McKinsey&Company

COMEXI
Consejo Mexicano de Asuntos Internacionales

Perspectiva de ciberseguridad en México

Junio 2018

Preámbulo

La ciberseguridad es un tema que aparece cada día con mayor frecuencia en nuestros medios y permea una amplia gama de campos. Los ciberataques que enfrentamos cada vez con mayor frecuencia pueden afectar desde la integridad de infraestructura crítica como los sistemas bancarios del país; a la incidencia de robos de identidades personales y otros delitos; y hasta contribuir a la cada vez más tenue credibilidad de datos e información general que compromete nuestra capacidad de discernir objetivamente en momentos en que tomamos decisiones importantes. Es un tema que afecta, incluso, a la seguridad emocional de los niños en un entorno social que se ha trasladado a lo digital. En resumen, afecta de alguna forma a todos los sectores sociales.

El presente documento, una colaboración del Consejo Mexicano de Asuntos Internacionales y McKinsey & Company, tiene como objetivo presentar un panorama amplio y general sobre el impacto de la ciberseguridad en importantes campos de nuestra sociedad y crear conciencia de la importancia que tiene entender los riesgos y actuar sobre ellos. Asimismo, señala algunas de las llamadas mejores prácticas, que se han desplegado en diversos países en esta materia. Aunque no es un diagnóstico detallado sobre la situación que guarda la ciberseguridad en nuestro país, consideramos que podría ser una referencia que contribuya a la creación de un amplio programa nacional sobre ciberseguridad.

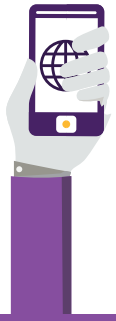
El problema es complejo y extenso y hacerle frente requiere de la participación amplia de la sociedad, no sólo por la urgencia del reto, sino porque un esfuerzo efectivo transitará por la creación de acuerdos sobre una serie de temas fundamentales que definen la naturaleza de una sociedad abierta y democrática como la que aspiramos ser. Por medio de este documento, esperamos contribuir a esta conversación.

Rafael Fernández MacGregor B

Coordinador Grupo Ciberseguridad de COMEXI

Contenido

LAS TECNOLOGÍAS DE LA INFORMACIÓN
SON CADA VEZ MÁS IMPORTANTES:



300 millones de dispositivos conectados para 2025 – **en México**

El crecimiento de 70% de dispositivos para el 2025 requerirá un crecimiento de más de **300% del poder computacional de centros de datos**

Más del **94% de este poder computacional estará en la nube**

PERO PRESENTAN **CADA VEZ MÁS RIESGOS:**

En México, más de **33 millones de personas fueron afectadas por el cibercrimen en 2017**

Es decir, una de cada cuatro personas

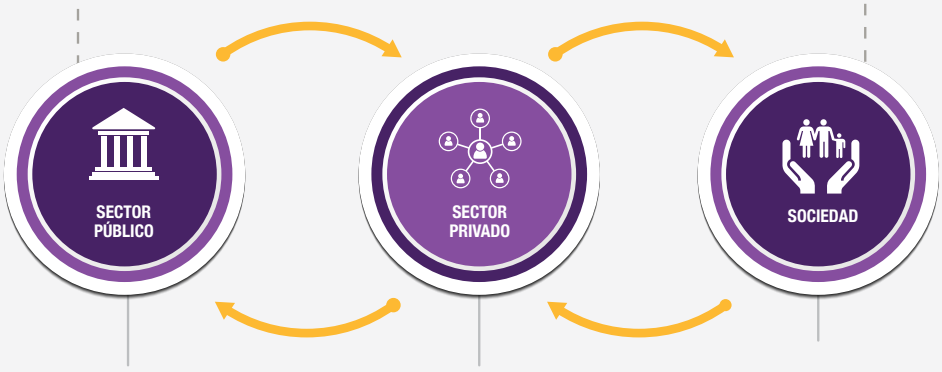
PARA **2019** SE ESTIMAN

PÉRDIDAS POR CIBERATAQUES DE HASTA **2 BILLONES DE DÓLARES A NIVEL MUNDIAL**

CIBERSEGURIDAD:
el conjunto de acciones tomadas por organizaciones e individuos para reducir la probabilidad de sufrir un ciberataque

CIBERRESILIENCIA:
la capacidad de organizaciones e individuos de enfrentar ciberataques en el largo plazo sin que afecte su capacidad de operar día con día

TEMAS DE AGENDA POR SECTOR



SECTOR PÚBLICO

- **Gobernanza efectiva**
- **Estrategia y marco normativo**
- **Mecanismos de respuesta operativa**
- **Gestión de talento y tecnología**
- **Desarrollo y protección infraestructura y sistemas críticos de datos**
- **Colaboración internacional para formar un marco multilateral**

SECTOR PRIVADO

- **Gobernanza corporativa**
- **Prevención y protección contra ciberriesgos**
- **Detección y combate de intentos de ataque**
- **Respuesta frente ataques exitosos**
- **Involucramiento interorganizacional**

SOCIEDAD

- **Concientización sobre ciberriesgos y cómo enfrentarlos**
- **Protección de la comunidad**
- **Evaluación de desempeño**

Resumen ejecutivo

El rápido crecimiento del ciberespacio constituido por el Internet, las redes sociales, los sistemas de información y los aparatos electrónicos, generó, entre otras cosas, una mayor calidad en los servicios que ofrecen las instituciones públicas. Además, propició la creación de nuevos modelos de negocio en el sector privado, la democratización y el acceso gratuito al conocimiento para la sociedad. Estos beneficios crecen exponencialmente y se reflejan en un aumento del PIB a nivel mundial: tan sólo el Internet representa más de 3% del PIB mundial, y las tecnologías de la información han potenciado la productividad y crecimiento de empresas en los demás sectores.

No obstante, con el crecimiento del ciberespacio también incrementaron los ciberataques: intentos de acceder ilegalmente a un sistema electrónico o a una red informática con el fin de extraer información o interrumpir su funcionamiento. Las entidades que tienen que defenderse de estos ataques son las organizaciones del sector público y sector privado, así como los individuos y grupos en la sociedad. Existen agencias de soporte, como reguladores y grupos de respuesta, que apoyan a estos organismos e individuos en su defensa contra ataques.

Por otro lado, hay una amplia gama de individuos y grupos que pueden lanzar ciberataques, desde individuos patrocinados por terceros –como activistas o compañías en competencia– hasta grupos de crimen organizado e incluso grupos de ciberespionaje. Las capacidades de los atacantes y el impacto de los incidentes aumentan de acuerdo con el nivel de influencia y recursos con los que cuenten sus patrocinadores.

La creciente dependencia de las tecnologías de la información y el incremento en número y severidad de ciberataques ha forzado a las organizaciones del sector privado y público a incrementar su gasto en ciberseguridad. A nivel mundial, éste ha crecido a una tasa mucho mayor que el crecimiento de la economía o el gasto en otros rubros de la tecnología de la información.

Aún con este incremento, los encargados de ciberseguridad de empresas consideran que los ciberatacantes están incrementando su sofisticación a una mayor velocidad que ellos, elevando el ciberriesgo al que las empresas están expuestas. Por su parte, la sociedad muestra cada vez mayor inquietud sobre los riesgos a los que enfrenta en el ciberespacio. Por ejemplo, en una encuesta reciente, 8 de cada 10 mexicanos expresaron preocupación por ser víctimas de una campaña de desinformación en línea (también conocido como *fake news*).

Para enfrentar esta creciente amenaza, actores del sector público, sector privado y la sociedad deben trabajar en conjunto bajo una agenda coordinada. Más allá de la ciberseguridad, esta agenda debe priorizar la ciberresiliencia de los mismos actores, es decir, incrementar su habilidad de enfrentar ciberataques en el largo plazo, sin que estos afecten su capacidad de operar día con día. Aunque cada sector enfrenta diferentes ciberriesgos y debe diseñar agendas específicas para enfrentarlos, la coordinación entre los tres sectores fortalece sus agendas específicas.

Los tres principales ciberriesgos que enfrenta el sector público son el posible robo o alteración a la información que resguarda sobre los ciudadanos, afectaciones a la operación de servicios públicos y operaciones de entidades gubernamentales, y el potencial daño a la confianza en instituciones. Para enfrentar estos riesgos, el sector público necesita, primero, asegurar una gobernanza efectiva, es decir un ente de coordinación centralizado que pueda definir y dirigir una estrategia nacional de ciberresiliencia, como lo es la Estrategia Nacional de Ciberseguridad (ENCS) de México. Esta estrategia, a su vez, puede funcionar como referencia para crear un marco normativo, incluyendo regulación (como la Ley Federal de Protección de Datos Personales en Posesión de los Particulares) y normativas para entidades públicas y privadas.

Para que este marco normativo se aplique de forma efectiva, y para responder a los ataques que enfrenta un país se necesitan mecanismos de respuesta operativa a ciberataques. En el caso de México, esto incluye entidades como el Centro Nacional de Investigación y Seguridad (CISEN), encargado de generar inteligencia y táctica para enfrentar ciberriesgos, y el CERT-MX, cuya tarea es responder a emergencias informáticas e investigación de cibercrímenes. La efectividad de estos organismos y de los equipos de respuesta del sector privado requieren de especialistas altamente entrenados, por lo que el sector público también necesita desarrollar una estrategia de gestión de talento y tecnología de ciberseguridad.

La agenda de ciberresiliencia del sector público también debe enfocarse en el desarrollo y protección de infraestructura y sistemas críticos de datos, debido a su importancia para el funcionamiento nacional. Por un lado, esto incluye el desarrollo y aplicación de normativas para la protección de infraestructura crítica, como la red eléctrica y de telecomunicaciones. Adicional a esto, implica la creación y protección de sistemas de datos que protejan a individuos de robo de identidad, y a organismos de posible fraude. Por último, la colaboración internacional para formar un marco multilateral de defensa facilita la cooperación entre países para enfrentar ciberriesgos.

Tal como el sector público, el sector privado enfrenta una multitud de ciberriesgos. Por un lado, el sector privado enfrenta riesgos individuales, es decir, vulnerabilidades a sistemas o al personal de empresas específicas. Asimismo, enfrentan ciberriesgos sistémicos: vulnerabilidades que aplican a sistemas utilizados por industrias enteras, o al personal de una gran cantidad de compañías.

La agenda de ciberresiliencia del sector privado comienza con la integración de ciberseguridad en la gobernanza corporativa de todas sus empresas. Esto incluye el establecimiento de un *Chief Information Security Officer* (CISO), encargado principal de seguridad informática en una organización. También que esta figura esté integrada en la organización de una forma que le permita cumplir sus funciones. Adicionalmente, las empresas deben implementar sistemas y procesos de prevención y

protección contra ciberriesgos, priorizando la defensa de activos críticos. Una estrategia de prevención de ciberriesgos se puede fortalecer fomentando una cultura de ciberseguridad en todos los empleados de la empresa.

Aún con una estrategia robusta de protección y prevención, no es posible evitar, por completo, los ciberataques que enfrentan las empresas. Por esto mismo, la agenda de ciberresiliencia también debe fortalecer la detección temprana y combate efectivo de intentos de ataque. Esto puede evitar que un intento de ataque tenga impactos negativos. En el caso de un ciberataque exitoso, las empresas pueden elaborar planes de respuesta para mitigar las afectaciones causadas por los mismos. La prevención, detección y respuesta a ataques se beneficia del involucramiento interorganizacional, incluyendo cooperación entre empresas y organismos públicos para enfrentar ciberriesgos. Un ejemplo de esta cooperación en México es la alianza de asociaciones industriales y autoridades del sector financiero bajo las Bases de Coordinación en Materia de Seguridad de la Información.

Como los organismos del sector público y el sector privado, los individuos y grupos en la sociedad también enfrentan ciberriesgos que pueden afectar su situación económica, su integridad física y emocional, y su capacidad de tomar decisiones de forma objetiva. Algunos de estos riesgos son específicos y afectan la vida de personas individuales. Estos incluyen el ciberacoso (*cyberbullying*) y el robo de identidad, pero pueden inclusive alcanzar al nivel de intimidación y espionaje de personas por su trabajo o afiliación política. Algunos de estos ciberataques y otros crímenes con afectación a individuos son facilitados por tecnologías de información que permiten el anonimato, como los *Darknets*.

Además de los riesgos específicos, la sociedad también se enfrenta a ciberriesgos grupales, que afectan la capacidad de grandes grupos de la sociedad de operar y tomar decisiones de forma objetiva. Uno de los principales riesgos de este tipo son las campañas de desinformación o *fake news*, que pueden ocurrir como parte de un esfuerzo concertado de un ciberatacante, o crecer orgánicamente a través de rumores en redes sociales. Estas campañas tienen la capacidad de distorsionar la percepción de la sociedad sobre temas críticos, e inclusive pueden llevar a episodios de violencia.

A diferencia de los organismos públicos y privados, las personas en la sociedad no cuentan con expertos de ciberseguridad para defenderlos de estos riesgos. Las asociaciones civiles y organizaciones no gubernamentales (ONGs) pueden cubrir este rol, implementando una agenda de ciberresiliencia para la sociedad.

El primer elemento de esta agenda es la concientización de la sociedad sobre cómo enfrentar ciberriesgos en su vida cotidiana, y sobre cómo ser ciudadanos cibernéticos responsables. Estos esfuerzos pueden hacerse en colaboración con el sector público y privado, por ejemplo, integrándose a los programas de educación pública y privada desde edades tempranas.

Las asociaciones civiles pueden concientizar a la sociedad sobre los ciberriesgos que enfrenta. Algunas ONGs, a nivel mundial, se han enfocado en ofrecer asistencia y consejería a víctimas de *cyberbullying* y, en México, organizaciones como *Verificado 2018* y Signa Lab se dedican a investigar y

combatir campañas de desinformación en las redes.

Finalmente, la sociedad civil puede tomar un rol de evaluación de desempeño vigilando la forma en la que las prácticas de organizaciones del sector público y privado afectan la ciberseguridad de la sociedad en general. Este esfuerzo incluye el seguimiento a las propuestas de legislación en materia de ciberseguridad. También considera la observación de las prácticas de empresas que manejan información de clientes o que gestionan redes sociales que pueden utilizarse para el ciberacoso o las campañas de desinformación.

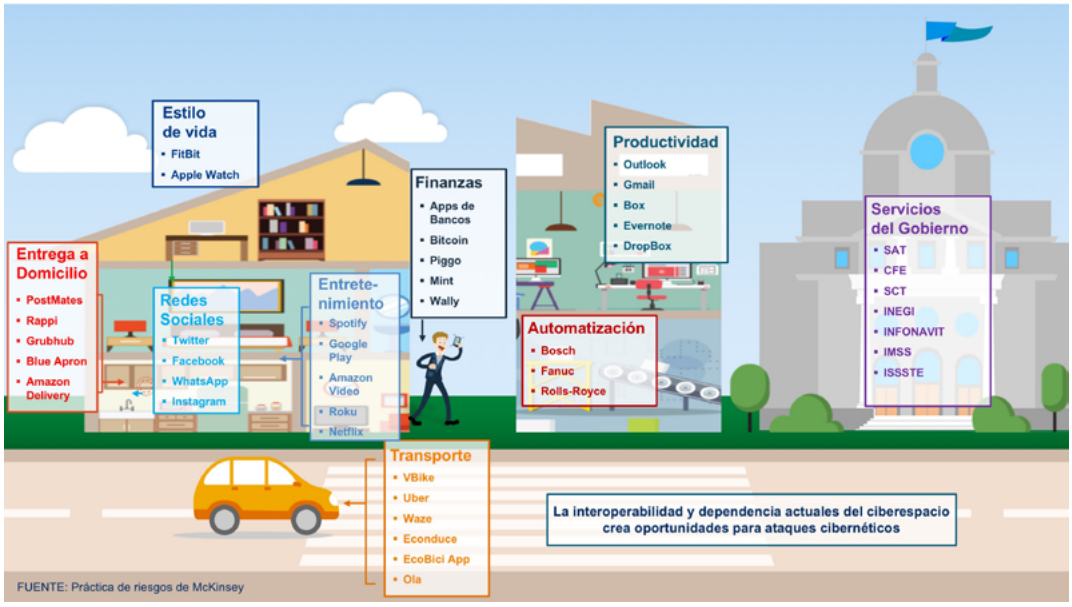
En los próximos años, es probable que crezca el uso de tecnologías de información en el sector público, sector privado y la sociedad, incrementando la amenaza de los ciberriesgos. Por lo tanto, el fomento de una verdadera ciberresiliencia por parte del sector público, el privado y la sociedad civil se convierte en una prioridad para el desarrollo de México. Aunque su relevancia es clara e indiscutible, el lanzamiento, la consolidación y la coordinación de una agenda holística de ciberresiliencia es un desafío que requiere el esfuerzo y la colaboración de todos, así como tomar acciones de forma proactiva.

Beneficios y riesgos de la tecnología de la información

El rol creciente de la tecnología de la información

Cada vez son más las actividades clave de nuestra sociedad que dependen de Tecnologías de la Información (TI). Casi todos los aspectos de nuestra vida cotidiana, desde la forma en la que nos comunicamos, trabajamos, nos transportamos e interactuamos con empresas y gobierno, están intrínsecamente vinculados a las TI *(véase figura 1)*. Estas favorecen la productividad de la población y mejoran la vida de casi 80 millones de ciudadanos con acceso a internet en México.[1]

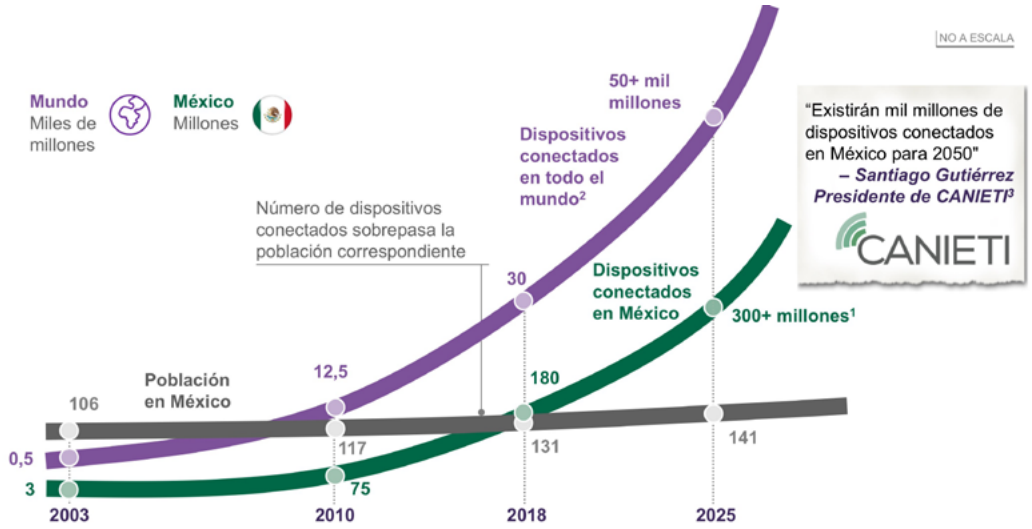
Figura 1: Innovación en diferentes ámbitos de la vida cotidiana



Como evidencia del rol creciente de la tecnología, sólo falta observar el crecimiento exponencial de dispositivos conectados a las redes. Se estima que para el año 2025 existan más de 300 millones de dispositivos con acceso a las redes en México, 70% más de los 180 millones que ya existen *(véase figura 2)*. Este incremento vertiginoso rebasará la tasa de crecimiento de la población, que para el mismo periodo se estima de 8%.

[1]Asociación de Internet.mx, *"14o Estudio sobre los Hábitos de los Usuarios de Internet en México 2018"*, mayo 2018

Figura 2: Cada vez más dospositivos conectados



El avance tecnológico que beneficia a la población se encuentra habilitado por una infraestructura invisible de sistemas digitales que permiten la transmisión y manejo de datos, así como complejos procesos computacionales. Esta red también afecta nuestras interacciones con negocios físicos (*brick and mortar*), y aunque realicemos actividades fuera de la red dependemos de la conectividad y de las TI.

Se estima que la carga computacional[2] de centros de datos crezca 19% anualmente en los próximos 7 años. Si la tasa se mantiene, el crecimiento de dispositivos para el 2025 necesitará más de 300% del poder computacional de centros de datos. Por lo menos 94% de este poder estará distribuido de forma global y descentralizada en la nube (*Cloud computing*).[3,4] Las operaciones de las empresas y organismos que empleen procesamiento en la nube dependen de la integridad de centros de datos distribuidos alrededor del mundo.

El sistema financiero, por ejemplo, es un sistema crítico que depende de la tecnología informática. Todas las transacciones realizadas entre clientes y comercios con tarjetas bancarias y medios de pago electrónicos ocurren de forma digital, involucrando interacciones complejas entre múltiples instituciones financieras. Con la creación de bitcoin y otras criptomonedas se abrió la posibilidad de realizar transacciones de forma anónima entre dos individuos u organizaciones, sin la injerencia de una institución bancaria. Estas nuevas tecnologías pudieran, eventualmente, suplantar en gran parte el intercambio físico de dinero.

Otros sistemas críticos también dependen de tecnologías de la información, como el sistema de agua potable, el sistema de energía eléctrica, los sistemas de producción y logística, y los sistemas de salud pública, por citar algunos. Esta interconexión entre organizaciones y sistemas digitales les permite operar con mayor eficiencia, brindándole comodidad a sus clientes. Adicionalmente, otorga mayor acceso al conocimiento y a un nivel de intercomunicación sin precedentes. Si bien este panorama

[2] Carga computacional o *workload* se define como el conjunto virtual o físico de recursos informáticos, incluido el almacenamiento, que se asignan para ejecutar una aplicación específica o proporcionar servicios de computación para uno o muchos usuarios.

[3] Según la definición oficial del National Institute of Standards and Technology (EUA), cloud computing es un modelo que permite el acceso a la red ubicuo, conveniente y bajo demanda a un grupo compartido de recursos informáticos configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden aprovisionarse rápidamente y lanzado con un mínimo esfuerzo de gestión o interacción del proveedor de servicios..

[4] Cisco Systems, *"Cisco Global Cloud Index: Forecast and Methodology, 2016–2021"*

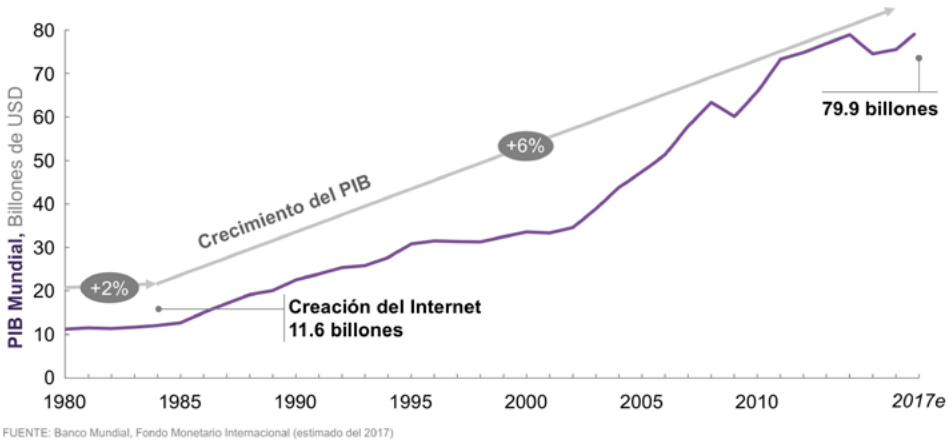
supone múltiples beneficios, también genera una dependencia absoluta de estos mismos sistemas.

El crecimiento acelerado de la tecnología digital trajo consigo beneficios importantes para el sector público, para el sector privado, y para la sociedad en general. El sector público se ha beneficiado a través de mayor interconexión y cooperación entre sus instituciones. Además, la comunicación con los ciudadanos es más cercana y los organismos públicos pueden proveer mejores servicios a menores costos. Hoy, por ejemplo, los mexicanos pueden acceder a más de 5,000 servicios digitales del gobierno federal a través del sitio web de la Ventanilla Única Nacional desde sus dispositivos electrónicos.[5]

Además de esto, el incremento en productividad y conveniencia de estas tecnologías tiene ya un impacto directo (y relevante) en el sector privado y la economía en general, que coincidie con una época de crecimiento acelerado del PIB mundial *(véase figura 3).* Individualmente, la industria del internet representa más del 3% del PIB en el mundo.[6] Sin embargo, el impacto de las tecnologías de la información sobre la economía mundial es mucho mayor, ya que ha habilitado la eficiencia y el crecimiento en otras industrias. Por ejemplo, un estudio[7] de pequeñas y medianas empresas identificó que aquellas que hacen uso extenso de estas tecnologías tienden a crecer al doble de la tasa de las que las que no lo hacen.

Esto es sólo una evidencia del enorme impacto de la tecnología digital en el avance industrial y comercial, incluyendo la generación de nuevos modelos de negocio, cambios de medios de producción, reducción de costo operativo y mayor acceso a consumidores.

Figura 3: Crecimiento del PIB Mundial



FUENTE: Banco Mundial, Fondo Monetario Internacional (estimado del 2017)

La sociedad, por su parte, ganó mayor acceso a la información y la tecnología. La apertura de redes sociales y de otras plataformas colectivas de conocimiento y de comunicación social incrementan la capacidad del ciudadano común de comunicarse e informarse de manera oportuna. Según un estudio de la Asociación de Internet.mx, el cibernauta promedio en México está conectado al Internet por más de 8 horas, y utiliza 5 redes sociales.[8] Todo lo anterior ha intensificado la transparencia de las actividades de los gobiernos y las empresas privadas, y su impacto sobre los ciudadanos. Al mismo tiempo, ha incrementado el acceso a la educación a través de la distribución masiva de contenidos

[5] Gob.mx, La Ventanilla Única Nacional, www.ventanillaunica.gob.mx , 2016

[6] Incluye el gasto en comercio y otros servicios en línea, y la inversión pública y privada en tenologías de la información relacionadas al internet.

[7] McKinsey Global Institute, *"The Net's sweeping impact on growth, jobs and prosperity"*, mayo 2011

[8] Asociación de Internet.mx, *"14o Estudio sobre los Hábitos de los Usuarios de Internet en México 2018",* mayo 2018.

didácticos. Otro estudio de la misma Asociación encontró que 36% de los mexicanos está cursando algún programa educativo utiliza la modalidad de educación en línea.[9]

Amenaza de riesgos cibernéticos y ciberataques

Figura 4: Estadísticas relacionadas al cibercrimen

Aunque, la interdependencia de organizaciones y sistemas ofreció acceso a los beneficios del ciberespacio, también presentó nuevos riesgos que debemos afrontar. Los **riesgos cibernéticos** son el conjunto de posibles afectaciones que las empresas, gobiernos y miembros de la sociedad podrían sufrir debido a una falla o vulneración de las tecnologías de información que utilizan. Esto puede reflejarse en una pérdida económica, daños a la reputación, pérdida de operatividad o en la toma de decisiones mal informadas.

Los riesgos cibernéticos pueden surgir de fallas accidentales, pero las mayores afectaciones suelen surgir de una falla causada por un ataque intencional. Un **ciberataque** es un intento no autorizado por la vía digital de acceder a un sistema de control, dispositivo electrónico y/o red informática, con el propósito de sabotear su funcionamiento, extraer información y recursos, o extorsionar a usuarios y organizaciones.

Por lo general, estos ataques se dividen en **ataques dirigidos y no dirigidos**, dependiendo de si el ciberatacante tiene como meta vulnerar la seguridad de un individuo o grupo, o tiene metas más generales *(véase figura 5).* Otra forma de categorizar los ciberataques es por su impacto: individual (afecta sólo una persona u organismo), o **sistémico** (vulnera la seguridad de un sistema completo con impacto en una red de individuos y organizaciones).

[9] Asociación de Internet.mx, *"Educación en Línea en México 2017"*, febrero 2018.

Figura 5: Tipos de ciberataques dirigidos y no dirigidos

Ataque dirigido — Tipo de ataque en el que se vulnera **la infraestructura, sistema o procesos de una entidad específica**

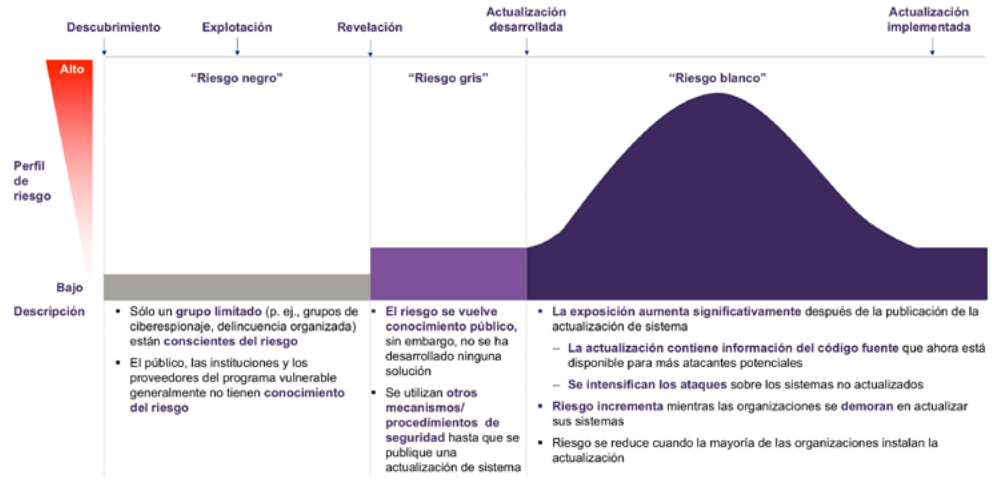
Ataque no dirigido — La forma más común y generalizada de lanzar un ciberataque, enfocada a causar daño a la infraestructura o sistemas **de un grupo de individuos o empresas de forma indiscriminada**

Tipo	Ejemplos de técnicas	Descripción del ataque	Ejemplo del ataque
Dirigido	*Spear-phishing*	Enviar correos electrónicos a individuos específicos que contengan un archivo adjunto con software malicioso.	**2015:** Un ataque a la Oficina de Administración Personal de los EE.UU; llevó al robo de información de más de 21.5 millones de personas
	Zero day	Explotar vulnerabilidades no conocidas públicamente a sistemas de empresas específicas.	**2012:** Un ataque a Saudi Aramco que destruyó 35,000 computadoras en unas cuantas horas.
	Subversión de cadena de suministro	Atacar a un equipo o software antes de que sea entregado a una organización.	El *adware Superfish*, preinstalado en las *notebooks* Lenovo, permitió a los atacantes hacerse pasar por diversas direcciones de internet
No dirigido	*Phishing*	Enviar correos electrónicos a un gran número de individuos pidiendo información sensible o alentándolos a entrar a una página con código malicioso.	**2016:** *Shamon 2* afectó a más de 15 instituciones privadas y agencias de gobierno en Arabia Saudita
	Ransomware	Diseminar *malware* enfocado a extorsionar a empresas e individuos (p.ej., malware que puede negar el acceso del usuario a su computadora a menos que se pague un rescate)	**2017:** El incidente *WannaCry* que afectó a más de 300,000 equipos y comprometió la seguridad de empresas en más de 150 países
	Denial of service	Utilizar código malicioso para dirigir a computadoras infectadas a abrumar un sitio o servicio en la red, afectando su funcionamiento	**2016:** El ciberataque *Dyn* afectó la disponibilidad de múltiples plataformas y servicios en internet
	Campañas de desinformación	Utilizar *bots*, sitios que emulan medios legítimos, redes sociales y otras herramientas para manipular la opinión pública o influir sobre la toma de decisiones de grupos.	**2017:** Esfuerzos para manipular los resultados de la elección francesa (*hack* al partido *En Marche!*, publicación de mails incluyendo correos falsos, etc.)

FUENTE: McKinsey, Universidad de Maryland, Universidad Carnegie Mellon, Infosec Institute

Además de tener un mayor impacto potencial, los ciberataques sistémicos son más difíciles de controlar porque no ocurren como un evento puntual y contenido. Asimismo, su crecimiento es exponencial, ya que cada sistema afectado puede, a su vez, infectar a otros más. El desarrollo de un parche o actualización para proteger a los sistemas de este ciberataque no lleva a su erradicación, incluso, puede incrementar el riesgo *(véase figura 6).* Para resolver estos incidentes, por lo general, se requiere el esfuerzo colectivo de usuarios y administradores de TI dentro de las organizaciones.

Figura 6: El ciclo de vida de un ciberataque sistémico



FUENTE: ETH Zurich, Delta Risk, McKinsey

No todos los ciberataques son consecuencia de una falla en la misma tecnología; en algunos casos el punto más débil y blanco de los atacantes es el usuario, quien es manipulado para abrir el acceso a su propio sistema. Otros ataques aprovechan el funcionamiento normal para cumplir un objetivo no intencionado. Tal es el caso de las campañas de desinformación (*fake news*) que aprovechan el carácter abierto y libre de la información de las redes sociales para manipular la percepción o acciones de un grupo. Este escenario afecta la confianza de la sociedad en fuentes de información en línea.

El número de activos expuestos a ciberataques por parte de instituciones públicas, del sector privado y de la sociedad es cada vez más alto. En el año 2017, 33 millones de mexicanos (50% más que en 2016)

fueron víctimas del cibercrimen – uno de cada cuatro habitantes del país. Al mismo tiempo, el impacto económico de estos crímenes fue de 7.7 mil millones de dólares, 40% más que el año anterior.[10] Se estima que, en el mundo, el costo total del cibercrimen, en el año 2019 alcanzará un monto de 2 billones de dólares.[11] Esta cifra no considera el impacto de diseminar información falsa con el propósito de influir en el público.

Aparte de su impacto económico directo, los ciberataques han forzado a las organizaciones a incrementar su gasto en medidas de defensa. El gasto en ciberseguridad ha crecido exponencialmente desde 2013, a una tasa cada vez mayor que el resto del gasto en tecnologías de la información (TI) *(véase figura 7)*. Según el International Data Corporation, los gobiernos también han incrementado su gasto en ciberseguridad de forma significativa. Por ejemplo, los gobiernos de estados y autoridades locales han incrementado su gasto de ciberseguridad a una tasa de 10.2% anual en los últimos 5 años: la única industria del sector privado que incrementó más su gasto en ciberseguridad en este periodo fue la de telecomunicaciones (11.2% anual).[12]

Figura 7: Crecimiento global de PIB, gasto en ciberseguridad y gasto en TI

Percepción de organismos e individuos sobre los ciberriesgos que enfrentan

Organizaciones en todo el mundo están conscientes de la creciente amenaza. De acuerdo con el reporte *Estado de la Ciberseguridad*[13] realizado en el 2017 por la *Asociación de Auditoría y Control de Sistemas de Información* (ISACA)[14], cuatro de cada cinco empresas consideran como probable, o muy probable, experimentar un ciberataque durante el próximo año. Además, 50% de las empresas indicaron que fueron blanco de más ataques que el año anterior.

A pesar de estos esfuerzos, la mayoría de los directores de seguridad de la información, CISOs[15], por sus siglas en inglés, considera que los atacantes continuarán tomando ventaja sobre los defensores *(véase figura 8)*. También reconocen que su lado más débil para responder a posibles incidentes son

[10] Symantec Corporation, "*Norton Cyber Security Insights Report*", 2016 y 2017

[11] AT&T, *"AT&T Cybersecurity Insights Report"*, 2017; en el documento se utilizará la palabra *"billón"* para determinar un millón de millones.

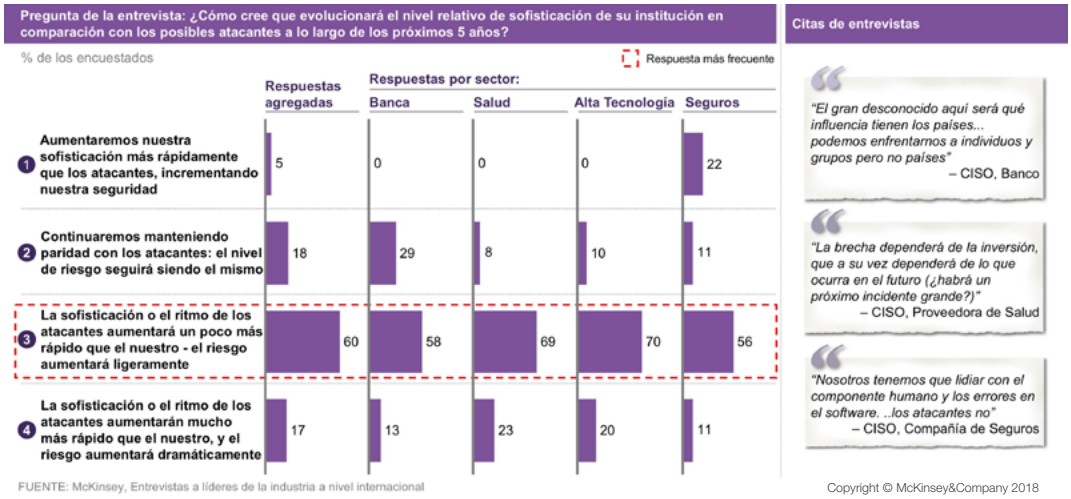
[12] International Data Corporation (IDC), "*World Semianual Security Spending Guide*", 2017

[13] Para desarrollar el reporte se encuestaron a más de 2,300 profesionales de ciberseguridad en el mundo.

[15] *Chief Information Security Officer,* puesto directivo en una organización encargado de la ciberseguridad y protección de datos

las capacidades de sus profesionistas: sólo 46% de las empresas confían en su equipo para manejar ciberataques de magnitud media[16]. La existencia de una brecha relevante en las capacidades de los profesionistas en seguridad cibernética torna aún más complejo el panorama.

Figura 8: Perspectiva de los CISOs sobre las capacidades internas de las empresas y los ataques cibernéticos que esperan enfrentar



La sociedad también percibe el riesgo, y expresa una creciente desconfianza en la información que recibe. De acuerdo con la encuesta mundial Edelman Trust Barometer, sobre confianza pública en instituciones, industrias y líderes; más de la mitad de los mexicanos desconfía de los medios de información. Aún más impactante es que ocho de cada diez mexicanos reportaron estar preocupados de que la información falsa se utilice como un arma en su contra. Ésta fue la tasa más alta entre 28 países encuestados.[17]

[16] ISACA, *"State of Cyber Security"*, 2017.

[17] Edelman, *"2018 Edelman Trust Barometer Global Report"*, febrero 2018

Ciberseguridad y ciberresiliencia

Definición de ciberseguridad

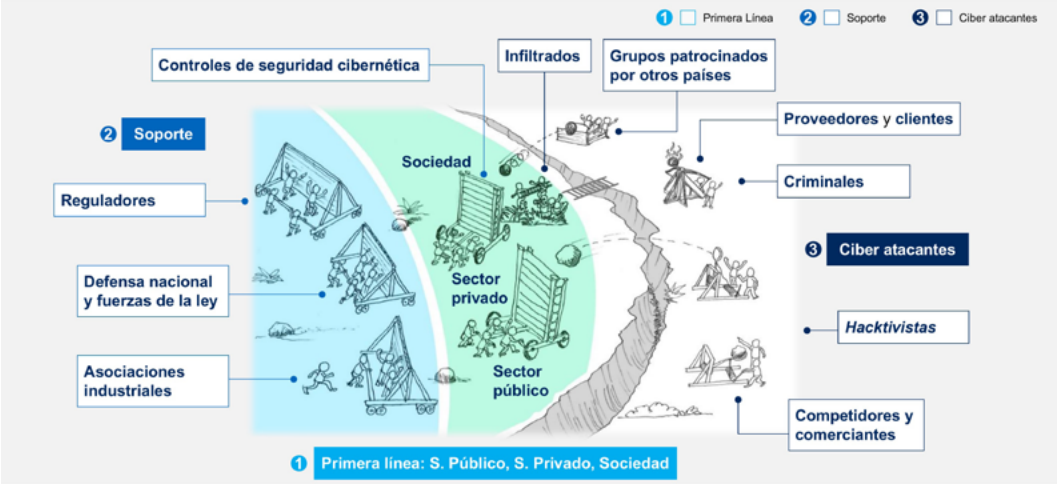
La **ciberseguridad** es el conjunto de acciones tomadas por organizaciones e individuos para mitigar los riesgos que enfrentan en el ciberespacio, con el propósito de disminuir la probabilidad de sufrir un ciberataque. Esto incluye soluciones tecnológicas como el uso de programas *anti-virus* o la actualización periódica de software; además de buenas prácticas en el uso de las tecnologías de la información, como no abrir archivos de direcciones de correos que provienen de fuentes desconocidas.

La ciberseguridad y los ciberataques viven una batalla campal que involucra a varios actores con roles distintos. En el frente de la ciberseguridad están la sociedad, las instituciones públicas y el sector privado; tres instancias que poseen los activos a los que buscan acceder los atacantes. Estos actores tienen que emplear las herramientas de la ciberseguridad para proteger sus activos en riesgo. En la retaguardia están las agencias de soporte que buscan apoyar a los actores del frente para combatir los ciberataques. Estas agencias no suelen encarar los ataques de forma directa, pero son cruciales para el esfuerzo de la ciberseguridad.

En el otro lado del conflicto están los ciberatacantes, que varían en nivel de capacidad y motivación. En algunas ocasiones los ciberatacantes están patrocinados por terceros, como compañías competidoras o grupos del crimen organizado. Los ciberataques, de acuerdo con sus autores y patrocinadores, pueden tener motivos económicos, políticos o militares. La capacidad de los atacantes y el impacto de los eventos perpetrados se incrementa de acuerdo con el nivel de influencia y recursos con los que cuentan los patrocinadores *(véase figura 9).*

Existen dos factores en este entorno que ponen en desventaja a los defensores frente a los atacantes. Primero, una sola vulnerabilidad en el sistema compartido (p. ej., los sistemas operativos de las computadoras o los servicios de *Cloud Computing*) puede ser utilizada por una gran cantidad de ciberatacantes para afectar a individuos y grupos que dependen de éste. Adicionalmente, la ciberseguridad resulta ser una función secundaria para los individuos y grupos vulnerables a los ataques, mientras que los ciberatacantes suelen ser individuos o grupos especializados en esta materia.

Figura 9: Actores de ciberseguridad y ciberataques



Definición de ciberresiliencia

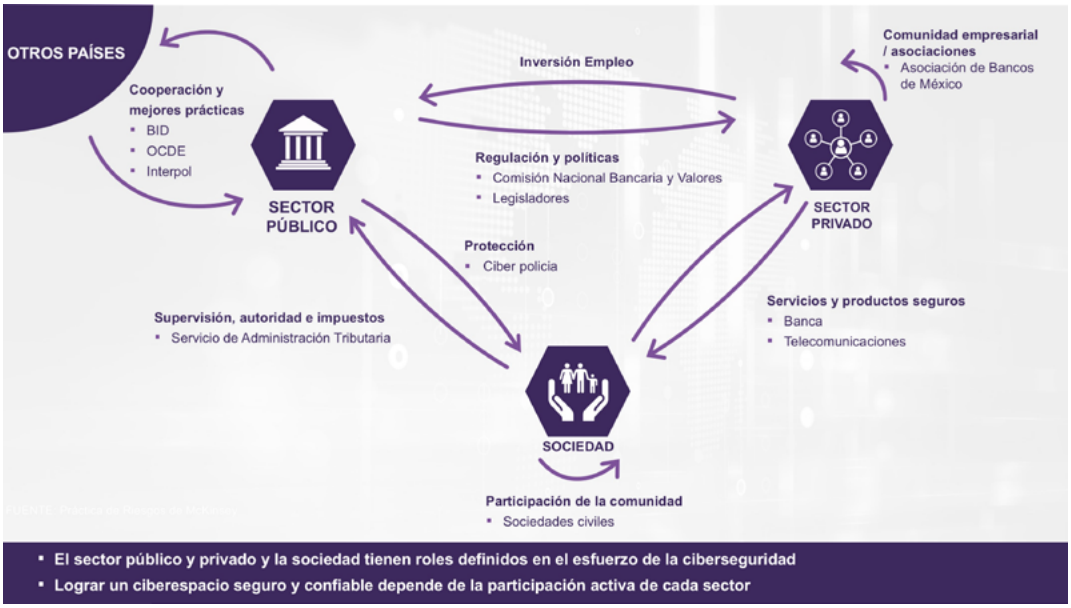
La capacidad de los sectores público, privado, y de la sociedad para enfrentar este entorno sin que afecte su habilidad de operar día con día se denomina **ciberresiliencia.** Este concepto incluye la capacidad de grupos e individuos para mantenerse seguros de forma sostenida en el largo plazo. Además, considera la facultad de una entidad u organismo para minimizar el impacto de ataques que penetren sus defensas, y su habilidad para restablecer la operación de forma rápida. Por último, la ciberresiliencia integra la destreza de todos para tomar decisiones con información imparcial y veraz.

Lograr la ciberresiliencia requiere de un esfuerzo sistémico. Es decir, mantener a un país protegido de estos riesgos necesita de la colaboración y coordinación del sector público, del sector privado y de la sociedad civil. Esta colaboración puede materializarse en diversas iniciativas, como la creación de un organismo formal de cooperación o la colaboración y comunicación no estructurada entre asociaciones civiles, asociaciones industriales y organismos gubernamentales. Lo importante es que las decisiones de ciberresiliencia no se enfrenten de forma individual o aislada.

A continuación, presentaremos una perspectiva sobre los riesgos cibernéticos enfrentados por organismos del sector público, empresas del sector privado y la sociedad en general en México y en el mundo. Adicionalmente, presentamos una agenda potencial para mejorar la ciberresiliencia en cada grupo, incluyendo ejemplos de iniciativas internacionales y de México.

Aunque estos temas se clasifican por su actor principal, existen amplias oportunidades para la cooperación intra-sectorial en cada uno de ellos *(véase figura 10)*. Por ejemplo, el sector privado puede colaborar con el gobierno para desarrollar conjuntamente una estrategia de desarrollo de talento de ciberseguridad. De igual forma, las mejores prácticas y tecnología desarrollada en la iniciativa privada son cruciales para asegurar la defensa de infraestructura y sistemas críticos en el sector público. Finalmente, la concientización y adopción de una cultura de ciberseguridad de la ciudadanía es una responsabilidad compartida de organismos públicos, privados, y asociaciones civiles.

Figura 10: Vínculos entre sectores en el diseño e implementación de estrategias de ciberresiliencia



FUENTE: Práctica de Riesgos de McKinsey

Dado el nivel de integración de las tecnologías de la información en todos los aspectos de nuestras vidas, definir una agenda de ciberresiliencia implica encontrar un balance entre fomentar la seguridad y asegurar los derechos individuales y colectivos de la sociedad. Algunas iniciativas de vigilancia de las redes para prevenir ciberataques pueden llegar a afectar los derechos de privacidad de los cibernautas. Por otro lado, la descentralización de fuentes de información y bases de datos pueden llevar a la democratización de la información y reducir el impacto de los ciberataques sobre las mismas, pero la centralización de datos e información puede brindar ventajas en protección de identidad, eficiencias de gestión, y validación de la información. Finalmente, la libertad de expresión y las iniciativas de activismo de unos grupos sociales en la red pueden llegar a interpretarse, en el extremo, como actos de *hacktivismo*[18] y diseminación de información falsa.

Antes de cimentar una agenda de ciberresiliencia nacional, los actores del sector privado, sector público y la sociedad tendrán que llegar a un acuerdo respecto a estos balances, de manera que reflejen los valores y preferencias de nuestro país.

[18] Palabra compuesta de hacker y activista, es decir activistas que realizan ciberataques.

Resiliencia del sector público

Riesgos cibernéticos enfrentados por el sector público

En México, como en el resto de los países, los organismos públicos tienen el compromiso de asegurar la ciberresiliencia nacional. Así, deben coordinar la estrategia nacional en materia, definir la regulación en ciberseguridad, y combatir el crimen cibernético. El sector tiene organismos que manejan datos valiosos o que gestionan procesos e infraestructura de manera directa. Los cuales están sujetos a riesgos y ataques, que impactan a empresas y personas que dependen de servicios públicos. Los riesgos cibernéticos enfrentados por el sector público amenazan la integridad de la información de los ciudadanos, de la infraestructura física gestionada por el gobierno, y la confiabilidad de las instituciones gubernamentales.

Riesgos sobre la información ciudadana

El gobierno almacena y administra importantes volúmenes de información relacionada con los ciudadanos, tales como datos de identificación, información electoral, tributaria, sobre educación y salud, entre otras. Es obligación del Estado proteger **la información de sus ciudadanos** frente a riesgos cibernéticos para garantizar su seguridad y minimizar las repercusiones. Los datos que resguarda pueden llegar a ser blanco de ataques potenciales. Por ejemplo, si un ciberatacante llegara a robar una base de datos sobre información personal de ciudadanos podría utilizarla para cometer crímenes como el robo de identidad o fraude.

En México se han presentado casos de vulnerabilidad a los sistemas del Sector Público, como el que afectó al Instituto Nacional Electoral (INE). Una base de datos del listado nominal de electores se alojaba en la nube de la empresa *Amazon Web Services* sin contraseña alguna, y se expusieron nombres, apellidos, direcciones y números de identidad de más de 93 millones de mexicanos (más del 70% de los habitantes del país).[19] De acuerdo con el INE, esto no fue un ciberataque al sistema; fue una vulnerabilidad causada por un grupo externo.[20]

Riesgos sobre infraestructura y sistemas

La **infraestructura y sistemas** del gobierno también enfrentan riesgos y pueden sufrir ataques. Los

[19] El Diario, *"Hackean los datos de 93 millones de votantes mexicanos"*, abril 2016.

[20] El Universal, *"Aclara INE que nunca ha sufrido ataque de piratas cibernéticos"*, septiembre 2017.

gobiernos poseen y operan infraestructura pública para proveer servicios a los ciudadanos, como electricidad, agua, manejo de desechos, telecomunicaciones, servicios de salud, educación y asistencia social. Estos activos podrían sufrir ciberataques que afectarían la prestación de servicios a millones de personas.

En 2017, la firma Symantec emitió un reporte sobre *Dragonfly,* un grupo de ciberespionaje enfocado a sistemas eléctricos y otra infraestructura crítica en varios países. El reporte identificó ciberataques a infraestructura en Estados Unidos, Suiza, Turquía y Ucrania que tenía el propósito de sabotear el acceso a servicios y extraer información estratégica. El incidente más notable causado por este grupo fue un ataque a la red eléctrica de Ucrania que provocó fallas en el servicio para cientos de miles de personas.[21]

Riesgos sobre integridad institucional

El gobierno debe proteger la **integridad institucional** del estado frente a ciberataques con el propósito de mantener la confianza sobre la gestión de procesos y de gobernabilidad. Algunos ciberataques enfocados en organismos públicos pueden tener como único propósito desprestigiar a dichos organismos o afectar su credibilidad, con el consecuente impacto negativo en su interacción con los ciudadanos.

Un ejemplo de ciberataque sobre integridad institucional es la afectación a los sistemas de un partido político u organismo electoral para influenciar los resultados de una elección. En la víspera de las elecciones presidenciales francesas, un grupo de ciberespionaje internacional vulneró las defensas del partido *En Marche!,* y publicó más de 20 mil correos de campaña en la plataforma WikiLeaks.[22] De acuerdo con los dirigentes del partido, el grupo de ciberespionaje insertó correos y documentos para sembrar información falsa.[23]

Pueden existir otros motivos detrás de un ciberataque a la integridad institucional de un gobierno: grupos autodenominados como hacktivistas atacan con el propósito de hacer una declaración política. Como el ataque simultáneo del grupo Ciber Protesta Mexicana en el año 2012, en donde por lo menos en 10 portadas de sitios web de gobierno, partidos políticos y prensa se publicaron mensajes de protesta. Este grupo, que ya había atacado de manera similar en 2009, posicionó su ciberataque como una protesta pacífica ante la situación política del país.[24]

Agenda de resiliencia del sector público

A pesar de las acciones tomadas por el gobierno para prevenir los ciberataques y combatir el ciberdelito, todavía existen áreas de oportunidad para estar a la altura de esta problemática. De acuerdo con el Índice Global de Ciberseguridad publicado por la Unión Internacional de Comunicaciones (ITU por sus siglas en inglés), una agencia de Naciones Unidas, México figura entre los países con nivel medio en cuanto a capacidad para enfrentar el tema.

Presentamos una agenda de ciberresiliencia para el sector público que podría ser utilizada como guía *(véase figura 11)*. Para cada uno de los seis temas se presentarán ejemplos de acciones emprendidas por países líderes en el área de ciberseguridad, así como algunos avances en nuestro país.

---

[21] Symantec, *"Dragonfly: Western energy sector targeted by sophisticated attack group"*, octubre 2017.

[22] The Telegraph, *"WikiLeaks releases thousands of hacked Macron campaign emails"*, julio 2017.

[23] DW, "Francia: Control Electoral pide no informar sobre documentos de Macron", mayo 2017.

[24] BBC, *"Mexico hackers hit official websites in cyber protest",* septiembre 2012.

Figura 11: Agenda de ciberresiliencia del sector público

Gobernanza efectiva

Aunque distintos organismos de un gobierno pueden implementar iniciativas de ciberresiliencia de forma independiente, la organización e integración de estos esfuerzos requiere de un organismo coordinador a nivel gobierno. Éste se encargaría del desarrollo, coordinación e implementación de la estrategia nacional de ciberseguridad. Asimismo, tomaría el rol de desarrollar protocolos, marcos operativos y responsabilidades para la ciberresiliencia, y gestionar su cumplimiento.

El establecimiento de una agencia central enfocada en la ciberseguridad supondría la designación de equipos especializados para atender temas y funciones específicas. Por ejemplo, puede existir un ente regulador, un cuerpo auditor que garantice el cumplimiento de la regulación, un equipo de respuesta a incidentes y un ente coordinador que ordene los diferentes grupos de los sectores público y privado. Los países con instituciones efectivas en esta área suelen contar con un cuerpo central encargado de establecer e implementar la estrategia nacional de ciberseguridad. En Estonia o Países Bajos, estas funciones están centradas en secretarías existentes, como la Secretaría de Defensa o de Seguridad y Justicia, respectivamente. Emiratos Árabes Unidos, Noruega y Reino Unido crearon cuerpos institucionales dedicados sólo a gestionar los programas nacionales de ciberseguridad. Por ejemplo, la Oficina de Seguridad Cibernética e Información en Reino Unido bajo la supervisión del Ministerio de la Oficina del Gabinete define, junto con la sociedad civil y el sector privado, las funciones y responsabilidades de cada objetivo en la Estrategia de Seguridad Cibernética.

En México, la necesidad de un ente coordinador se contempla en la Estrategia Nacional de Ciberseguridad (ENCS). El documento fue elaborado por Presidencia de la República y la OEA a finales de año 2017. En específico, se asigna a la Subcomisión de Ciberseguridad (dentro de la Comisión Intersecretarial para el Desarrollo de Gobierno Digital) el rol de gestionar la implementación de la ENCS y coordinar la actualización de procesos de los distintos organismos de la administración pública.[25] Este organismo es el primer paso para establecer la gobernanza de la ciberresiliencia en el país.

Estrategia y marco normativo

Una estrategia nacional de ciberresiliencia tiene como propósito presentar las metas, prioridades y

[25] Compuesta por Presidencia de la República, las secretarías de la Función Pública, Gobernación, Economía, Educación, Hacienda y a la Procuraduría General de la República, y miembros invitados permanentes de SEDENA, SEMAR, SAT, CNBV, PROFECO, Condusef, IPN y Conacyt

necesidades del gobierno, del sector privado y de la sociedad en esta materia. Asimismo, mapea las iniciativas técnicas, de procesos, de política y de regulación que necesitan implementar las distintas agencias de gobierno para cumplir con estas metas. Por último, establece el mecanismo mediante el cual se implementarán y gestionarán dichas iniciativas.

Muchos son los gobiernos que han desarrollado estrategias nacionales para alcanzar la ciberresiliencia ya están en su segunda o tercera versión de la misma *(véase figura 12).* Estonia, por ejemplo, un país líder en ciberseguridad, actualizó su primera estrategia en 2014. Aquel país dio continuidad a la implementación de las iniciativas de la estrategia previa, pero complementó el documento original con propuestas para enfrentar nuevas amenazas.[26] Aunque las estrategias nacionales de ciberresiliencia se enfocan en acciones del sector público, las estrategias de algunos países como Finlandia tienen un enfoque en la cooperación intersectorial.

Figura 12: Ejemplos de estrategias nacionales de ciberseguridad a lo largo del tiempo

FUENTE: Búsqueda web, estrategias nacionales de ciberseguridad

En México, recién se han acordado estrategias de ciberseguridad para el sector financiero y para el país en general. En octubre de 2017, la Secretaria de Hacienda y Crédito Público dio a conocer la Estrategia Nacional en Materia de Ciberseguridad, que busca evitar riesgos cibernéticos en el sector financiero del país. Esta estrategia tiene cinco pilares: fortalecer controles para la prevención de ciberdelitos, colaborar en proyectos para su prevención, crear mecanismos para intercambio seguro de información entre instituciones del sector, actualizar el marco regulatorio, y fomentar la cultura de ciberseguridad.

En noviembre del mismo año se presentó un esfuerzo amplio en colaboración con la OEA: la Estrategia Nacional de Ciberseguridad de México. Este esfuerzo cubre cinco objetivos: sociedad y derechos, economía e innovación, instituciones públicas, seguridad pública, y seguridad nacional. Para la eventual implementación de esta estrategia u otra similar será necesaria la definición detallada de iniciativas y la asignación de responsables para su implementación.

Una vez definida la estrategia nacional de ciberresiliencia es preciso asegurar que las políticas y regulaciones sobre información y tecnología existentes definan las obligaciones del gobierno, la sociedad y las instituciones privadas en su implementación, en donde se proteja la privacidad y la información de manera holística. Un marco legal analizado en su conjunto es un habilitador de la

[26] Estonia Ministry of Economic Affairs and Communication, *"Estonian National Cyber Security Strategy"*, enero 2014.

ciberseguridad nacional en cualquier país. Asimismo, debe estar enfocado en fortalecer la prevención de ciberataques y responder de manera correcta ante los incidentes.

Es necesario asegurar que los crímenes cibernéticos estén tipificados de manera clara y que la investigación y fiscalización de estas actividades delictivas sea eficaz. Los ciberdelitos abarcan una gran cantidad de conductas, desde afectaciones financieras y tecnológicas, hasta robo de identidad y trata de personas. Por un lado, tales conductas caen dentro de figuras legales tradicionales, como robo, falsificación o fraude, pero el uso de la tecnología para cometer el ilícito llevó a la necesidad de tipificarlas de forma específica.

La Directiva de Seguridad de Red e Información (Directiva NIS) es la piedra angular de la legislación de ciberseguridad en la Unión Europea, y establece obligaciones de seguridad cibernética para los operadores y proveedores de servicios digitales.

La regulación de ciberseguridad de la Unión Europea (UE) es buen ejemplo de un marco normativo robusto. La Directiva de Seguridad de Red e Información (Directiva NIS) es la piedra angular de la legislación de ciberseguridad en esta región, y establece obligaciones de seguridad cibernética para los operadores y proveedores de servicios digitales. Además, el Reglamento General de Protección de Datos (GDPR) realiza una importante revisión de la legislación europea con el objetivo de proteger la información. Las disposiciones clave imponen obligaciones de seguridad a los controladores y procesadores de datos personales y establecen obligaciones de notificación. Por último, la Directiva de Servicios de Pago 2 (DSP 2), una directiva sectorial, impone requisitos de ciberseguridad a los proveedores de servicios de pago, incluidos los bancos. Las organizaciones afectadas están obligadas a reportar incidentes de seguridad a los reguladores y a clientes cuyos intereses financieros estuvieran expuestos.

En el caso de México, existe un marco legal para la protección de datos personales cubierto principalmente por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (para organismos no gubernamentales) y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (para organismos gubernamentales). Este marco legal tiene como núcleo la obligación de toda entidad, que maneja datos personales, de establecer y mantener medidas de seguridad administrativa técnicas y físicas. Estas permiten proteger la información personal contra daño, pérdida, destrucción, uso, acceso o tratamiento no autorizado. El marco legal también especifica obligaciones de confidencialidad, que definen los casos específicos en los que se puede compartir información privada con otras entidades, y las precauciones debidas para esa transacción.

Para la implementación de medidas de seguridad de datos, los responsables deben considerar el riesgo existente, las posibles consecuencias para los titulares de los datos y el desarrollo tecnológico que se encuentre disponible. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), desarrolla y publica material para asistir a organismos que manejan datos personales, y así cumplir sus responsabilidades. Cualquier organización que no se apegue a este marco legal está sujeta a sanciones, pero estas pueden atenuarse si la autoridad considera que la organización siguió las recomendaciones del INAI.

El marco legal mexicano también tipifica el ciberdelito aunque de manera desconcentrada. Por

La complejidad tecnológica de los crímenes y su diversidad son factores que dificultan su persecución y eventual sanción.

su diversidad, estas conductas, en ocasiones están reguladas por códigos locales o federales, lo mismo que su persecución. La complejidad tecnológica de los crímenes y su diversidad son factores que dificultan también su eventual sanción. Los organismos claves de investigan y persiguen crímenes a nivel federal (la Policía Federal y la PGR) se han involucrado en el desarrollo de capacidades y en acuerdos colaborativos para enfrentar al cibercrimen.

Mecanismos de respuesta operativa

Para que el marco regulatorio y la estrategia en materia de ciberresiliencia sean operativos se requieren establecer los siguientes mecanismos: de defensa activa, de respuesta y de mitigación del impacto de ciberataques dentro de los organismos de gobierno, de recopilación y difusión de inteligencia, y de combate al cibercrimen. Dichos mecanismos deben incluir planes de contingencia de operación, comunicaciones, y manejo de reputación de las instituciones afectadas.

Los organismos del gobierno que gestionen infraestructura crítica, que manejen información privada de los ciudadanos, o que sean responsables de un proceso crítico, deben tener sus propios mecanismos de defensa y respuesta. Estos podrían colaborar con la solución de ataques sistémicos.

En conjunto, estos mecanismos deben poder identificar y prevenir riesgos cibernéticos, así como medir y mitigar el impacto de ciberataques exitosos, incluyendo la identificación de sistemas afectados y la evaluación de información extraída. Estos organismos también tienen como misión identificar cómo ocurrió el ciberataque (para evitar que se repita), investigar quién fue el ciberatacante detrás del incidente, y hacer cumplir la ley. Finalmente, como parte del plan de respuesta a ciberataques de alto impacto, estos organismos deben coordinar la estrategia de comunicaciones con la prensa y el público general, recomendar cambios necesarios a políticas y prácticas de organismos vulnerables, y asignar responsabilidades a otros organismos del gobierno.

Algunos países ya tienen organismos y procesos para mejorar su capacidad de respuesta ante ciberataques. Por ejemplo, Reino Unido cuenta con un Equipo de Respuesta ante Emergencias Informáticas (CERT) que coordina la ciberseguridad del país, enfrenta incidentes de importancia nacional, y proporciona consejos y alertas sobre riesgos cibernéticos. Malasia, por su parte, estableció CyberSci, un laboratorio con capacidad de análisis forense digital, así como recuperación de dispositivos y datos.

En México se han creado dependencias como el Centro Nacional de Investigación y Seguridad (CISEN), que genera inteligencia, táctica y operatividad para preservar la estabilidad e integridad del gobierno, incluyendo la mitigación de riesgos cibernéticos. También se estableció el CERT-MX dentro de la Policía Federal, con funciones y atribuciones similares a los CERTs de otros países. Para complementar las capacidades de ciberseguridad nacional, la Secretaría de Defensa Nacional (SEDENA) está en proceso de crear un Centro de Operaciones del Ciberespacio. Un listado completo de autoridades de respuesta a ciberataques se encuentra en la figura 13.

También se han establecido equipos enfocados a la respuesta a ciberataques dentro de algunos organismos que gestionan activos críticos. Por ejemplo, a principio del 2018, el Banco de México (Banxico) estableció la Dirección de Ciberseguridad como respuesta al ataque relacionado con el

Sistema de Pagos Electrónicos Interbancarios (SPEI). [27] Esta dirección tiene como objetivo proponer lineamientos y establecer políticas de seguridad para mantener resguardada la información que gestiona el organismo.

México puede mejorar la habilidad de respuesta a ciberataques incrementando la capacidad de organismos de respuesta existentes. También puede fomentar la creación de departamentos de ciberseguridad dentro de organismos públicos que gestionan activos y procesos críticos del estado.

Figura 13: Autoridades de respuesta a ciberataques

Autoridad	Mandato
Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas adscrita a la Agencia de Investigación Criminal	▪ Instancia de inteligencia encargada de la ejecución y supervisión de las acciones policiales que apoyen las investigaciones relacionadas con medios electrónicos y tecnológicos bajo la conducción y mando del Ministerio Público de la Federación.
Policía Federal, a través, de su División Científica, auxiliada, entre otras, por: ▪ Coordinación para la Prevención de Delitos Electrónicos ▪ Dirección General de Prevención de Delitos Cibernéticos ▪ Dirección General del Centro Especializado en Respuesta Tecnológica ▪ Dirección General de Tecnologías de Información Emergentes ▪ Dirección General de Laboratorios de Investigación Electrónica y Forense	▪ Organismo público enfocado a salvaguardar la vida, la integridad, la seguridad y los derechos de las personas, así como preservar las libertades, el orden y la paz públicos. Esto implica aplicar y operar la política de seguridad pública en materia de prevención y combate de delitos, prevenir la comisión de delitos, e investigar la comisión de delitos bajo el Ministerio Público de la Federación. ▪ Para lo anterior, la División Científica de la Policía establece mecanismos, lineamientos, políticas, protocolos y procedimientos para la aplicación de herramientas de naturaleza técnico-científicas. Selecciona e implementa tecnologías en los procesos y servicios de investigación de delitos electrónicos, criminalística, seguridad de la información y aquellos otros donde se necesite aplicar tecnología en las labores policiales. ▪ La Policía Federal también opera un Centro de Respuesta a Emergencias de Cómputo (CERT-MX), el cual realiza intercambio de información con agencias internacionales e identifica y da seguimiento a los delitos cibernéticos y a la protección de infraestructuras críticas en México.
Centro de Investigación y Seguridad Nacional (CISEN)	▪ Órgano desconcentrado de la Secretaría de Gobernación, cuyo propósito es operar tareas de inteligencia que contribuyan a preservar la integridad, estabilidad y permanencia del Estado Mexicano

FUENTE: Acuerdo A/076/17 por el que se crea la Unidad de Investigaciones Cibernéticas y Operaciones Tecnológicas, Ley de la Policía Federal y su Reglamento, Ley de Seguridad Nacional

Gestión de talento y tecnología

Como se mencionó, mantener la ciberresiliencia requiere del esfuerzo conjunto de empresas y organismos de gobierno. Para que las instituciones públicas y las organizaciones privadas hagan frente a estos ataques se requiere talento y tecnología. Sin embargo, existe una brecha entre oferta y demanda en este talento. Algunas organizaciones estiman un déficit mundial de 2 millones de profesionistas en ciberseguridad para el año 2019.[28] En México se pronostica que casi 148 mil puestos en tecnologías de redes no se podrán ocupar para el 2019; cerca de 36 mil de estos puestos de trabajo estarán relacionados con ciberseguridad.[29]

Para formar profesionistas capaces de cubrir esta brecha es importante incrementar la disponibilidad de programas educativos de calidad. Asimismo, es trascendental generar interés en los jóvenes, apoyarlos para que estudien carreras profesionales relacionadas y se especialicen. Por último, es posible emplear las asociaciones público-privadas para fomentar el desarrollo de empresas de

[27] Este incidente se discutirá a mayor detalle en la sección de sector privado.

[28] Estimado de Information Systems Audit and Control Association (ISACA), reportado en Forbes *"The Fast-Growing Job with A Huge Skills Gap: Cyber Security"* Marzo 2017

[29] *Brecha de 36 mil profesionistas de ciberseguridad estimada como el 49% de la brecha de 75 mil puestos de destrezas esenciales en materia de redes para México. A nivel Latinoamérica, 49% de la brecha de destrezas esenciales corresponde a ciberseguridad. Información de IDC, "Destrezas en materia de redes en América Latina", mayo 2016*

ciberseguridad fortaleciendo la disponibilidad de tecnología y talento en el país. Estas asociaciones también pueden funcionar como redes de soporte. Con esto se asegura que el gobierno pueda utilizar el apoyo técnico necesario para mantener su ciberresiliencia.

Un ejemplo de estrategia nacional de talento en ciberseguridad es la Federal Cybersecurity Workforce Strategy del gobierno de Estados Unidos, que busca mejorar la atracción y retención de talento en ciberseguridad. Como parte de la estrategia, el gobierno invirtió en expandir programas de educación de ciberseguridad en universidades; otorgó becas para carreras profesionales en el gobierno; rediseñó la estrategia de reclutamiento de talento de ciberseguridad de agencias gubernamentales; y diseñó trayectorias profesionales para expertos de ciberseguridad.

El sector público, el sector privado y la sociedad civil pueden colaborar en el desarrollo de talento de ciberseguridad. Un ejemplo al respecto es la colaboración entre la Information *Systems Audit and Control Association* (ISACA) –una ONG internacional de gobernanza de datos– y el *Malaysia Digital Economy Corporation* (MDEC), una entidad del gobierno de Malasia enfocada a impulsar la industria digital en el país. Bajo esta alianza, ISACA compartirá con MDEC su experiencia en capacitación y certificación en temas de ciberseguridad y gobernanza de datos para fortalecer la industria en Malasia.[30]

En México, algunas de las principales universidades, ya ofrecen maestrías o diplomados en seguridad cibernética (p.ej., UNAM, ITAM, ITESM, IPN, UNITEC). La Universidad Autónoma de Nuevo León (UANL) ofrece la Licenciatura en Seguridad en Tecnologías de la Información.[31]

Para complementar esta oferta académica, es importante asegurar que los programas se alineen con las necesidades del mercado. El gobierno y las asociaciones industriales de México también se beneficiarían de implementar estrategias integrales de desarrollo de talento de ciberseguridad. En el corto plazo, los organismos públicos y las empresas del sector privado tendrán que encontrar formas para atraer el mejor talento en el área a pesar de su escasez, lo que puede incluir la necesidad de flexibilizar límites y escalafones salariales.

Desarrollo y protección de infraestructura y sistemas críticos de datos

Aunque los mecanismos de respuesta a ciberataques descritos mejoren la capacidad del sector público para enfrentarse a incidentes que ya ocurrieron, es igual de crítico proteger los activos más importantes del gobierno y prevenir ataques sobre ellos. Para lograrlo es necesario identificar y determinar el ciberriesgo sobre los activos gubernamentales cruciales para la seguridad nacional, el funcionamiento del gobierno, la productividad del sector privado, y el bienestar de la sociedad en general. Esto incluye infraestructura y sistemas de datos, como las bases de identidad de los ciudadanos. Por lo general, los gobiernos designan como infraestructura crítica los sistemas de telecomunicaciones, sistemas financieros, infraestructura de energía, y de otros servicios públicos.

Una vez identificados los activos críticos es necesario hacer una evaluación sobre el grado de riesgo que corre cada uno, sobre las posibles acciones a tomar para incrementar su protección, y el costo o potenciales desventajas. Por ejemplo, maximizar el nivel de seguridad de los sistemas financieros podría repercutir en la conveniencia de los usuarios, y en la rapidez en el flujo de la información. Por último, se deberán diseñar e implementar los mecanismos y herramientas necesarias para proteger y vigilar los activos identificados buscando un balance entre la necesidad de incrementar seguridad y el costo de hacerlo.

[30] ISACA, *"ISACA and Malaysia Digital Economic Corporation Partner to Enhance Business Technology Professions"*, septiembre 2017

[31] Sitios web de universidades mencionadas (UNAM, ITAM, Tec de Monterrey, IPN UNITEC)

La ciberseguridad de infraestructura clave aún representa un reto para países avanzados en el tema, como Estados Unidos. En el 2017, el Departamento de Energía publicó un reporte indicando que la red eléctrica del país estaba en riesgo inminente de un ciberataque.[32] En respuesta, la Comisión Federal de Regulación Energética propuso una nueva normativa para la ciberseguridad de sistemas de control de redes eléctricas que entró en vigor a inicios de 2018.[33]

Otros países han buscado mejorar su entendimiento y experiencia sobre posibles ataques a infraestructura crítica a través de wargames, o juegos de guerra, que son simulaciones detalladas de un ciberataque en un ambiente controlado.

Otros países han buscado mejorar su entendimiento y experiencia sobre posibles ataques a infraestructura crítica a través de wargames, o juegos de guerra, que son simulaciones detalladas de un ciberataque en un ambiente controlado. En Locked Shields, un juego de guerra anual atendido por autoridades de ciberseguridad de países de la OTAN[34], se simuló la defensa ante ciberataques a sistemas eléctricos, redes de telecomunicaciones y bases aéreas, entre otros.

En México, la protección de infraestructura crítica se contempla en la Estrategia Nacional de Ciberseguridad del 2017. Más allá del marco estratégico y normativo, algunas agencias han detectado riesgos puntuales y están tomando acciones para enfrentarlos. Por ejemplo, el Instituto Nacional Electoral (INE) firmó un acuerdo con la Comisión Federal de Energía para colaborar con la continuidad del funcionamiento de la red eléctrica durante las elecciones de 2018.

Además de la infraestructura crítica, otro activo del sector público sujeto a posibles ciberataques son los sistemas de información personal de ciudadanos. Por ejemplo, distintos organismos públicos resguardan y utilizan información electoral, financiera, médica, y jurídica, entre otras. Existen dos tipos de ataques a los que estos activos están sujetos: el robo de la base de datos, y aunque de menor escala, pero alto impacto individual, la manipulación de bases de datos o falsificación de documentos que las avalan. Ambos permiten a los ciberatacantes cometer fraudes frente a organismos públicos y empresas, y exponen a ciudadanos al robo de identidad.

Como respuesta a problemas en bases de datos de identidad, registros para programas públicos con beneficiarios duplicados o fantasmas; India implementó el sistema de identificación biométrica Aadhaar. Consiste en un número de identificación que reúne datos personales[35] y biométricos[36] almacenado en una base de datos centralizada. El identificador Aadhaar es fácilmente verificable en línea, es costo-eficiente y robusto para eliminar los identificadores duplicados y falsos en bases de datos gubernamentales y privadas.

---

[32] Department of Energy, “Quadrennial Energy Review”, enero 2017

[33] La normativa en cuestión se titula *Critical Infrastructure Protection (CIP) Reliability Standard CIP-003-7 (Cyber Security – Security Management Controls)*

[34] Department of Energy, "*Quadrennial Energy Review*", enero 2017

[35] Nombre, teléfono, dirección, profesión, etc.

[36] Huella dactilar e iris del ojo.

Esta iniciativa reduce el riesgo de falsificación de documentos o manipulación de bases de datos, y le abre acceso a múltiples servicios a personas que previamente no contaban con identificación. Sin embargo, la integridad operacional y la protección de datos de la base única se torna prioritaria. El documento es crítico para todo tipo de interacciones entre personas y entidades del sector público y privado, lo que incrementa la probabilidad de un ciberataque y el impacto potencial del mismo.

México podría adoptar los beneficios vistos en el ejemplo de Aadhar a través de un sistema de identificación biométrico adicional o de la interconexión de sistemas de identificación existentes.

Hoy, México cuenta con tres sistemas principales de identificación personal: la Clave Única de Registro de Población (CURP), la credencial del Instituto Nacional Electoral (INE), y el Registro Federal del Contribuyente (RFC). La CURP es un código de identificación que se construye a partir del nombre completo del individuo, lugar, fecha de nacimiento y dígitos aleatorios para evitar duplicidad. Aunque la CURP cubre a la gran mayoría de la población, no integra información biométrica, lo que limita su uso como herramienta para validar la identidad de individuos. De los otros sistemas de identificación, la credencial para votar del INE tiene información biométrica del solicitante. Sin embargo, esta credencial sólo se emite para mayores de 18 años y no es obligatorio tramitarla, por lo que no cubre a toda la población. México podría adoptar los beneficios vistos en el ejemplo de Aadhar a través de un sistema de identificación biométrico adicional o de la interconexión de sistemas de identificación existentes.

Colaboración internacional para formular un marco multilateral

Nuestra información y operaciones dependen, cada vez más, de centros de datos de cloud computing a lo largo del planeta. De igual forma, los potenciales ciberataques a los que están expuestos el sector público, el sector privado, y la sociedad en México pueden ser perpetrados desde cualquier parte. Por esto es que la cooperación internacional en materia de ciberseguridad es clave para establecer estándares legislativos y de respuesta para la protección de dichos incidentes. La cooperación internacional también permite homologar estándares de seguridad y facilitar el intercambio de información para rastrear a ciberatacantes.

El Convenio de Ciberdelincuencia, también conocido como el Convenio de Budapest, es el primer tratado internacional sobre delitos cometidos a través de internet y otras redes informáticas. Se ocupa especialmente de infracciones sobre derechos de autor, fraude informático, pornografía infantil y violaciones de la seguridad de la red. Su principal objetivo es perseguir una política criminal común, dirigida a la protección de la sociedad contra el delito cibernético. Esto, mediante la adopción de una legislación apropiada y el fomento de la cooperación internacional por la naturaleza transnacional del tema. A la fecha, el Convenio de Budapest ha sido ratificado por 57 países, de los cuales, 14 no son miembros del Consejo Europeo, incluyendo Estados Unidos, Canadá, Chile, Costa Rica y República Dominicana.

En septiembre de 2006 México expresó al Consejo de Europa su deseo de adherirse a dicho Convenio, pero todavía no sucede. Aun así, México es parte del Convenio Iberoamericano de

Cooperación sobre Investigación y Aseguramiento de Prueba en Materia de Ciberdelincuencia de los Estados miembros de la Conferencia de Ministros de Justicia de los Países Iberoamericanos (COMJIB) desde 2014. Su objetivo es la cooperación para adoptar medidas de aseguramiento y obtención de pruebas en la lucha contra la ciberdelincuencia.

México ha participado en diversos foros internacionales de ciberseguridad[37], en donde ha establecido lazos de cooperación con otros países. No obstante, todavía hay potencial de fortalecerlos para incrementar la coordinación y cooperación entre naciones, incluyendo la participación en juegos de guerra y otros ejercicios colaborativos de ciberseguridad.

[37] Incluyendo foros de la Organización de los Estados Americanos (OEA) y la Cumbre de Líderes de América del Norte (NALS).

Resiliencia del sector privado

Riesgos cibernéticos enfrentados por el sector privado

El sector privado es el principal actor de la economía en México. En la mayoría de los países suele ser pionero en el desarrollo y adopción de tecnologías de la información. Este sector tiene una gran cantidad de activos de alto valor amenazados por riesgos cibernéticos.

Un ciberataque puede explotar vulnerabilidades en cualquier elemento de una empresa, desde sus sistemas hasta los comportamientos de su personal y usuarios. Existen dos tipos de riesgos cibernéticos: los que afectan a empresas específicas y los que tienen el potencial de afectar a un grupo de empresas que comparten el uso de sistemas.

Riesgos cibernéticos específicos o individuales

Un **ciberriesgo individual** es aquel que impacta de forma específica a una sola empresa o entidad. Por lo general, explotar uno de estos riesgos requiere un ataque dirigido. Es decir, los ciberatacantes necesitan identificar las vulnerabilidades específicas de una empresa o entidad y lanzar un ataque enfocado.

Los riesgos cibernéticos individuales pueden estar relacionados con vulnerabilidades en sistemas informáticos que aplican a una empresa específica. Los ciberatacantes identifican dicha falla y diseñan un ataque especializado para explotarla. Éste fue el caso de Equifax Estados Unidos, una agencia de reporte de crédito de los consumidores. Los *hackers* obtuvieron información confidencial de 143 millones de estadounidenses.[38] Los atacantes tuvieron acceso a un sitio web de soporte a cliente debido a que Equifax utilizó software desactualizado para esta plataforma.[39]

Otra empresa de tecnología, Yahoo, sufrió un ciberataque individual a sistemas que tuvo importantes repercusiones económicas. En diciembre de 2016, dicha empresa reveló que comprometieron su ciberseguridad a finales de 2013, y que la información de mil millones de cuentas fue robada.[40] En el momento del anuncio, Verizon Communications estaba en proceso de comprar Yahoo, y esta revelación redujo el precio final de venta por 350 millones de dólares.[41]

[38] The New York Times, *"Equifax Says Cyberattack May Have Affected 143 Million in the U.S."*, septiembre 2017.

[39] CNN Tech, *"How the Equifax data breach happened: What we know now"*, septiembre 2017.

[40] Forbes, *"Yahoo: Hackers Stole Data on Another Billion Accounts"*, diciembre 2016.

[41] Business Insider, *"Verizon tried to cut the price it's buying Yahoo for by $925 million but got rebuffed"*, marzo 2017

Los riesgos cibernéticos individuales también pueden estar relacionados con el personal de una empresa, y su capacidad para evitar ciberataques. Algunos atacantes lanzan campañas enfocadas en manipular al personal de empresas específicas. Esto se facilita si tienen acceso a información personal de empleados, o conocimiento detallado de los procesos internos de la empresa. En algunos casos, se tiene la colaboración de empleados actuales o exempleados, quienes cuentan con accesos o información privilegiada. Ejemplo de esto es el ataque que afectó a Ubiquiti, una empresa de tecnología. En este incidente, actores externos se hicieron pasar por empleados de la empresa para convencer al departamento de finanzas de realizar transferencias fraudulentas con un monto de casi 47 millones de dólares.[42]

Algunos atacantes también buscan infiltrar los sistemas de las empresas con el propósito de extorsionarlas. El objetivo es robar información confidencial y publicarla si la empresa no realiza un pago o cumple sus condiciones. Esto puede dañar severamente la imagen pública y los resultados financieros futuros de la organización. Basta recordar lo que ocurrió en Disney: un grupo de *hackers* robó una película y amenazó a la compañía con transmitirla si no pagaba el rescate. De manera similar se extrajeron películas, información personal de empleados y correos electrónicos de los servidores de Sony Pictures Entertainment, amenazando con publicarlos si la empresa no realizaba un pago. En una segunda etapa amenazaron a la compañía con un ataque físico en las salas de cine si se estrenaba la película *The Interview.* Las intenciones de estos grupos no siempre son económicas.[43]

Ataques sistémicos

Existen riesgos cibernéticos que no son específicos de una empresa y están relacionados con vulnerabilidades de sistemas utilizados por industrias enteras.

Existen riesgos cibernéticos que no son específicos de una empresa y están relacionados con vulnerabilidades de sistemas utilizados por industrias enteras. Estos ataques pueden provocar cierre de operaciones con un alto impacto operativo y perjudicial para miles de personas. A diferencia de las vulnerabilidades en empresas individuales, estos riesgos pueden ser explotados por distintos atacantes a lo largo del tiempo, sin tener una solución completa hasta que la vulnerabilidad se elimine por completo. Además, su naturaleza indiscriminada lleva a que estos ataques afecten tanto a empresas como a individuos.

Un ataque sistémico puede enfocarse en una vulnerabilidad de un sistema específico de una industria. En particular, el sistema financiero es un blanco atractivo para *hackers*, debido a su alta dependencia de sistemas electrónicos, y la sensibilidad de los datos que maneja. Un ataque en estos sistemas puede interrumpir transacciones bancarias y operaciones de pagos, o permitir a los atacantes robar recursos de bancos y clientes. Por ejemplo, el Banco Nacional de Ucrania declaró que varios bancos y firmas financieras del país se vieron afectados por un ataque de *malware*.[44]

El 27 de abril de este año, ciberatacantes aprovecharon la vulnerabilidad de algunos servidores de instituciones financieras conectadas al Sistema de Pagos Electrónicos Interbancarios (SPEI) para sustraer alrededor de 300 millones de pesos desde distintas instituciones financieras. Estos servidores reciben las órdenes de pago de los clientes y las preparan para ser enviadas al SPEI.

[42] Business Insider, *"Verizon tried to cut the price it's buying Yahoo for by $925 million but got rebuffed",* marzo 2017.

[43] Krebson Security, *"Tech Firm Ubiquiti Suffers $46M Cyberheist"*, agosto 2015.4

[44] New York Times, *"Sony Drops 'The Interview' Following Terrorist Threats",* diciembre 2014

Sin embargo, algunas instituciones no tenían actualizados sus sistemas de conexión, lo que fue identificado por los ciberatacantes. Estos crearon cuentas falsas para enviar instrucciones de pago fraudulentas por medio de un código malicioso. Al no identificar que las cuentas eran inexistentes, los bancos emisores transmitieron la información de las órdenes de pago al Banco de México a través del SPEI, como normalmente ocurre.

Cuando Banxico recibe la información de las órdenes de pago, transfiere el dinero de la cuenta de trabajo del banco emisor a la del banco receptor. Al recibirlo, el banco receptor lo deposita en la cuenta del beneficiario. Los que formaron parte del ciberataque retiraron el dinero a minutos de que fuera transferido logrando uno de los ciberataques más sofisticados que se hayan visto.

Al momento de identificar que existían fallas en los sistemas de algunas instituciones financieras, Banco de México migró las operaciones a un canal alterno de contingencia para retrasar las órdenes de pago y evitar que continuaran las transferencias fraudulentas. Esto provocó que muchas transferencias por internet de usuarios convencionales, sufrieran retrasos. Lo que refuta la suposición de que el retraso fue creado por los ciberatacantes a través de un ataque de denegación de servicio distribuido (DDoS), en el que se abruma el servicio en línea a través del tráfico de muchas fuentes provocando que deje de estar disponible.

Los ataques sistémicos también pueden dirigirse a programas o software de uso general incrementando aún más su potencial efecto. Un ejemplo reciente y con mayor impacto mundial fue *ransomware*[45] *WannaCry*, que comprometió la seguridad de más de 300,000 equipos en 150 países en mayo del 2017.[46] Este *ransomware* entraba a las redes cuando un usuario descargaba archivos infectados o hacía clic en un enlace malicioso. Se cree que el vector inicial de infección para WannaCry fue un correo electrónico de phishing con un PDF adjunto.

En general, la vulnerabilidad explotada por *Wannacry* se debe al uso de copias desactualizadas del sistema operativo Windows . Dos meses antes del ataque, Windows[47] publicó una actualización *(patch)* resolviendo esta vulnerabilidad. Pero la lenta adopción de empresas e individuos logró que el ataque fuera exitoso. Una de las instituciones afectadas fue el Servicio Nacional de Salud (NHS, por sus siglas en inglés) de Reino Unido: 45 de sus organizaciones fueron infectadas.[48] Hasta 70,000 de sus dispositivos, incluyendo computadoras, escáners de resonancia magnética, equipos de refrigeración de sangre y equipo de cirugía, sufrieron alteraciones.[49]

Otras instituciones importantes también fueron afectadas por el ataque de *WannaCry*, incluyendo FedEx, Telefónica, Deutsche Bahn, el Ministerio Interior de Rusia y Renault-Nissan. Al menos cinco fábricas, de ésta última, detuvieron o redujeron la producción de manera temporal por culpa del virus.[50] En México no hubo impacto sustancial; de acuerdo con Kaspersky Lab, una empresa de ciberseguridad, México fue el onceavo país más afectado por *WannaCry*, y el segundo en Latinoamérica.[51]

---

[45] Un programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción.

[46] The Telegraph, *"NHS cyber-attack: Everything you need to know about 'biggest ransomware' offensive in history"*, mayo 2017

[47] BBC, *"Windows 7 hardest hit by WannaCry worm"*, mayo 2017.

[48] UK National Audit Office, *"Investigation: WannaCry cyber attack and the NHS"*, abril 2017.

[49] The Times, *"Cyber-attack guides promoted on YouTube"*, mayo 2017.

[50] Business Insider, *"Renault-Nissan is resuming production after a global cyberattack caused stoppages at 5 plants"*, mayo 2017.

[51] El Economista, *"México, entre los más afectados por el malware WannaCry",* mayo 2018.

Aunque la propagación de este virus se detuvo por la detección de un kill switch dentro de su programación, este ciberriesgo sigue latente. Otros virus como *NotPetya* explotan la misma vulnerabilidad que *WannaCry* sin contar con un *kill-switch* o alguna forma de controlarlo. Las próximas amenazas pueden ser más dañinas, por ejemplo, *NotPetya* no libera los archivos del equipo aun cuando se paga la recompensa. Otros virus similares amenazan con publicar en internet la información encriptada.[53]

Agenda de resiliencia para empresas del sector privado

Para asegurar su operatividad y resultados financieros adecuados, todas las empresas del sector privado necesitan proteger sus activos vulnerables a ciberriesgos, y reaccionar de forma efectiva si sus defensas son penetradas y llegan a sufrir un ataque. La agenda de ciberresiliencia para el sector privado trasciende las funciones del CISO *(Chief Security Information Officer)* involucrando a la totalidad de los departamentos de las empresas. Por último, así como hay ciberriesgos de naturaleza individual y sistémica, la agenda de ciberresiliencia debe incluir iniciativas de empresas, así como esfuerzos interorganizacionales.

A continuación, presentamos una agenda de ciberresiliencia para el sector privado y las empresas que lo componen *(véase figura 14)*.

Figura 14: Agenda de ciberresiliencia para empresas del sector privado

FUENTE: Práctica de Riesgos de McKinsey

Las dimensiones de esta agenda son relevantes para la mayoría de las empresas que dependan de tecnología de la información en sus operaciones. Sin embargo, las iniciativas prioritarias para alcanzar la ciberresiliencia variarán entre empresas e industrias. Para determinar los próximos pasos se deben estimar varias dimensiones de la resiliencia actual de cada empresa; como el nivel de vulnerabilidad y riesgos, la efectividad de tácticas de prevención y respuesta que se tiene, y el grado de cooperación con organizaciones externas.

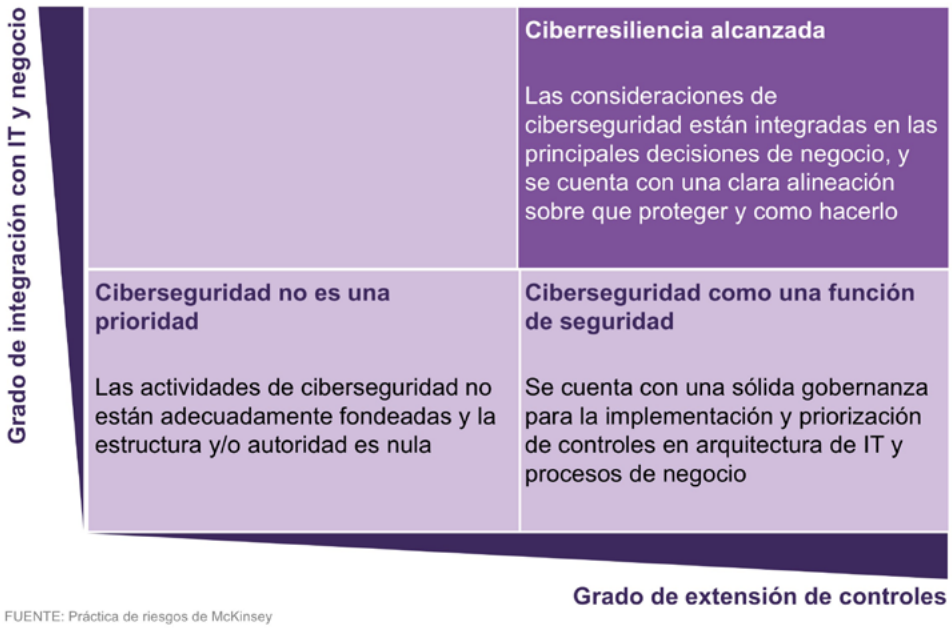
Gobernanza corporativa

Aunque las funciones de ciberseguridad de una empresa suelen estar enfocadas a la protección de sistemas de tecnologías de la información, la ciberresiliencia es un esfuerzo conjunto de los departamentos y de todo el personal de una empresa. Por esto es necesario asegurar que la ciberresiliencia se considere desde el nivel más alto de la compañía, y en todas las decisiones. Para

[53] The Guardian, *"WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017"*, diciembre 2017.

alcanzar el objetivo es necesario contar con una gobernanza corporativa sólida *(véase figura 15)*.

Figura 15: El rol de la gobernanza corporativa en la resiliencia digital



FUENTE: Práctica de riesgos de McKinsey

Existen diferentes arquetipos o modelos de gobernanza que deben adaptarse a las características de las organizaciones. Esto incluye atributos internos de la empresa; como su estructura organizacional y los sistemas de TI, y activos vulnerables a ciberriesgos que deben gestionar. Sin embargo, también debe considerarse el entorno de la organización, los requerimientos regulatorios de ciberseguridad que enfrentan, la industria en la que operan y su relación con tomadores de decisiones externos.

Dependiendo de las respuestas y otros factores relevantes, la organización podrá encontrar el modelo que se adapte a sus necesidades. Por ejemplo, en empresas pequeñas y medianas con ciberriesgos significativos, el CISO puede depender directamente del Director Ejecutivo de la empresa y colaborar con el CIO y CRO.[54] Al mismo tiempo, su equipo puede estar estructurado en torno a funciones, unidades empresariales, o geografías; dependiendo del origen de sus ciberriesgos.

En organizaciones más grandes, el CISO puede depender de la función del CIO o del CRO. Para empresas con alto nivel de ciberriesgos individuales y alta dependencia de sistemas o plataformas, el CISO dependerá y estará en estrecha coordinación con el CIO. En otras industrias, las empresas pueden tener al CISO como una función dependiente del CRO, sobre todo si enfrentan una mezcla variada de riesgos operativos.

En todos los casos, es necesario que las tres figuras (CISO, CIO y CRO) estén en constante coordinación, y que el CEO considere implicaciones de ciberseguridad en su proceso de toma de decisiones. Adicionalmente, los consejos directivos de las empresas pueden integrar a consejeros externos con experiencia en la materia para fortalecer su toma de decisiones.

Prevención y protección contra ciberriesgos

La principal defensa de una empresa contra ciberataques es una estrategia de prevención y protección contra ciberriesgos. El primer paso es identificar los principales riesgos a los que está expuesta una

[54] Chief Information Officer (encargado principal de información y sistemas) y Chief Risk Officer (encargado principal de control de riesgos)

empresa. Esta revisión deberá ser un proceso continuo porque los ciberatacantes frecuentemente descubren nuevas vulnerabilidades. La constante comunicación con otras empresas y organismos de ciberseguridad también puede ayudar a identificar posibles riesgos de forma más rápida.

Otra forma poco convencional pero altamente efectiva para identificar riesgos son los programas de recompensas para la identificación de vulnerabilidades *(bug bounties)*. Bajo esta modalidad, las empresas invitan a *hackers* para que encuentren fallas en sus sistemas, y les pagan cientos de miles de dólares por su identificación y reporte. Estos programas son utilizados por empresas de tecnología (como Apple, Microsoft o Google), pero también son empleados por organizaciones en otras industrias, como General Motors, Fiat Chrysler, Tesla, Lufthansa, Western Union, Starbucks, y el Departamento de Defensa de Estados Unidos.[55]

Después de identificar posibles riesgos se deben implementar los sistemas y procesos de control necesarios, priorizando la protección de activos de mayor valor y mayor exposición a ciberataques. Existen diversas herramientas y tecnologías que una empresa puede implementar para proteger sus sistemas, como programas anti-virus, encriptación de datos, y *firewalls*.[56] Otra alternativa es que las empresas aíslen sus activos críticos de amenazas a través del uso de virtualización de clientes. Bajo esta tecnología, los dispositivos individuales (llamados "clientes") no ejecutan programas críticos o guardan información valiosa, sólo conectan al usuario con una instancia virtual de un computador que está siendo ejecutado en un servidor central. Un virus que afecte a dispositivos que utilizan virtualización de cliente tienen un impacto limitado en los sistemas del resto de la empresa.

Otro elemento clave en una estrategia de protección contra ciberriesgos es el seguimiento consistente de procedimientos y protocolos de ciberseguridad. Uno de los procesos más relevantes es la actualización constante de todo el software utilizado por una empresa. También es importante controlar la instalación y uso de software no soportado por el departamento de sistemas. Por último, se debe limitar el acceso a activos y sistemas críticos al mínimo personal posible, y asegurar que estos tomen capacitaciones especiales sobre el tema.

El seguimiento consistente de estos procedimientos presenta diversos retos, en especial para empresas grandes que manipulan miles de dispositivos y múltiples activos de alto valor. Los empleados pueden mostrarse renuentes a actualizar su software si esto implica una interrupción o inconveniencia durante su horario laboral. Asimismo, las necesidades cambiantes de las empresas pueden llevar al departamento de sistemas a hacer excepciones y permitir la instalación de software no soportado en casos específicos. Para enfrentar estos retos es importante gestionar y auditar el seguimiento de procedimientos de ciberseguridad.

A pesar del uso de sistemas y procesos de ciberseguridad robustos es imposible eliminar por completo la exposición a ciberriesgos. Todos los empleados de una empresa con acceso a cualquier red o equipo necesitan mantener vigilancia continua; un error de un solo usuario puede exponer a toda la empresa. Para lograr esta vigilancia se requiere fomentar una cultura de ciberseguridad en todo el personal. Impulsando cambios de comportamiento en los empleados es posible cambiar de manera gradual la forma en que utilizan sus equipos, además de su capacidad para percibir y evitar riesgos *(véase figura 16)*.

[55] Financial Times, *"Big companies bring in cyber bounty hunters"*, noviembre 2017

[56] Un *firewall* es un sistema de seguridad de redes que monitorea y regula la entrada y salida de datos de una red.

Figura 16: Trayectoria para alcanzar cultura de ciberseguridad

FUENTE: Práctica de Riesgos de McKinsey

Por lo general, el cambio cultural sostenido ocurre a mediano o largo plazo. Si se intentan todos los comportamientos en poco tiempo existe el riesgo de sobrecargar de información. El esfuerzo de cambio cultural y de comportamiento debe estar alineado con la mitigación de los mayores riesgos humanos a los que la compañía se enfrenta para minimizar la vulnerabilidad a ciberataques. Los riesgos clave y los comportamientos más relevantes se pueden identificar a través de talleres de opinión. En suma, es importante reiterar los comportamientos aprendidos, para evitar que se pierdan.

Detección y combate de intentos de ataque

Las organizaciones del sector privado están asediadas a diario por una multitud de intentos de ataques dirigidos y no dirigidos. Es probable que algunos de ellos pudieran penetrar la primera línea de defensa y conseguir internarse en los sistemas de una empresa. Por lo tanto, la segunda función de ciberdefensa es detectar ataques incipientes de forma oportuna y prevenir un impacto generalizado.

Esta función es crítica porque –como en el caso de las enfermedades– la detección y eliminación temprana de un *malware* puede minimizar su impacto. Por ejemplo: el impacto de *ransomware*, que opera como *WannaCry*, en un solo computador es limitado, pero si se distribuye a sistemas críticos, el impacto puede frenar las operaciones de la organización.

Otro ejemplo son los ataques dirigidos a explotar una vulnerabilidad específica de los sistemas de una empresa. Algunas veces, estos tienen un impacto gradual que crece en el tiempo. Por ejemplo, la agresión sobre los sistemas de Yahoo en 2013 permitió el robo de información personal de usuarios que accedían a una dirección específica de correo requiriendo su transmisión gradual para ser exitoso.[57] En otras ocasiones, los ciberatacantes prueban las defensas de sistemas con golpes pequeños y difíciles de percibir en preparación de uno mayor. Éste fue el caso del ataque a sistemas de conexión de bancos con el SPEI. Desde octubre del 2017, seis meses antes del incidente, diversas instituciones financieras sufrieron embestidas de menor escala con características similares.[58]

Es importante implementar sistemas de detección de intentos de intrusión y asegurar su vigilancia continua por especialistas de ciberseguridad que cuenten con la capacidad y herramientas para aislar equipos y sistemas vulnerados. A través de esta implementación es posible presentar una segunda y tercera línea de defensa para atacantes que consiguieron acceso a la red general de la empresa.

[57] Bitdefender Labs, *"Unpatched WordPress Instance on Yahoo Blog Leads to Cookie Theft"*, enero 2013

[58] El Universal, "Bancos ignoran 5 hackeos anteriores", mayo 2018.

Además, es preciso llevar una bitácora de las amenazas cibernéticas que han ocurrido dentro de la organización y en toda la industria, para incrementar la capacidad de detección de nuevas amenazas. Por la velocidad de un ciberataque y su posibilidad de afectar a toda la empresa puede resultar retador para el personal de ciberseguridad y sistemas coordinar a tiempo la defensa. Resultará aún más complicado si ésta requiere involucrar otros departamentos encargados de la operación. Para enfrentar este escenario, se recomienda que las empresas desarrollen un *Cyber Common Operational Picture* (CyCOP), o Panorama Común Operacional. Este término (tomado de la teoría militar) representa una imagen única de la situación operativa compartida de los ciberriesgos y los intentos de ciberataque de una empresa entre todos los responsables de la seguridad de sistemas. El concepto puede extenderse a nivel industria con la creación de un CyCOP compartido entre los CISOs de sus principales empresas.

Cualquier sistema de detección de intrusiones está limitado por el elemento humano, es decir, por su capacidad de procesar información y actuar sobre ella. Así, aunque el CyCOP debe integrar toda la información relevante sobre ciberriesgos e integridad de sistemas, también necesita ayudar a sus usuarios a priorizar la información. Por ejemplo, si el algoritmo de alertas de intrusión no prioriza entre amenazas menores y mayores será difícil identificar cuándo existe un riesgo significativo para la empresa. Pero si es demasiado selectivo corre peligro de no alertar sobre una intrusión relevante. Encontrar este balance requerirá un conocimiento profundo de los activos prioritarios de la empresa y del panorama de ciberriesgos que enfrenta.

Respuesta frente a ataques exitosos

Es posible que los sistemas y procesos de protección y detección tengan fallas, o no estén diseñados para enfrentar el riesgo específico que se vulneró. Gran parte del impacto negativo de un ciberataque suele ocurrir en los días o meses posteriores a que se ejecutó de manera inicial, debido a la falta de respuesta de las empresas afectadas.

Así, una empresa ciberresiliente necesita tener la capacidad de responder de forma efectiva a un ciberataque para recuperar operaciones y minimizar el impacto sobre su reputación y situación financiera. En la mayoría de los casos es conveniente que la respuesta empresarial (por ejemplo, del departamento legal, de comunicaciones y de operaciones) sea tan contundente como la respuesta técnica (del departamento de TI y riesgos). Por eso se recomienda desarrollar planes de respuesta a incidentes que incluyan a toda la organización. *(véase figura 17)*

Figura 17: Ejemplo de plan de respuesta a incidentes

1 *Business Information Security Officer*, encargado de seguridad a nivel unidad de negocio.

El plan de respuesta debe iniciar con el control y tipología del incidente. Primero, el departamento de ciberseguridad necesita evaluar el alcance de daños y la información que fue vulnerada. El segundo paso es identificar la vulnerabilidad empleada por los ciberatacantes para irrumpir en el sistema, y recopilar información relevante sobre el ataque. Una vez identificada la vulnerabilidad en el sistema, el equipo de ciberseguridad debe enfocarse en contener la falla y resolverla para evitar ataques futuros. Mientras tanto, el departamento de sistemas o ingeniería debe ocuparse en recuperar la operatividad afectada por el ciberataque.

Como se mencionó, la respuesta a un ciberataque no debe limitarse a lo técnico. El equipo de riesgos y cumplimiento legal deben involucrarse y entender las implicaciones del ataque respecto a la regulación de protección de datos, y decidir si se debe informar a las autoridades (p.ej. CERT-MX). Por último, el equipo de riesgo y de comunicaciones deben determinar la forma y la audiencia del comunicado sobre el ataque; esto incluye a grupos industriales, empresas de software de seguridad, clientes y proveedores. La decisión es crítica porque no publicar información sobre un ataque puede proteger la reputación de una empresa en el corto plazo, pero representa un riesgo de mayor impacto en el futuro[59].

Para asegurar su relevancia y efectividad, los planes de respuesta a incidentes deben someterse a pruebas exhaustivas, simulando la urgencia y la ambigüedad de un ataque real. Los expertos en ciberseguridad de una empresa no enfrentan ataques continuos de alto impacto, pero podrían poner a prueba sus mecanismos de respuesta con juegos de guerra, descritos en el capítulo anterior. Este procedimiento involucra a participantes no sólo de seguridad de la información, sino también de infraestructura de TI, atención al cliente, operaciones, mercadotecnia, asuntos legales y gubernamentales, y comunicación corporativa. Con este ejercicio es posible desarrollar una memoria institucional de reacción que incrementa la efectividad del personal involucrado al enfrentar un ataque real. Los conocimientos adquiridos en el juego también permiten la actualización y mejora de los planes de respuesta.

Involucramiento interorganizacional

Como se vio en este capítulo, la capacidad de una empresa para proteger, detectar y responder frente a ciberriesgos depende de una acción temprana. Por la naturaleza sistémica de estos riesgos, la comunicación y cooperación en temas de ciberseguridad entre múltiples entidades incrementan la capacidad de prevenir posibles ciberataques apoyando el desarrollo de un ciberespacio seguro. Por último, las empresas que dependen de forma significativa de equipos y sistemas de terceros deben coordinarse con sus proveedores para asegurar que estos no introduzcan vulnerabilidades.

En México existen organismos de involucramiento interorganizacional del sector privado en materia de ciberseguridad. Uno ejemplo relevante y actual son las Bases de Coordinación en Materia de Seguridad de la Información, firmadas por 12 asociaciones gremiales del sector financiero, seis autoridades financieras, y la Procuraduría General de la República. Bajo este acuerdo, desarrollado a partir del ciberataque al SPEI, estos 19 organismos participarán en un Grupo de Respuesta Inmediata permitiendo la coordinación frente a futuros ciberataques al sistema financiero mexicano. Además, los signatarios se comprometen a establecer unidades de respuesta interna y a informar a las autoridades sobre ataques relevantes.[60] Siguiendo este ejemplo, las empresas mexicanas en otros sectores

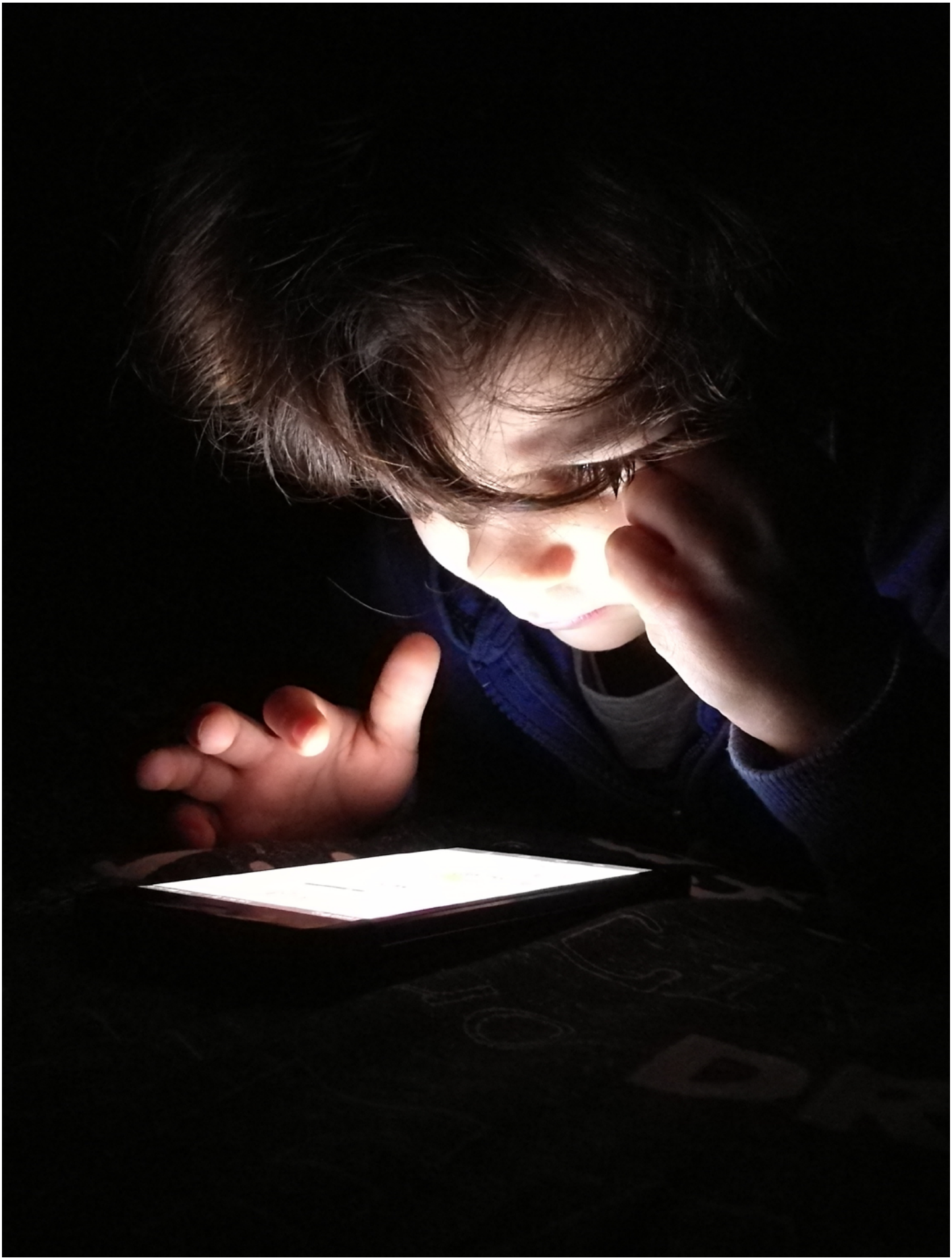
[59] Un ejemplo es el ciberataque a Yahoo que comprometió la información de 500 millones de cuentas de usuarios en el 2014. El ataque se descubrió en el 2016, causando que varios senadores de EE.UU. dirigieran una carta a la empresa denunciando la lentitud de su respuesta y pidiendo una audiencia para explicar las condiciones del ataque; The Guardian, *"Senators call Yahoo's delay in revealing breach of 500m accounts 'unacceptable'",* septiembre 2016.

[60] Comisión Nacional Bancaria y de Valores, *"Comunicado Conjunto, Bases de coordinación en materia de seguridad de la información"*, mayo 2018.

pueden formar acuerdos de cooperación y con las autoridades de su área.

También se han desarrollado interacciones entre jugadores locales e internacionales. Por ejemplo, en febrero del 2017, Microsoft firmó un acuerdo con la Policía Federal de México para lanzar un Centro de Ciberseguridad. Esta iniciativa tiene como objetivo proteger, detectar y responder a posibles riesgos. Además, tiene como objetivo reforzar la seguridad operacional y contribuir con el desarrollo de la región. [61]

[61] Microsoft Corporation, *"Microsoft abre Centro de Ciberseguridad para la protección de los mexicanos",* febrero 2017



Resiliencia de la sociedad

Ciberriesgos enfrentados por la sociedad

El uso de las tecnologías de la información en una gran parte de las actividades de la sociedad desencadenó nuevos riesgos para individuos y comunidades. Estos impactan la operación de organismos públicos y privados, el bienestar de la sociedad, y la forma en que las personas perciben el mundo y toman decisiones.

Riesgos individuales o específicos

El ciberespacio permitió que grupos e individuos malintencionados atenten en contra de personas vulnerables. Gran parte de la población está expuesta al riesgo por el uso intensivo de las tecnologías de la información, y porque empresas y organismos que nos ofrecen servicios también las utilizan.

Algunos riesgos individuales afectan, en su mayoría, a grupos vulnerables específicos. Por ejemplo, el *cyberbullying* (o ciberacoso) afecta en mayor medida a niños y adolescentes. Los resultados psicológicos y emocionales son parecidos a los del acoso escolar tradicional. Sin embargo, éste suele terminar cuando el alumno regresa a su casa; mientras que el ciberacoso puede continuar todo el día.

En México, más de 25% de mexicanos entre 12 y 19 años reportan haber sido víctimas de ciberacoso, de acuerdo con estadísticas del INEGI. El riesgo es aún mayor para las niñas y mujeres en este rango de edad, ya que 28% lo ha padecido. Las estadísticas revelan que este fenómeno en México toma múltiples formas: llamadas, mensajes, contenido multimedia, robo de identidad y publicación de información personal. El común denominador de estos ataques suele ser el anonimato; casi 80% de los jóvenes que sufrieron ciberacoso indican no conocer la identidad de su atacante.[62] El impacto de este delito no debe ser subestimado; cerca del 60% de suicidios entre adolescentes en México están vinculados con diversos tipos de *bullying*, incluyendo el ciberacoso.[63]

El espacio cibernético también puede facilitar la comisión de crímenes que afecten a grupos vulnerables. La *Dark Web* es un segmento del ciberespacio donde se pueden realizar transacciones de forma anónima a través del uso de programas especializados llamados *Darknets*. Estas redes suelen ser utilizadas por grupos e individuos que buscan realizar actividades ilícitas y de ciberespionaje.

[62] INEGI, *"Módulo sobre ciberacoso MOCIBA 2015: principales resultados"*, 2016

[63] Congreso de la Unión, *"El Bullying o Acoso Escolar, Estudio Teórico conceptual, de Derecho Comparado, e Iniciativas Presentadas en el Tema",* Noviembre 2016.

Algunas afectaciones: compraventa de información personal robada, trata de personas y explotación infantil, entre otras.

Los ciudadanos también pueden enfrentar el robo de su información personal como resultado de un ataque a una empresa u organismo público, o a través de un ataque a su sistema personal. Cualquiera con un perfil en redes sociales u otro portal en el ciberespacio debe ser cuidadoso sobre la información que publica, y debe saber que una gran cantidad de individuos tendrá acceso a sus datos. No tener certeza de quién puede revisar la información individual puede poner en riesgo la seguridad personal. Por ejemplo, en 2012 Facebook estimó que existían 83 millones de perfiles falsos o duplicados en su plataforma; para 2017 declaró que este número creció a 270 millones de cuentas .

Los individuos no sólo deben proteger su información personal en línea; también son responsables de cuidar la de sus contactos. Un incidente encabezado por la firma de análisis de datos Cambridge Analytica ilustra la importancia de esta responsabilidad. En el 2015, un asociado de esta empresa lanzó una aplicación que encuestaba a usuarios de Facebook para uso presuntamente académico. Aunque menos de 300,000 personas bajaron la aplicación se recopilaron datos de 87 millones de usuarios. [65] Al aceptar los términos de uso, las 300,000 personas autorizaron el uso de la información de sus amigos. Este caso puso en discusión si estos usuarios tenían derecho sobre la información de sus contactos.

Los individuos también pueden ser víctimas de intimidación o espionaje por su trabajo o afiliación política. De acuerdo con una investigación de Amnesty International –una ONG global de derechos de humanos– redes de *trolls*[66] en México han ejecutado campañas de intimidación, desinformación y acoso contra periodistas y activistas. Estas pueden llegar a incluir amenazas de muerte. En otro episodio, 21 personas - políticos, burócratas, periodistas y activistas - fueron víctimas de ciberespionaje a través del *spyware*[67] Pegasus, de acuerdo con una investigación del *Citizen Lab* de la Universidad de Toronto y del New York Times. [68]

Riesgos grupales o a nivel sociedad

La libre publicación y acceso a información en la red fortalecen la libertad de expresión y transparencia. Sin embargo, también abren la puerta a la desinformación, y para los individuos cada vez es más difícil distinguir entre verdad y mentira. La propagación de información falsa, y la capacidad de manipular percepciones y acciones de la comunidad representan un **ciberriesgo a nivel sociedad.**

Una campaña de desinformación puede manifestarse de manera orgánica como un rumor a través de las redes sociales. Pero también puede ser obra de un ciberatacante manejando fuentes de información dedicadas a publicar noticias falsas *(fake news)*. De acuerdo con los análisis del Oxford Internet Institute, citados en el *Munich Security Report 2017,* en las elecciones presidenciales estadounidenses de 2016 una gran cantidad de noticias falsas fueron distribuidas por medio de redes sociales. Por ejemplo, en el día de la elección, los usuarios de Facebook interactuaron más con noticias falsas que con noticias de fuentes validadas *(véase figura 18)*.

[64] The BBC, *"Facebook has more than 83 million illegitimate accounts"*, 2012; Telegraph, *"Facebook admits up to 270m users are fake and duplicate accounts"*, 2017.

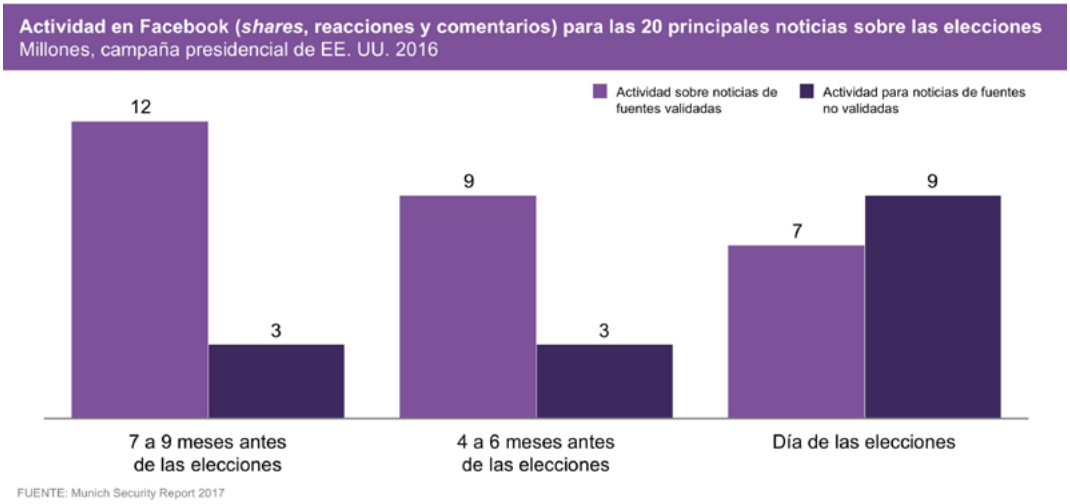
[65] Fortune, *"Facebook Cambridge Analytica Scandal: 10 Questions Answered"*, abril 2018.

[66] Individuos dedicados a acosar, ofender y provocar a individuos o grupos en redes sociales, generalmente de forma anónima.

[67] Un tipo de virus enfocado a recopilar información sobre usuarios del aparato infectado, que puede incluir registros de uso, video y audio del usuario, etc.

[68] El Economista, *"¿Quiénes han sido espiados con Pegasus en México?"*, agosto 2017

Figura 18: Interacciones de Facebook durante las elecciones presidenciales de EUA en 2016



Otra herramienta muy efectiva para manipular la percepción pública son los bots. Estas cuentas automatizadas en redes sociales pueden utilizarse para distribuir noticias falsas o publicar comentarios de forma masiva alterando la percepción de la realidad de los usuarios. La robusta cobertura de prensa sobre cómo los bots fueron clave para incidir en la percepción de las personas durante las elecciones estadounidenses de 2016 son evidencia de este fenómeno. Más del 20% de los tweets relacionados con campañas políticas provenían de cuentas automatizadas.

En el caso de México, grupos de acosadores *(o trolls)* emplean una combinación de bots y cuentas administradas por sus miembros para impulsar mensajes de violencia y miedo colectivo en plataformas como *Twitter.* De acuerdo con un análisis de Signa Lab, un laboratorio multidisciplinario del Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO), el *trending topic*[69] "#SaqueaUnWalmart" surgió como una campaña coordinada de uno de estos grupos para elevar el descontento social a partir del incremento de precios de la gasolina en el 2017. [70]

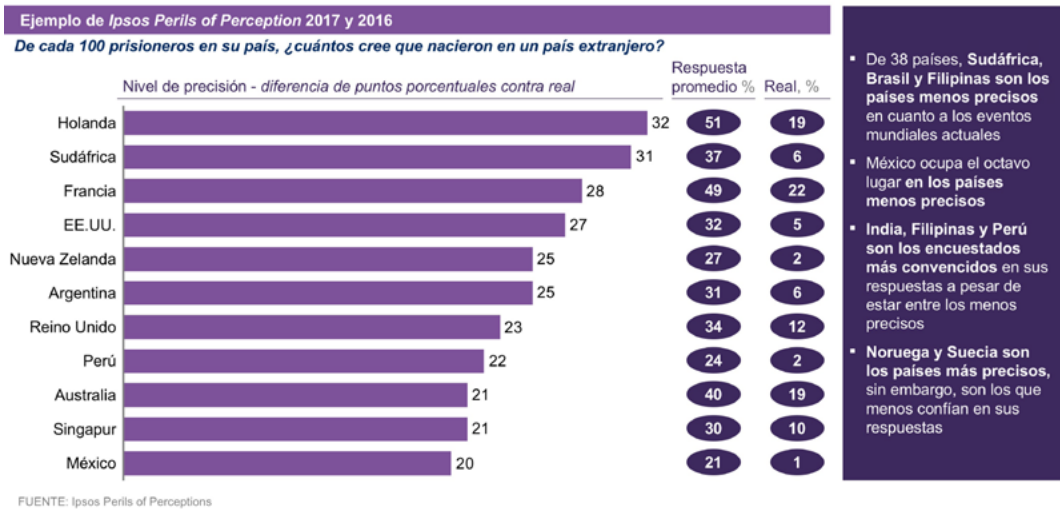
La desinformación en redes sociales –intencional o no– modifica la forma en que el público percibe el mundo a su alrededor. La encuesta de *Ipsos Perils of Perception*[71] 2017, aplicada en 38 países entre el público que navega en internet, señala las percepciones equivocadas que se tienen sobre los problemas mundiales. Por ejemplo, en temas como muertes por terrorismo, o embarazos adolescentes, la situación no es tan grave como los individuos la perciben *(véase figura 19).*

[69] En Twitter, un trending topic es un tema que tiene un incremento significativo en popularidad de forma repentina. Los más compartidos aparecen en la página principal de Twitter.

[70] Signa Lab, *"Del #Gasolinazo a #SaqueaUnWalmart: Mapeando la batalla en línea durante la crisis gasolinera en México"*, febrero 2017

[71] Encuesta sobre la diferencia entre la percepción pública y la realidad en torno a problemáticas y temas controversiales.

Figura 19: Ejemplo de resultados de Perils of Perceptions



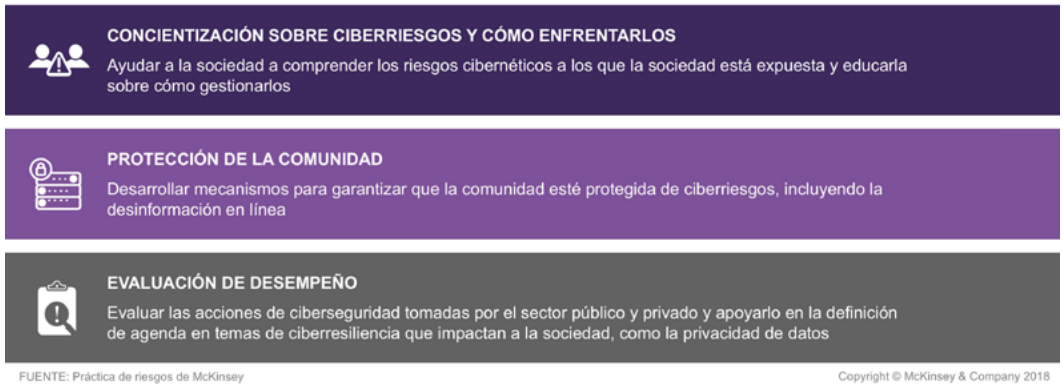
Los errores de percepción pueden afectar la toma de decisiones de los ciudadanos y, en algunos casos, incitar actos violentos. En el año 2015, en Ajalpan, Puebla, lincharon a dos encuestadores porque vía Facebook se advirtió a la comunidad sobre supuestos secuestros de jóvenes y se solicitaba reportar personas sospechosas. De acuerdo con el secretario municipal de Ajalpan, el ajusticiamiento estuvo relacionado, en parte, por la distribución irresponsable de información falsa en la red social.[72]

Agenda de resiliencia de las asociaciones civiles

A diferencia de los otros sectores analizados, la sociedad está compuesta por individuos y no por organizaciones. Aunque cada ciudadano tiene responsabilidades respecto al uso de tecnologías de la información, implementar una agenda coordinada de ciberresiliencia de la sociedad recae en las asociaciones civiles. Para lograr este objetivo, los organismos necesitarán apoyarse en la colaboración del sector privado y público, y en el compromiso de la ciudadanía por un México resiliente a ciberataques.

Presentamos una agenda de ciberresiliencia para asociaciones civiles. El propósito es delinear los esfuerzos que ONGs y otras entidades pueden realizar para incrementar la resiliencia de la sociedad mexicana *(véase figura 20)*. Para cada uno de los temas se presentan ejemplos de los logros en países líderes en el área de ciberseguridad, y avances en nuestro país.

Figura 20: Agenda de ciberresiliencia de las asociaciones civiles



[74] Associated Press, *"In frightened Mexico town, a mob kills 2 young pollsters"*, octubre 2015

Concientización sobre ciberriesgos y cómo enfrentarlos

La sociedad debe crear consciencia sobre los ciberriesgos existentes. Las personas están expuestas a múltiples peligros, pero su conocimiento sobre estos suele ser limitado. Además, los ciudadanos tienen poca información sobre cómo prevenir o enfrentar un incidente.

El primer paso para generar consciencia y preparación pública sobre los ciberriesgos es identificar a grupos vulnerables que pueden convertirse en víctimas de ciberataques. Después, la sociedad civil en conjunto con el sector público y privado pueden desarrollar campañas específicas y personalizadas otorgando las herramientas para prevenir y enfrentar los ataques a los que están más expuestos.

Las campañas de cultura cibernética y de concientización comunitaria deben tomar en cuenta las diferencias formativas de las audiencias a las que se dirigen. Esto con el objetivo de adaptar la comunicación a los valores específicos de cada grupo. Es recomendable concentrarse en una o dos iniciativas de comportamientos por trimestre. Para evitar el abandono de buenos hábitos, y mantener informada a la comunidad se requiere tener comunicación continua con la audiencia meta a través de redes sociales u otros medios masivos.

Adicionalmente, se recomienda que estas campañas incluyan otros contenidos relevantes, como la higiene digital, un concepto que incluye buenas prácticas como el uso apropiado de contraseñas y la escritura adecuada de correos electrónicos, con el propósito de facilitar al receptor distinguir entre correos auténticos y correos de *phishing*. Otro concepto relevante para una campaña de concientización es el civismo digital, o las reglas a seguir para ser un buen ciudadano cibernético. Bajo este concepto, se le pide a los individuos reportar comportamiento sospechoso que observen en las redes, evitar compartir cadenas de correo (conocido como *spam*) y noticias de fuentes no fidedignas, y evitar participar en el *cyberbullying*.

En algunos de los países líderes en ciberseguridad, el proceso de concientización sobre ciberriesgos comienza desde temprana edad. Por ejemplo, en Estonia, los programas educativos para educación básica, media y superior contemplan materiales de educación en ciberseguridad. La sociedad civil complementa esfuerzos a través de programas adicionales. Por ejemplo, la Fundación de Tecnología de la Información para la Educación (HITSA) es la principal fuente de capacitación y diseño de campañas de sensibilización, y programas dirigidos a niños desde edad preescolar.

La Campaña Ciberseguridad México 2017 de la Policía Federal está enfocada en mejorar el manejo de datos personales, prevenir el cyberbullying y evitar la distribución de noticias falsas, entre otros temas.

En México existen esfuerzos para concientizar a la población en normas de ciberseguridad y de buen comportamiento en las redes: la "Campaña Ciberseguridad México 2017" de la Policía Federal está enfocada en mejorar el manejo de datos personales, prevenir el *cyberbullying* y evitar la distribución de noticias falsas, entre otros temas.[73] La Fundación RSI donó contenido educativo digital para proteger a la población infantil en el Internet. Éste es un ejemplo del rol que las Asociaciones Civiles pueden tomar en el tema.[74]

[73] El Universal, "Lanzan campaña de ciberseguridad", marzo 2017

[74] Fundación RSI, "Fundación RSI y CNS por la ciberseguridad infantil de México", marzo 2017

Para fomentar la cultura de ciberseguridad en la población, el gobierno y la sociedad civil pueden incrementar el alcance de programas de concientización sobre ciberriesgos, e integrarlos a la educación pública y privada desde nivel preprimaria.

Protección de la comunidad

El segundo papel que puede desempeñar la sociedad es el de proteger a la comunidad de ciberriesgos. Por ejemplo, las instituciones académicas podrían colaborar con el sector público y privado en las funciones de investigación de amenazas y análisis forense de ataques previos. Asimismo, las asociaciones civiles pueden proteger a la sociedad de campañas de desinformación y rumores en las redes sociales. Esto se puede lograr realizando un catálogo de fuentes confiables en línea, o revisando de forma puntual la veracidad de las principales noticias y tendencias en redes sociales.

Distintas asociaciones civiles han tomado un rol activo protegiendo a la sociedad de ciberriesgos. Un ejemplo es la Cybersmile Foundation, una ONG internacional enfocada a combatir el *cyberbullying*. Además de dirigir campañas de concientización sobre el tema, Cybersmile Foundation ofrece apoyo y asesoría a víctimas de *cyberbullying* a través de profesionistas entrenados en el tema.

Otras asociaciones civiles se han enfocado en proteger a la sociedad del riesgo de las *fake news*. Por ejemplo, en Lituania se creó una red ciudadana de personas interesadas en enfrentar información falsa con información verídica, conocida como *elves* (duendes). Otra solución a este problema es *Tribeworthy,* una app que permite a los usuarios clasificar cada artículo de noticias por su nivel de confiabilidad. El programa también compila el promedio de calificaciones de los artículos para asignar a cada publicación un nivel de confiabilidad promedio.

En México, ya existen organismos civiles que buscan cumplir el rol de discernir entre información real y falsa. *Verificado 2018* es una iniciativa creada con el propósito de combatir noticias falsas y la manipulación de los datos en torno a las elecciones del 2018. Este organismo tiene el apoyo de casi 60 medios de comunicación y organizaciones civiles incluyendo universidades. Otro ejemplo es Signa Lab del ITESO, que protege a la sociedad civil a través de investigación y vigilancia de las actividades de grupos de acosadores en línea *(trolls)*.

La sociedad civil en México puede continuar ofreciendo servicios para proteger a ciudadanos de los ciberriesgos que enfrentan, como el *cyberbullying*, campañas de desinformación en línea, y el robo de identidad e información personal.

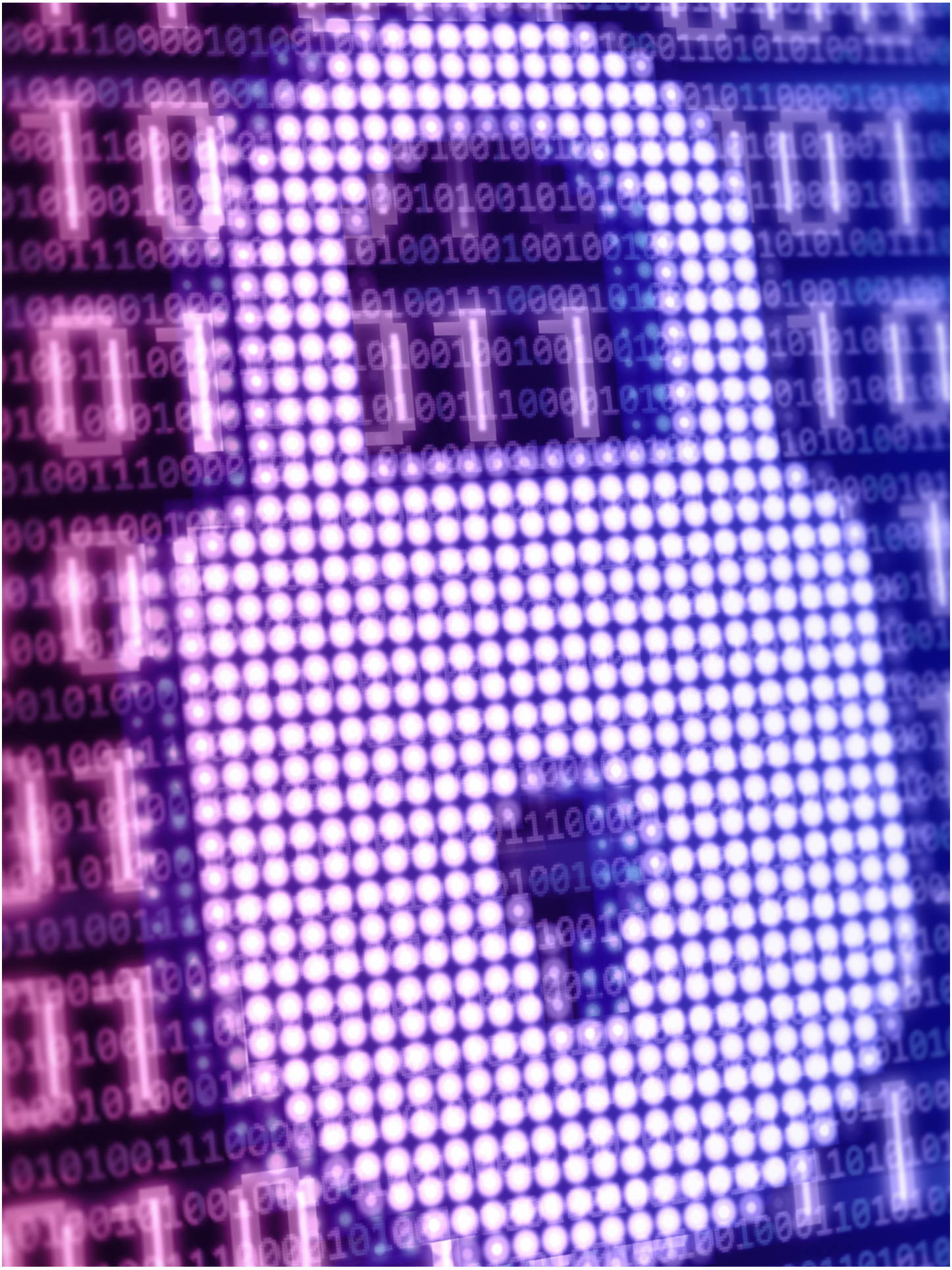
Evaluación de desempeño

Las organizaciones civiles y las personas pueden vigilar y opinar sobre las acciones de los gobiernos para asegurar que cumplan su rol de proteger a la comunidad de riesgos cibernéticos. Además, la sociedad civil puede tomar un rol de auditor con las empresas privadas asegurando que sus prácticas protejan la información de los usuarios y combatan la diseminación de noticias falsas.

Como primer paso para lograr estas metas se debe fomentar la comunicación abierta y transparente entre la sociedad, organizaciones civiles que se ocupan de temas de ciberseguridad, empresas que manejan datos privados de usuarios, y gobierno. Para conseguirlo se puede motivar la participación de la sociedad en decisiones nacionales de ciberseguridad a través de herramientas en línea, y foros de opinión sobre el tema. Otra medida posible es incluir a ciudadanos, con conocimiento relevante, en consejos consultivos que apoyen a las entidades encargadas de ciberseguridad.

Un ejemplo de ONG global que juega un rol de vigilancia sobre las acciones de gobiernos y empresas es Privacy International. Esta organización vigila los derechos de privacidad y protección de datos de ciudadanos en el mundo. Por ejemplo, tuvo un rol activo en la revisión y rondas de discusión sobre el borrador de ley del *General Data Protection Regulation* (GDPR). Asimismo, ha trabajado con empresas para mejorar sus prácticas en esta materia. De acuerdo con la organización, estos esfuerzos llevaron a cambios en las políticas de privacidad de algunas de las mayores empresas de tecnología.[75]

[77] Privacy International, *"Striking Silicon Valley at Formative Moments"*, revisado en 2018.



Conclusión

Los riesgos del ciberespacio para la sociedad

Vivimos en un mundo tecnológico que define la forma en la que interactuamos y llevamos a cabo nuestras actividades diarias, como individuos y como sociedad. Las tecnologías de información se han vuelto un motor de productividad y han facilitado las actividades de la vida diaria para más de 80 millones de internautas en México. Esto se ha traducido en beneficios significativos para el sector público, para el sector privado y para la sociedad en general.

Para el sector público la tecnología ha promovido mayor interconexión y cooperación entre sus instituciones. Además, ha favorecido una comunicación más cercana con los ciudadanos y procurado mayor acceso a servicios públicos. Para el sector privado, la tecnología ha potenciado la productividad y favorecido el desarrollo de nuevos modelos de negocio. Para la sociedad en general, la tecnología ha significado un incremento radical del acceso a la información y la interconexión entre individuos tanto nacional como internacionalmente, lo que ha facilitado la transparencia y permitido un activismo político y social a un nivel jamás imaginado. Sin duda, hoy existe mucho mayor acceso a material educativo para todo el que quiera encontrarlo y utilizarlo.

El valor que el ecosistema tecnológico ha creado para la sociedad también conlleva una serie de riesgos que se tornan críticos en el contexto de la alta interdependencia entre organizaciones, individuos y los sistemas que soportan sus interacciones. El sector público, el sector privado y la sociedad están expuestos a ciberriesgos que se pueden materializar en ataques dirigidos, afectando a personas y organismos específicos, así como ataques no dirigidos, con impacto en sistemas enteros y grupos amplios de usuarios.

Por un lado, el sector público enfrenta ciberriesgos críticos asociados al resguardo de la información de los ciudadanos, a la integridad de la infraestructura gestionada por el gobierno, y a la confiabilidad y reputación de las instituciones gubernamentales. Por otro lado, como actor principal de la economía, en el sector privado los riesgos se presentan en empresas individuales o en sistemas a través de varias compañías e industrias.

Por último, la sociedad en general enfrenta grandes desafíos en el contexto de la libertad de expresión, y la manipulación de las percepciones y acciones de los individuos. Aunque las tecnologías de la información han fomentado la intercomunicación ciudadana, también en ocasiones se ha complicado la movilización hacia la acción debido a la naturaleza multidimensional de los problemas relacionados con el ciberespacio, y debido a la interferencia de ciberatacantes. En términos de transparencia, al mismo tiempo que ha dado una plataforma para mayor visibilidad, al multiplicar exponencialmente las fuentes de información y contenido, también ha enturbiado la verdad objetiva. Hoy coexisten, lado a lado, fuentes de muy variada veracidad y rigor periodístico, sin que exista una referencia objetiva sobre la calidad de su contenido.

Ejes potenciales en la agenda de ciberresiliencia en México

En el contexto de una sociedad interconectada y dependiente de la tecnología, surge la necesidad de desarrollar una agenda holística que fomente la ciberresiliencia en el sector público, en el privado, y en la misma sociedad, a través de diversos ejes clave.

En el sector público la agenda de resiliencia ha mostrado avances en su consolidación, pero podría explorar mayor robustecimiento. En temas de gobernanza se podría otorgar más poder y relevancia a la actual Estrategia Nacional de Ciberseguridad (ENCS) mediante la creación de una agencia nacional dedicada a este objetivo. Para reforzar el marco normativo podría trabajarse en una mejor y más clara tipificación del ciberdelito, la cual hoy se encuentra fragmentada en códigos locales y federales.

Por su parte, la existencia del Centro Nacional de Investigación y Seguridad (CISEN), el establecimiento de la Dirección de Ciberseguridad en el Banco de México y la creación del CERT-MX dentro de la Policía Federal, muestran avances en los mecanismos de respuesta nacional. Además, podrían replicarse a profundidad estas experiencias a nivel estatal y en otras dependencias clave para asegurar que las entidades disponen de capacitación adecuada y puedan colaborar efectivamente entre ellas.

En el sector público, en cuanto a gestión de talento, existe una gran oportunidad de alinear la demanda de nuevos roles con la oferta mediante el fomento de programas y carreras enfocadas a la ciberresilencia. Se puede integrar un plan para formar a las nuevas generaciones de expertos en el tema de ciberseguridad mediante una coordinación profunda con el sector educativo del país. Asimismo, se necesitarán esquemas que permitieran contratar en el corto plazo al talento de clase mundial para hacer frente a los temas de ciberseguridad en los gobiernos. El objetivo es permitir que este recurso humano, con alta demanda global, pueda tener cabida dentro de los escalafones rígidos de sueldo de los gobiernos federal y locales.

Además, para complementar los esfuerzos de protección de la infraestructura y sistemas críticos, como el acuerdo entre el INE y la CFE que asegura continuidad eléctrica durante las elecciones, se debe seguir el objetivo establecido en la ENCS de consolidar un marco normativo para la protección de estos elementos a nivel nacional. Por último, para participar en la colaboración internacional se

podrían extender esfuerzos ya realizados en foros regionales, y cumplir con la adhesión al Convenio de Ciberdelicuencia de Budapest, una aspiración establecida en 2006.

La agenda de ciberresiliencia del sector privado también puede robustecerse en diversos elementos. En la gobernanza se puede explorar la consolidación de estándares que fomenten estructuras organizacionales a nivel industria que reconozcan la relevancia de la ciberresiliencia, estableciendo roles como el CISO *(Chief Information Security Officer)* y el CRO *(Chief Risk Officer),* así como la incorporación en los consejos directivos de consejeros independientes con experiencia en el tema. Para asegurar la efectividad de estos roles, las empresas el sector privado necesitarían invertir en la contratación de personal calificado en ciberseguridad, independientemente de su costo comparativo.

Aunado a esto, para la prevención y protección oportuna contra ataques, las empresas pueden trabajar en la detección, la priorización y el establecimiento de controles en activos críticos, mediante auditorías exhaustivas y métodos más innovadores como competencias abiertas de detección de vulnerabilidades *(bug bounties)*. El esfuerzo se puede complementar con el fomento de una cultura organizacional que mitigue el riesgo operativo asociado con el ciberespacio. En última instancia, la mayoría de los ataques que más llaman la atención tienen como raíz común una falla humana.

La agenda del sector privado puede considerar también el desarrollo de una plataforma o herramienta con una perspectiva única de los esfuerzos de ciberresiliencia. Esto se debería procurar dentro de una empresa y entre empresas de una industria, con el objetivo de tener con una visión consolidada sobre los esfuerzos, los controles y los ataques, y así poder desarrollar un panorama común operacional (conocido como *Cyber Common Operational Picture*).

Para obtener una respuesta adecuada ante ataques exitosos, es importante fomentar el desarrollo de protocolos, acciones y decisiones que consideren a todas las áreas de una empresa, y ponerlos a prueba de forma periódica. En el tema del involucramiento interorganizacional ya se han presentado avances positivos en la industria financiera. Claro ejemplo es el caso de las Bases de Coordinación en Materia de Seguridad de la Información. Estos esfuerzos podrían replicarse en otras industrias clave de la economía mexicana.

Así también, se debe fortalecer la agenda de ciberresiliencia de las asociaciones civiles en México para concientizar a la población en temas de ciberseguridad y en los comportamientos que la fomentan. Para lograr esto, se pueden diseñar programas que sensibilicen a la sociedad de los peligros cibernéticos que enfrentan adultos y niños en el ciberespacio, ya sea en las redes sociales, en donde se manifiesta con mayor frecuencia la práctica de *cyberbullying*, así como en la vida digital en que se desempeñan diariamente la mayoría de los mexicanos. Estos programas también podrían difundir mejores prácticas de higiene digital y civismo digital para niños y adultos por igual. El contenido de los programas podría integrarse a la educación básica pública y privada desde edades tempranas, en aras de fomentar los cambios generacionales.

Por último, prepondera el combate a la desinformación mediante la mejora de algunos esfuerzos en marcha que buscan verificar información y evitar que se manipule la percepción de la sociedad sobre

temas claves y sensibles. Para cumplir este rol, los actuales y futuros *fact checkers* deben ganarse la confianza de la sociedad como árbitros efectivos de objetividad.

Con el propósito de consolidar esta agenda, se pueden fortalecer entidades que ofrezcan puntual seguimiento a los esfuerzos nacionales de ciberresiliencia, y herramientas y plataformas que muestren los cumplimientos y las fallas en la agenda nacional.

El camino hacia adelante

La compleja relación que tiene la sociedad con el ciberespacio implica que todos los agentes sean más vulnerables ante la creciente existencia y sofisticación de los ciberriesgos. Por lo tanto, el fomento de una verdadera ciberresiliencia por parte del sector público, el privado y la sociedad civil se convierte en una prioridad para el cuidado y protección de todos los individuos afectados por estos sectores.

Como todos los demás países en los que se ha profundizado en la creación de una agenda y un marco normativo sobre ciberseguridad, México tendrá que enfrentar una serie de decisiones de manera directa. Estas decisiones requerirán definir balances que toda sociedad abierta necesita enfrentar explícitamente. Algunos de estos balances son:

- El derecho a la privacidad individual en línea, frente a la capacidad de detectar y enfrentar de manera efectiva el cibercrimen.

- El uso de una base nacional de identidad para evitar el robo de identidad, asegurar que el padrón de votantes y contribuyentes fiscales sea fidedigno, y distribuir los beneficios sociales de forma equitativa, frente al temor de que se abuse esta base de información.

- La descentralización masiva de fuentes de información diseminadas a través de redes sociales, frente a la capacidad de juzgar la autenticidad de una fuente de información o de un contenido específico.

- El acceso universal a medios de pago, frente a la capacidad de vigilar la procedencia lícita de fondos.

- El incremento de efectividad de gestión derivado del uso de bases de datos centralizadas a las que se pude acceder de forma descentralizada, frente a los riesgos de tener dichas bases y otorgar dichos accesos.

- El empoderamiento en lo político y social que permite a individuos tomar acción en causas específicas a ellos, frente a la necesidad de negociación y construcción de consensos que comprendan un conjunto de causas o temas interconectados, particularmente ante entornos en que presentan ataques cibernéticos con diversos fines.

Desde luego, como se puede constatar en la prensa de muchos países, no se ha podido llegar a conclusiones definitivas uniformemente aceptadas en cada uno de estos y otros temas. Sin embargo, esto no implica que no se deban debatir abiertamente estos temas, en aras de garantizar la validez de los entornos digitales en los que se expresan.

Enfrentar este gran problema, considerando todos estos desafíos, implicará la ejecución de diversos esfuerzos por parte de múltiples agentes, por un período significativo de tiempo. Algunos podrán ser ejecutados por cada agente relevante en su rol y espacio, pero muchos requerirán del apoyo y colaboración de otros agentes y sectores. También requerirán conocimiento y experiencia de jugadores locales e internacionales. Si bien el camino hacia adelante no será sencillo, debemos iniciarlo con premura y con determinación.

Coordinador
Rafael Fernández MacGregor B

Autores

David Abusaid, McKinsey & Company
Andrea Cristofori, McKinsey & Company
Rafael Fernández MacGregor, COMEXI
Sergio Waisser, McKinsey & Company

COMEXI y McKinsey & Company agradecen enormemente el trabajo y las valiosas contribuciones puntuales de todos los expertos y colaboradores sin cuyo apoyo este documento no podría haberse materializado.

Integrantes del grupo de McKinsey & Company

Joshua Blackburn
Jim Boehm
Marcela Crespo
James Kaplan
Elizabeth Kerr Rivera
Alberto Ramos
Martha Salazar
Nicolás Schiaffino
Sofía Vargas
Marlene Oechler, asesor externo

Integrantes del grupo de Ciber Seguridad de COMEXI

Enrique Alanís
Adolfo Arreola
Cynthia Bretón
Héctor Cárdenas
Cristina Contreras Zamora
Adrián Castillo
Rafael Funes
Ana Carla García Franco
Tomás Alejandro González
Miguel Guevara
Santiago Gutiérrez Gutiérrez
William Jensen
Fan Jua Rivas
Rafael Lechuga López
Carlos López-Portillo
Sebastián Miralles
Hugo Rodríguez Nicolat
Ruth Ornelas
Francisco Javier Salazar
Mónica Trigos Padilla

Junio 2018