XUNTA DE GALICIA

Nota Sectorial

Ciberseguridade en México

XUNTA DE GALICIA

Esta nota sectorial foi elaborada por
Belén Bouzas Duro

Baixo a supervisión da Antena Igape México

Abril 2024

XUNTA DE GALICIA

Índice Xeneral

1. Resumo executivo

A presente nota sectorial, ten como obxectivo a análise do sector da ciberseguridade en México. Ao longo da mesma, trataranse aspectos craves como o panorama actual no país, os principais actores, o marco legal que rexe a materia, as organizacións e feiras máis relevantes do mercado mexicano.

2. Definición do sector

A seguridade informática, tamén coñecida co nome de Ciberseguridade refírese a calquera tecnoloxía, medida ou práctica para previr ataques informáticos ou mitigar o seu impacto. A ciberseguridade ten como obxectivo protexer os sistemas, as aplicacións, os dispositivos informáticos, os datos confidenciais e os activos financeiros de persoas e organizacións contra virus informáticos simples e molestos, ao igual, que contra os virus máis sofisticados e custosos.

As tendencias das tecnoloxías da información (TI) dos últimos anos fortemente influenciadas pola pandemia e a adaptación do mundo a un ritmo vertixinoso á nova realidade, supuxeron un aumento considerable da adopción da computación na nube, a complexidade das redes, o traballo remoto e dende casa, os programas "bring your own device" (BYOD) e os dispositivos e sensores conectados a outros dispositivos, deron lugar a enormes vantaxes empresariais e ao progreso humano, pero tamén crearon un novo marco de actuación onde cada vez existen máis formas de atracada para os delincuentes cibernéticos.

Actualmente, a tendencia apunta cara a acceder, modificar ou destruír información confidencial, extorsionar aos usuarios e interromper a continuidade do negocio.

2.1 Ameazas comúns para a ciberseguridade

Segundo unha estimación realizada por IBM a ciberdelincuencia custaralle á economía mundial 10.5 billóns de dólares no ano 2025.

Os tipos de ameaza máis comúns na ciberseguridade son:

1. Malware: en galego "software malicioso", é un software que un cibercriminai ou un hacker creou para interromper ou danar o equipo dun usuario lexítimo. Con frecuencia programado a través dun arquivo adxunto de correo electrónico non solicitado ou dunha descarga de aparencia lexítima. Case todos os ciberataques modernos implican algún tipo de malware.

Os hackers e os delicuentes cibernéticos crean e utilizan malware para obter acceso non autorizado a sistemas informáticos e datos confidenciais, secuestrar sistemas informáticos e operalos de forma remota, interromper ou danar os sistemas informáticos ou reter datos ou sistemas como reféns por grandes sumas de diñeiro.

Hai **diferentes tipos de malware**, entre os que se inclúen os seguintes:

- *Virus:* é un tipo de programa ou código malicioso escrito para modificar o funcionamento dun equipo. Ademais, está deseñado para propagarse dun equipo a outro- Os virus insérense ou se anexan a un programa ou documento lexítimo que admite macros a fin de executar o seu código.
- *Troyanos:* é un tipo de malware que se disfraza como sofware lexítimo. Os cibercriminais enganan os usuarios para que carguen troyanos ás súas computadoras, onde causan danos ou recompilan datos.

- *Spyware:* é un tipo de software que se instala no computador sen que o usuario teña constancia diso. Adoita vir oculto xunto a outros programas que se instalan de maneira consciente, o que fai moi difícil de detectar. Unha vez no computador, recompila información para enviala a terceiros.
- *Ransomware:* é un tipo de programa daniño que restrinxe o acceso a determinadas partes ou arquivos do sistema operativo infectado e pide un rescate a cambio de quitar esta restrición.
- *Adware:* software de publicidade que pode utilizarse para difundir malware.
- *Botnets:* redes de computadoras con infección de malware que os cibercriminais utilizan para realizar tarefas en liña sen o permiso do usuario.

2. Phishing: é cando os cibercriminais atacan ás súas vítimas con correos electrónicos que parecen ser dunha empresa lexítima que solicita información confidencial. Os ataques de phishing utilízanse a miúdo para inducir a que as persoas entreguen os seus datos de tarxetas de crédito ou outra información persoal.

3. "Man in the middle": es un tipo de ciberameaza na que un cibercriminal intercepta a comunicación entre dous individuos para roubar os datos. Por exemplo, nunha rede Wi-fi non segura, un atacante podería interceptar os datos que se transmiten desde o dispositivo da victima e a rede.

4. Inxección de código SQL: as súas siglas en inglés significan Structured Query Language, é un tipo de ciberataque utilizado para tomar o control e roubar datos dunha base de datos. Os cibercriminais aproveitan a vulnerabilidades das aplicacións baseadas en datos para inserir código malicioso nunha base de datos mediante unha instrución SQL maliciosa. Isto bríndalles acceso á información confidencial contida na base de datos.

5. Ataque de denegación de servizo (DDoS): é cando os cibercriminais impiden que un sistema informático satisfaga solicitudes lexítimas sobrecargando as redes e os servidores con tráfico. Isto fai que o sistema sexa inutilizabel e impide que unha organización realice funcións vitais. O volume global de ataques DDoS disparouse durante a pandemia de COVID-19. Cada vez máis, os atacantes combinan ataques de DDoS con ataques de ransomware.

6. Ameazas internas: son ameazas que se orixinan de usuarios autorizados que intencional ou accidentalmente fan mal uso do acceso lexítimo ou cuxas contas son secuestradas por delincuentes cibernéticos. As ameazas internas poden ser máis difíciles de detectar que as ameazas externas porque teñen as marcas de actividade autorizada e porque son invisibles para o software antivirus, devasas e outras solucións de seguridade destinadas a bloquear ataques externos.

2.2 Tipos de ciberseguridade

Unha estratexia de ciberseguridade sólida protexe todas as capas ou dominios relevantes da infraestrutura de TI contra as ciberameazas e a ciberdelincuencia.

1. **Seguridade da infraestrutura crítica:** protexe os sistemas informáticos, as aplicacións, as redes, os datos e os recursos dixitais dos que depende unha sociedade para a seguridade nacional, a integridade económica e a seguridade pública.

2. **Seguridade da rede:** evita o acceso non autorizado aos recursos de rede, detecta e detén os ciberataques e as violacións de seguridade da rede en curso, ao mesmo tempo que garante que os usuarios autorizados teñan acceso seguro aos recursos de rede que necesitan, cando os requiren.

3. **Seguridade de endpoint:** os servidores, computadores de mesa, portátiles e dispositivos móbiles seguen sendo o principal punto de entrada dos ciberataques. A seguridade de endpoints protexe estes dispositivos e aos seus usuarios contra ataques e tamén protexe a rede contra os adversarios que aproveitan os endpoints para lanzar ataques.

4. **Seguridade das aplicacións:** protexen as aplicacións que se executan "on premises" e na nube, evitando o acceso e o uso non autorizados de aplicacións e datos relacionados, evitando fallos ou vulnerabilidades no deseño das aplicacións que os hackers poidan utilizar para infiltrarse na rede.

5. **Cloud security:** protexe os servizos, activos, aplicacións, datos, almacenamento, as ferramentas de desenvolvemento, os servidores virtuais e a infraestrutura na nube. En termos xerais, a seguridade na nube opera segundo o modelo de responsabilidade compartida: o provedor da nube é responsable de protexer os servizos que ofrecen e a infraestrutura, mentres que o cliente é responsable de protexer os seus datos, o seu código e outros activos que almacena ou executa na nube.

6. **Seguridade da información:** refírese á protección de toda información importante para unha organización: arquivos, datos dixitais, documentos en papel, medios físicos, incluso o fala humana, contra o acceso, a divulgación, o uso ou a alteración non autorizados. A seguridade e protección dos datos e a información dixital é o enfoque da maioría das medidas de InfoSec relacionadas coa seguridade cibernética.

2.3 Tecnoloxías crave de ciberseguridade e mellores prácticas

As seguintes prácticas e tecnoloxías poden axudar ás organizacións para implantar unha ciberseguridade sólida que reduza a súa vulnerabilidade fronte aos ataques cibernéticos e protexa os seus sistemas de información críticos, sen que interfiran na experiencia do usuario ou do cliente.

1. Concientización sobre seguridade: moitos usuarios non entenden como accións aparentemente inofensivas aumentan o seu propio risco de ataque ou o da súa organización. A concienciación sobre seguridade combinada con políticas de seguridade de datos ben pensadas, poden axudar aos empregados a protexer os datos confidenciais, tanto de carácter persoal como privados da organización. Estas capacitacións ou programas de concienciación poden axudar aos empregados para recoñecer e evitar ataques de phishing e malware.

2. Xestión de identidade e acceso: a xestión de identidade e acceso (IAM) define os roles e privilexios de acceso para cada usuario, así como as condicións baixo as cales se lle outorgan ou negan accesos. As tecnoloxías de IAM inclúen autenticación multifactor, que require polo menos unha credencial ademais de nome de usuario e contrasinal.

3. Xestión da superficie de ataque: é o descubrimento, análise, corrección e vixilancia continuo das vulnerabilidades de ciberseguridade e os posibles puntos débiles que conforman a superficie de ataque dunha organización. A diferenza doutras disciplinas de defensa cibernética, a perspectiva desde o que se analiza o escenario e as medidas para adoptar é desde o punto de vista do hacker. Identifica os obxectivos e avalía os riscos en función das oportunidades que presentan a un atacante malicioso.

4. Detección, prevención e resposta a ameazas: debido a que é imposible deter todos os ataques cibernéticos, as organizacións confían nas tecnoloxías impulsadas en analytics intelixencia artificial (IA)para identificar e responder a posibles ataques ou a ataques reais en curso. Estas tecnoloxías poden incluír entre outras, xestión de eventos e información de seguridade, orquestración, automatización, resposta á seguridade e detección e

resposta de endpoints. Normalmente, estas tecnoloxías utilízanse e forman parte do plan formal de resposta ante incidentes.

5. Recuperación ante desastres: Aínda que non se utiliza tecnoloxía de ciberseguridade, as capacidades de recuperación ante desastres adoitan desempeñar un papel crave no mantemento da continuidade de negocio en caso dun ciberataque. Por exemplo, a capacidade de poder aloxar unha copia de seguridade nunha localización remota pode permitir que unha empresa renove as operacións rapidamente despois dun ataque de ransomware e sen necesidade de ter que pagar un rescate.

2.4 Consellos de ciberseguridade

- **Actualizar o software e o sistema operativo:** desta forma estará actualizado e contando coas últimas revisións de seguridade.
- **Utilizar software antivirus:** as solucións de seguridade tentarán detectar e eliminar as máximas ameazas posibles.
- **Utilizar contrasinais seguros:** asegúrese de que os seus contrasinais non sexan fáciles de adiviñar.
- **Non abrir arquivos adxuntos de correos electrónicos de remitentes descoñecidos:** poderían estar infectados con malware.
- **Non facer clic nos vínculos dos correos electrónicos de remitentes ou sitios web descoñecidos:** é unha forma común de propagación de malware.
- **Evitar o uso de redes Wi-fi non seguras en lugares públicos:** as redes non seguras déixano exposto e vulnerable a ataques do tipo "Man in the middle".

3. A ciberseguridade en México

O índice de Ciberseguridade Global (ICG) é unha iniciativa da Unión Internacional de Telecomunicacións (ITU), o organismo das Nacións Unidas especializado nas tecnoloxías da información e das comunicacións (TIC). É unha ferramenta que avalía o compromiso dos países coa ciberseguridade. Este índice proporciona unha clasificación global que mostra o nivel de desenvolvemento da ciberseguridade en diferentes países. Avalía factores como a lexislación, a capacidade técnica, a cooperación internacional e a concienciación pública en ciberseguridade.

A última versión publicada da clasificación é a do ano 2020, México posiciónase no posto número 52 cunha puntuación de 81.68 sobre 100 puntos, mellorando 11 posicións respecto a a anterior clasificación do ano 2018, o que implica que nos últimos anos o país implementou medidas relacionadas coa ciberseguridade que melloraron a súa situación en xeral. Dentro do continente americano sitúase na posición cuarta, tras EEUU, Canadá e Brasil. España pola súa banda posiciónase no cuarto lugar da clasificación global tras EEUU, Reino Unido e Estonia, cunha puntuación de 98.52 sobre 100.

3.1 A problemática de México

No ano 2023 celebrouse en México o "World Legal Summit". Neste congreso falouse sobre como o mundo está cada vez máis interconectado e como a ciberseguridade converteuse nunha preocupación capital e de vital importancia para todas as nacións do mundo. Ademais abordaron cales son os retos máis significativos que o país enfronta nesta área, cales son os seus principais problemáticas e como o país debe de abordalas para fortalecer a súa postura en ciberseguridade.

3.1.1 Falta de coñecemento en materia de ciberseguridade

Un dos principais problemas do país radica na falta de coñecemento dos usuarios mexicanos en materia de ciberseguridade. A gran maioría das persoas descoñecen os mecanismos de protección na internet, así como as boas prácticas para manter protexida a información que se xera a través do tempo.

Doutra banda, descoñécense os mecanismos que utilizan os delincuentes cibernéticos para extraer a información privilexiada, aumentando a vulnerabilidade dos usuarios e causando que estes caian en trampas que fan que a súa información caia nas mans equivocadas.

3.1.2 Falta de dimensión dos danos causados por ataques informáticos

Outro desafío é a falta de conciencia sobre a gravidade dos danos causados polos ataques informáticos. Moitos usuarios subestiman a probabilidade de ser vítimas e, en caso dun incidente, non comprenden a magnitude das perdas potenciais.

Algún dos bens que deben de ser protexidos por parte dos usuarios, así como dos provedores de sistemas informáticos son, entre outros, datos persoais, privados e financeiros.

En canto ás empresas, resulta máis amplo o alcance dos bens para protexer, información confidencial, alianzas estratéxicas, status xurídico e financeiro, estratexias e estrutura organizativa, son en definitiva, algúns dos bens que deben de ser protexidos.

3.1.3 Falta de desenvolvemento de ferramentas de ciberseguridade

Aínda que é certo que existen algunhas organizacións que provén algúns produtos ou mecanismos que protexan os bens intanxibles e a información dos usuarios, son poucas as empresas que ofrecen solucións específicas e avanzadas en materia de ciberseguridade, por iso, México enfronta unha falta de desenvolvemento de ferramentas avanzadas neste campo.

É esencial identificar empresas que se enfoquen nas necesidades individuais, empresariais e institucionais e promover a implementación de mecanismos de defensa adecuados.

3.1.4 Políticas públicas mal enfocadas

As políticas públicas relacionadas coa ciberseguridade en México aínda non recibiron a prioridade e atención adecuada. A pesar dos esforzos, o país non logra abordar de maneira completa ou eficaz as necesidades que se viven na realidade do país, proba diso é que a lexislación por parte do Estado, así como o orzamento destinado á ciberseguridade son insuficientes.

3.1.5 Ausencia de homologación da lexislación en delitos cibernéticos

Tanto o Código penal Federal, como os códigos penais estatais contemplan os delitos cibernéticos definindo a conduta delituosa, así como a sanción que conleva o devandito comportamento.

Con todo, tanto no ámbito federal como nos diferentes estados do país non é uniforme a definición da conduta

delituosa en materia de seguridade, nin contemplan as mesmas penas ou sancións para quen incorra neste tipo de accións. Este punto de discrepancia xera incerteza xurídica e requírese dunha maior uniformidade para brindar claridade aos usuarios de sistemas cibernéticos.

3.1.6 Falta de cooperación entre actores

A cooperación entre os actores involucrados en incidentes de ciberseguridade é esencial. Tanto os usuarios finais como os provedores de sistemas e outros actores deben colaborar para previr e abordar os ataques de maneira efectiva.

3.2 Cifras craves

Os efectos da dixitalización na sociedade mexicana, a permanencia do traballo remoto e a irrupción da intelixencia artificial han salientado a necesidade de contar cunha estratexia nacional de ciberseguridade e a importancia deste sector na sociedade, tanto no ámbito empresarial como no individual.

México rexistrou no ano 2023 un total de 94 mil millóns de ataques cibernéticos, o que o converte no primeiro país de América Latina, xa que case a metade dos ciberataques rexistrados en o mesmo período, un total de 200 mil millóns teñen como obxectivos o país, seguido de Brasil e Colombia.

No último trimestre do 2023 observouse un alarmante aumento exponencial nas actividades maliciosas detectadas, experimentando un crecemento do 950% en comparación co ano anterior. No devandito incremento destaca a crecente sofisticación e agresividade dos ciberataques, o que pon de manifesto a imperiosa necesidade de reforzar as medidas de ciberseguridade das organizacións.

Pola súa banda, o ransomware continuou sendo unha ameaza no mercado mexicano colocándose como o sexto país do mundo que máis ataques deste tipo recibe, ademais observouse unha presenza significativa de ameazas vinculadas a aplicacións de Microsoft Office, como Excel, Word e PowerPoint, as cales representaron case 50% de todas as detección de malware no país.

En 2024 o país recibe unha media de 19 mil ataques diarios, o que lle converte nun dos países máis expostos á inseguridade dixital.

3.3 Principais actores

A economía e localización xeoestratexica de México son un obxectivo para as actividades cibernéticas ilícitas, por unha banda, o país goza dun investimento estranxeiro directo importante e unha evolución positiva do produto interior bruto (PIB) e, por outro, segue sendo relativamente vulnerable en ciberseguridade e ciberdefensa.

3.3.1 Organismos públicos

En México existen diferentes organismos con competencias en materia de ciberseguridade, pero, principalmente hai dous organismos gobernamentais a nivel federal que están a cargo da ciberseguridade en México, o CERT-MX e o Instituto Nacional de Transparencia, Acceso á Información e Protección de Datos Persoais (INAI).

- **Centro de Resposta a Incidentes da Dirección Xeral Científica da Garda Nacional (CERT-MX):** apoia a aquelas institucións do país que teñan unha infraestrutura crítica de información ante o sufrimento dun ataque. Trátase dun organismo central para a ciberseguridade en México, xa que debe brindar un servizo de axuda informático logo de perpetrarse un delito informático. Outra das súas tarefas é a de controlar que as institucións gobernamentais cumpran co Manual Administrativo de Aplicación Xeral de Tecnoloxías de Información e Comunicacións e de Seguridade da Información. Desta maneira, é posible asegurarse de que os organismos que teñen información sensible estean a aplicar unha estratexia adecuada de ciberseguridade no país. O CERT-MX depende da *Secretaría de Seguridade Pública e Protección Cidadá,* responsable de deseñar, planear, executar e coordinar as políticas gobernamentais en materia de seguridade pública.
- **Instituto Nacional de Transparencia, Acceso á Información e Protección de Datos Persoais (INAI):** ten o deber de protexer a transparencia, o acceso e a integridade dos datos persoais. Trátase dun organismo constitucional que posúe autonomía e que foi creado polos convencionais co obxectivo de protexer os dereitos elementais: o de acceso á información pública e o dos datos persoais.
- **Secretaría da Marina - Armada de México:** O acordo secretarial 335/2022 do 1 de xuño de 2022 dispuxo que a Unidade de Ciberseguridade (UNICIBER) constituísese na Coordinadora Xeral de Ciberespazo (EMCOGCIBER), dependendo operativa, orgánica e administrativamente do Estado Maior Xeneral da Armada. Encárgase de protexer o ciberespazo e conta cunha Estratexia Institucional para o Ciberespazo (2021- 2024).
- **Banco de México:** A principal institución financeira de México conta cunha estratexia de protección fronte a ciberataques que se pode consultar na súa web.

3.3.2 Organismos privados, asociacións e centros de investigación

O mercado da ciberseguridade é global. En México, moitas das empresas que operan no mercado proveñen dos Estados Unidos, referente do sector. Empresas globales de ciberseguridade como CISCO México (EEUU), Fortinet (EEUU), IBM (EEUU), Palo Alto Networks (EEUU), Trellix (antigas McAfee + Fire Eye) (EEUU) ou ATOS (Francia) tamén teñen en México unha considerable cota do mercado. Con todo, cada vez máis, outros actores irrompen no mercado debido ás posibilidades que ofrece o país.

As empresas mexicanas máis importantes do sector en México son: SCITUM (división de Telmex), Octapus (antiga 2Secure), CERO, Grupo Scanda, Totalsec (Grupo Salinas), NETRIX, IQSEC, Delta Protect, KIO Networks ou ProtekNet.

Algunhas das asociacións relevantes no sector son:

- **Asociación Mexicana da Ciberseguridade (AMECI):** organización que ofrece consultoría, capacitación, servizos e solucións relacionadas coa seguridade da información.
- **Asociación Mexicana da Industria das Tecnoloxías e da Información (AMITI):** representa ás empresas de tecnoloxía de México, para impulsar a interacción dentro da industria e facilitar a conexión entre a administración pública, a educación e outros organismos empresariais nacionais e internacionais.
- **Asociación da Internet de México (AIMX):** prové información sobre distintas temáticas do mundo dixital. Actúa como marco de referencia en temas craves para o desenvolvemento e implementación de proxectos normativos e de política pública que axuden na produtividade e a competitividade de México.

México conta tamén con algúns dos centros de investigación do sector da ciberseguridade máis importantes de América Latina.

- **Centro de Investigación en Computación (CIC):** é parte do Instituto Politécnico Nacional (IPN) e dedícase á investigación en áreas de computación, incluíndo a ciberseguridade.
- **Instituto Nacional de Astrofísica, Óptica e Electrónica (INAOE):** aínda que o seu enfoque principal é a astrofísica e a óptica, tamén realiza investigacións en ciberseguridade, particularmente no desenvolvemento de tecnoloxías de seguridade da información.
- **Centro de Investigación e de Estudios Avanzados do Instituto Politécnico Nacional (CINVESTAV):** ten varios departamentos dedicados á investigación en tecnoloxía da información e a comunicación, onde se inclúen temas de ciberseguridade.
- **Centro Nacional de Investigación e Desarrollo Tecnolóxico (CENIDET):** especializase na investigación aplicada en áreas como a electrónica, as telecomunicacións e a computación cun enfoque na seguridade cibernética.
- **Centro de Investigación en Matemáticas (CIMAT):** ainda que o seu enfoque principal é a investigación matemática, tamén realiza investigacións en áreas relacionadas ca seguridade informática e a criptografía.
- **Clúster TIC de Nuevo León (CSOFTMTY):** subcomité do clúster TIC de Monterrey onde se educa e investiga sobre o coñecemento integral acerca da protección da información.

3.4 A oferta galega e española

O sector da ciberseguridade cada vez vai adquirindo maior relevancia en España e proba diso é o crecente número de empresas que se dedican ao sector e que fan del, grazas á diversificación de actividades dentro do mesmo un dos principais países do mundo en materia de ciberseguridade.

Do mesmo xeito que no resto de España, o sector da ciberseguridade en Galicia experimentou un crecemento significativo e nos últimos anos leváronse a cabo iniciativas que impulsan o sector e o desenvolvemento de solucións de alto valor tecnolóxico. Con este obxectivo naceu o proxecto da Cidade das TIC situada en Coruña para fomentar a innovación dixital, crear unha contorna forte que se poida retroalimentar en diferentes disciplinas e que convertan a Galicia nun hub tecnolóxico dixital de referencia a nivel nacional e internacional.

Algunhas das empresas galegas máis destacadas no mercado da ciberseguridae son: Tarlogic, Forensic&Security, Softwariza3, Digintec, Redegal (presente en México), Legalforma, Conecta Comunicaciones y Medios e Inprosec (presente en México).

Algunhas das empresas españolas no 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.

Segundo un informe de DBK, os produtos con maior penetración son os relacionados coa protección das comunicacións (26%), o control de acceso, a autenticación (18%) e o antimalware (15%).

En canto aos servizos, a maior penetración está na área de cumprimento legal (57%), a auditoría técnica (54%), a implantación de solucións (54%) e o soporte e mantemento (42%).

3.5 Oportunidades do mercado

En México abunda o talento e o capital humano, con todo, no sector da ciberseguridade existen carencias de persoal cualificado que faga fronte á crecente necesidade de protección fronte ás ameazas. Con todo, existen

oportunidades no mercado e características favorables para o comercio entre ambos países nesta materia como son: o idioma e os prezos máis competitivos que os de EEUU, a fiabilidade e traxectoria de España e a Unión Europea (Europa é o continente máis seguro e menos atacado dixitalmente) na protección do ciberespazo, en termos de calidade-prezo-coñecemento, axudan ao posicionamento do produto nacional no país.

Os sectores de especial interese de demanda de servizos de ciberseguridade en México son:

- **Sector financeiro:** dada a sensibilidade da información é un dos sectores con máis perigo de recibir ataques.
- **Administración pública:** o Goberno xestiona gran parte da infraestrutura críticas do país o que lle fai propenso a un ataque.
- **Sanidade:** sucede o mesmo que co sector financeiro, dada a natureza sensible do tipo de información que manexa sobre os usuarios.
- **Sector retallista:** o desenvolvemento de plataformas de e-commerce abre a porta a que os comercios reciban máis ataques a medida que dixitalizan os seus negocios.
- **Sector industrial:** é un dos de maior tamaño na economía mexicana, o que aumenta a súa exposición para ser atacado, a medida que se implanta máis tecnoloxía na produción.

Dous factores potenciarán as oportunidades no mercado mexicano:

- **Intelixencia artificial:** a IA pode detectar e previr potenciais ameazas, desenvolvendo modelos preditivos de ciberataques. Doutra banda, a IA tamén poderá utilizarse para cometer delitos cibernéticos con maior precisión e sofisticación, o que incrementa o risco na rede. En definitiva, pode converterse nunha arma de dobre fío. A pesar de todo, existen oportunidades nun futuro próximo, xa que, vai permitir que as compañías reformulen os seus procesos administrativos e produtivos, o que implicará un aumento do investimento en ciberseguridade.
- **CISO:** o papel do CISO (Chief Information Security Officer) será fundamental nos próximos anos. En México estes profesionais - polo momento escasos- enfróntanse a orzamentos reducidos pola falta de conciencia nas organizacións sobre as ameazas cibernéticas, polo que, neste aspecto, poderíase considerar como unha oportunidade conseguir concienciar ás empresas mexicanas da importancia que ten unha boa estratexia de ciberseguridade e o desenvolvemento que terá o papel destes profesionais no futuro.

3.6 Craves de acceso o mercado

3.6.1 Distribuición

A cadea de distribuición da ciberseguridade comprende tres tipos de axentes en xeral: fabricantes, distribuidores e prestadores de servizos que ofertan hardware, software ou servizos especializados.

A pesar de que os servizos de ciberseguridade pódense prestar de forma remota, en México é importante estar presente fisicamente, xa que, é un feito que o mercado valora moito e que xera imaxe de marca. Recoméndase a creación dunha filial que dea soporte técnico e atención ao cliente ou establecer alianzas estratéxicas con socios locais con capacidade de venda e distribución de produtos ou servizos que xa conten cunha dilatada experiencia e coñecemento sobre o mercado mexicano.

3.6.2 Lexislación aplicable e outros requisitos

En canto á lexislación en materia de ciberseguridade en México, o certo é que aínda queda moito por facer. A crecente cantidade de ataques cibernéticos favoreceron a que as autoridades empezasen a comprender a gravidade do problema e comprendan a urxente necesidade de actuar con firmeza e decisión.

A día de hoxe a Lei Federal de Ciberseguridade non foi aprobada polo Congreso e é un tema pendente que, sen dúbida, axudará a combater e castigar o cibercrimen. Desde o 2018 propuxéronse 11 iniciativas de leis sobre ciberseguridade diferentes e en decembro de 2022 esperábase a aprobación e publicación no Diario Oficial da Federación da Lei Federal de Ciberseguridade, con todo, este feito non chegou a producirse. Esta última proposta de Lei ten 11 títulos e 71 artigos e xira ao redor dos seguintes eixos: garantir a seguridade nacional mediante a defensa do espazo dixital, crear un marco legal que permita sancionar ou tipificar os ciberataques, realización de probas de penetración ou pentesting anualmente ás institucións públicas e privadas e crear unha Axencia Nacional de Ciberseguridade controlada polo poder Executivo, seguindo o exemplo da UE, EEUU ou Brasil.

Aínda así, existen outras leis que abordan a temática desde un lugar secundario. Entre elas atópase a propia Constitución, a Norma Federal de Transparencia e Acceso á Información Pública, o Código Federal Penal, que tipifica algúns delitos informáticos e a Estratexia Nacional de Ciberseguridade de 2017.

O Goberno Federal anunciou a creación da Comisión Intersecretarial de Tecnoloxías da Información e Comunicación y da Seguridade da Información (CITICSI) cuxa finalidade é coordinar e implementar as políticas federais en materia de TIC e de seguridade da información, impulsando actividades e estratexias para o seu aproveitamento. Previsiblemente as súas decisións impactarán no contido da nova Lei de Ciberseguridade.

A Estratexia Nacional de Ciberseguridade en México

En 2017 dende o Goberno mexicano estableceuse unha estratexia de ciberseguridade co obxectivo de oermitir o uso das TIC de unha forma responsable parao desenvolvemento sostido de México.

É unha estratexia cun enfoque económico, xa que busca protexer maiormente a economía e a innovación. É importante para o desenvolvemento da industria mexicana que haxa boas medidas en materia de ciberseguridade que permitan que as compañías poidan traballar sen inconvenientes. A estratexia ten como obxectivo dar unha maior liberdade de acción aos individuos, pois, entende que o ciberespazo é un lugar moi importante para que a poboación poida exercer os seus dereitos plenamente.

Outro dos eixos transversais desta estratexia é lograr instalar unha cultura de ciberseguridade en México. Isto consiste en concienciar, educar e formar ás persoas e empresas en seguridade informática.

3.7 Feiras

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