XUNTA DE GALICIA

Nota Sectorial

Ciberseguridad en México

XUNTA DE GALICIA

Esta nota sectorial ha sido elaborada por
Belén Bouzas Duro

Bajo la supervisión de la Antena Igape México

Abril 2024

XUNTA DE GALICIA

Índice General

XUNTA DE GALICIA

1. Resumen ejecutivo

La presente nota sectorial, tiene como objetivo el análisis del sector de la ciberseguridad en México. A lo largo de la misma, se tratarán aspectos clave como el panorama actual en el país, los principales actores, el marco regulatorio, las organizaciones y ferias más relevantes del mercado mexicano.

2. Definición del sector

La seguridad informática, también conocida con el nombre de Ciberseguridad se refiere a cualquier tecnología, medida o práctica para prevenir ataques informáticos o mitigar su impacto. La ciberseguridad tiene como objetivo proteger los sistemas, las aplicaciones, los dispositivos informáticos, los datos confidenciales y los activos financieros de personas y organizaciones contra virus informáticos simples y molestos, al igual, que contra los virus más sofisticados y costosos.

Las tendencias de las tecnologías de la información (TI) de los últimos años fuertemente influenciadas por la pandemia y la adaptación del mundo a un ritmo vertiginoso a la nueva realidad, supusieron un aumento considerable de la adopción de la computación en la nube, la complejidad de las redes, el trabajo remoto y desde casa, los programas “bring your own device” (BYOD) y los dispositivos y sensores conectados a otros dispositivos, han dado lugar a enormes ventajas empresariales y al progreso humano, pero también han creado un nuevo marco de actuación donde cada vez existen más formas de atraque para los delincuentes cibernéticos.

Actualmente, la tendencia apunta hacia acceder, modificar o destruir información confidencial, extorsionar a los usuarios e interrumpir la continuidad del negocio.

2.1 Amenazas comunes para la Ciberseguridad

Según una estimación realizada por IBM la ciberdelincuencia le costará a la economía mundial 10.5 billones de dólares en el año 2025.

Los tipos de amenaza más comunes en la ciberseguridad son:

1. Malware: en castellano “software malicioso”, es un software que un cibercriminal o un hacker ha creado para interrumpir o dañar el equipo de un usuario legítimo. Con frecuencia programado a través de un archivo adjunto de correo electrónico no solicitado o de una descarga de apariencia legítima. Casi todos los ciberataques modernos implican algún tipo de malware.

Los hackers y los delincuentes cibernéticos crean y utilizan malware para obtener acceso no autorizado a sistemas informáticos y datos confidenciales, secuestrar sistemas informáticos y operarlos de forma remota, interrumpir o dañar los sistemas informáticos o retener datos o sistemas como rehenes por grandes sumas de dinero.

Hay **diferentes tipos de malware**, entre los que se incluyen los siguientes:

- *Virus:* es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código.

- *Troyanos:* es un tipo de malware que se disfraza como software legítimo. Los cibercriminales engañan a los usuarios para que carguen troyanos a sus computadoras, donde causan daños o recopilan datos.
- *Spyware:* es un tipo de software que se instala en el ordenador sin que el usuario tenga constancia de ello. Suele venir oculto junto a otros programas que se instalan de manera consciente, lo que hace muy difícil de detectar. Una vez en el ordenador, recopila información para enviarla a terceros.
- *Ransomware:* es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción.
- *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.

2. Phishing: es cuando los cibercriminales atacan a sus víctimas con correos electrónicos que parecen ser de una empresa legítima que solicita información confidencial. Los ataques de phishing se utilizan a menudo para inducir a que las personas entreguen sus datos de tarjetas de crédito u otra información personal.

3. "Man in the middle": es un tipo de ciberamenaza en la que un cibercriminal intercepta la comunicación entre dos individuos para robar los datos. Por ejemplo, en una red Wi-Fi no segura, un atacante podría interceptar los datos que se transmiten desde el dispositivo de la víctima y la red.

4. Inyección de código SQL: sus siglas en inglés significan Structured Query Language, es un tipo de ciberataque utilizado para tomar el control y robar datos de una base de datos. Los cibercriminales aprovechan la vulnerabilidades de las aplicaciones basadas en datos para insertar código malicioso en una base de datos mediante una instrucción SQL maliciosa. Esto les brinda acceso a la información confidencial contenida en la base de datos.

5. Ataque de denegación de servicio (DDoS): es cuando los cibercriminales impiden que un sistema informático satisfaga solicitudes legítimas sobrecargando las redes y los servidores con tráfico. Esto hace que el sistema sea inutilizable e impide que una organización realice funciones vitales. El volumen global de ataques DDoS se disparó durante la pandemia de COVID-19. Cada vez más, los atacantes combinan ataques de DDoS con ataques de ransomware.

6. Amenazas internas: son amenazas que se originan de usuarios autorizados que intencional o accidentalmente hacen mal uso del acceso legítimo o cuyas cuentas son secuestradas por delincuentes cibernéticos. Las amenazas internas pueden ser más difíciles de detectar que las amenazas externas porque tienen las marcas de actividad autorizada y porque son invisibles para el software antivirus, los cortafuegos y otras soluciones de seguridad destinadas a bloquear ataques externos.

2.2 Tipos de ciberseguridad

Una estrategia de ciberseguridad sólida protege todas las capas o dominios relevantes de la infraestructura de TI contra las ciberamenazas y la ciberdelincuencia.

1. Seguridad de la infraestructura crítica: protege los sistemas informáticos, las aplicaciones, las redes, los datos y los recursos digitales de los que depende de una sociedad para la seguridad nacional, la integridad económica y la seguridad pública.

2. Seguridad de la red: evita el acceso no autorizado a los recursos de red, detecta y detiene los ciberataques y las violaciones de seguridad de la red en curso, al mismo tiempo que garantiza que los usuarios autorizados tengan acceso seguro a los recursos de red que necesitan, cuando los requieran.

3. Seguridad de endpoint: los servidores, ordenadores de mesa, portátiles y dispositivos móviles siguen siendo el principal punto de entrada de los ciberataques. La seguridad de endpoints protege estos dispositivos y a sus usuarios contra ataques y también protege la red contra los adversarios que aprovechan los endpoints para lanzar ataques.

4. Seguridad de las aplicaciones: protegen las aplicaciones que se ejecutan "on premises" y en la nube, evitando el acceso y el uso no autorizados de aplicaciones y datos relacionados, evitando fallos o vulnerabilidades en el diseño de las aplicaciones que los hackers puedan utilizar para infiltrarse en la red.

5. Cloud security: protege los servicios, activos, aplicaciones, datos, almacenamiento, las herramientas de desarrollo, los servidores virtuales y la infraestructura en la nube. En términos generales, la seguridad en la nube opera según el modelo de responsabilidad compartida: el proveedor de la nube es responsable de proteger los servicios que ofrecen y la infraestructura, mientras que el cliente es responsable de proteger sus datos, su código y otros activos que almacena o ejecuta en la nube.

6. Seguridad de la información: se refiere a la protección de toda información importante para una organización: archivos, datos digitales, documentos en papel, medios físicos, incluso el habla humana, contra el acceso, la divulgación, el uso o la alteración no autorizados. La seguridad y protección de los datos y la información digital es el enfoque de la mayoría de las medidas de InfoSec relacionadas con la seguridad cibernética.

2.3 Tecnologías clave de ciberseguridad y mejores prácticas

Las siguientes prácticas y tecnologías pueden ayudar a las organizaciones a implantar una ciberseguridad sólida que reduzca su vulnerabilidad frente a los ataques cibernéticos y proteja sus sistemas de información críticos, sin que interfieran la experiencia del usuario o del cliente.

1. Concientización sobre seguridad: muchos usuarios no entienden como acciones aparentemente inofensivas aumentan su propio riesgo de ataque o el de su organización. La concienciación sobre seguridad combinada con políticas de seguridad de datos bien pensadas, pueden ayudar a los empleados a proteger los datos confidenciales, tanto de carácter personal como privados de la organización. Estas capacitaciones o programas de concienciación pueden ayudar a los empleados a reconocer y evitar ataques de phishing y malware.

2. Gestión de identidad y acceso: la gestión de identidad y acceso (IAM) define los roles y privilegios de acceso para cada usuario, así como las condiciones bajo las cuales se le otorgan o niegan accesos. Las tecnologías de IAM incluyen autentificación multifactor, que requiere al menos una credencial además de nombre de usuario y contraseña.

3. Gestión de la superficie de ataque: es el descubrimiento, análisis, corrección y monitoreo continuo de las vulnerabilidades de ciberseguridad y los posibles puntos débiles que conforman la superficie de ataque de una organización. A diferencia de otras disciplinas de defensa cibernética, la perspectiva desde el que se analiza el escenario y las medidas a adoptar es desde el punto de vista del hacker. Identifica los objetivos y evalúa los riesgos en función de las oportunidades que presentan a un atacante malicioso.

4. Detección, prevención y respuesta a amenazas: debido a que es imposible detener todos los ataques cibernéticos, las organizaciones confían en las tecnologías impulsadas en analytics e inteligencia artificial (IA) para identificar y responder a posibles ataques o a ataques reales en curso. Estas tecnologías pueden incluir entre otras, gestión de eventos e información de seguridad, orquestación, automatización y respuesta a la seguridad y detección y respuesta de endpoints. Normalmente, estas tecnologías se utilizan y forman parte del plan formal de respuesta ante incidentes.

5. Recuperación ante desastres: Si bien no se utiliza tecnología de ciberseguridad, las capacidades de recuperación ante desastres suelen desempeñar un papel clave en el mantenimiento de la continuidad de negocio en caso de un ciberataque. Por ejemplo, la capacidad de poder alojar una copia de seguridad en una ubicación remota puede permitir que una empresa reanude las operaciones rápidamente después de un ataque de ransomware y sin necesidad de tener que pagar un rescate.

2.4 Consejos de ciberseguridad

- **Actualizar el software y el sistema operativo:** de esta forma estará actualizado y contando con las últimas revisiones de seguridad.
- **Utilizar software antivirus:** las soluciones de seguridad intentarán detectar y eliminarán las máximas amenazas posibles.
- **Utilizar contraseñas seguras:** asegúrese de que sus contraseñas no sean fáciles de adivinar.
- **No abrir archivos adjuntos de correos electrónicos de remitentes desconocidos:** podrían estar infectados con malware.
- **No hacer clic en los vínculos de los correos electrónicos de remitentes o sitios web desconocidos:** es una forma común de propagación de malware.
- **Evitar el uso de redes Wi-Fi no seguras en lugares públicos:** las redes no seguras lo dejan vulnerable a ataques del tipo “Man in the middle”.

3. La Ciberseguridad en México

El Índice de Ciberseguridad Global (ICG) es una iniciativa de la Unión Internacional de Telecomunicaciones (ITU), el organismo de las Naciones Unidas especializado es las TIC (tecnologías de la información y de la comunicación). Es una herramienta que evalúa el compromiso de los países con la ciberseguridad. Este índice proporciona una clasificación global que muestra el nivel de desarrollo de la ciberseguridad en diferentes países. Evalúa factores como la legislación, la capacidad técnica, la cooperación internacional y la concienciación pública en ciberseguridad.

La última versión publicada del ranking es la del año 2020, en el México se posiciona en el puesto número 52 con una puntuación de 81.68 sobre 100 puntos, mejorando 11 posiciones respecto a la anterior clasificación del año 2018, lo que implica que en los últimos años el país ha implementado medidas relacionadas con la ciberseguridad que mejoraron su situación en general. Dentro del continente americano se sitúa en la posición cuarta, tras EEUU, Canadá y Brasil. España por su parte se posiciona en el cuarto lugar del ranking global tras EEUU, Reino Unido y Estonia, con una puntuación de 98.52 sobre 100.

3.1 La problemática de México

En el año 2023 se celebró en México el "World Legal Summit". En este congreso se habló sobre como el mundo está cada vez más interconectado y como la ciberseguridad se ha convertido en una preocupación capital y de vital importancia para todas las naciones del mundo. Además, abordan cuales son los retos más significativos que el país enfrenta en esta área, cuáles son sus principales problemáticas y como el país debe de abordarlas para fortalecer su postura en ciberseguridad.

3.1.1 Falta de conocimiento en materia de ciberseguridad

Uno de los principales problemas del país radica en la falta de conocimiento de los usuarios mexicanos en materia de ciberseguridad. La gran mayoría de las personas desconocen los mecanismos de protección en internet, así como las buenas prácticas para mantener protegida la información que se genera a través del tiempo.

Por otro lado, se desconocen los mecanismos que utilizan los delincuentes cibernéticos para extraer la información privilegiada, aumentando la vulnerabilidad de los usuarios y causando que estos caigan en trampas que hacen que su información caiga en las manos equivocadas.

3.1.2 Falta de dimensión de los daños causados por ataques informáticos

Otro desafío es la falta de conciencia sobre la gravedad de los daños causados por los ataques informáticos. Muchos usuarios subestiman la probabilidad de ser víctimas y, en caso de un incidente, no comprenden la magnitud de las pérdidas potenciales.

Alguno de los bienes que deben de ser protegidos por parte de los usuarios, así como de los proveedores de sistemas informáticos son, entre otros, datos personales, privados y financieros.

En cuanto a las empresas, resulta más amplio el alcance de los bienes a proteger, información confidencial, alianzas estratégicas, estatus jurídico y financiero, estrategias y estructura organizativa, son en definitiva, algunos de los bienes que deben de ser protegidos.

3.1.3 Falta de desarrollo de herramientas de ciberseguridad

Si bien es cierto que existen algunas organizaciones que proveen algunos productos o mecanismos que protejan los bienes intangibles y la información de los usuarios, son pocas las empresas que ofrecen soluciones específicas y avanzadas en materia de ciberseguridad, por eso, México enfrenta una falta de desarrollo de herramientas avanzadas en este campo.

Es esencial identificar empresas que se enfoquen en las necesidades individuales, empresariales e institucionales y promover la implementación de mecanismos de defensa adecuados.

3.1.4 Políticas públicas mal enfocadas

Las políticas públicas relacionadas con la ciberseguridad en México aún no han recibido la prioridad y atención adecuada. A pesar de los esfuerzos, el país no logra abordar de manera completa o eficaz las necesidades que se viven en la realidad del país, prueba de ello es que la legislación por parte del Estado, así como el

presupuesto destinado a la ciberseguridad son insuficientes.

3.1.5 Ausencia de homologación de la legislación en delitos cibernéticos

Tanto el Código Penal Federal, como los códigos penales estatales contemplan los delitos cibernéticos definiendo la conducta delictiva, así como la sanción que conlleva dicho comportamiento.
Sin embargo, tanto en el ámbito federal como en los diferentes estados del país no es uniforme la definición de la conducta delictiva en materia de seguridad, ni contemplan las mismas penas o sanciones para quienes incurran en este tipo de acciones. Este punto de discrepancia genera incertidumbre jurídica y se requiere de una mayor uniformidad para brindar claridad a los usuarios de sistemas cibernéticos.

3.1.6 Falta de cooperación entre actores

La cooperación entre los actores involucrados en incidentes de ciberseguridad es esencial. Tanto los usuarios finales como los proveedores de sistemas y otros actores deben colaborar para prevenir y abordar los ataques de manera efectiva.

3.2 Cifras clave

Los efectos de la digitalización en la sociedad mexicana, la permanencia del trabajo remoto y la irrupción de la inteligencia artificial han enfatizado la necesidad de contar con una estrategia nacional de ciberseguridad y la importancia de este sector en la sociedad, tanto en el ámbito empresarial como en el individual.

México registró en el año 2023 un total de 94 mil millones de ataques cibernéticos, lo que le convierte en el primer país de América Latina, ya que casi la mitad de los ciberataques registrados en el mismo período, un total de 200 mil millones tienen como objetivos el país, seguido de Brasil y Colombia.

En el último trimestre del 2023 se observó un alarmante aumento exponencial en las actividades maliciosas detectadas, experimentando un crecimiento del 950% en comparación con el año anterior. En dicho incremento destaca la creciente sofisticación y agresividad de los ciberataques, lo que pone de manifiesto la imperiosa necesidad de reforzar las medidas de ciberseguridad de las organizaciones.

Por su parte, el ransomware continuó siendo una amenaza en el mercado mexicano colocándose como el sexto país del mundo que más ataques de este tipo recibe, además se observó una presencia significativa de amenazas vinculadas a aplicaciones de Microsoft Office, como Excel, Word y PowerPoint, las cuales representaron casi 50% de todas las detecciones de malware en el país.

En 2024 el país recibe una media de 19 mil ataques diarios, lo que le convierte en uno de los países más expuestos a la inseguridad digital.

3.3 Principales actores

La economía y ubicación geoestratégica de México son un objetivo para las actividades cibernéticas ilícitas, por un lado, el país disfruta de una inversión extranjera directa importante y una evolución positiva del PIB (producto interior bruto) y, por otro, sigue siendo relativamente vulnerable en ciberseguridad y ciberdefensa.

3.3.1 Organismos públicos

En México existen diferentes organismos con competencias en materia de ciberseguridad, pero, principalmente hay dos organismos gubernamentales a nivel federal que están a cargo de la ciberseguridad en México, el CERT-MX y el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

- **Centro de Respuesta a Incidentes Cibernéticos de la Dirección General Científica de la Guardia Nacional (CERT-MX):** apoya a aquellas instituciones del país que tengan una infraestructura crítica de información ante el sufrimiento de un ataque. Se trata de un organismo central para la ciberseguridad en México, ya que debe brindar un servicio de ayuda informático luego de haberse perpetrado un delito informático. Otra de sus tareas es la de controlar que las instituciones gubernamentales cumplan con el Manual Administrativo de Aplicación General de Tecnologías de Información y Comunicaciones y de Seguridad de la Información. De esta manera, es posible asegurarse de que los organismos que tienen información sensible estén aplicando una estrategia adecuada de ciberseguridad en el país. El CERT-MX depende de la *Secretaría de Seguridad Pública y Protección Ciudadana*, responsable de diseñar, planear, ejecutar y coordinar las políticas gubernamentales en materia de seguridad pública.
- **Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI):** tiene el deber de proteger la transparencia, el acceso y la integridad de los datos personales. Se trata de un organismo constitucional que posee autonomía y que fue creado por los convencionales con el objetivo de proteger los derechos elementales: el de acceso a la información pública y el de los datos personales.
- **Secretaría de Marina - Armada de México:** El acuerdo secretarial 335/2022 del 1 de junio de 2022 dispuso que la Unidad de Ciberseguridad (UNICIBER) se constituyera en la Coordinadora General de Ciberespacio (EMCOGCIBER), dependiendo operativa, orgánica y administrativamente del Estado Mayor General de la Armada. Se encarga de proteger el ciberespacio y cuenta con una Estrategia Institucional para el Ciberespacio (2021- 2024).
- **Banco de México:** La principal institución financiera de México cuenta con una estrategia de protección frente a ciberataques que se puede consultar en su web.

3.3.2 Organismos privados, asociaciones y centros de investigación

El mercado de la ciberseguridad es global. En México, muchas de las empresas que operan en el mercado provienen de Estados Unidos, referente del sector. Empresas globales de ciberseguridad como CISCO México (EEUU), Fortinet (EEUU), IBM (EEUU), Palo Alto Networks (EEUU), Trellix (antiguas McAfee + Fire Eye) (EEUU) o ATOS (Francia) también tienen en México una considerable cuota del mercado. Sin embargo, cada vez más, otros actores irrumpen en el mercado debido a las posibilidades que ofrece el país.

Las empresas mexicanas más importantes del sector en México son: SCITUM (división de Telmex), Octapus (antiguo 2Secure), CERO, Grupo Scanda, Totalsec (Grupo Salinas), NETRIX, IQSEC, Delta Protect, KIO Networks o ProtekNet.

Algunas de las asociaciones relevantes en el sector son:

- **Asociación Mexicana de Ciberseguridad (AMECI):** organización que ofrece consultoría, capacitación, servicios y soluciones relacionadas con la seguridad de la información.
- **Asociación Mexicana de la Industria de las Tecnologías de la Información (AMITI):** representa a las empresas de tecnología de México, para impulsar la interacción dentro de la industria y facilitar la

conexión entre la administración pública, la educación y otros organismos empresariales nacionales e internacionales.

- **Asociación de Internet de México (AIMX):** provee información sobre distintas temáticas del mundo digital. Actúa como marco de referencia en temas claves para el desarrollo e implementación de proyectos normativos y de política pública que ayuden en la productividad y la competitividad de México.

México cuenta también con algunos de los centros de investigación del sector de la ciberseguridad más importantes de América Latina.

- **Centro de Investigación en Computación (CIC):** es parte del Instituto Politécnico Nacional (IPN) y se dedica a la investigación en áreas de computación, incluyendo la ciberseguridad.
- **Instituto Nacional de Astrofísica, Óptica y Electrónica (INAOE):** aunque su enfoque principal es la astrofísica y la óptica, también realiza investigaciones en ciberseguridad, particularmente en el desarrollo de tecnologías de seguridad de la información.
- **Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional (CINVESTAV):** tiene varios departamentos dedicados a la investigación en tecnología de la información y la comunicación, donde se incluyen temas de ciberseguridad.
- **Centro Nacional de Investigación y Desarrollo Tecnológico (CENIDET):** se especializa en investigación aplicada en áreas como la electrónica, las telecomunicaciones y la computación con un enfoque en la seguridad cibernética.
- **Centro de Investigación en Matemáticas (CIMAT):** aunque su enfoque principal es la investigación matemática, también realiza investigaciones en áreas relacionadas con la seguridad informática y la criptografía.
- **Clúster TIC de Nuevo León (CSOFTMTY):** subcomité del Clúster TIC de Monterrey donde se educa e investiga sobre el conocimiento integral acerca de la protección de la información.

3.4 La oferta gallega y española

El sector de la ciberseguridad cada vez va adquiriendo mayor relevancia en España y prueba de ello es el creciente número de empresas que se dedican al sector y que hacen de él, gracias a la diversificación de actividades dentro del mismo, uno de los principales países del mundo en materia de ciberseguridad.

Al igual que en el resto de España, el sector de la ciberseguridad en Galicia ha experimentado un crecimiento significativo y en los últimos años se han llevado a cabo iniciativas que impulsan el sector y el desarrollo de soluciones de alto valor tecnológico. Con este objetivo nació el proyecto de la Ciudad de las TIC ubicada en Coruña para fomentar la innovación digital, crear un entorno fuerte que se pueda retroalimentar en diferentes disciplinas y que se convierta en un hub tecnológico digital de referencia a nivel nacional e internacional.

Algunas de las empresas gallegas más destacadas en el mercado de la ciberseguridad son: Tarlogic, Forensic&Security, Softwariza3, Digintec, Redegal (presente en México), Legalforma, Conecta Comunicaciones y Medios e Inprosec (presente en México).

Algunas de las empresas españolas en el mercado mexicano son: Telefónica Tech, Minsait (Grupo Indra), Ayesa, S21Sec, S2 grupo, Innotec Security (Grupo Enrelgy), Mnemo, OpenCloudFactory, One Esecurity, Ondata Mex, Encora, Grupo Antea, Irum, Konfido, Ikusi (Grupo Velatia), Veridas, Hornet Security, Panda Security, Indra, Grupo Satec, Gestact o CS2.

Según un informe de DBK (observatorio sectorial), los productos con mayor penetración son los relacionados con la protección de las comunicaciones (26%), el control de acceso y la autentificación (18%) y el antimalware (15%).

En cuanto a los servicios, la mayor penetración está en el área de cumplimiento legal (57%), la auditoria técnica (54%), la implantación de soluciones (54%) y el soporte y mantenimiento (42%).

3.5 Oportunidades del mercado

En México abunda el talento y el capital humano, sin embargo, en el sector de la ciberseguridad existen carencias de personal cualificado que haga frente a la creciente necesidad de protección frente a las amenazas. No obstante, existen oportunidades en el mercado y características favorables para el comercio entre ambos países en esta materia como son: el idioma y los precios más competitivos que los de EEUU, la fiabilidad y trayectoria de España y la Unión Europea (Europa es el continente más seguro y menos atacado digitalmente) en la protección del ciberespacio, en términos de calidad-precio-conocimiento, ayudan al posicionamiento del producto nacional en el país.

Los sectores de especial interés de demanda de servicios de ciberseguridad en México son:

- **Sector financiero:** dada la sensibilidad de la información es uno de los sectores con más peligro de recibir ataques.
- **Administración pública:** el Gobierno gestiona gran parte de la infraestructura críticas del país lo que le hace propenso a un ataque.
- **Sanidad:** sucede lo mismo que con el sector financiero, dada la naturaleza sensible del tipo de información que maneja sobre los usuarios.
- **Sector minorista:** el desarrollo de plataformas de e-commerce abre la puerta a que los comercios reciban más ataques a medida que digitalizan sus negocios.
- **Sector industrial:** es uno de los de mayor tamaño en la economía mexicana, lo que aumenta su exposición a ser atacado, a medida que se implanta más tecnología en la producción.

Dos factores potenciarán las oportunidades en el mercado mexicano:

- **Inteligencia artificial:** la inteligencia artificial (IA) puede detectar y prevenir potenciales amenazas, desarrollando modelos predictivos de ciberataques. Por otro lado, la IA también podrá utilizarse para cometer delitos cibernéticos con mayor precisión y sofisticación, lo que incrementa el riesgo en la red. En definitiva, puede convertirse en un arma de doble filo. A pesar de todo, existen oportunidades en un futuro cercano, ya que, va a permitir que las compañías replanteen sus procesos administrativos y productivos, lo que implicará un aumento de la inversión en ciberseguridad.
- **CISO:** el papel del CISO (Chief Information Security Officer) será fundamental en los próximos años. En México estos profesionales - por el momento escasos- se enfrentan a presupuestos reducidos por la falta de conciencia en las organizaciones sobre las amenazas cibernéticas, por lo que, en este aspecto, se podría considerar como una oportunidad conseguir concienciar a las empresas mexicanas de la importancia que tiene una buena estrategia de ciberseguridad y el desarrollo que tendrá el papel de estos profesionales en el futuro.

3.6 Claves de acceso al mercado

3.6.1 Distribución

La cadena de distribución de la ciberseguridad comprende tres tipos de agentes en general: fabricantes, distribuidores y prestadores de servicios que ofertan hardware, software o servicios especializados.

A pesar de que los servicios de ciberseguridad se pueden prestar de forma remota, en México es importante estar presente físicamente, ya que, es un hecho que el mercado valora mucho y que genera imagen de marca. Se recomienda la creación de una filial que dé soporte técnico y atención al cliente o establecer alianzas estratégicas con socios locales con capacidad de venta y distribución de productos y/o servicios que ya cuenten con una dilatada experiencia y conocimiento sobre el mercado mexicano.

3.6.2 Legislación aplicable y otros requisitos

En cuanto a la legislación en materia de ciberseguridad en México, lo cierto es que aún queda mucho por hacer. La creciente cantidad de ataques cibernéticos favorecieron a que las autoridades empezaran a comprender la gravedad del problema y comprendan la urgente necesidad de actuar con firmeza y decisión.

A día de hoy la Ley Federal de Ciberseguridad no ha sido aprobada por el Congreso y es un tema pendiente que, sin duda, ayudará a combatir y castigar el cibercrimen. Desde el 2018 se han propuesto 11 iniciativas de leyes sobre ciberseguridad diferentes y en diciembre de 2022 se esperaba la aprobación y publicación en el Diario Oficial de la Federación de la Ley Federal de Ciberseguridad, sin embargo, este hecho no llegó a producirse. Esta última propuesta de Ley tiene 11 títulos y 71 artículos y gira en torno a los siguientes ejes: garantizar la seguridad nacional mediante la defensa del espacio digital, crear un marco legal que permita sancionar o tipificar los ciberataques, realización de pruebas de penetración o pentesting anualmente a las instituciones públicas y privadas y crear una Agencia Nacional de Ciberseguridad controlada por el poder Ejecutivo, siguiendo el ejemplo de la UR, EEUU o Brasil.

Aun así, existen otras leyes que abordan la temática desde un lugar secundario. Entre ellas se encuentra la propia Constitución, la Norma Federal de Transparencia y Acceso a la Información Pública, el Código Federal Penal, que tipifica algunos delitos informáticos y la Estrategia Nacional de Ciberseguridad de 2017.

El Gobierno Federal anunció la creación de la Comisión Intersecretarial de Tecnologías de Información y Comunicación y de la Seguridad de la Información (CITICSI) cuya finalidad es coordinar e implementar las políticas federales en materia de TIC y de seguridad de la información, impulsando actividades y estrategias para su aprovechamiento. Previsiblemente sus decisiones impactarán en el contenido de la nueva Ley de Ciberseguridad.

La Estrategia Nacional de Ciberseguridad en México

En 2017 desde el Gobierno mexicano se estableció una estrategia nacional de ciberseguridad con el objetivo de permitir el uso de las TIC de una forma responsable para el desarrollo sostenido de México.

Es una estrategia con un enfoque económico, ya que busca proteger mayormente la economía y la innovación. Es importante para el desarrollo de la industria mexicana que haya buenas medidas en materia de ciberseguridad que permitan que las compañías puedan trabajar sin inconvenientes. La estrategia tiene como objetivo dar una mayor libertad de acción a los individuos, pues, entiende que el ciberespacio es un lugar muy importante para que la población pueda ejercer sus derechos plenamente.

Otro de los ejes transversales de esta estrategia es lograr instalar una cultura de ciberseguridad en México.

Esto consiste en concientizar, educar y formar a las personas y empresas en seguridad informática.

3.7 Ferias

Info SecutiryMéxico: próxima edición 22 - 23 de octubre de 2024
Expo Seguridad México: próxima edición 27 - 29 de mayo de 2025