Vigilancia tecnológica en CIBERSEGURIDAD

Boletín No. 1, 7 de junio de 2022.

El ABC de la ***Ciberseguridad***

Tipología de ***Ciberataques***

Reacción de ***Actores clave***

Universidad Nacional Autónoma de México

ICAT Instituto de Ciencias Aplicadas y Tecnología

HUAWEI

Directorio

Universidad Nacional Autónoma de México

Rector
Dr. Enrique Graue Wiechers

Coordinador Investigación Científica
Dr. William Henry Lee Alardín

Instituto de Ciencias Aplicadas y Tecnología

Directora
Dra. Ma. Herlinda Montiel Sánchez

Coordinador del Grupo de Gestión Estratégica de la Innovación
Dr. José Luis Solleiro Rebolledo

Autores
José Luis Solleiro Rebolledo
Rosario Castañón Ibarra
Ángel David Guillén Valencia
Tania Yadira Hernández Molina
Norma Solís Mérida

Cuidado de la edición
Norma Solís Mérida

Apoyo en el cuidado de la edición
Eréndira Velázquez Campoverde

Diseño Editorial
Mariana Itzel Barajas Tinoco
Mariana García Delgado
María Fernanda Gasca Alcántara

Contacto
boletinciberseguridadicat@gmail.com

Índice

Presentación

El mundo avanza rápidamente hacia la digitalización. La emergencia de nuevas tecnologías que facilitan el flujo masivo de datos y la conectividad, aunada a la necesidad de trabajo remoto impuesta por la pandemia de COVID-19, ha generado conciencia sobre la importancia de contar con un ciberespacio seguro y confiable. Desafortunadamente, la innovación en tecnologías de la información y comunicación (TIC) ha estado acompañada por formas cada vez más sofisticadas de intervención en los sistemas, delitos cibernéticos y robo de datos e identidad.

Ante esto, la ciberseguridad ha tomado cada vez mayor relevancia, por lo que se han desarrollado innovaciones para proteger sistemas, equipos y redes. La relación entre la ciberseguridad y la innovación es en dos vías: por un lado, la ciberseguridad permite que la innovación se introduzca en prácticamente todos los sectores de la economía digital al generar un ambiente de confianza en los usuarios de las tecnologías de la información y, por el otro, las diversas innovaciones tecnológicas permiten a las empresas dedicadas a ciberseguridad generar dispositivos y sistemas para mejorar la protección de organizaciones, redes y datos.

Por ejemplo, la inteligencia artificial está usándose para mejorar la detección de posibles ataques y acelerar la respuesta ante amenazas; la técnica de *machine learning* se utiliza ahora para descubrir vulnerabilidades, realizar investigaciones sobre eventos de riesgo y mejorar la respuesta ante ataques cibernéticos. También se generan invenciones para mejorar la ciberseguridad relacionadas con reconocimiento de imágenes, aprendizaje profundo, realidad virtual, reconocimiento de discurso, chatbots, manejo masivo de datos, procesamiento de lenguaje natural, *blockchain*, internet de las cosas, manejo cuántico de información, etc.

Pero la ciberseguridad no es sólo un asunto técnico. También surgen nuevas estrategias organizacionales, políticas públicas y reglas de comportamiento en la red que constituyen conocimientos suaves y activos intangibles que son críticos para contar con un entorno de ciberseguridad eficaz y económicamente viable.

El Instituto de Ciencias Aplicadas y Tecnología (ICAT), ante este ambiente de cambio tecnológico e institucional en materia de ciberseguridad, ha decidido lanzar una serie de boletines de vigilancia tecnológica en ciberseguridad en la que se aborden los principales avances que se realizan en el mundo, los actores relevantes y los factores críticos para generar un ecosistema de ciberseguridad confiable.

En este primer número se revisan temas generales para introducir al lector al concepto de ciberseguridad, los principales riesgos en la materia y los componentes de una estrategia integral para abordarlos.

En las siguientes ediciones se profundizará en el análisis de innovaciones tecnológicas para reforzar la ciberseguridad, el surgimiento de iniciativas de normalización y certificación, y las estrategias de la industria para contender no sólo con riesgos informáticos, sino también con la protección de datos.

José Luis Solleiro Rebolledo

Contexto e importancia de la ciberseguridad

La ciberseguridad es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos (IBM, 2022; Kaspersky, 2022a).

Ciertamente, en la actualidad hay diversas definiciones de ciberseguridad, pues se trata de un vocablo que surgió en el entorno de la revolución de las tecnologías de la información y comunicación (TIC), y se ha visto impactado por el desarrollo que éstas han registrado en los últimos 30 años[1].

1 El sociólogo Manuel Castells ubica el inicio de la revolución de las TIC hacia finales de la década de 1960 y principios de la de 1970, debido a que fue en esos años cuando acontecieron descubrimientos y sucesos fundamentales en términos de las tecnologías de la información (Castells, 1996; Castell; 1999):

- En 1969, la Agencia de Proyectos de Investigación del Departamento de Defensa de Estados Unidos (ARPA) estableció una nueva red electrónica de comunicación, la cual crecería durante los años 70 para convertirse en lo que hoy se conoce como internet.
- El microprocesador, elemento clave en la difusión de la microelectrónica fue inventado en 1971 y comenzó a difundirse a mediados de los 70.
- La microcomputadora fue construida en 1975 y el primer producto comercialmente exitoso, Apple II, fue introducido en abril de 1977. Aproximadamente en esa misma época Microsoft comenzó a producir sistemas operativos para microcomputadoras.
- La Xerox Alto, matriz de muchas tecnologías de *software* para las PC de los años 90, fue desarrollada en los laboratorios PARC en Palo Alto en 1973.

Definiciones sobre ciberseguridad

Unión Internacional de Telecomunicaciones

"(…) conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno" (UIT, 2010: 20).

Asociación Global del Ecosistema Móvil

"(…) disciplina que tiene por objetivo asegurar que los recursos de tecnología de la información estén disponibles y accesibles para ser utilizados por los autorizados a hacerlo y, por el contrario, sean inaccesibles para quienes no lo están. Como tal, abarca diversos aspectos de las redes de telecomunicaciones fija, móvil e Internet. Incluye desde la integridad física de los equipos hasta la seguridad de la información en ellos contenida" (GSMA Latin America, 2018:24).

Unión Europea

"(…) todas las actividades necesarias para la protección de las redes y sistemas de información, de los usuarios de tales sistemas y de otras personas afectadas por las ciberamenazas (Reglamento de Ciberseguridad de la UE)" (Parlamento Europeo y Consejo de la Unión Europea, 2019: 32).

Instituto Federal de Telecomunicaciones (México)

"(…) conjunto de herramientas políticas, conceptos, acciones, prácticas idóneas y tecnologías que pueden utilizarse para proteger a los usuarios, sus dispositivos y la información transmitida y/o almacenada, de los riesgos de seguridad que hay en el ciberentorno" (IFT, s.f.).

Palo Alto*

"(…) se refiere a la protección de los sistemas conectados a Internet, incluyendo *hardware, software* y datos críticos contra ataques, daños o acceso no autorizado" (Palo Alto Networks, 2022).

*Palo Alto ocupó el primer lugar en The Top 25 Cybersecurity Companies of 2021, realizado por The Software Report.

Fuente: elaboración propia con información de IFT (s.f.), UIT (2010) GSMA Latin America, (2018); Parlamento Europeo y Consejo de la UE (2019) y Palo Alto Networks (2022).

En la actual era digital, las sociedades se interconectan cada vez más con apoyo de las tecnologías de la información (TI) y la infraestructura digital. Sin embargo, esta interconectividad también crea interdependencia y vulnerabilidad frente a amenazas emergentes que atentan contra la integridad, seguridad y confiabilidad de la información.

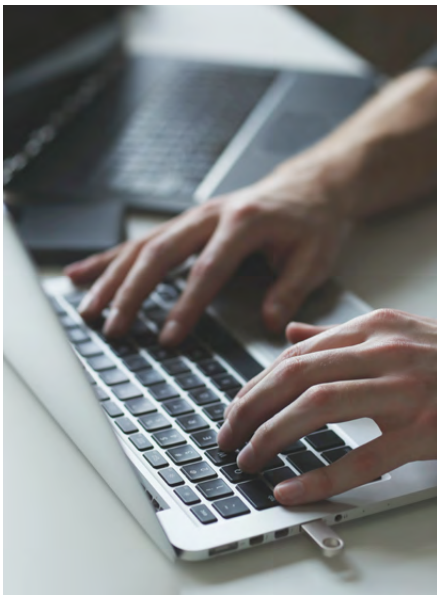
De acuerdo con la edición 2021 del informe líder *Cost of a Data Breach Report*[2], de 2020 a 2021 a nivel mundial, el costo[3] de una filtración de datos pasó de USD $3.86 millones a USD $4.24 millones; éste es el costo total promedio más alto jamás registrado[4]. Según el mismo reporte, las regiones con el mayor aumento promedio del costo son América Latina (aumento del 52.4%), Sudáfrica (aumento del 50%), Australia (aumento del 30.2%), Canadá (aumento del 20%) (IBM Segurity, 2021). Además de los costos económicos, los ataques informáticos también tienen afectaciones a la infraestructura crítica, la cohesión social y el bienestar mental de la población (World Economic Forum, 2022; ITU, 2022).

2 Este informe se ha convertido en una herramienta de referencia líder que, para el cálculo de los costos en su edición 2021, analizó una base de 537 fugas reales de información.

3 Estos costos incluyen los gastos de descubrir y responder a la infracción, el costo relacionado con el tiempo de inactividad y la pérdida de ingresos, así como el daño a la reputación a largo plazo de una empresa y su marca.

4 Para México, el Centro Nacional de Respuestas a Incidentes Cibernéticos, cada ataque cibernético exitoso dirigido a una pyme podría ocasionar en promedio una pérdida de 50,000 dólares, lo que para algunas significaría un daño que ocasionaría el cierre de la empresa (CERT-MX, 2020).

La velocidad con la que los gobiernos, las sociedades y las empresas se apoyan en la tecnología para administrar desde los servicios públicos hasta los procesos comerciales, crece a un ritmo exponencial. Es un rasgo de la creciente digitalización.



Por otra parte, el cambio al trabajo remoto (potencializado por la COVID-19) ha acelerado la adopción de una mayor variedad de plataformas y dispositivos conectados en entornos residenciales de poca protección contra la intrusión cibernética, aumentando drásticamente la oportunidad para que información de valor sea robada, manipulada o dañada en perjuicio de sus propietarios.

De acuerdo con Riquelme (2022), "ni sector público, ni la iniciativa privada, ni la ciudadanía se salvaron en este 2021 de tener que lidiar con incidentes de seguridad y ciberataques que pudieron afectar su reputación, su credibilidad y hasta sus finanzas. Según Kaspersky, en México ocurren 299 intentos de infecciones maliciosas por minuto, muchas de las cuales logran penetrar las barreras con las que tanto el gobierno, como las empresas y los individuos intentan proteger su información y su identidad".

Paralelamente, el desarrollo exponencial de múltiples tecnologías que están brindando enormes oportunidades para mejorar la eficiencia, calidad y productividad del sector industrial (entre ellas, por ejemplo, la inteligencia artificial —IA—, internet de las cosas —IoT—/cadena de bloques, 5G, entre otras), exponen cada vez más a los usuarios a formas elevadas y más perjudiciales de riesgos digitales. Es decir que a medida que la sociedad continúa migrando hacia el mundo digital, también crece un panorama de amenazas cibernéticas más complejo (World Economic Forum, 2022).

En este contexto de dependencia generalizada de sistemas digitales, las ciber-amenazas pueden superar la capacidad de las sociedades para prevenir y gestionar de manera eficaz amenazas cibernéticas. Por ejemplo, la digitalización de las cadenas de suministro crea nuevas vulnerabilidades porque esas cadenas dependen de proveedores de tecnología y otros servicios de terceros, que también están expuestos a amenazas similares y potencialmente contagiosas.

En el futuro, la interconexión y la convergencia de estas herramientas digitales seguirán aumentando, por ejemplo, a medida que la sociedad adopte la próxima versión de internet basada en la tecnología *blockchain* o mediante el uso masivo del *metaverso*, red de espacios virtuales 3D donde los humanos interactúan social y económicamente como avatares a través de un soporte lógico en un ciberespacio que actúa como una metáfora del mundo real (Chohan, 2022).

En el mismo sentido, cuando la nueva generación de tecnología de comunicación móvil 5G alcance una masa crítica impactará a casi todas las organizaciones, constituyendo un nuevo reto para la atención de ciberataques en una gran variedad de industrias (Jayakody, 2019) y en el ámbito de la comunicación móvil.

En este contexto, sociedad y gobiernos enfrentan retos y responsabilidades cada vez mayores en ámbitos como (World Economic Forum, 2022):

1. El aseguramiento de la infraestructura crítica.
2. Protección a la integridad de procesos y los servicios públicos.
3. Legislar el ciberdelito.
4. Capacitar y educar a la sociedad en materia de ciberseguridad.
5. Garantizar la disponibilidad de recursos para la economía digital.
6. Proteger los datos.

Sumado a lo anterior, un reto importante para los gobiernos es el de manejar con responsabilidad la supervisión del ciberespacio, coordinar acciones con los operadores para legislar y generar un marco digital que coadyuve a reducir ataques, así como abordar las amenazas que conjugan seguridad y desinformación. Implementar de manera inadecuada estas políticas podría convertirse rápidamente en un vehículo para la pérdida de confianza pública, correspondiente rezago y descontento social.

Finalmente, otra arista de gran interés a atender reside en que la población más vulnerable a los ataques de ciberseguridad es la que recientemente se está conectando por vez primera a internet. Alrededor del 40% de la población mundial aún no está conectada y estas personas ya enfrentan desigualdades en seguridad digital (World Economic Forum, 2022).

En tal escenario, además de los esfuerzos por aumentar la ciberseguridad, resulta de suma importancia la alfabetización digital, la cual se refiere no sólo al conjunto de conocimientos, habilidades y actitudes para manejar eficazmente herramientas y desenvolverse en entornos digitales, sino que también implica "la apropiación de los nuevos conocimientos a partir de aprender a utilizar los componentes del hardware, los aplicativos y programas, los mecanismos de búsqueda y la información disponible en ambientes electrónicos, como finalidad en sí misma" (Ferreira y Didziak, 2004, citadas en Silvera, 2005: 3)

En los próximos años, el impacto de los ciberataques podría ser financieramente devastador para las sociedades que no inviertan en la protección de su infraestructura digital. Las entidades que no demuestren un gobierno corporativo sólido en torno a la ciberseguridad, por ejemplo, mediante la implementación de sistemas sólidos y protocolos de supervisión de procesos, podrían sufrir daños catastróficos (ITU, 2022; World Economic Forum, 2022).

El ABC de la ciberseguridad

Como se ha mencionado, la ciberseguridad es la práctica de proteger los sistemas críticos y la información confidencial de los ataques digitales, es decir, busca garantizar la consistencia, integridad y confiabilidad de la información que se gestione a través de medios tecnológicos.

La ciberseguridad abarca todo lo relacionado con la protección de datos personales, información de identificación personal, información de salud, propiedad intelectual, datos y sistemas de información gubernamentales y de la industria contra el robo y el daño por parte de ciberdelincuentes y otras entidades que intenten ingresar en una red privada. La ciberseguridad aplica en diferentes contextos, desde los negocios hasta la informática móvil y puede dividirse en algunas categorías comunes (Kaspersky, 2022a; Proofpoint, 2022; Avansis, 2021):

- **Seguridad de red:** es la práctica de proteger una red informática de intrusos.
- **Seguridad de las aplicaciones**: se enfoca en mantener el *software* y los dispositivos libres de amenazas.
- **Seguridad de la información:** protege la integridad y la privacidad de los datos, tanto en el almacenamiento como en el tránsito.
- **Seguridad operativa:** incluye los procesos y decisiones para manejar y proteger los recursos de datos (por ejemplo, los permisos que tienen los usuarios para acceder a una red y los procedimientos que determinan cómo y dónde pueden almacenarse o compartirse los datos).

- **Seguridad del usuario:** atiende la información de identificación personal de los usuarios (por ejemplo, nombres, direcciones, números de identificación, número de seguro social, códigos fiscales, etcétera) y la información para fines económicos tales como los números de la tarjeta de crédito.
- **Recuperación ante desastres y la continuidad del negocio:** definen la forma en que una organización responde a un incidente de ciberseguridad o a cualquier otro evento que cause que se detengan sus operaciones o se pierdan datos.
- **Seguridad móvil:** se refiere a las estrategias, infraestructuras y *software* que se utilizan para proteger cualquier dispositivo móvil (teléfonos celulares, computadoras portátiles, *tablets*, etc.). Implica la protección de datos en el dispositivo local, en los *endpoints* conectados al dispositivo y en los equipos de redes.
- **Seguridad de *hardware:*** se dirige a garantizar la protección del dispositivo físico, desde aparato en si hasta el contenido que éste almacena y la forma en que la información transcurre a través de sus diferentes componentes.

Tipología de ciberataques más comunes

Las amenazas a las que se enfrenta la ciberseguridad, según sus motivaciones, son (Candau, 2021):

Delito cibernético: se refiere a todas las figuras delictivas del crimen tradicional, pero adaptadas al ciberespacio. Normalmente su motivación es el rendimiento económico y sus objetivos son más indiscriminados, es decir víctimas que dispongan de vulnerabilidad y con capacidad financiera para atender a sus demandas.

Ciberterrorismo: tiene como objetivo debilitar los sistemas electrónicos para causar pánico o temor.

Ciberespionaje: ciberataques realizados para obtener secretos de Estado, información comercial sensible o datos de carácter personal.

Los métodos más comunes para amenazar la ciberseguridad son (IBM, 2022; Kaspersky, 2022a; Jiménez, 2021):

Malware

Software malicioso que brinda acceso no autorizado o causa daños a una computadora. Los ataques de *malware* son cada vez más "sin archivos" y están mejor diseñados para eludir los métodos de detección tradicionales, como las herramientas antivirus. Existen diferentes tipos de *malware*:

- **Virus:** programa capaz de reproducirse que se incrusta un archivo limpio y se extiende por todo el sistema informático e infecta a los archivos con código malicioso.
- **Troyanos:** *malware* que se disfraza como *software* legítimo para engañar a usuarios e instalarse en los equipos causando daños o para recopilar datos.
- ***Spyware:*** programa que registra en secreto lo que hace un usuario para que los cibercriminales puedan utilizar esta información. Por ejemplo, el *spyware* podría capturar los detalles de las tarjetas de crédito.
- ***Adware:*** *software* de publicidad que puede utilizarse para difundir *malware*.
- ***Botnets:*** redes de computadoras con infección de *malware* que los cibercriminales utilizan para realizar tareas en línea sin el permiso del usuario.
- ***Ransomware* (secuestro de datos)**: *malware* que bloquea archivos, datos o sistemas, y amenaza con borrar, destruir o publicar los datos confidenciales o privados, a menos que se pague un rescate. Los recientes ataques de *ransomware* se han dirigido a los gobiernos estatales y locales, que son más fáciles de violar que las organizaciones y están bajo presión para pagar rescates.

Phishing/ingeniería social

Se engaña a los usuarios para que proporcionen información confidencial. Una forma de *phishing* que ha cobrado relevancia son los correos electrónicos o mensajes de texto que, al simular ser de una empresa legítima, solicita información confidencial.

Credential Stuffing/compromised credential

Usa las interfaces digitales y los flujos de trabajo, como los formularios de inicio de sesión, para obtener acceso no autorizado a las cuentas de los clientes. El *credential stuffing* comienza con la automatización, la extración de las credenciales y, finalmente, llega al robo de cuentas y fraudes.

Amenazas internas

Los empleados actuales o anteriores, socios comerciales, contratistas o cualquiera que haya tenido acceso a sistemas o redes en el pasado pueden considerarse una amenaza interna si abusan de sus permisos de acceso.

Ataques distribuidos de denegación de servicio (DDoS)

Un ataque DDoS intenta colapsar un servidor, sitio web o red al sobrecargarlo con tráfico, generalmente de múltiples sistemas coordinados. Esto ocasiona que el sistema sea inutilizable e impide que una organización realice funciones vitales.

Amenazas persistentes avanzadas (APT)

Un intruso se infiltra en un sistema y permanece sin ser detectado durante un periodo prolongado con el objetivo de espiar la actividad comercial o robar datos confidenciales.

Inyección de código SQL (Structured Query Language)

Ciberataque en el que se aprovechan las vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso (mediante instrucción SQL) en una base de datos con el objetivo de tomar el control y robar información.

Ataque de tipo "Man-in-the-middle"

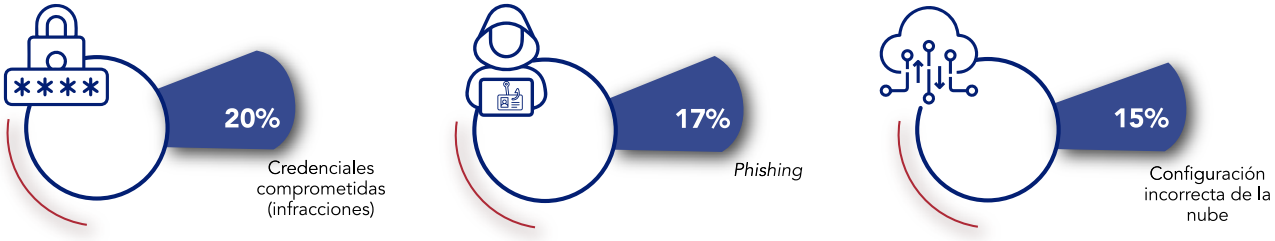
Ciberamenaza en la que se intercepta la comunicación entre dos individuos para robar datos. Por ejemplo, en una red Wi-Fi no segura.

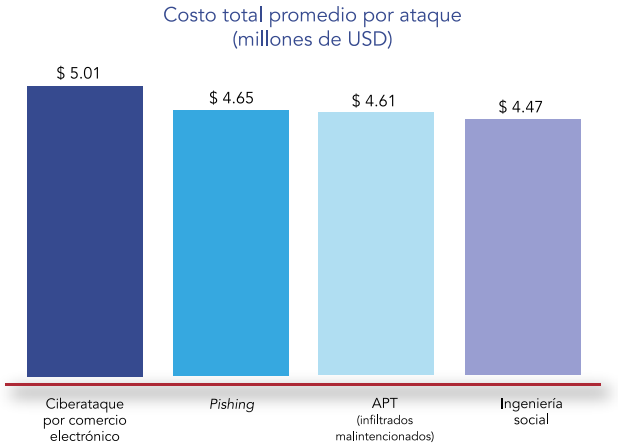
Configuración incorrecta de la nube

Todos aquellos errores de configuración que ponen en riesgo los servicios y el contenido alojados en la nube. Puede ocurrir, por ejemplo, configuración incorrecta de almacenamiento y de administración de identidad; también son errores la exposición de los datos a todos los usuarios globales de la misma plataforma en la nube; dejar claves de cifrado y contraseñas en repositorios abiertos.

Ataques más frecuentes en 2021 de acuerdo con *Cost of a Data Breach Report 2021*

En **2021** los ataques más frecuentes fueron:





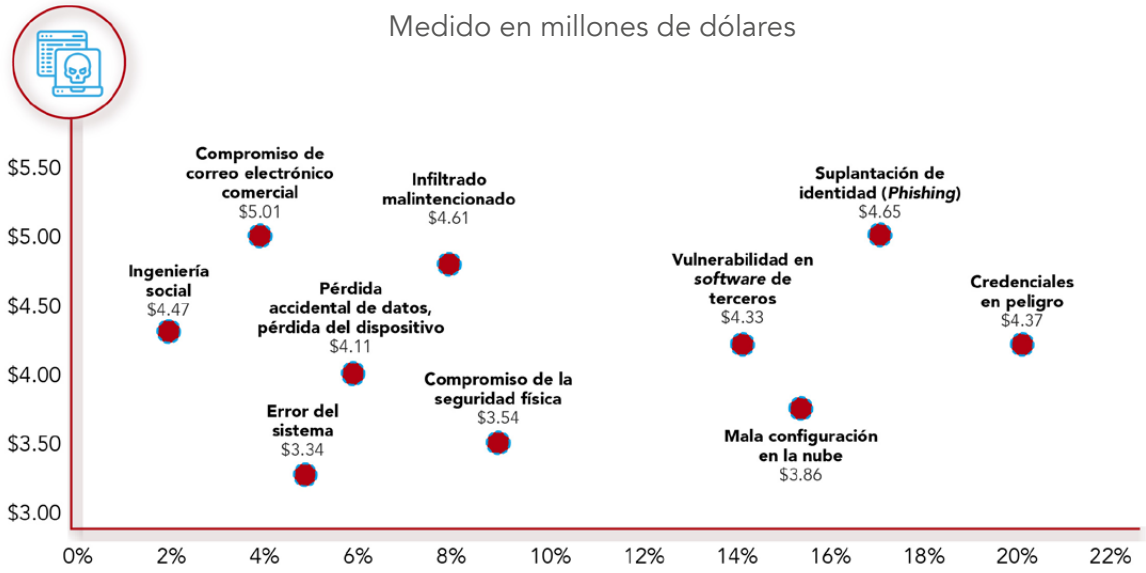
Los ciberataques por comercio electrónico fueron responsables de sólo el

4%

de las infracciones, pero tuvieron el costo total promedio más alto para los afectados.

Fuente: elaboración propia con información de IBM Segurity (2021).

Costo total medio y frecuencia de violación de datos por vector de ataque inicial



Fuente: adaptada de IBM Segurity (2021).

Según se señala en la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (Endutih) 2019*, en dicho año, los usuarios en México se enfrentaban a los siguientes problemas, relacionados con el tema de ciberseguridad, al navegar por internet (Inegi, 2020):

Problema	Número de usuarios que sufren este problema	Porcentaje del universo total de usuarios de internet en México
Exceso de información no deseada	20.5 millones	25.5%
Mensajes de personas desconocidas	16.4 millones	20.3%
Infección por virus	10.6 millones	13.1%
Fraudes con información financiera personal	3.2 millones	4.0%
Violación a la privacidad	2.5 millones	3.1%

En tanto, en mayo pasado, la Asociación de Internet MX dio a conocer, en el *18° Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022*, los principales riesgos que perciben los usuarios al realizar actividades en línea[5] (The CIU, 2022):

Fuente: adaptada de The CIU (2022)

5 El estudio es elaborado por los especialistas de la consultora The Competitive Intelligence Unit (CIU).

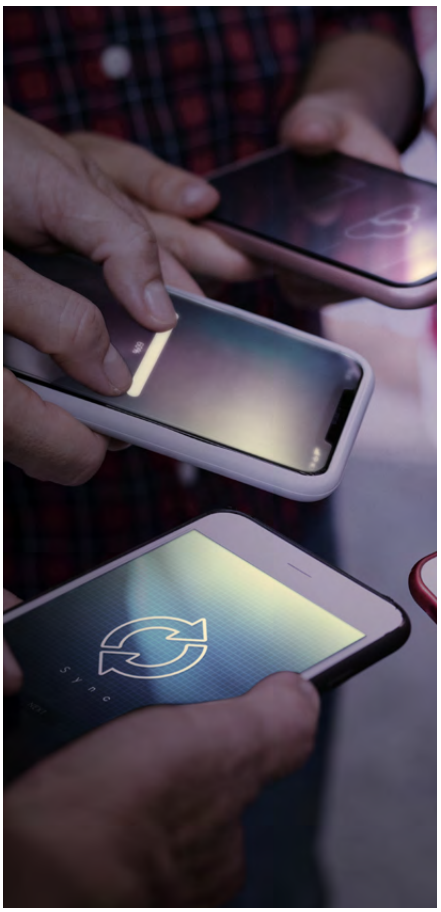
En 2021, "según datos recabados por FortiGuard Labs, el laboratorio de inteligencia de amenazas de Fortinet, México fue el país latinoamericano que más intentos de ataques recibió (156 mil millones), seguido de Brasil (88.5 mil millones), Perú (11.5 mil millones) y Colombia (11.2 mil millones)" (Cortés, 2022).

En el estudio de FortiGuard Labs se indica que gran cantidad de amenazas a la ciberseguridad corporativa reportadas en 2021 deriva del creciente número de personas conectadas a sus trabajos mediante computadoras y dispositivos móviles. Las técnicas de escaneo masivo han permitido a los ciberatacantes identificar vulnerabilidades. También se han detectado ataques relacionados con ejecución remota de código (RCE) en diversos dispositivos, como cámaras, micrófonos y enrutadores domésticos, lo cual tiene el objetivo de identificar sistemas empresariales vulnerables.

En cuanto a la ciberseguridad y 5G, existen algunas preocupaciones particulares (Kaspersky, 2022b):

- Seguridad descentralizada. Los sistemas dinámicos basados en *software* de la 5G tienen muchos más puntos de contacto de tráfico (*hardware*) respecto de las redes 2, 3 y 4G. Para estar completamente seguros, todos estos puntos necesitan supervisión, lo cual aumenta sustancialmente la necesidad de ejecutar estrategias de ciberseguridad.
- Un ancho de banda mayor pondrá a prueba la supervisión de seguridad actual. Derivado de la mayor velocidad y el creciente volumen de datos de las redes 5G, surgen nuevas complicaciones para supervisar la seguridad en tiempo real.
- Gran variedad de nuevos dispositivos de IoT conectados a 5G. No todos los fabricantes dan prioridad a la ciberseguridad, como se observa en muchos dispositivos inteligentes de baja gama. A medida que se fomenta la conexión de miles de millones de dispositivos con diversos niveles de seguridad, significan miles de millones de posibles puntos de brechas de seguridad.

Como se ha señalado, el número mayor de dispositivos y el alto uso de la virtualización están abriendo la posibilidad de nuevas amenazas, peligros y ataques digitales. La actividad maliciosa está proliferando, en parte debido a las crecientes vulnerabilidades, pero también a las pocas barreras de entrada para los participantes en la industria del *ransomware* y poco riesgo de extradición, enjuiciamiento o sanción. El "*ransomware* como servicio" permite que incluso los delincuentes no técnicos ejecuten ataques, una tendencia que podría intensificarse con el advenimiento del *malware* impulsado por inteligencia artificial (AI, por sus siglas en inglés) (World Economic Forum, 2022).



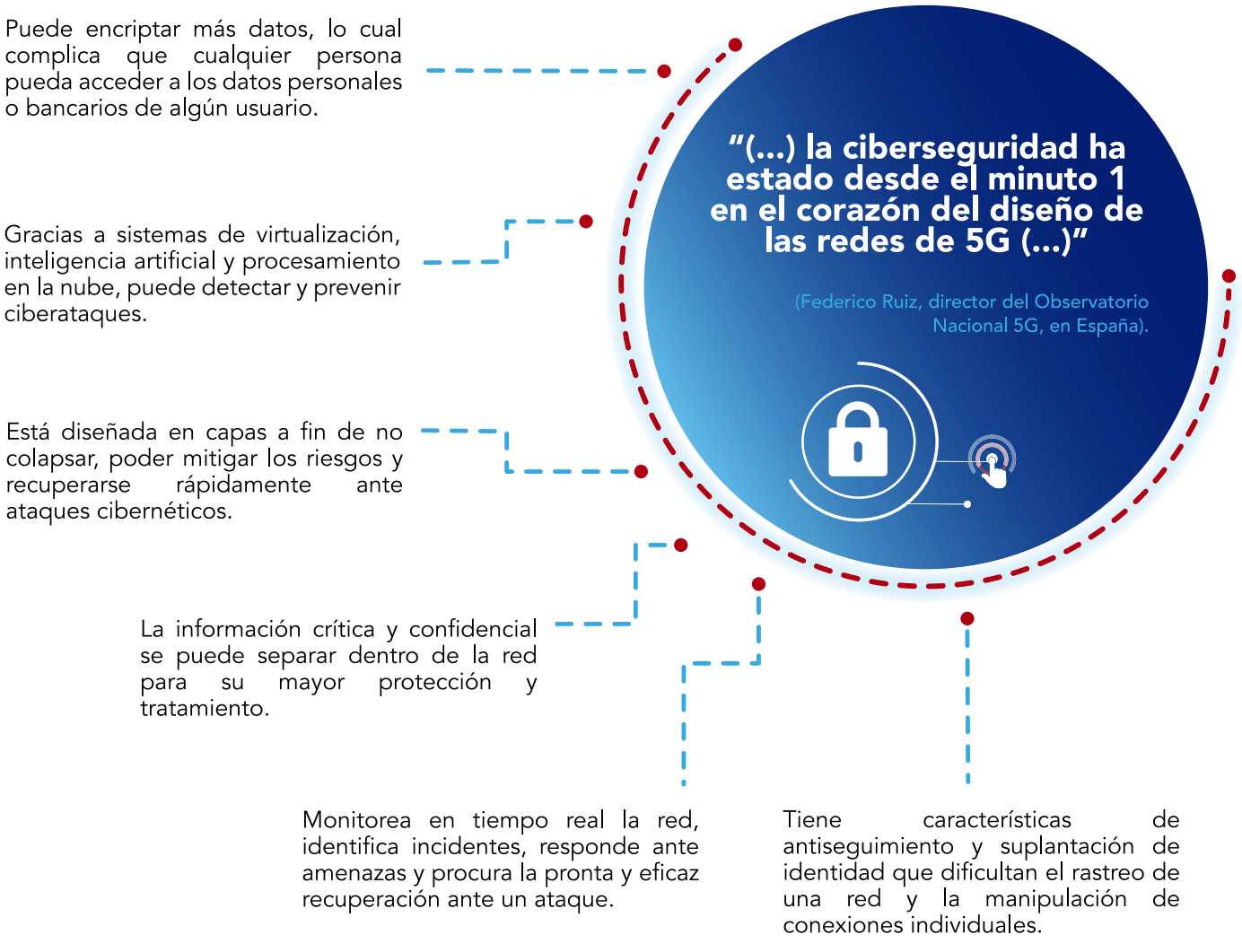
Ante tales inquietudes algunos investigadores precisan que, ciertamente, la tecnología 5G permitirá más puntos de entrada para los ciberataques, pero no debido a que presentaría más o mayores vulnerabilidades que las tecnologías anteriores, sino "justamente porque es mejor y más rápida, por lo que aumentará el número y la variedad de dispositivos que la usen (desde refrigeradores a ampolletas o comederos para mascotas)" (Hoehn, 2021: 6).

De hecho, la arquitectura de la 5G presenta características de seguridad mejoradas respecto a las generaciones que las precedieron, tales mejoras se han producido en la autenticación, el cifrado y la garantía de disponibilidad, integridad y privacidad (Aranta, Sacoto, Haro y Astudillo, 2021)

Asimismo, otros especialistas en el tema, así como proveedores de infraestructuras de TIC y equipos de telecomunicación, aseveran que la ciberseguridad ha sido un elemento que ha acompañado a la 5G desde que ésta empezó a generarse; aunque reconocen que alcanzarla y responder adecuadamente a los retos que supone, demandan una responsabilidad compartida en la que participan desde los operadores móviles, los desarrolladores de tecnología, los organismos internacionales, los gobiernos y sus órganos reguladores, hasta los usuarios finales.

"Ningún país o empresa puede afrontar la problemática de la ciberseguridad por sí solo y para encontrar la solución se necesitan estándares globales basados en la colaboración, siempre bajo una estricta revisión de todos los componentes de la cadena" (DPL News, 2022: 5).

5G: ventajas respecto a la ciberseguridad



Fuente: elaboración propia con información de *El País* (2021), Catania (2021), Bravo (2022) y DPL News (2022).

Estrategias de la industria en materia de ciberseguridad: el caso de Huawei

En la configuración y rápido desarrollo del mundo digital, la ciberseguridad y la protección de datos se han convertido en requisitos inherentes, en capacidades esenciales. Consciente de ello y de que "el éxito empresarial resulta imposible sin seguridad" (Laroca, 2022), Huawei (proveedor de infraestructura de TIC y dispositivos inteligentes) ha implementado una serie de medidas y una estrategia a fin de mejorar la seguridad de sus productos y servicios[6].

Algunas medidas de Huawei en materia de ciberseguridad

1

Definir un principio ABC en seguridad cibernética que consiste en:
A: Assume nothing (no asumir nada)
B: Belive nobody (no creer en nadie)
C: Check everything (verificar todo)

2

Invertir en **I+D** en ciberseguridad. Cada año, la empresa destina el **5%** de su presupuesto a esa actividad. De hecho, en 2021, el gasto total en I+D de Huawei ascendió a CNY142,700 millones, lo que equivale al **22.4 %** de los ingresos totales de la empresa.

3

Desarrolla y ofrece una gama de productos relacionados con ciberseguridad para empresas.

4

Implementa proyectos y acciones en pro de la ciber-resilencia, tales como:

- En 2016 estableció un marco unificado de gobernanza de la privacidad de acuerdo con el Reglamento General de Protección y Datos de Europa.
- En 2021 realizó evaluaciones de riesgos de seguridad a más de 4000 proveedores de todo el mundo y rectificó los problemas identificados.
- Se incorporó como miembro de la cooperación islámica para la respuesta a emergencias informáticas; estableció, junto con China Mobile, un centro de innovación sobre seguridad 5G en Zhejiang.

Nota: La resiliencia es una cualidad inherente a un organismo, entidad, empresa o estado que le permite enfrentar una crisis sin que su actividad se vea afectada (Carrasco, 2015). La ciber-resiliencia se refiere a "la capacidad de una organización de mantener su propósito principal e integridad frente a la amenaza latente de los ataques de ciberseguridad" (Panda Security, 2018: 3).

Fuente: elaboración propia con información de DPL News (2022) y Huawei (2022).

6 Huawei es una empresa china fundada en 1987. Tiene aproximadamente 195,000 empleados y opera en más de 170 países, sirve a más de 3000 millones de personas alrededor del mundo.

En cuanto a la "estrategia de ciberseguridad de adentro hacia afuera y de extremo a extremo" que Huawei ha desplegado, ésta se caracteriza por iniciar al interior de la empresa e implica:

- Contar con un Comité Global de Ciberseguridad Cibernética y Protección de la Privacidad del Usuario.
- Incorporar, la metodología de seguridad cibernética, a 12 procesos corporativos y módulos comerciales:

1. Estrategia y gobernanza
2. Procesos
3. Legislación y regulación
4. Recursos humanos
5. Investigación y desarrollo
6. Verificación
7. Gestión de proveedores
8. Manufactura y logística
9. Prestación segura de servicios
10. Resolución de problemas
11. Trazabilidad
12. Auditoría

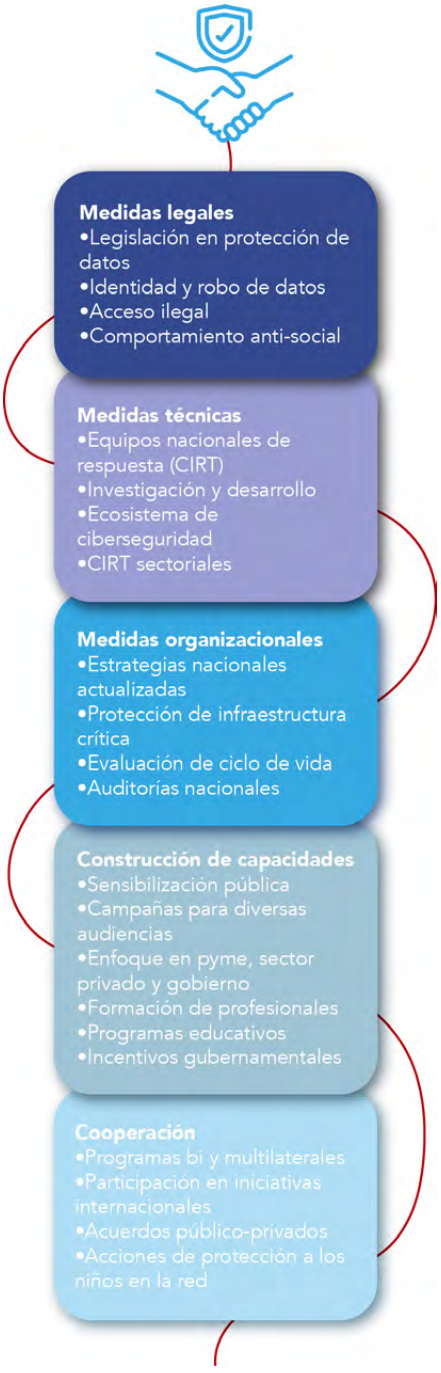
Reacción de gobiernos, industria y sociedad ante el contexto de ciberseguridad

La regulación, la gestión y el establecimiento de mecanismos que aseguren los derechos y deberes de los usuarios es una labor fundamental para caminar con seguridad hacia una era más digital. Respecto del compromiso con la ciberseguridad, a nivel mundial se han producido iniciativas en ámbitos con distintos alcances: global, como es el caso de Naciones Unidas a través de la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés); regional, como son la Unión Europea y la Organización de Estados Americanos (OEA), o incluso nacional como, en el caso de México, el Centro Nacional de Respuestas e Incidentes Cibernéticos (Ramírez, 2015; CERT-MX, 2020).

Con el objetivo de comprender mejor los compromisos de los países con la seguridad cibernética, identificar brechas, fomentar la incorporación de buenas prácticas y proporcionar información útil para que los países mejoren sus posturas de seguridad cibernética, la ITU ha lanzado el *Global Cybersecurity Index* (GCI), índice que analiza el nivel de desarrollo o compromiso de cada país/región, a través de la evaluación de cinco pilares (ITU, 2020):

- Medidas legales: se analizan intervenciones de ciberseguridad dentro del marco legal de un país midiendo la presencia de 1) requisitos básicos que deben cumplir los actores públicos y privados; 2) instrumentos legales que prohíban las acciones dañinas.
- Medidas técnicas: analiza el despliegue de 1) equipos de respuesta a incidentes informáticos (CIRT) o equipos de respuesta ante emergencias informáticas (CERTs por sus siglas en inglés) que permiten que los países respondan a incidentes utilizando un punto de contacto centralizado y promover una acción rápida y sistemática, habilitando a los países para aprender de su experiencia y construir resiliencia en materia de ciberseguridad.
- Medidas organizativas: examinan los mecanismos de gobernanza y coordinación dentro de los países, para asegurar que la ciberseguridad sea atendida a los máximos niveles del ejecutivo y que se asignen tareas y responsabilidades a diversas entidades nacionales y que se les exija rendición de cuentas por sus acciones en materia de ciberseguridad.
- Desarrollo de capacidades: la capacitación en ciberseguridad es clave porque contribuye a la reducción de asuntos como la brecha digital y los riesgos. Los conocimientos y experiencia en materia de ciberseguridad refuerzan las capacidades colectivas y facilitan la cooperación internacional y las alianzas para responder a los desafíos de la seguridad digital.
- Cooperación y acción colectiva en ciberseguridad: la seguridad del ecosistema cibernético global no puede ser garantizada ni gestionada por una sola parte interesada, y necesita la cooperación nacional, regional e internacional para ampliar el alcance y el impacto.

Pilares para evaluar el compromiso con la seguridad cibernética de acuerdo con el *Global Cybersecurity Index* (GCI)

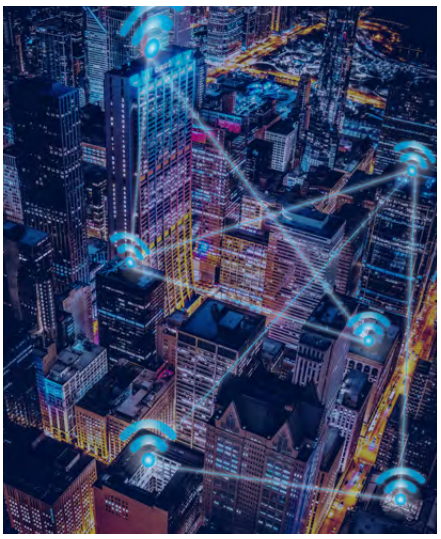


Fuente: elaboración propia con información de ITU (2020).

En la edición más actual del GCI (2020) se concluye que, para avanzar en materia de ciberseguridad, los países deben considerar:

- Desarrollar evaluaciones regulares de sus compromisos de seguridad cibernética, incluidas métricas.
- Promover el desarrollo continuo de los CIRT nacionales y el establecimiento adicional de CIRT para sectores específicos.
- Monitorear y actualizar las estrategias nacionales de seguridad cibernética con planes de implementación claros.
- Promover la inclusión y diversidad, especialmente de grupos subrepresentados como mujeres y jóvenes, dentro de la fuerza laboral de seguridad cibernética.
- Promover la participación regular en actividades internacionales para compartir buenas prácticas, estudios de casos y mejorar la capacidad de preparación y respuesta.
- Mejorar la capacidad de seguridad cibernética de las micro, pequeñas y medianas empresas (mipyme).
- Promover la participación regular de todas las partes interesadas relevantes en la seguridad cibernética, incluido el sector privado, la academia y la sociedad civil.

Los gobiernos que han desarrollado estrategias nacionales para alcanzar la ciber-resiliencia ya están en su segunda o tercera versión. Estonia, por ejemplo, un país líder en ciberseguridad actualizó su primera estrategia en 2014 y ha dado continuidad a la implementación de las iniciativas de la estrategia previa (McKinsey & Company, 2018).

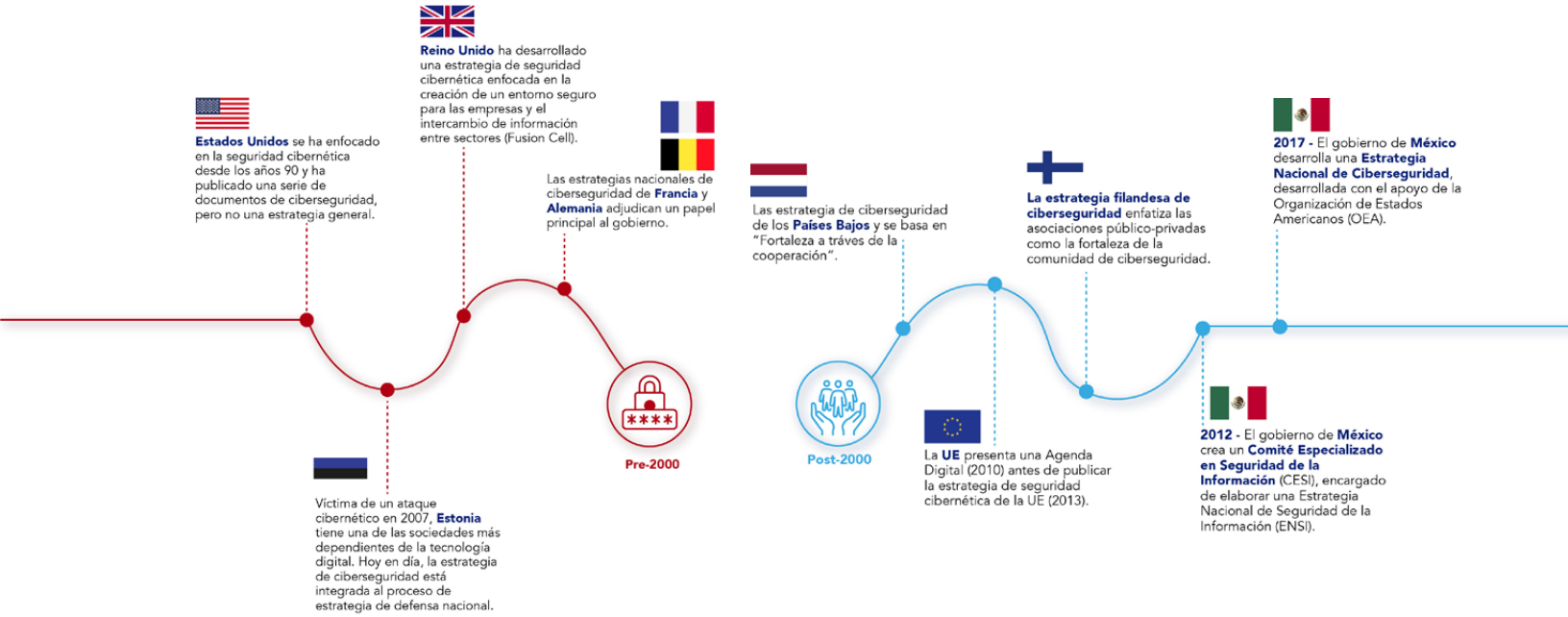


Por otra parte, aunque las estrategias nacionales de ciber resiliencia se enfocan en acciones del sector público, las estrategias de algunos países como Finlandia tienen un enfoque en la cooperación intersectorial (McKinsey & Company, 2018), sobre todo considerando que las empresas operan en un mundo en el que el 95% de los problemas de seguridad cibernética pueden atribuirse a un error humano, y donde las amenazas internas (intencionales o accidentales) representan el 43% de todas las infracciones (World Economic Forum, 2022).

En Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) ha creado un marco de ciberseguridad. Para contrarrestar la proliferación de código malicioso y ayudar en la detección temprana, en ese marco se recomienda el monitoreo continuo y en tiempo real de todos los recursos electrónicos. En Australia, el Centro Australiano de Seguridad Cibernética (ACSC) publica periódicamente orientaciones sobre la forma en que las organizaciones pueden contrarrestar las últimas amenazas a la ciberseguridad (Kaspersky, 2022a).

En México, a fin de proveer una herramienta práctica que permita incrementar la resiliencia cibernética de las mipymes, la Guardia Nacional ha elaborado un *Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa (mipyme)* en el que describe buenas prácticas y recomendaciones para el debido cumplimiento de obligaciones respecto al manejo de información privada (CERT-MX, 2020).

Documentos de estrategia nacional de ciberseguridad publicados en 2008-2017 en los países de la OCDE

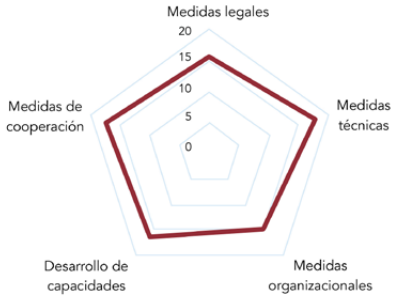


Fuente: adaptada de McKinsey & Company (2018).

En el *Índice Global de Ciberseguridad 2020*, México ocupa el lugar 52 de 182 países, con una calificación de 81.68 puntos sobre 100 posibles. En tal estudio se señala que las principales áreas en las que México requiere mejorar son: legislación y la de medidas organizacionales, lo cual indica un norte para la promoción de mejoras en esta materia.

México en el *Índice Global de Ciberseguridad 2020*

México



Nivel de desarrollo:
Desarrollo del país

Áreas relevantes
Medidas técnicas y de cooperación

Áreas de crecimiento potencial
Medidas organizacionales

Puntaje general	Medidas legales	Medidas técnicas	Medidas organizacionales	Desarrollo de capacidades	Medidas de cooperación
81.68	15.61	17.90	14.70	16.13	17.34

Fuente: adaptada de ITU (2020).

Orientación para mejorar las políticas de ciberseguridad

Con el objetivo proporcionar un marco útil, flexible y fácil de usar para establecer el contexto de la visión socioeconómica de un país y ayudar a los responsables de la formulación de políticas para el desarrollo de una estrategia que tenga en cuenta la situación específica de un país, la ITU ha desarrollado diferentes versiones de la *Guide to Developing a National Cybersecurity Strategy*. Se trata de documentos que proporcionan un marco que ha sido acordado por organizaciones con experiencia demostrada y diversa en esta área temática y se basa en su trabajo previo y experiencia exitosas (ITU, 2021) .

Es claro que la ciberseguridad ya no puede considerarse un tema exclusivamente técnico que se delegue en el personal de tecnologías de la información de las organizaciones, sino que debe abordarse como tema estratégico que alcanza a toda la organización. A medida que las amenazas cibernéticas continúan creciendo, los seguros contra riesgos informáticos serán cada vez más precarios y las propias empresas aseguradoras enfrentarán posibles juicios y represalias por intentar frenar los pagos por *ransomware.* Por lo tanto, cuando ocurre un ataque, las empresas se verán obligadas a pagar rescates cada vez más altos o sufrir las consecuencias reputacionales, financieras, regulatorias y legales de los ciberataques. Lo mejor es tener una estrategia robusta y coordinada dentro del ecosistema.

Finalmente, de acuerdo con el análisis más reciente del Instituto Español de Estudios Estratégicos, son diez los aspectos clave que pueden dirigir el futuro de la ciberseguridad (Candau, 2021):

- Estrategia Nacional de Ciberseguridad, donde se establece la visión, el alcance, los objetivos y las prioridades.
- Instauración de una estructura de gobierno clara, que identifique e involucre a las partes interesadas: gobernanza.

- Realizar un balance de las políticas, regulaciones y capacidades existentes: desarrollo reglamentario viable con apoyo en un marco jurídico operativo y eficaz.
- Incrementar la capacidad de prevención, detección y respuesta ante ciberamenazas.
- Desarrollo e implementación de sistemas de alerta temprana, fortaleciendo la capacidad de detección y establecimiento de mecanismos de notificación de incidentes.
- Incremento de la vigilancia, con un servicio de evaluación continua basado en centros de operaciones de ciberseguridad que permitan conocer en cada momento la superficie de exposición ante una posible amenaza.
- Desarrollar y mantener actualizados perfiles profesionales cualificados en todos los niveles (dirección, gestión, implantación y usuarios) para protegerse de las ciberamenazas.
- Impulso de acciones destinadas a reforzar la colaboración público-privada y la seguridad y robustez de las redes, productos y servicios de las TIC empleados por el sector industrial. Institucionalizar la cooperación entre los organismos públicos y la empresa privada como clave para construir comunidad.
- Implementar mecanismos confiables de intercambio de información entre organismos, públicos y privados, tanto de análisis de ciberamenazas como de notificación de ciberincidentes.
- Comunicación y sensibilización en ciberseguridad para toda la ciudadanía.

En resumen, como conclusión de este primer boletín de vigilancia tecnológica, se puede afirmar que la ciberseguridad es un tema estratégico que compromete el desarrollo económico y social de un país, dada la importancia que tienen las tecnologías de la información y comunicación. Los desafíos son cada vez mayores porque las redes de interconexión crecen exponencialmente debido al internet de las cosas que pone en contacto dispositivos inteligentes y sensores instalados en los más diversos equipos, así como por el enorme aumento de capacidad que conlleva 5G.

La atención a esos desafíos debe involucrar a múltiples actores a diferentes niveles: los gobiernos son responsables de generar una regulación efectiva, basada en un esquema innovador de gestión de riesgos; las empresas proveedoras de equipos, redes y sistemas deben habilitar esquemas de protección y cumplir con estándares de buenas prácticas; los operadores son el punto de contacto con los usuarios y, por ello, tienen a su cargo la implementación de sistemas eficaces de protección; las empresas de ciberseguridad deben mantener una tasa de innovación acorde con las necesidades de candados más seguros y sofisticados que preserven la integridad de los sistemas; los usuarios empresariales deben preocuparse, en su mejor interés, de contar con herramientas de protección y esquemas de buenas prácticas; y, finalmente, los usuarios individuales deben sensibilizarse sobre la importancia de evitar conductas que ponen en riesgo no sólo sus dispositivos sino redes completas. Se trata de un asunto sistémico que requiere una respuesta estratégica y sinérgica.

Trabajos citados

Aranda, J., Sacoto, Erwin J., Haro, D. y Astudillo, F. (2021). Redes 5G: una revisión desde las perspectivas de arquitectura, modelos de negocio, ciberseguridad y desarrollos de investigación. Recuperado de http://scielo.senescyt.gob.ec/pdf/rns/v4n1/2631-2654-rns-4-01-00006.pdf

Avancis (2021). Tipos de seguridad informática y ciberseguridad. Recuperado de https://www.avansis.es/ciberseguridad/tipos-de-seguridad-informatica/#Seguridad_de_software

Bravo, J. (2022). 5G y ciberseguridad. *El Economista.* Recuperado de https://www.eleconomista.com.mx/opinion/5G-y-ciberseguridad-20220520-0029.html

Candau, J. (2021). Ciberseguridad. Evolución y tendencias. IEEE. Recuperado de https://www.ieee.es/Galerias/fichero/docs_marco/2021/DIEEEM11_2021_JAVCAND_Ciberseguridad.pdf

Castells, M. (1999). La revolución de la tecnología de la información. Recuperado de https://1library.co/document/6zkl2j8y-manuel-castells-la-revolucion-de-las-tic.html

Castells, M. (1996). *La era de la información. Economía, sociedad y cultura*, (Vol. 1). México: Siglo XXI.

Catania, C. (2021). ¿Es más seguro el 5G que el 4G? *A adsl Zone*. Recuperado de https://www.adslzone.net/noticias/redes/diferencias-evolucion-seguridad-4g-5g/

Centro Nacional de Respuesta a Incidentes Cibernéticos [CERT-MX] (2020). *Manual Básico de Ciberseguridad para la Micro, Pequeña y Mediana Empresa.* CDMX: Secretaría de Seguridad y Protección Ciudadana y Guardia Nacional. Recuperado de https://www.gob.mx/cms/uploads/attachment/file/682364/MANUAL_B_SICO_CIBERSEGURIDAD_MIPYMES_2021_11_18.pdf

Chohan, U. W. (2022). Metaverse or Metacurse? SSRN. Recuperado de doi:http://dx.doi.org/10.2139/ssrn.4038770

Cortés, M. (15 de febrero de 2022). México sufrió más de 156 mil millones de intentos de ciberataques en 2021. *CIO México*. Recuperado de https://cio.com.mx/mexico-sufrio-mas-de-156-mil-millones-de-intentos-de-ciberataques-en-2021/

DPL News (2022). Huawei: transparencia ante el mundo y cuidado end to end para reducir el riesgo a cero. Recuperado de https://dplnews.com/wp-content/uploads/2022/05/Huawei-transparencia-ante-el-mundo-y-cuidado-end-to-end-para-reducir-el-riesgo-a-cero-ciberseguridad.pdf

El País (2021). Ciberseguridad y 5G: una tecnología más segura en un entorno más complejo. Recuperado de https://elpais.com/tecnologia/5g-el-futuro-es-ahora/2021-10-29/ciberseguridad-y-5g-una-tecnologia-mas-segura-en-un-entorno-mas-complejo.html

GSMA Latin America (2018). Seguridad y privacidad en las redes móviles Desafíos, propuestas y consideraciones para los gobiernos. Recuperado de https://www.gsma.com/latinamerica/wp-content/uploads/2018/04/Seguridadyprivacidad.pdf

Hoehn, M. (junio de 2021). Desafíos de seguridad del 5G. Serie Minutas N° 57-21. Biblioteca del Congreso Nacional, Departamento de Estudios, Extensión y Publicaciones. Recuperado de https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/32305/1/N_57_21_Desafios_seguridad_5G.pdf

Huawei Technologies (2022). Información de la empresa: ¿Quiénes somos? *Huawei.* Recuperado de https://www.huawei.com/mx/corporate-information

IBM (5 de mayo de 2022). What is cybersecurity? Recuperado de https://www.ibm.com/topics/cybersecurity

IBM Segurity (2021). *Cost of a Data Breach Report.* eBook: IBM Corporation. Recuperado de https://info.techdata.com/rs/946-OMQ-360/images/Cost_of_a_Data_Breach_Report_2021.PDF?msclkid=19e1d063d0a211ec8530d8a3a1ef14cd

Instituto Federal de Telecomunicaciones [IFT] (s.f.). Glosario de Ciberseguridad. Recuperado de http://www.ift.org.mx/sites/default/files/contenidogeneral/usuarios-y-audiencias/glosariodeciberseguridadift.pdf

International Telecommunication Union [ITU] (2022). *Guilde to Developing a National Cybersegurity Strategy.* ITU. Recuperado de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx

ITU (2021). The NCS Guide 2021. *Guide to Developing a National Cybersecurity Strategy.* ITU. Recuperado de https://ncsguide.org/the-guide/

ITU (2020). *Global Cybersecurity Index 2020.* ITU. Recuperado de https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Instituto Nacional de Estadística y Geografía [Inegi] (2020). En México hay 80.6 millones de usuarios de internet y 86.5 millones de usuarios de teléfonos celulares: Endutih 2019. Recuperado de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2020/OtrTemEcon/ENDUTIH_2019.pdf

Jayakody, D. N. (2019). *5G Enabled Secure Wireless Networks.* eBook: Sprinnger.

Jiménez, J. (2021). No configurar bien la nube es culpable de la mayoría de vulnerabilidades. Redes Zone. Recuperado de https://www.redeszone.net/noticias/seguridad/configurar-mal-nube-vulnerabilidades/

Kaspersky Lab. (2022a). ¿Qué es la ciberseguridad? AO *Kaspersky Lab.* Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky Lab. (2022b). ¿Es peligrosa la tecnología 5G? Pros y contras de la red 5G. *AO Kaspersky Lab.* Recuperado de https://www.kaspersky.es/resource-center/threats/5g-pros-and-cons

Larocca, N. (2022). Huawei: transparencia ante el mundo y cuidado end to end para reducir el riesgo a cero. Especiales DPL Ciberseguridad. Recuperado de https://dplnews.com/especiales-dpl-ciberseguridad-huawei-transparencia-ante-el-mundo-y-cuidado-end-to-end-para-reducir-el-riesgo-a-cero/

McKinsey & Company (2018). *Perspectiva de ciberseguridad en México. CDMX:* McKinsey & Company. Recuperado de https://consejomexicano.org/multimedia/1528987628-817.pdf

Paloalto Networks (2022). Cybersecurity. Recuperado de https://www.paloaltonetworks.com/cyberpedia/cyber-security

Panda Security Summit [PASS] (2018). Ciber Resiliencia: la clave de la seguridad empresarial. Recuperado de https://www.pandasecurity.com/es/mediacenter/src/uploads/2018/05/Informe-Ciber-resiliencia-ES.pdf

Parlamento Europeo y Consejo de la Unión Europea (2019). Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»). *Diario Oficial de la Unión Europea.* Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=FR

Proofpoint (2022). ¿Qué es la seguridad móvil? Recuperado de https://www.proofpoint.com/es/threat-reference/mobile-security

Ramírez, D. (2015). La visión internacional de la ciberseguridad. IEEE. Recuperado de https://www.ieee.es/Galerias/fichero/docs_informativos/2015/DIEEEI02-2015_VisionInternacional_Ciberseguridad_DRM.pdf

Riquelme, R. (9 de enero de 2022). Ciberseguridad México 2021: ramsomware y robo de credenciales. *El Economista.* Recuperado de https://www.eleconomista.com.mx/tecnologia/Ciberseguridad-Mexico-2021-ransomware-y-robo-de-credenciales-20220107-0046.html

Salvador de, L. (2015). Ciber-resiliencia. Instituto Español de Estudios Estratégicos, IEEE. Recuperado de https://dialnet.unirioja.es/servlet/articulo?codigo=7685521

Silvera, C. (2005). La alfabetización digital: una herramienta para alcanzar el desarrollo y la equidad en los países de América latina y el Caribe. Acimed, 12(1). Recuperado de http://eprints.rclis.org/6354/1/Alfabetizacion.pdf

The Competitive Intelligence Unit [The CIU] (mayo de 2022). *18° Estudio sobre los Hábitos de Personas Usuarias de Internet en México 2022.* Asociación de Internet. Recuperado de https://irp.cdn-website.com/81280eda/files/uploaded/18%C2%B0%20Estudio%20sobre%20los%20Habitos%20de%20Personas%20Usuarias%20de%20Internet%20en%20Mexico%202022%20%28Publica%29_5nrP1CIgQ6AQyAPByamX.pdf

Unión Internacional de Telecomunicaciones [UIT] (2010). Ciberseguridad. Recuperado de https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf

World Economic Forum (2022). *The Global Risks Report 2022.* World Economic Forum. Recuperado de https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Universidad Nacional Autónoma de México

ICAT
Instituto de Ciencias Aplicadas y Tecnología

HUAWEI