en la protección y manejo de datos, así como poner fin a los ciberataques a la infraestructura vital.

Cuestiones pendientes y oportunidades futuras

Si bien lo que se ha planteado en secciones anteriores implica un esfuerzo para avanzar en tema de legislación en ciberseguridad lo cierto es que hasta este momento no dejan de ser propuestas que no han logrado que se consolide una estrategia ya sea para posicionar a México en el escenario internacional, para la implementación de ENC de 2017, y contar con un marco normativo que dote de una infraestructura institucional capaz de estar a la altura de los desafíos globales en materia de ciberseguridad.

Por lo anterior, emitir lineamientos para el uso y aprovechamiento de las tecnologías, así como el manejo de los riesgos y vulnerabilidades presenta una oportunidad para fomentar una cultura de ciberseguridad entre usuarios y autoridades. En este sentido, otra oportunidad es que, tanto en el Congreso como en órganos autónomos como el INAI, encargado de la protección de datos personas, han estado abriendo espacios, los cuales incluyen diálogos con la Guardia Nacional, quien hasta ahora lleva a cabo distintas operaciones contra delitos cibernéticos.

Por último, es necesaria la vinculación y coordinación entre los distintos actores que inciden en el desarrollo de la agenda pública para asegurar la confianza digital. Una gran ventaja es el reconocimiento latente a que la ciberseguridad es un aspecto clave para el desarrollo de la economía y su salvaguarda es esencial para el óptimo aprovechamiento de las TICs, para ello será también necesario crear los mecanismos que permitan la participación de los distintos sectores.

Compromisos internacionales de México en materia de Ciberseguridad

Hacemos hincapié en la necesidad de impulsar el cumplimiento de compromisos internacionales existentes para favorecer avances en la creación del fortalecimiento en el marco regulatorio pendiente. En los acuerdos de comercio internacional suscritos por México se encuentran disposiciones que, aunque tienen un espíritu de cooperación, ya destacan la importancia de abordar el tema de la ciberseguridad. Tal es el caso del Tratado México, Estados Unidos y Canadá (T-MEC), Tratado Integral Progresista de Asociación Transpacífico (CP TPP, por sus siglas en inglés) y la Alianza del Pacífico.

En ellos se reconocen las afectaciones que pueden tener las ciberamenazas en el crecimiento del comercio electrónico, por lo que es de gran importancia la creación de marcos que promuevan la confianza en el espacio digital. Para ello, el T-MEC, incluye un artículo sobre Cooperación en comercio digital y uno en ciberseguridad, donde, establece que las partes procurarán el desarrollo de capacidades para dar respuesta a incidentes de ciberseguridad, así como el fortalecimiento de mecanismos de colaboración para la identificación y mitigación de ciberamenazas y el intercambio de información entre las partes. Asimismo, promueve el intercambio de información y compartir experiencias sobre regulaciones en relación de comercio digital así como el desarrollo de mecanismos para ayudar a los usuarios a presentar denuncias transfronterizas en relación con la protección de la información personal.

Por otro lado, el CP TPP tiene disposiciones similares respecto a la cooperación, en asuntos de ciberseguridad estipula que se procurará utilizar 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 de las Partes.

En la Alianza del Pacífico se pacta el compromiso de compartir información y experiencias sobre regulación relacionada con protección de la información personal, protección del consumidor, seguridad en las comunicaciones electrónicas, autenticación, derechos de propiedad intelectual, y gobierno electrónico.

Incorporación de estándares de ciberseguridad mínimos

Los riesgos de ciberseguridad afectan a las empresas en general haciendo factible que se produzcan amenazas a todo el sistema, por mencionar un ejemplo el impacto de Notpeya en Ucrania, donde a través de una descarga de *software* comprometido con *malware* atacando varios sistemas informáticos desencadenando afectaciones en diversas compañías de manera económica y en la interrupción de sus operaciones.

En el escenario internacional tenemos el caso de Estonia, quien cuenta con una regulación en materia de ciberseguridad que incluye como objetivos principales fortalecerse como una sociedad digital que se apoya en una fuerte resiliencia tecnológica y la conformación de una industria en materia de ciberseguridad, industria, investigación y desarrollo de proyectos, para lo cual la prevención y la legislación es crucial en el desarrollo de estrategias eficaces.

La ciberseguridad es parte de la administración de riesgo general de cualquier compañía. Requiere un entendimiento claro de los factores de negocios de una organización y de sus consideraciones de seguridad.

La nueva regulación en ciberseguridad debe incluir un Estándar Mínimo de Ciberseguridad (EMC); las bases para ello pueden ser traídas del Centro de Seguridad en Internet (CIS, por sus siglas en inglés). Los controles son un conjunto de mejores prácticas basados en ataques reales y sus defensas efectivas por lo que mitigan el riesgo de los ataques más comunes. En México se reconoce a CIS por sus guías de configuración de línea base (*baseline* o *hardening*) para Sistemas Operativos, Bases de Datos, y Servidores Web, como un punto de partida para definir configuraciones.

El CIS propone 20 controles, divididos como sigue:

- Controles 1-6. Controles Base de “Higiene Cibernética”, básicos o elementales, esta categoría se enfoca en Gestión de Activos, de Vulnerabilidades -Debilidades-, Configuraciones seguras, alias: bastionado, *hardening* y/o *technical compliance*, en estaciones de trabajo, infraestructura de servidores, y la trazabilidad en el uso de sistemas.

- Controles 7-16. Controles Fundamentales, esta categoría se enfoca en la protección de sistemas y servicios de amenazas, la gestión de control de acceso a red, sistemas y

aplicaciones, y configuraciones seguras (alias: bastionado, *hardening* y/o *technical compliance*) en la infraestructura de red.

- Controles 17-20, Controles Organizacionales, enfocada en personas y procesos, esta categoría se enfoca en la concientización del personal, desarrollo seguro, la respuesta a incidentes y la validación de efectividad de los controles.

Propuesta de estándares de ciberseguridad mínimos

El marco del Centro de Seguridad de Internet permite cambios a planes de ciberseguridad, pero también puede adaptarse a cambios tecnológicos. Cada organización puede variar en las preocupaciones específicas de su industria y prioridades de datos. Es necesario desarrollar una metodología para clasificar una organización, de acuerdo con qué tan vulnerable es la organización y los daños que pueden ser causados por ataques cibernéticos. Las categorías son: 1) Sin riesgo; 2) Riesgo bajo a moderado; 3) Riesgo moderado a alto; y 4) Riesgo extremo.

De acuerdo con la categoría de riesgo a la que pertenezcan las organizaciones, el marco CIS establece que deben cumplir con los siguientes Estándares Mínimos:

// Propuesta de estándares de ciberseguridad mínimos

Tipo de acciones dependiendo del riesgo	EMC (CIS Controles sujetos a cumplimiento)
Sin riesgo	NA
Riesgo bajo a moderado	1-6
Riesgo moderado a alto	1-16
Riesgo extremo	1-20

Una vez que los Estándares Mínimos de Ciberseguridad han sido implementados, las organizaciones deben hacer pruebas o evaluaciones periódicas de vulnerabilidades para asegurar que están en cumplimiento con dichos estándares. Es importante mencionar que, el modelo y los procesos de análisis de riesgos deben actualizarse y ejecutarse periódicamente para tener visibilidad de aquellos activos que presenten una mayor exposición a la materialización del riesgo, en función del impacto que produce al negocio.

Estímulos fiscales para incentivar la inversión en ciberseguridad

Las nuevas regulaciones deben incluir estímulos fiscales (al menos temporales), con reducciones fiscales a las inversiones en ciberseguridad. En este sentido, a pesar de que otorgar estímulos fiscales es un paso necesario para fomentar la ciberseguridad, el estudio Global Cybersecurity Index 2020 realizado por la Unión internacional de Telecomunicaciones muestra que 124 países no tienen ninguna iniciativa fiscal con relación a la ciberseguridad.

En el caso de México, los estímulos fiscales para incentivar la inversión en ciberseguridad han sido abordados. En las mesas temáticas organizadas por la Subsecretaría de Comunicaciones de la Secretaría de Comunicaciones y Transportes, llevadas a cabo del 13 al 31 de mayo de 2019 para hablar de las Habilidades en Ciberseguridad para Telecomunicaciones y Radiodifusión, se concluyó que para desarrollar habilidades en ciberseguridad se sugiere otorgar estímulos fiscales a las MiPyME para tomar cursos de ciberseguridad. Sin embargo, estas conclusiones no reflejan necesariamente la posición oficial de la Secretaría y en el marco normativo mexicano no están materializadas.

Por otro lado, México cuenta con un Estímulo Fiscal a la Investigación y Desarrollo de Tecnología, a pesar de que no hace una mención específica a la ciberseguridad, busca incentivar la inversión de las empresas en actividades y proyectos relacionados con la investigación, el desarrollo tecnológico y la innovación. Este crédito equivale al 30% de los gastos e inversiones realizados en Investigación y desarrollo de tecnología, por los contribuyentes del impuesto sobre la renta (ISR) en el ejercicio fiscal, contra el ISR causado en el ejercicio por el contribuyente.

Diferente es el caso de otros países, por ejemplo, Estados Unidos, donde la administración del presidente Biden implementó créditos fiscales en 2021 para ayudar a financiar las tecnologías cibernéticas para la red eléctrica. El crédito recompensará la construcción de al menos 20 gigavatios de líneas eléctricas con capacidad de alto voltaje que fomentarán capacidades de ciberseguridad más sólidas.

Recomendaciones

1. Fomentar la consolidación de una comunidad consciente

La prevención y concientización en materia de ciberseguridad es una tarea transversal que requiere de la cooperación del sector público, privado, academia, sociedad civil y otros actores para impulsar la consolidación de una comunidad consciente en ciberseguridad. Es necesario promover espacios para visibilizar acciones que lleven la cultura de la ciberseguridad a cada rincón, debido a la rápida digitalización de procesos y al avance tecnológico en el que nos encontramos.

Debemos tener en cuenta que es una tarea de todos los actores que se promuevan espacios para hablar de ciberseguridad, visibilizar las acciones realizadas y así seguir trabajando en la construcción de un espacio digital seguro y confiable.

2. Fortalecimiento Institucional

El sector público y privado deben reconocer la necesidad de contar con marcos normativos sólidos e innovadores que puedan hacer frente a las amenazas en el ciberespacio enfocadas en la prevención y atención de los delitos que se cometan a través y en contra de las TICs. Por lo cual, si bien en un primer momento pareciera que una agencia única dedicada al manejo de la ciberseguridad a nivel nacional podría ayudar a establecer el establecimiento del as mejores prácticas de ciberseguridad, lo cierto es que el involucramiento de los actores y de los diferentes órdenes de gobierno debe hacerse de manera transversal en el que se dote de adecuadas competencias a las instituciones para que así se implementen las medidas que contribuyan a tener un espacio digital seguro y confiable.

Actualmente hay diversas instituciones que intervienen en ciberdelitos como es el caso de la policía cibernética de Ciudad de México, el Centro Nacional de Inteligencia o la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico. Esta compleja estructura crea confusión y muchas veces problemas de competencia alrededor de las diferentes autoridades.

3. Capacitación y Formación Académica

Fomentar la formación y desarrollo de talento en materia de ciberseguridad en México debe ser prioritario. La educación y concientización en seguridad digital son necesarias para que la población conozca por un lado los fundamentos básicos de la seguridad en el espacio digital, así como los beneficios y riesgos que conlleva el uso de la tecnología y el ciberespacio. Es necesario tener mecanismos para crear, impulsar y fomentar la alfabetización digital de los

usuarios donde participen expertos de la academia, la industria, la sociedad civil y el gobierno. Existen en la actualidad proyectos que se enfocan en la formación y capacitación para estudiantes para que estos desarrollen habilidades profesionales en materia de ciberseguridad. Por lo que, se recomienda se socialicen estas iniciativas con la intención de que lleguen a cada vez más personas.

Apreciaciones Finales

A grandes rasgos podemos identificar que nadie está inmune a sufrir riesgos cibernéticos, sin embargo, podemos enfocarnos en tomar las medidas preventivas necesarias para reducir vulnerabilidades.

La ciberseguridad debe verse como una prioridad en la agenda pública, debemos reconocer que los esfuerzos en México no son suficientes, es urgente reducir el rezago que tenemos en la materia, es importante desarrollar una infraestructura institucional que atienda el tema, pero para ello debemos contar con un marco regulatorio sólido e innovador que esté a la altura de los desafíos en el ecosistema digital.

Imagen: La Ciberseguridad es un asunto de ética que corresponde a toda la comunidad.

Es importante que las iniciativas en materia de ciberseguridad en el Congreso tomen en cuenta definiciones y conceptos acordados en la agenda internacional puesto que el tema no se reduce al contexto nacional, de igual manera se debe considerar que la ciberseguridad debe incluir a otros actores y no es un asunto exclusivo del Estado mexicano.

La ciberseguridad es un asunto de ética que corresponde a toda la comunidad. Es una tarea transversal que requiere de la cooperación del sector público y privado, la academia, la sociedad civil y organismos internacionales donde se impulse la creación de herramientas, el intercambio y la adopción de mejores prácticas para la consolidación de una comunidad consciente que ejecute la toma de decisiones sobre las responsabilidades de seguridad compartida.

Para maximizar los beneficios que nos ofrece las TICs, es fundamental que exista la estructura institucional necesaria, así como un marco regulatorio sólido para propiciar un espacio digital seguro y confiable. Como se ha mencionado anteriormente, México, ha realizado acciones encaminándose al abordaje de una adecuada legislación en materia de ciberseguridad, sin embargo, aun hay temas pendientes por plantear y algunos otros que aun no son debidamente analizados

Enfrentar los problemas y retos que implican las ciberamenazas, requiere de la implementación de los esfuerzos que aquí se han señalado, así como del compromiso de todos los actores. Sin duda el camino no será sencillo, pero debemos recordar que no hay que claudicar puesto que la ciberdelincuencia no lo hará.

Referencias

1. Instituto Nacional de Estadística y Geografía. (2020). *Estadísticas a propósito del Día Mundial del Internet* (p. 1). Recuperado el 23 de marzo de 2021 de: https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2020/eap_internet20.pdf

2. RiskIQ. (2020). *The Evil Internet Minute 2020.* Recuperado el 23 de marzo de 2021 de: https://www.riskiq.com/resources/infographic/evil-internet-minute-2020/

3. Banco Interamericano de Desarrollo (BID). (2020). *Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe, Reporte Ciberseguridad 2020* (p.10). Recuperado el 23 de marzo de 2021 de: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

4. Sánchez, S. (2020, abril 29). *México creció 500% sus ventas en línea por el confinamiento en casa: Kantar.* Forbes México, Recuperado el 23 de marzo de 2021 de: https://www.forbes.com.mx/negocios-mexico-crecio-500-sus-ventas-en-linea-por-el-confinamiento-en-casa-kantar/

5. Association of Certified Fraud Examiners (ACFE). (2020). *Fraud in the wake of COVID-19: Benchmarking Report* (pp. 4-5). Recuperado el 23 de marzo de 2021 de: https://www.acfe.com/uploadedFiles/ACFE_Website/Content/covid19/Covid-19%20Benchmarking%20Report%20December%20Edition.pdf

6. World Economic Forum (WEF). (2020). *Covid-19 Risks Outlook: A Preliminary Mapping and Its Implications* (pp. 42). Recuperado el 23 de marzo de 2021 de: http://www3.weforum.org/docs/WEF_COVID_19_Risks_Outlook_Special_Edition_Pages.pdf

7. Banco Interamericano de Desarrollo (BID). (2020). *Ciberseguridad: Riesgos, Avances y el Camino a Seguir en América Latina y el Caribe. Reporte Ciberseguridad 2020* (p. 16). Recuperado el 23 de marzo de 2021 de:

https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

8. Martínez, C. (2020). *México ocupa el tercer lugar en la región por ciberataques*. El Universal. Recuperado el 23 de marzo de 2021 de: https://www.eluniversal.com.mx/cartera/mexico-ocupa-el-tercer-sitio-en-la-region-por-ciberataques

9. Banco de México. (2019). *Estrategia de Ciberseguridad del Banco de México 2019 (p. 3).* Recuperado el 23 de marzo de 2021 de: https://www.banxico.org.mx/sistema-financiero/d/%7B1C588DE0-FC6F-5C53-E43B-2A6079957069%7D.pdf

10. CNN Expansión. (2020). *Los aspectos prioritarios en ciberseguridad para 2021.* Recuperado el 23 de marzo de 2021 de: https://expansion.mx/bespoke-ad/2020/10/27/los-aspectos-prioritarios-en-ciberseguridad-para-2021

11. Notipress. (2021). *Ciberataques a empresas en México pueden costar hasta 2 millones de dolares*. Recuperado el 10 de septiembre de 2021 de: https://notipress.mx/tecnologia/ciberataques-empresas-mexico-pueden-costar-2-millones-de-dolares-8248)

12. Unión Internacional de Telecomunicaciones. (2018) *Índice de Ciberseguridad Global 2018* (p. 58). Recuperado el 23 de marzo de 2021 de: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

13. Expansión. (2020). *Los ciberataques aumentan un 24% en América Latina.* Recuperado el 10 de septiembre de 2021 de: https://expansion.mx/tecnologia/2021/08/31/los-ciberataques-aumentan-un-24-en-america-latina

Bibliografía

1. Organización para la Cooperación y el Desarrollo Económico (OCDE). (2020). *Perspectivas Económicas de América Latina 2020 Transformación Digital para Una Mejor Reconstrucción* (pp. 25-39). Recuperado el 23 de marzo de 2021 de: http://www.oecd.org/dev/latin-american-economic-outlook-20725140.html

2. ONU Noticias. (2021, enero 28). *Acabar con el COVID-19 y luchar contra el cambio climático entre las 10 prioridades del Secretario General de la ONU para 2021*. Recuperado el 23 de marzo de 2021 de: https://news.un.org/es/story/2021/01/1487222

3. Gallegos-García, G. (2020, marzo 11). *Ciberseguridad: Una línea transversal en la Educación* [Archivo de Vídeo]. Recuperado el 23 de marzo de 2021 de: http://cudi.edu.mx/videoteca/ciberseguridad-una-l%C3%ADnea-trasversal-en-la-educación

4. Congreso de la Ciudad de México. (2021). *Buscan crear la Ley de Ciberseguridad para la Ciudad de México.* Recuperado el 23 de marzo de 2021 de: https://congresocdmx.gob.mx/comsoc-buscan-crear-ley-ciberseguridad-ciudad-mexico-1936-1.html