CUADERNO DE INVESTIGACIÓN
No. 87

MARZO 2022

Ciberseguridad, desafío para México y trabajo legislativo

Dr. Juan Pablo Aguirre Quezada

DIRECCIÓN GENERAL DE ANÁLISIS LEGISLATIVO

Ciberseguridad, desafío para México y trabajo legislativo

Autor:
Juan Pablo Aguirre Quezada

Diseño editorial: Denise Velázquez Mora

Cómo citar este documento:
Aguirre Quezada, J.P. (2022). "Ciberseguridad, desafío para México y trtabajo legislativo" *Cuaderno de investigación* No. 87, Instituto Belisario Domínguez, Senado de la República, Ciudad México, 23p.

Biblioteca digital del Instituto:
http://bibliodigital.senado.gob.mx

Ciberseguridad, desafío para México y trabajo legislativo [1]

Puntos principales

- La Asociación Mexicana de Ciberseguridad (Ameci) refiere que "el riesgo de ciberataques suscita preocupación en varios ámbitos, entre ellos: pérdida de datos, costos, daños a la organización y la reputación ante la visión de sus clientes y socios" (Ameci, 2021).

- Durante la LXIV Legislatura (2018-2021) se presentaron, tanto en el Senado de la República como en la Cámara de Diputados, 11 iniciativas. De ésas, diez están en calidad de pendientes de discusión en las comisiones de sus cámaras de origen. En tanto, una ya se encuentra en las comisiones de la Cámara revisora.

- En cuanto a la normatividad propuesta a modificar, cuatro de estas iniciativas inciden en el Código Penal Federal; cuatro implican la promulgación de una Ley nueva; tres son propuestas de reforma a la Ley de Seguridad Nacional. En tanto, dos están enfocadas a la creación de una efeméride; una es propuesta de cambio a la Constitución; una implica modificaciones a la Ley Federal de Austeridad Republicana; y finalmente, otra más a la Ley General del Sistema Nacional de Seguridad Pública.

- La ciberseguridad es una preocupación mundial debido a los alcances que pueden surgir a su fácil vinculación con otros tipos de delitos y sus impactos por la delincuencia organizada trasnacional.

- La Oficina de Lucha contra el Terrorismo (OLCT) de la ONU es la agencia encargada de coordinar el tema de ciberseguridad en el máximo organismo internacional, mediante la iniciativa 2341 de 2017.

- La Unión Internacional de Telecomunicaciones (UIT) realiza el Índice de *Ciberseguridad Global* (ICG) de forma periódica. En la última versión (2020) México se situó en lugar 52 de 182 países evaluados, con una calificación de 81.68.

- De acuerdo con esta medición, los países mejor posicionados frente a los desafíos de la ciberseguridad son: Estados Unidos de América (100); Reino Unido (99.54); Arabia Saudita (99.54); Estonia (99.48); Corea del Sur (98.52); Singapur (98.52); y España (98.52) son los que están mejor posicionados.

- En contraste, los países peor calificados para el tema de ciberseguridad a escala mundial son: Guinea Ecuatorial (1.46); Corea del Norte (1.35); Micronesia (0); el Vaticano (0); y Yemen (0).

[1]El autor agradece el apoyo de las pasantes Abigail Suárez López y María Vanessa Mondragón Martínez (DGAL) en la elaboración del presente documento.

- A escala continental, los países mejor posicionados en materia de seguridad, de acuerdo con el índice de la UIT, son: Estados Unidos (100); Canadá (97.67); Brasil (96.6); México (81.68); Uruguay (75.15); y República Dominicana (75.07).

- El Gerente de Instituciones del Banco Interamericano de Desarrollo (BID), Moisés J. Schwartz, dio a conocer que "el crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo" (BID, 2020: 10).

- 2 millones 745 mil 738 quejas de fraude cibernético se recibieron en el segundo trimestre de 2021, cifra 5% menor respecto al dato de 2021.

- Del total de fraudes cibernéticos al segundo semestre de 2021, de acuerdo con las reclamaciones iniciadas por Condusef, dos millones 534,130 fueron en comercio por internet; 119 mil 179 por banca móvil; 89 mil 324 corresponden a operaciones por Internet de personas físicas; 3 mil 076 operaciones por Internet de personas morales; y 29 pagos por celular.

Abstract

La seguridad informática -conocida también como ciberseguridad- es una de las características de las tecnologías de la información y comunicación (TIC´s) a fin de brindar protección a la información y los datos personales de las y los usuarios de internet. El presente estudio aborda diferentes desafíos de la ciberseguridad en México, el trabajo legislativo en el tema, así como experiencias internacionales de interés.

Palabras clave: ciberseguridad, digital, información, informática, protección.

Introducción

La ciberseguridad es definida, de acuerdo con Álvaro Gómez, como "cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática cuyos efectos puedan conllevar daños sobre la información, equipo o software" (IIUNAM, 2021). Asimismo, de acuerdo con la Coordinación de Seguridad en la Información de la Universidad Nacional Autónoma de México (CSI -UNAM), este concepto "requiere la participación activa de los altos directivos de las empresas y debe ser parte integral del gobierno corporativo para lograr los objetivos de las empresas" (CSI, 2018). Por tanto, brindar un entorno que permita a las y los usuarios de internet, así como a instituciones públicas y privadas un uso seguro de las tecnologías de la información y comunicación es un derecho regulado en diferentes leyes, tanto nacionales como postulados internacionales. E

ste tema es importante para afrontar diferentes delitos tales como robo de identidad, fraudes, fuga de datos personales, acoso, extorsiones, violación a la privacidad, estafas, flujos financieros ilegales, entre otros. Sin embargo, tanto gobiernos de diferentes órdenes como empresas tienen especial interés en el tema, debido a los riesgos que pueden existir tanto para la seguridad nacional, como financiera, lo que representa un deber para la aplicación de políticas públicas que busquen la protección tanto del patrimonio de la sociedad como de las actividades de la administración pública.

Por tanto, la ciberseguridad es un tema de prioridad ante las relaciones humanas que han sido apoyadas en gran medida por las herramientas Tic´s, de hecho, algunas fuentes consideran que:

> la protección de su información es generalmente más importante que la protección misma del software o su equipo, razón por la cual, para garantizar la seguridad de los datos, es preciso cumplir con tres componentes fundamentales: integridad, que significa que la información debe ser modificada solo por entidades autorizadas; disponibilidad, es decir, tener acceso a la información cuando se lo requiera; y confidencialidad, donde solo instancias facultadas para ello podrán visualizar los datos (IIUNAM, 2021).

Otra definición de ciberseguridad la brinda la American Chamber México al referir que es:

> … el conjunto de herramientas, políticas, directrices, métodos de gestión de riesgos, acciones, formaciones, prácticas idóneas, garantías y tecnologías que pueden utilizarse para proteger la disponibilidad, integridad y confidencialidad de los activos de la infraestructura conectada pertenecientes al gobierno, a las organizaciones privadas y a los ciudadanos; estos activos incluyen los dispositivos informáticos conectados, el personal, la infraestructura, las aplicaciones, los servicios, los sistemas de telecomunicaciones y los datos en el mundo cibernético (ACM, 2017: 3).

Teniendo en cuenta la importancia del cuidado de la información en medios digitales, así como las oportunidades en el uso por parte de los titulares, el presente estudio se divide en cuatro puntos principales. Al inicio se revisarán conceptos básicos, así como riesgos relativos al tema de ciberseguridad como una reflexión general del tema. Posteriormente, se reflexionará acerca de la situación de la seguridad informática en nuestro país, a fin de entender la importancia de ésta como factor de estabilidad. A continuación, se realizará un análisis del trabajo legislativo en cuanto a ciberseguridad en las iniciativas presentadas en las LXIV y la LXV legislaturas. Finalmente, se analizarán algunas experiencias internacionales para afrontar los desafíos que implica el uso seguro de las tecnologías de la información y comunicación.

1. Problemas y desafíos que afronta a ciberseguridad

De acuerdo con la Asociación Mexicana de Ciberseguridad (Ameci), "el riesgo de ciberataques suscita preocupación en varios ámbitos, entre ellos: pérdida de datos, costos, daños a la organización y la reputación ante la visión de sus clientes y socios" (Ameci, 2021). Por lo que esos hackeos muestran las vulnerabilidades de diferentes sistemas de almacenamientos de datos, al tiempo de generar diferentes tipos de ilícitos, en perjuicio de personas, dependencias públicas, empresas, universidades, asociaciones, entre otras organizaciones.

La Unión Internacional de Telecomunicaciones (UIT) refiere que:

> …64% de los países había adoptado una estrategia nacional de ciberseguridad (ENC) a finales de año, mientras que más del 70% llevó a cabo campañas de sensibilización a la ciberseguridad en 2020, en comparación con el 58% y el 66%, respectivamente, en 2018 (UIT, 2021a).

Por tanto, este tema de seguridad pública y nacional tiene mayor interés a escala mundial debido a los riesgos existentes y las afectaciones que puede ocasionar.

Dicha organización publica el *Índice de Ciberseguridad Global* (ICG) que señala:

> la ciberseguridad es realmente un problema de desarrollo y que existe una necesidad urgente de abordar la creciente brecha de cibercapacidad entre los países desarrollados y en desarrollo fomentando el conocimiento, la mejora de las habilidades y la creación de competencias. Necesitamos cerrar esta brecha yendo a las raíces y creando capacidad en términos de infraestructura digital, habilidades digitales y recursos en el mundo en desarrollo (UIT, 2021b).

De acuerdo con esta medición, los países mejor posicionados frente a los desafíos de la ciberseguridad son: Estados Unidos de América (100); Reino Unido (99.54); Arabia Saudita (99.54); Estonia (99.48); Corea del Sur (98.52); Singapur (98.52); y España (98.52) son los mejores posicionados. En contraste, los países peor calificados para el tema de ciberseguridad a escala mundial son: Guinea Ecuatorial (1.46); Corea del Norte (1.35); Micronesia (0); el Vaticano (0); y Yemen (0). A escala continental, los países mejor posicionados en materia de seguridad de acuerdo con el índice de la UIT son: Estados Unidos (100); Canadá (97.67); Brasil (96.6); México (81.68); Uruguay (75.15); y República Dominicana (75.07). Esta medición es útil para encontrar áreas de oportunidad y mejora para el tema de seguridad cibernética, y evitar riesgos para la población, la administración pública, y las empresas.

Al tiempo de que diferentes fuentes abordan el tema de ciberseguridad, también hay estrategias para la prevención de delitos informáticos. En ese sentido una entrevista realizada al ingeniero Frederick Ferro Mojica -docente de la Universidad Central de Colombia- refirió que:

> "Debemos verificar las fuentes de información antes de cualquier acción. Por ejemplo, a muchos les envían mensajes de texto pidiendo su clave o número de cuenta, o les anuncian que ganaron un premio y les piden sus datos personales aprovechándose del afán y la ingenuidad de la gente. Así logran capturar datos que permiten hacer transacciones de una forma irregular" (Ramírez, 2020).

Por lo que estas medidas de prevención dirigidas a la población son muy necesarias a fin de evitar la pérdida de sus bienes o patrimonios, al tiempo de mitigar los objetivos de la delincuencia organizada vía cibernética, lo que coadyuva a la generalización de la importancia de concientizar al público para evitar caer en este tipo de riesgos.

Por su parte, el Banco Interamericano de Desarrollo (BID) publicó un estudio denominado "Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe". En dicho documento, el Gerente de Instituciones de dicho organismo, Moisés J. Schwartz, dio a conocer que "el crimen en línea ya supone, aproximadamente, la mitad de todos los delitos contra la propiedad que tienen lugar en el mundo" (BID, 2020: 10). Lo que hace evidente la necesidad de afrontar estos riesgos mediante el uso de la tecnología y la cultura de la prevención.

En dicha investigación, también resalta que "las brechas de ciberseguridad y las filtraciones de datos se estaban convirtiendo en los principales obstáculos de la economía digital" (BID, 2020: 28). Por lo que estas actividades delictivas causan un grave daño tanto a las economías de las naciones como el patrimonio de particulares. Por tanto, los temas de la seguridad electrónica merman el crecimiento económico reflejado en variantes del Producto Interno Bruto (PIB). Algunos especialistas consideran que en países menos desarrollados el impacto ha sido mayor debido al incremento del uso de las tecnologías de la información y comunicación (TIC´s) como efecto social consecuencia de la pandemia de covid-19.

Los riesgos de la ciberseguridad no sólo traspasan fronteras, sino que se encuentra en peligro la vida de las personas; tal como sucede en la aviación de pasajeros y comercial. Al respecto, la Organización de Aviación Civil Internacional (OACI) ha emitido diferentes propuestas para reducir riesgos como hackeos o actos terroristas que se puedan generar bajo esta modalidad. Asimismo, también existen riesgos de afectación en la logística naviera de todo el mundo. De acuerdo con la Organización Marítima Internacional (OMI):

> el riesgo cibernético marítimo se refiere a la medida del nivel de amenaza de un activo tecnológico por una circunstancia o suceso posibles, que podrían causar fallos operacionales, de seguridad o protección del transporte marítimo al corromperse, perderse o ponerse en peligro información o sistemas (OMI, 2021).

Por lo que es indispensable contar con estándares de seguridad informática que permitan el desarrollo de diferentes actividades comerciales, logísticas, científicas, navales, entre otras.

A escala mundial se han experimentado casos graves de ataques cibernéticos, los cuales han ocasionado millonarias pérdidas económicas, además de afectaciones a los usuarios. Uno de estos sucesos fue el llamado correo electrónico *ilove you*, que en cuestión de horas afectó a "los cinco continentes. Se calcula que los afectados por el conocido VBS.LoveLetter fueron tres millones de ordenadores tan sólo en las primeras 24 horas. El número total se desconoce, pero aproximadamente dejó alrededor de 50 millones de víctimas informáticas" (Rojas, 2017). Si bien este acontecimiento data del año 2000, mostró vulnerabilidad, además de la baja capacidad de reacción y defensa ante la propagación de un virus informático; así como las pérdidas millonarias que podrían suceder ante una emergencia de este tipo.

Como respuesta a estos desafíos, algunos expertos señalan que una forma de contrarrestar esos efectos negativos es mediante la capacitación y profesionalización de especialistas que permitan ser contratados por empresas y gobiernos para desactivar las amenazas de la delincuencia organizada en la modalidad de ciberseguridad. Por otra parte, diferentes empresas realizan informes anuales para detectar riesgos, al tiempo de coadyuvar en la mejora de herramientas electrónicas para eliminar los aspectos vulnerables, además de crear mejoras en los programas antivirus.

Mención especial merece el tópico de los ciberataques, los cuales son definidos como:

> …un intento malicioso y deliberado por parte de un individuo o una organización para irrumpir en el sistema de información de otro individuo u otra organización. Usualmente, el atacante busca algún tipo de beneficio con la interrupción de la red de la víctima (Cisco, 2021).

Entre los diferentes tipos de ciberataques, -de acuerdo con esta fuente-, son: malware, phishing o suplantación de identidad, ataque de intermediario, inyección de SQL, tunelización de DNS, ataques de día cero y de denegación de servicios, entre otros (Cisco, 2021).

Cabe destacar que, de acuerdo con la compañía Cisco, "los ciberdelitos crecen año a año a medida que las personas intentan beneficiarse de los sistemas comerciales vulnerables. A menudo, los atacantes buscan rescates: el 53 % de los ciberataques da como resultado daños por USD 500 000 o más" (Cisco, 2021). Por lo que este tipo de agresiones son chantajes o apropiaciones indebidas a bienes de empresas o instituciones públicas, lo cual afecta gravemente su patrimonio.

Los ciberataques en diferentes partes del mundo aumentaron en frecuencia en los últimos meses, al coincidir con un mayor uso de ordenadores debido a los estragos por la pandemia de covid-19. Al respecto, la compañía Kaspersky dio a conocer que, de enero a agosto de 2020 se incrementó en 24% el número de este tipo de incidentes en América Latina. Con ello, se realizan docenas de ataques por segundo en todo el continente, al referir que "Brasil lidera la región con más de 1,390 intentos de infección por minuto, seguido de México (299 por minuto); Perú (96 por minuto), Ecuador (89 por minuto) y Colombia (87 por minuto)" (Kaspersky, 2021). Lo cual es una muestra de la magnitud del riesgo actual por esta amenaza en esta región.

El robo de datos para manipular cuentas bancarias de los usuarios, así como el uso de programas informáticos piratas son dos de los principales factores que afectan la ciberseguridad tanto de personas como empresas o la administración pública de todo el mundo. En ese sentido, Dmitry Bestuzhev, funcionario de Kaspersky, resaltó que "por utilizar programas piratas, no reciben los parches de seguridad oficiales. Como resultado, vemos que el ransomware WannaCry sigue circulando por todas las industrias, incluso después de cuatro años de haberse emitido el parche" (Kaspersky, 2021). Esta es una razón por la cual no se han podido eliminar amenazas antiguas a la ciberseguridad, y que se acumulan con los riesgos más recientes como un peligro para la infraestructura digital.

Cabe destacar que otros expertos también enfatizan en que el problema nacional de ciberseguridad es más difícil de solucionar debido a los software piratas o ilegales, los cuales no pueden recibir las actualizaciones que pueden prevenir los ataques informáticos. Por tanto:

> los piratas informáticos son conscientes de que estas herramientas se están utilizando para nuevos procesos de trabajo y transportan una gran cantidad de datos valiosos. En lugar de tratar de encontrar debilidades técnicas en las herramientas específicamente, los piratas informáticos buscarán explotar a los usuarios a través de la suplantación de identidad (Canales TI, 2021).

Por lo que también existen riesgos a la seguridad informática en las plataformas de comunicación, así como en documentos que se comparten en diferentes modalidades de las TIC's.

Es importante destacar las consecuencias de los ciberataques, que tienen dos principales afectados. Por una parte, están las organizaciones o personas que directamente son víctimas. Mientras que en un segundo escenario están los terceros involucrados, que pueden ser clientes o beneficiados de los servicios que presta la institución afectada, lo que propaga los perjuicios y puede afectar el patrimonio de personas ajenas. Del primer caso, algunas fuentes refieren que:

> sus efectos repercuten en toda la infraestructura empresarial bloqueando sus sistemas e, incluso, pudiendo paralizar su proceso de producción. El funcionamiento normal de la empresa es imposible en estos casos lo que puede generar graves repercusiones económicas (Global Technology, 2021).

En tanto, respecto a los daños a terceros, esta compañía refiere que "los datos personales que manejan las compañías, independientemente de su tamaño y actividad, son uno de los activos más valiosos para los hackers. Por eso es uno de los elementos que más peligro corren en un ciberataque" (Global Technology, 2021). Por lo que además de la inversión en programas cibernéticos que eviten este tipo de riesgos, también se requiere el cumplimiento debido a las leyes de protección de datos personales en posesión de empresas, instituciones o particulares, a fin de evitar ataques a la integridad y el patrimonio de las y los usuarios, quienes pueden denunciar penalmente a la organización por no contar con las medidas adecuadas para garantizar la seguridad digital.

2. Situación de la ciberseguridad en México.

La Secretaría de Comunicaciones y Transportes (SCT) publicó la *Guía de Ciberseguridad*, que data de junio de 2020. Cabe destacar que este documento busca apoyar las actividades que se realizan por teletrabajo, como política pública para afrontar los efectos de la pandemia del covid-19; así como identificar las amenazas que puede afectar la ciberseguridad en los hogares. La publicación advierte que la modalidad "teletrabajo improvisado, ciberataque asegurado, es importante continuar el desarrollo de instrumentos que… contribuyan a seguir avanzando en el impulso del uso seguro de las telecomunicaciones en apoyo al teletrabajo, en beneficio de todas y todos los mexicanos" (SCT. 2020: 17). Por lo que se muestra que, ante la emergencia sanitaria, se establecieron diferentes políticas públicas a fin de concientizar a la población de los riesgos existentes en materia de seguridad informática.

Por su parte, la Unión Internacional de Telecomunicaciones (UIT) realiza el Índice de Ciberseguridad Global (ICG) de forma periódica. En la última versión (2020) México se situó en lugar 52 de 182 países evaluados, con una calificación de 81.68. Por lo que, si bien se tienen avances importantes en la materia, no se brinda una seguridad cibernética total que evite a la población ser vulnerable ante los riesgos y delitos asociados.

Ejemplo de estos riesgos es la debilidad legal existente en la materia de acuerdo con diferentes fuentes especializadas. En ese sentido, el Banco Interamericano de Desarrollo (BID) refiere que:

> México no cuenta con una ley dedicada de delito cibernético, pero el artículo N° 211 del Código Penal prevé el delito informático. Sin embargo, estas disposiciones son limitadas y dejan varias lagunas, lo que dificulta la lucha contra el cibercrimen (BID, 2020: 125).

Entre los impactos ocasionados por la falta de leyes armoniosas con el tema de ciberseguridad destaca que "79% de los ataques de ciberseguridad que sucedieron el año pasado fueron a pymes; hubo más de 4,000 millones de intentos por atacarlas" (Cueto, 2021). Es decir, la falta de precauciones adecuadas en el rubro de ciberseguridad daña el desarrollo económico y la cadena productiva de gran parte de las empresas mexicanas.

De acuerdo con American Chamber México, los principales desafíos en la materia en nuestro país, así como la cantidad de usuarios afectados, son:

- Exceso de información no deseada (20.5 millones).
- Mensajes de personas desconocidas (16.4 millones).
- Infección por virus (10.6 millones).
- Fraudes con información financiera personal (3.2 millones).
- Violación a la privacidad (2.5 millones) (ACM, 2017).

Debido a las disposiciones suscritas en el Tratado entre México, Estados Unidos y Canadá (T-MEC), el tema de ciberseguridad está considerado como un elemento que daña la confianza en el comercio digital, tal como lo establece el artículo 19.15 de dicho instrumento. Lo que obliga a los países integrantes a:

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

- (b) fortalecer los mecanismos de colaboración existentes para cooperar en identificar y mitigar las intrusiones maliciosas o la diseminación de códigos maliciosos que afecten a las redes electrónicas y utilizar esos mecanismos para tratar rápidamente los incidentes de ciberseguridad (TMEC, 2020: 441).

Además de la cooperación entre las tres naciones en esta materia, el T-MEC mandata que los gobiernos nacionales deben fortalecer sus políticas públicas de prevención y respuestas a estos ataques dirigidos a las empresas, así como promover mejores prácticas a fin de minimizar los riesgos.

Pese a no existir una Ley propia en materia de ciberseguridad, el acuerdo firmado por el T-MEC, así como algunas disposiciones del Código Penal constituyen la normatividad aplicable. No obstante, en el Poder Legislativo se han realizado diferentes iniciativas a fin de crear y fortalecer las leyes que ayuden a prevenir, erradicar y aplicar sanciones a los delitos asociados a la seguridad informática.

Debido al costo de los daños ocasionados por temas de ciberseguridad, algunas compañías han incorporado en su oferta seguros de daños a las empresas, a fin de cubrir parte de los gastos ocasionados por un ataque informático. En nuestro país "las primas en materia de ciberseguridad se ofrecen únicamente a empresas, sin embargo, en el futuro, no se descarta que la industria de seguros global empiece a pensar en coberturas individuales" (Mendoza, 2021). Por lo que este tipo de productos muestran el crecimiento de riesgos que pueden existir ante las amenazas de delitos asociados a la seguridad cibernética.

Otras dependencias gubernamentales han tenido que fortalecer sus acciones en materia de ciberseguridad en los últimos meses, a fin de prevenir ataques que afecten sus funciones o causen pérdidas millonarias. En ese sentido, el Banco de México (Banxico) realizó ajustes de mejoras en rubros tales como:

1) Gobernanza, Cumplimiento y Organización.
2) Protección de Datos.

3) Gestión de Riesgos de Seguridad.
4) Gestión de Identidad y Autenticación.
5) Respuesta a Incidentes.
6) Administración de Terceros y Proveedores.
7) Protección de Equipos de Punto Final.
8) Protección de Aplicaciones y Bases de Datos.
9) Protección de Redes y Centros de Datos.
10) Capacitación y Concientización en Seguridad (Banxico, 2020: 4).

Por otra parte, algunas fuentes consideran que el robo de identidad es uno de los pendientes en materia de ciberseguridad que más afecta a las y los mexicanos. En ese sentido, dicha variante "ha dejado pérdidas anuales por 5 mil mdp y al menos 200 víctimas por mes, aunado al acoso por internet y ataques informáticos a siete instituciones gubernamentales" (Melgar, 2021). La dimensión de los riesgos asociados a la seguridad informática en México es proporcional al uso generalizado de teléfonos celulares y computadoras con conexión a internet; además de los equipos utilizados por las empresas.

El Banco de México (Banxico) y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) divulgaron diferentes estadísticas para comprender la magnitud del fraude cibernético. Al respecto, 2 millones 745,738 quejas de fraude cibernético se recibieron en el segundo trimestre de 2021, cifra 5% menor respecto al dato de 2021. Cabe destacar que "el monto reclamado de los fraudes cibernéticos ascendió a $6,532mdp; se bonificó sólo el 41% y 84 de cada 100 fraudes cibernéticos se resolvieron a favor del usuario" (Condusef, 2022). El tema de ciberseguridad ha afectado de forma patrimonial a millones de mexicanos, al tiempo de facilitar la obtención de recursos por parte de las bandas delictivas.

Del total de fraudes cibernéticos al segundo semestre de 2021, de acuerdo con las reclamaciones iniciadas por Condusef, 2 millones 534,130 fueron en comercio por internet; 119 mil 179 por banca móvil; 89 mil 324 corresponden a operaciones por Internet de personas físicas; 3 mil 076 operaciones por Internet de personas morales; y 29 pagos por celular.

El tema de la ciberseguridad también afecta diferentes derechos humanos, tales como el derecho a la vida, libertad de prensa, protección de datos personales, del patrimonio, entre otros. Al respecto, la American Chamber México señaló que "al igual que todo derecho humano, la estrategia de ciberseguridad debe regirse por los principios de universalidad, interdependencia, indivisibilidad y progresividad" (ACM, 2017: 3). Por lo que, debido a la vinculación de datos personales del derecho mexicano, y el uso de las tecnologías de la información y comunicaciones, es importante abordar este desafío de forma multidimensional a fin de proteger las garantías individuales de las personas que viven y transitan por nuestro país.

La ciberseguridad es un problema de seguridad pública en constante evolución, por lo que las personas que realizan este tipo de actividades buscarán nuevos mecanismos a fin de conseguir sus objetivos, en perjuicio del patrimonio y la seguridad de familias y empresas. En ese sentido, algunos analistas consideran que el mayor uso de las TIC´s es por una generalización de la población, así como por las reacciones de un uso masivo ante la situación social de la pandemia de covid-19, al referir que "aceleró la transformación digital y nos hizo movernos a un esquema distinto muy rápido, ¿qué generó esto? que las empresas con el fin de mantener la operación, adaptaron sus sistemas de acceso rápidamente y esto los ciberdelincuentes lo aprovecharon al máximo" (Perales, 2021). Por lo que en el futuro inmediato la ciberseguridad continuará siendo un desafío en materia de seguridad pública.

Otros expertos también consideran que estos cambios pueden generar impactos individuales, por lo que es importante que todas las personas usuarias estén alertas de posibles ataques. Al respecto, entre las opiniones expresadas destacan:

> esto es una industria y se está mutando, tratando de perjudicar más a las empresas, y el daño no solo es económico, son los daños reputacionales que genera esto, está latente y cada vez sucede más, donde afecta más a las grandes empresas (Perales, 2021).

Por lo que parte de las estrategias para prevenir los delitos asociados a la ciberseguridad es la prevención, desde lo individual hasta lo colectivo.

3. Trabajo Legislativo en el tema

Durante la LXIV Legislatura (2018-2021) se presentaron, tanto en el Senado de la República como en la Cámara de Diputados, 11 iniciativas. De éstas, diez están en calidad de pendientes de discusión en las comisiones de sus cámaras de origen. En tanto, una ya se encuentra en las comisiones de la Cámara revisora (Tabla 1).

Tabla 1. Iniciativas presentadas en la LXIV Legislatura del Congreso mexicano (2018-2021) acerca de ciberseguridad.

Iniciativa y fecha de presentación	Objetivo	Presentada por	Estatus
Iniciativa con Proyecto de Decreto por el que se adiciona la fracción XIV al Artículo 5 de la Ley de Seguridad Nacional. 4 de noviembre de 2018	La iniciativa tiene por objeto establecer medidas para hacer frente a ciberataques. Parta ello propone señalar que son amenazas a la Seguridad Nacional los actos que vulneren la ciberseguridad y que lesionen a los habitantes y a las instituciones.	Sen. José Ramón Enríquez Herrera	Pendiente en comisión(es) de cámara de origen 4 de noviembre de 2020
Iniciativa que adiciona los artículos 5° y 6° de la Ley de Seguridad Nacional. 8 de enero de 2020	La iniciativa tiene por objeto establecer mecanismos legales en materia de ciberseguridad, como parte de la Estrategia Digital Nacional.	Dip. María Eugenia Hernández Pérez	Pendiente en comisión(es) de cámara de origen 8 de enero de 2020
Iniciativa con Proyecto de Decreto que declara el 23 de noviembre de cada año como "Día Nacional de la Ciberseguridad" 12 de agosto de 2020	La iniciativa tiene por objeto declarar el 23 de noviembre de cada año, como -Día Nacional de la Ciberseguridad-.	Dip. María Eugenia Hernández Pérez	Pendiente en comisión(es) de cámara de origen 12 de agosto de 2020

La tabla 1, continúa en la siguiente página

Iniciativa y fecha de presentación	Objetivo	Presentada por	Estatus
Iniciativa con Proyecto de Decreto que declara el mes de octubre, como "El Mes Nacional de la Ciberseguridad" 23 de octubre de 2018	La iniciativa tiene por objeto declarar el mes de octubre de cada año como -El Mes Nacional de la Ciberseguridad-.	Sen. Alejandra Lagunes Soto Ruíz	Pendiente en comisión(es) de cámara revisora 5 de noviembre de 2019
Iniciativa con Proyecto de Decreto por el que se expide la Ley General de Ciberseguridad y se derogan diversas disposiciones del Código Penal Federal. 6 de abril de 2020	La iniciativa tiene por objeto regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad.	Sen. Jesús Lucía Trasviña Waldenrath	Pendiente en comisión(es) de cámara de origen 6 de abril de 2021
Iniciativa con Proyecto de Decreto por el que se expide la Ley que crea la Universidad de Tecnologías de la Información, Comunicaciones e Innovación. 12 de agosto de 2020	La iniciativa tiene por objeto crear el marco regulatorio para la Universidad encargada de impartir educación superior a nivel licenciatura, especialidad, maestría, doctorado y opciones terminales, en materia de desarrollo tecnológico e innovación en el país, como organismo público con personalidad jurídica, patrimonio propio, autonomía técnica y de gestión, como institución de educación pública del Estado Mexicano	Dip. Carlos Iván Ayala Bobadilla	Pendiente en comisión(es) de cámara de origen 12 de agosto de 2020
Iniciativa que reforma el artículo 16 de la Ley Federal de Austeridad Republicana. 2 de marzo de 2021	La iniciativa tiene por objeto establecer austeridad en la adquisición y arrendamiento de equipo y servicios de cómputo que se usan para garantizar la operación de programas sociales y labores de ciberseguridad.	Dip. José Salvador Rosas Quintanilla	Pendiente en comisión(es) de cámara de origen 2 de marzo de 2021
Iniciativa que reforma el Artículo 73 de la Constitución Política De Los Estados Unidos Mexicanos. 29 de octubre de 2019	La iniciativa tiene por objeto facultar al Congreso de la Unión para legislar en materia de ciberseguridad.	Dip. Javier Salinas Narváez	Pendiente en comisión(es) de cámara de origen 29 de octubre de 2019

La tabla 1, continúa en la siguiente página

Iniciativa y fecha de presentación	Objetivo	Presentada por	Estatus
Iniciativa con aval del grupo parlamentario que contiene Proyecto de Decreto que reforma y adiciona diversas disposiciones del Código Penal Federal, de la Ley General del Sistema Nacional de Seguridad Pública, de la Ley de Seguridad Nacional; y, expide la Ley General de Ciberseguridad. 2 de septiembre de 2019	La iniciativa tiene por objeto establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la ciberseguridad en las instituciones del Estado y la sociedad.	Sen. Miguel Ángel Mancera Espinosa	Pendiente en comisión(es) de cámara de origen 2 de septiembre de 2019
Iniciativa con Proyecto de Decreto por el que se reforman y adicionan diversas disposiciones del Código Penal Federal, en materia de delitos cibernéticos. 25 de marzo de 2021	La iniciativa tiene por objeto prevenir y sancionar los delitos cibernéticos.	Sen. Gustavo Enrique Madero Muñoz	Pendiente en comisión(es) de cámara de origen el 25-mar-2021
Iniciativa con Proyecto de Decreto por el que se reforman y derogan diversas disposiciones del Título Noveno, Libro Segundo del Código Penal Federal y se expide la Ley de Seguridad Informática. 27 de marzo de 2019	Propone reformar y derogar diversas disposiciones del Código Penal Federal relativos a ciberdelitos o delitos cometidos por medio de sistemas informáticos, dando paso a crear una Ley especializada en la materia de Ciberdeltios, a fin de erradicar el mal uso de las herramientas dentro del campo de la tecnología de la información, ya que estos influyen directamente sobre la sociedad moderna y que actualmente dentro del ciberespeacio es utilizado con fines legítimos. La iniciativa tiene por objeto establecer las bases de integración y acción para preservar la seguridad informática nacional	Sen. Jesús Lucía Trasviña Waldenrath	Pendiente en comisión(es) de cámara de origen el 27-mar-2019

Fuente: Obtenido de Sistema de Información Legislativa (SIL). Secretaría de Gobernación. Disponible en: http://sil.gobernacion.gob.mx/ (fecha de consulta: 20 de octubre de 2021).

Acerca del tema de ciberseguridad, seis de estas iniciativas fueron presentadas por legisladores en el Senado de la República, mientras que cinco fueron propuestas en la Cámara de Diputados. En cuanto a la normatividad propuesta a modificar, cuatro de estas iniciativas inciden en el Código Penal Federal; cuatro implican la promulgación de una Ley nueva; tres son propuestas de reforma a la Ley de Seguridad Nacional. En tanto, dos están enfocadas a la creación de una efeméride; una es propuesta de cambio a la Constitución; una

implica modificaciones a la Ley Federal de Austeridad Republicana; y finalmente, otra más a la Ley General del Sistema Nacional de Seguridad Pública.

Cabe destacar que la Dip. María Eugenia Hernández Pérez presentó dos iniciativas acerca de temas de ciberseguridad, caso único en el trabajo realizado en la anterior legislatura (Tabla 2).

Tabla 2. Modificaciones al marco legal de acuerdo con las Iniciativas presentadas en la LXIV Legislatura del Congreso mexicano (2018-2021) acerca de ciberseguridad.

Propuesta de legislador	Ley de Seguridad Nacional	Efeméride	Código Penal Federal	Nueva Ley	Ley Federal de Austeridad Republicana	Reforma Constitucional	Ley General del Sistema Nacional de Seguridad Pública
Sen. José Ramón Enríquez Herrera	X						
Dip. María Eugenia Hernández Pérez	X						
Dip. María Eugenia Hernández Pérez		X					
Sen. Alejandra Lagunes Soto Ruíz		X					
Sen. Jesús Lucía Trasviña Waldenrath (1)			X	X			
Dip. Carlos Iván Ayala Bobadilla				X			
Dip. José Salvador Rosas Quintanilla					X		
Dip. Javier Salinas Narváez						X	

La tabla 2, continúa en la siguiente página

Propuesta de legislador	Ley de Seguridad Nacional	Efeméride	Código Penal Federal	Nueva Ley	Ley Federal de Austeridad Republicana	Reforma Constitucional	Ley General del Sistema Nacional de Seguridad Pública
Sen. Miguel Ángel Mancera Espinosa	X		X	X			X
Sen. Gustavo Enrique Madero Muñoz			X				
Sen. Jesús Lucía Trasviña Waldenrath			X	X			

Fuente: elaboración propia con datos del Sistema de Información Legislativa de la Secretaria de Gobernación. Disponible en: http://sil.gobernacion.gob.mx/portal (Fecha de consulta:29 de octubre de 2021).

En cuanto a las iniciativas presentadas en el primer periodo del primer año de la LXV Legislatura en el tema de ciberseguridad, en ese lapso se inscribieron dos propuestas en la materia; una en el Senado de la República y otra en Cámara de Diputados. Ambos documentos se encuentran pendientes de revisar en las comisiones de la sede de origen (Tabla 3).

Tabla 3. Iniciativas presentadas en el primer periodo del primer año de la LXV Legislatura del Congreso mexicano (2021) acerca de ciberseguridad.

Iniciativa y fecha de presentación	Objetivo	Presentada por	Estatus
Que reforma diversos artículos de la Ley General del Sistema Nacional de Seguridad Pública. 14 de octubre de 2021	Regular la integración, organización y funcionamiento la Comisión Nacional de Ciberseguridad. Entre lo propuesto destaca: 1) definir que los órganos de ciberseguridad son la Comisión Nacional de Ciberseguridad (CNC) y las instituciones de la federación, entidades federativas y municipios que realicen funciones de ciberseguridad; 2) establecer la Comisión Nacional de Ciberseguridad estará integrada por la o el titular de la SSPC, Sedena, Semar, Segob, SRE, SCT, Sener, SHCP, SE, SEP, FGR y	Sen. Jesús Lucía Trasviña Waldenrath	Pendiente en comision(es) de Cámara de origen 14 de octubre de 2021

La tabla 3, continúa en la siguiente página

Iniciativa y fecha de presentación	Objetivo	Presentada por	Estatus
	y las y los gobernadores de los estados; 3) determinar que la CNC estará integrada por una Conferencia; 4) indicar que la CNC cumplirá sus objetivos y fines, formulará políticas integrales y sistemáticas, así como programas y estratégias en materia de ciberseguridad; y, 5) señalar que la CNC planteará la Estrategia Nacional de Ciberseguridad y el Programa Nacional de Ciberseguridad procurando su ejecución y evaluación anual. Para tal fin modifica los artículos 5, 10 y 38 bis de la Ley General del Sistema Nacional de Seguridad Pública.		
Que reforma los artículos 11 y 13 de la Ley de la Fiscalía General de la República. 2 de diciembre de 2021	Crear la Fiscalía Especializada en materia de Ciberseguridad. Para ello propone: 1) señalar que la FGR contará con la Fiscalía Especializada en materia de Ciberseguridad para el ejercicio de sus facultades; y, 2) señalar que la Fiscalía Especializada en materia de Ciberseguridad podrá investigar y perseguir los delitos de competencia Federal en el que los medios electrónicos y tecnológicos constituyan o representen un medio de comisión relevante y trascendente, a excepción de delincuencia organizada.	Dip. Lidia García Anaya	Pendiente en comisión(es) de Cámara de origen 15 de diciembre de 2021

Fuente: Obtenido de Sistema de Información Legislativa (SIL). Secretaría de Gobernación. Disponible en: http://sil.gobernacion.gob.mx/ (fecha de consulta: 18 de enero de 2022).

Las dos iniciativas presentadas en el transcurso de la LXV Legislatura en este rubro plantean la creación de una dependencia federal especializada para combatir este tipo de delitos. La presentada por la Sen. Jesús Lucía Trasviña Waldenrath propone su operación desde la Administración Pública Federal, mediante la modificación de la Ley General del Sistema Nacional de Seguridad Pública. Por su parte, la iniciativa de la Dip. Lidia García Anaya propone abordar esta gestión desde una institución adscrita a la Fiscalía General de la República. Ambas propuestas muestran una preocupación por reducir los riesgos ocasionados por los delitos cibernéticos.

4. Contexto internacional en el tema

Chile

En aquel país andino se desarrolla la Política Nacional de Ciberseguridad debido a que:

> la masificación en el uso de tecnologías de información y comunicaciones (TIC), junto con servir al desarrollo del país, conlleva riesgos que pueden afectar los derechos de las personas, la seguridad pública, las infraestructuras críticas, el gobierno digital, los intereses esenciales y la seguridad exterior de Chile" (BCN, 2017: 11).

Por lo que el gobierno chileno realiza una serie de políticas públicas para salvaguardar la integridad de las personas, empresas y su patrimonio por los riesgos que pueden existir ante el uso inapropiado del internet.

Como metas a alcanzar en 2022 destacan:

- El país contará con una infraestructura de la información robusta y resiliente, preparada para resistir y recuperarse de incidentes de ciberseguridad, bajo una óptica de gestión de riesgos.
- El Estado velará por los derechos de las personas en el ciberespacio.
- Chile desarrollará una cultura de la ciberseguridad en torno a la educación, buenas prácticas y responsabilidad en el manejo de tecnologías digitales.
- El país establecerá relaciones de cooperación en ciberseguridad con otros actores y participará activamente en foros y discusiones internacionales.
- El país promoverá el desarrollo de una industria de la ciberseguridad, que sirva a sus objetivos estratégicos (BCN, 2017: 16, 18, 21-23).

España

El Ministerio de Asuntos Económicos y Transformación Digital de España coordina al Instituto Nacional de Ciberseguridad (Incibe), el cual:

> es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional (Incibe, 2021).

Por tanto, este organismo acompaña a instituciones de gobierno, empresas, particulares con políticas públicas gratuitas, confidenciales y soporte vía telefónica o redes sociales, con servicio durante doce horas al día todo el año, con un número de emergencia. Asimismo, existen áreas al interior de la institución dedicadas al cuidado del acceso de menores al internet, además de ocuparse del cuidado del patrimonio de los usuarios de las Tic´s mediante acciones enfocadas a la seguridad informática.

Entre las modalidades detectadas por Incibe como formas de actuación de la delincuencia en contra de las personas, o situaciones de riesgo al navegar por internet son:

- Bulo covid
- Suplantación de identidad RRSS
- Estafa
- Robo cuenta videojuego
- Suplantación de identidad SMS
- Ciberacoso
- Uso excesivo
- Phishing
- Formularios web (Incibe, 2021).

Estados Unidos de América

En la Unión Americana se realiza cada mes de octubre jornadas nacionales acerca de la concienciación en seguridad cibernética, a fin de evitar amenazas a los usuarios de redes sociales tales como posibles fraudes, estafas, robo de información, entre otros delitos. Entre el marco jurídico en la materia destacan tres principales normas:

- Ley de Responsabilidad y Portabilidad del Seguro de Salud de 1996 (HIPAA)
- Ley Gramm-Leach-Bliley de 1999
- Legislación de Seguridad Nacional de 2002, que incluyó la Ley Federal de Gestión de Seguridad de la Información (FISMA) (Ciberseguridad, 2021).

Asimismo, la condición federal de los Estados Unidos ha permitido que sus demarcaciones realicen diferentes leyes locales a fin de proteger datos personales, fortalecer la seguridad cibernética, cumplimiento en medidas de salvaguarda de información, normas de protección a la industria, entre otros tópicos asociados.

Entre los delitos informáticos que más afectan a las y los estadounidenses destacan:

- hackeo de ordenadores;
- robo de identidad;
- espionaje económico;
- robo de secretos comerciales;
- irrumpir en sistemas informáticos y acceder, modificar o eliminar datos;
- robar información confidencial;
- desfigurar sitios web de Internet; y
- inundar sitios web con grandes volúmenes de tráfico de Internet irrelevante para hacer que los sitios web no estén disponibles para clientes reales (Ciberseguridad, 2021).

Japón

El país del sol naciente es considerado como el más seguro del mundo en el rubro de ciberseguridad, pese a diferentes ataques que se han registrado en los últimos años. En gran medida, las condiciones

favorables en cuanto a la seguridad digital han sido posibles debido a los recursos que se han destinado para su protección, al tiempo de la conciencia social acerca de la protección de datos.

> En ese sentido, algunos estudios refieren que:
> los problemas relacionados con la ciberseguridad que más preocupan al individuo japonés en el hogar son, en general: la difusión o publicación no autorizada de información personal, la posibilidad de resultar infectados por virus informáticos y la desconfianza en la seguridad de los métodos de pago electrónicos, lo cual se refleja especialmente en las bajas compras en marketplaces extranjeros (Icex, 2020. 4-5).

En ese sentido, este estudio también alerta de preocupaciones en materia de ciberseguridad por parte de otras organizaciones privadas y de la administración pública japonesa, tales como contar con el personal capacitado para prevenir y atender emergencias del rubro, fortalecer los mecanismos de transparencia y rendición de cuentas, realizar actualizaciones efectivas, evitar riesgos en el traspaso y operación de recursos, mejora del internet de las cosas, entre otros puntos sensibles.

Organización de las Naciones Unidas (ONU).

Los Objetivos de Desarrollo Sostenible (ODS) impulsados por este organismo internacional plantean en su objetivo 16 la meta de promover sociedades justas, pacíficas e inclusivas. En este sentido, existen puntos que se pueden asociar al combate de los riesgos de la ciberseguridad, tales como:

- 16.3 Promover el estado de derecho en los planos nacional e internacional y garantizar la igualdad de acceso a la justicia para todos.

- 16.4 De aquí a 2030, reducir significativamente las corrientes financieras y de armas ilícitas, fortalecer la recuperación y devolución de los activos robados y luchar contra todas las formas de delincuencia organizada.

- 16.10 Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales.

- 16.a Fortalecer las instituciones nacionales pertinentes, incluso mediante la cooperación internacional, para crear a todos los niveles, particularmente en los países en desarrollo, la capacidad de prevenir la violencia y combatir el terrorismo y la delincuencia (ONU ODS, 2021).

Por tanto, la ciberseguridad es una preocupación mundial debido a los alcances que pueden surgir debido a su fácil vinculación con otros tipos de delitos y sus impactos mediante la delincuencia organizada trasnacional. Al respecto, es la Oficina de Lucha contra el Terrorismo (OLCT) de la ONU la agencia encargada de coordinar el tema de ciberseguridad en el máximo organismo internacional, mediante la iniciativa 2341 de 2017, que señala:

> el Consejo de Seguridad exhorta a los Estados Miembros a "establecer o reforzar las alianzas nacionales, regionales e internacionales con las partes interesadas, tanto públicas como privadas, según proceda, para intercambiar información y experiencias

> a fin de prevenir, proteger, mitigar e investigar los daños causados por atentados terroristas contra instalaciones de infraestructura vital, así como para responder a ellos y recuperarse de ellos, en particular mediante actividades conjuntas de capacitación, y la utilización o el establecimiento de redes de alerta de emergencia o de comunicación pertinentes. (OLT, 2021).

Por tanto, la ciberseguridad es un tema prioritario para afrontar los riesgos de delitos tales como el financiamiento y operación de grupos terroristas, así como la distribución de fuentes ilícitas de flujo de efectivo. Al respecto, este organismo ofrece como una acción para contrarrestar estos efectos el Programa de Ciberseguridad y Nuevas Tecnologías, que fomenta:

> las capacidades de los Estados Miembros y las organizaciones privadas en la prevención de ciberataques realizados por actores terroristas contra infraestructuras críticas. El proyecto también busca mitigar los efectos de los ataques y recuperar y restaurar los sistemas que sean el blanco de estos, si llegasen a ocurrir (OLT, 2021).

Es decir, son líneas de trabajo coordinado para reducir los riesgos de incidencias.

Suiza

Aquella nación ha realizado diferentes políticas públicas para enfrentar los riesgos de la ciberseguridad, lo cual ha permitido compartir experiencias ante la generalización de nuevas tecnologías como la red 5G. En ese sentido, "las Escuelas Politécnicas Federales de Zúrich (EPFZ) y Lausana (EPFL) ofrecen una formación de clase mundial en los campos de la informática y de las tecnologías de la comunicación" (Swiss Info, 2019). Por lo que una de las respuestas brindadas en Suiza es la formación de especialistas capaces de afrontar estas emergencias cibernéticas.

Aunado a lo anterior, algunas fuentes refieren ventajas estratégicas de ese país para la aplicación de mejoras en la materia, ya que "las fortalezas de Suiza, como la neutralidad, la seguridad jurídica y la estabilidad política, también son válidas en el sector de la ciberseguridad. Su mayor ventaja radica en un alto nivel de protección de la privacidad y una baja densidad de regulaciones" (SGE, 2021). Por lo que muchas de las soluciones en materia de seguridad digital vendrán de desarrollos que realicen diferentes empresas establecidas en el país helvético.

Comentarios finales

La ciberseguridad es uno de los temas más importantes para brindar una cultura de paz en la población, debido a que es una estrategia para preservar el patrimonio y la seguridad de organizaciones y personas. No obstante, existen diferentes riesgos de ciberataques a cada minuto a escala mundial, en general, y nacional, en particular, lo que es muestra de los riesgos y vulnerabilidades existentes.

La actual situación sanitaria mundial ocasionada por el impacto del covid-19 han generado un mayor uso de computadoras, sobre todo en el hogar, debido a la adaptación social para el trabajo o la educación a distancia. En ese sentido, también ha implicado un mayor número de ataques cibernéticos debido a las diferentes modalidades usadas por las redes criminales para acceder a los datos personales sensibles de los usuarios. Por tanto, la prevención se ha convertido en una estrategia básica, a fin de evitar que los cibernautas puedan eludir estas trampas usadas por la delincuencia organizada trasnacional.

En el caso de México, la delincuencia cibernética ha generado graves daños al patrimonio de personas, familias y empresas. Asimismo, los ciberataques también pueden afectar funciones de la Administración Pública, por lo que es uno de los delitos actuales que plantean mayores desafíos para las fuerzas de seguridad de nuestro país. Parte de los daños se han agravado debido a un mayor uso de equipos por la contingencia del covid-19, la falta de actualización de los equipos, así como el uso de programas no originales, lo que ha evitado una mejor actualización por parte de las compañías creadoras de software.

Finalmente, delitos como robo de autos, hackeo de portales web institucionales, fraudes a la banca, robo de identidad, acoso en línea, estafas, alteración de bases de datos, daños patrimoniales, entre otros, estarán asociados a la ciberseguridad y continuarán afectando a la sociedad en un futuro. Si bien la prevención y educación son acciones importantes a fin de reducir el riesgo de caer en estos incidentes, también son indispensables la implementación y mejora de políticas públicas y del marco normativo que, en suma, afronten a la ciberdelincuencia de forma eficaz.

Referencias documentales

American Chamber México (ACM, 2017). Estrategia de Ciberseguridad en México. Disponible en: https://bit.ly/3lTIrCs (Fecha de consulta: 11 de diciembre de 2021).

Asociación Mexicana de Ciberseguridad (Ameci, 2021). *Ciberseguridad y protección de datos en México.* Disponible en: https://bit.ly/2YipReU (Fecha de consulta: 3 de noviembre de 2021).

Banco de México (Banxico, 2021). *Estrategia de Ciberseguridad del Banco de México*. Disponible en: https://bit.ly/3q6i3Xt (Fecha de consulta: 11 de diciembre de 2021).

Banco Interamericano de Desarrollo (BID, 2020). *Ciberseguridad, riesgos, avances y el camino a seguir en América Latina y el Caribe*. Disponible en: https://bit.ly/3Ig0NYb (Fecha de consulta: 29 de noviembre de 2021).

Biblioteca del Congreso Nacional de Chile (BCN, 2017). *Política Nacional de Ciberseguridad*. Disponible en: https://bit.ly/3nVy01I (Fecha de consulta: 29 de octubre de 2021).

Canales TI (Canales TI, 2021). Predicciones para 2022 sobre Ciberseguridad y Tecnología. 14 de diciembre. Disponible en: https://bit.ly/3fyZ56W (Fecha de consulta: 17 de enero de 2022).

Ciberseguridad, 2021. (Ciberseguridad, 2021). *EE. UU*. Disponible en: https://bit.ly/3EYQTHL (Fecha de consulta: 8 de noviembre de 2021).

Cisco (Cisco, 2021). *¿Cuáles son los ciberataques más comunes?* Disponible en: https://bit.ly/3do8I7t (Fecha de consulta: 6 de diciembre de 2021).

Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef, 2022). Cifras relevantes de Banco de México en comercio electrónico. Disponible en: https://bit.ly/3qeH1oJ (Fecha de consulta: 11 de enero de 2022).

Coordinación de Seguridad en la Información de la Universidad Nacional Autónoma de México (CSI, 2018). Ciberseguridad. Seguridad en la nube en los próximos años. UNAM. Disponible en: https://bit.ly/3BX9keO (Fecha de consulta: 20 de octubre de 2021).

Cueto, Héctor (Cueto, 2021). "Expertos urgen la creación de un marco regulatorio de ciberseguridad en México". *Business Insider*. Disponible en: https://bit.ly/3DEypLB (Fecha de consulta: 9 de diciembre de 2021).

Global Technology. (Global Technology, 2021). Consecuencias de un ciberataque. Disponible en: https://bit.ly/3rKmvgM (Fecha de consulta: 7 de diciembre de 2021).

Instituto de Ingeniería de la Universidad Nacional Autónoma de México (IIUNAM, 2021). *Seguridad Informática*. Disponible en: https://bit.ly/3jzuZCw (Fecha de consulta: 25 de octubre de 2021).

Instituto Nacional de Ciberseguridad (Incibe, 2021). *Conoce Incibe*. Disponible en: https://www.incibe.es/que-es-incibe (Fecha de consulta: 29 de octubre de 2021).

Kaspersky (Kaspersky, 2021). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021*. Disponible en: https://bit.ly/3EvClzn (Fecha de consulta: 6 de diciembre de

Melgar, Ivonne. (Melgar, 2021). "Ciberseguridad, tema espinoso sin atender; reforma congelada por falta de consensos en San Lázaro". Excélsior, 26 de diciembre. Disponible en: https://bit.ly/3fcYkQG (Fecha de consulta: 10 de enero de 2022).

Mendoza Escamilla, Viridiana (Mendoza, 2021). "Ciberseguridad, el otro siniestro que preocupa a las aseguradoras". *Forbes.* 18 de noviembre. Disponible en: https://bit.ly/3p3ACwe (Fecha de consulta: 15 de diciembre de 2021).

Oficina Económica y Comercial de la Embajada de España en Tokio (Icex, 2020). *El mercado de la ciberseguridad en Japón.* Disponible en: https://bit.ly/3DDJ1eI (Fecha de consulta: 18 de noviembre de 2021).

Oficina de Lucha contra el Terrorismo de Naciones Unidas (OLT, 2021). Ciberseguridad. Disponible en: https://bit.ly/3naacaX (Fecha de consulta: 12 de noviembre de 2021).

Organización de las Naciones Unidas (ONU- ODS, 2021). *Objetivo 16: Promover sociedades justas, pacíficas e inclusivas.* Disponible en: https://bit.ly/3gWU1Yr (Fecha de consulta: 10 de noviem-

Organización Marítima Internacional (OMI, 2021). *Riesgo cibernético marítimo*. Disponible en: https://bit.ly/3ok9Oan (Fecha de consulta: 3 de diciembre de 2021).

Perales, Mariana (Perales, 2021). "Ciberseguridad, una necesidad vital en la nueva realidad post COVID-19". Conecta. Disponible en: https://bit.ly/33EI2O6 (Fecha de consulta: 17 de enero de 2022).

Ramírez Gil. Karen Tatiana (Ramírez, 2020). ¿Cómo evitar ser víctima de delitos cibernéticos? Disponible en: https://bit.ly/3EVE1lJ (Fecha de consulta: 8 de noviembre de 2021).

Rojas Rodríguez, Alexandra (Rojas, 2017). '*I love you'… y todo se colapsó.* Disponible en: https://www.bbva.com/es/i-love-you-se-colapso/ (Fecha de consulta: 3 de diciembre de 2021).

Secretaría de Comunicaciones y Transportes (SCT, 2020). *Guía de Ciberseguridad para el uso seguro de redes y dispositivos de telecomunicaciones en apoyo al teletrabajo.* Disponible en: https://bit.ly/3dwp2mr (Fecha de consulta: 8 de diciembre de 2021).

Secretaría de Gobernación (TMEC, 2020). *Decreto Promulgatorio del Protocolo por el que se Sustituye el Tratado de Libre Comercio de América del Norte por el Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá, hecho en Buenos Aires, el treinta de noviembre de dos mil dieciocho; del Protocolo Modificatorio al Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá, hecho en la Ciudad de México el diez de diciembre de dos mil diecinueve; de seis acuerdos paralelos entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de los Estados Unidos de América, celebrados por intercambio de cartas fechadas en Buenos Aires, el treinta de noviembre de dos mil dieciocho, y de dos acuerdos paralelos entre el Gobierno de los Estados Unidos Mexicanos y el Gobierno de los Estados Unidos de América, celebrados en la Ciudad de México, el diez de diciembre de dos mil diecinueve.* Disponible en: https://bit.ly/3Gx4RBw (Fecha de consulta: 13 de diciembre de 2021).

Secretaría de Gobernación. *Sistema de Información Legislativa* (SIL, 2021). Disponible en: https://bit.ly/3xRLpME (Fecha de consulta: 3 de diciembre de 2021).

Switzerland Global Enterprise (SGE, 2021). *Suiza como centro de seguridad cibernética.* Disponible en: https://bit.ly/3DzEklP (Fecha de consulta: 19 de noviembre de 2021).

Swiss Info (Swiss Info, 2019). *Suiza afila sus armas contra la ciberdelincuencia*. 25 de marzo de 2019. Disponible en: https://bit.ly/30GbAK5 (Fecha de consulta: 4 de noviembre de 2021).

Unión Internacional de Telecomunicaciones (UIT, 2021b). *Índice de ciberseguridad global 2020*. Disponible en: https://bit.ly/3cPnhR8 (Fecha de consulta: 25 de noviembre de 2021).

Unión Internacional de Telecomunicaciones (UIT, 2021a). *Los países refuerzan sus estrategias de ciberseguridad.* Disponible en: https://bit.ly/3wgRGRf (Fecha de consulta: 4 de noviembre de 2021).

Este análisis se encuentra disponible en la página de internet
del Instituto Belisario Domínguez:
http://bibliodigitalibd.senado.gob.mx/handle/123456789/1870

Para informes sobre el presente documento, por favor comunicarse
a la Dirección General de Análisis Legislativo, al teléfono (55) 5722-4800 extensión 4831

INSTITUTO BELISARIO DOMÍNGUEZ, SENADO DE LA REPÚBLICA
Donceles 14, Colonia Centro Histórico, Alcaldía Cuauhtémoc, 06020 México, Ciudad de México
Distribución gratuita. Impreso en México.

Instituto
Belisario Domínguez
Senado de la República

El Instituto Belisario Domínguez es un órgano especializado encargado de realizar investigaciones estratégicas sobre el desarrollo nacional, estudios derivados de la agenda legislativa y análisis de la coyuntura en campos correspondientes a los ámbitos de competencia del Senado con el fin de contribuir a la deliberación y la toma de decisiones legislativas, así como de apoyar el ejercicio de sus facultades de supervisión y control, de definición del proyecto nacional y de promoción de la cultura cívica y ciudadana.

El desarrollo de las funciones y actividades del Instituto se sujeta a los principios rectores de relevancia, objetividad, imparcialidad, oportunidad y eficiencia.