Publicado en Ciudad de México el 17/01/2024

# [Minsait comparte las lecciones aprendidas en ciberseguridad durante el 2023](http://www.notasdeprensa.es)

## Inician el año compartiendo un análisis detallado sobre las lecciones aprendidas en ciberseguridad durante el año 2023, cortesía de Erik Moreno, Director de Ciberseguridad de Minsait, una empresa de Indra, en México. En este informe, Erik destaca los desafíos y riesgos que han marcado el panorama de la ciberseguridad, ofreciendo una perspectiva única sobre la situación en México. Se exploran temas críticos, como los sectores más vulnerables, las amenazas constantes y su impacto en la seguridad digital

 El 2023, fue un año que transcurrió con sobresaltos en los ámbitos social, político, económico y climático, que se quedará en la memoria colectiva por mucho tiempo. El conflicto entre Rusia y Ucrania, por ejemplo, ha mostrado que una guerra ya no se libra solamente en un territorio limitado y que los riesgos de ser víctima de un ciberataque son reales. Es también una oportunidad para ver en perspectiva los riesgos y amenazas que han puesto en la mira a distintos sectores del país, así como su impacto a lo largo de los últimos doce meses. Una visión local permite hacer una evaluación objetiva de dónde se encuentran los eslabones más débiles para enfocar la estrategia de ciberseguridad, hoy y en el futuro, para proteger las "joyas de la corona" de las organizaciones. Los sectores más vulnerables De acuerdo con datos del Cybersecurity Defense Center de Minsait, son dos los principales sectores que han sido más impactados por las amenazas: gubernamental y financiero. En el caso del primero, el 50% de los ataques se dirigieron a organismos centralizados y descentralizados del gobierno mexicano. Uno de los incidentes con mayor resonancia fue el de Guacamaya Leaks, que logró exfiltrar información altamente confidencial de los sistemas del Ejército Nacional. El financiero tuvo un porcentaje igual de ataques (50%) en el periodo comprendido entre 2019 y 2023, afectando no solo a las organizaciones del sector, sino también a sus usuarios. En estos cuatro años, las entidades del sistema financiero mexicano han reportado 106 incidentes de ciberseguridad a la Comisión Nacional Bancaria y de Valores (CNBV), lo que, para autoridades y especialistas, puede ser menor a la sufrida en realidad, pues no todos los ataques se reportan. El Índice de Riesgo de Ciberataques en México, en el Reporte de Estabilidad Financiera, revela que las amenazas cibernéticas más frecuentes de los últimos años incluyen la venta de información de tarjetas bancarias, código malicioso y el secuestro de datos. A los anteriores les siguen los sectores minorista, industrial y de cadena de suministro, que, en conjunto, fueron blanco de un 25% de las amenazas. Cabe señalar que la cadena de suministro figura por primera vez en la lista, lo que significa que las pequeñas y medianas empresas que participan en este nicho son menos maduras desde una perspectiva de ciberseguridad y tecnología a diferencia de las grandes organizaciones. Amenazas constantes El equipo del Cybersecurity Defense Center también ha hecho un análisis exhaustivo para identificar cuáles son las principales amenazas que se dirigen constantemente a las organizaciones del país. Ransomware. Esta amenaza no solamente sigue creciendo, sino que también evoluciona continuamente. El ransomware contemporáneo busca tanto cifrar la información como extraerla en grandes cantidades. Para las organizaciones mexicanas esto representa un enorme desafío, pues los ciberdelincuentes pueden hacerse con su información y con la de sus clientes, proveedores, empleados, así como sus estados financieros, poniendo en grave riesgo su reputación y continuidad. El Cybersecurity Defense Center da cuenta de que el 64.3% de la actividad sospechosa fue ransomware. Amenazas persistentes avanzadas (APT). Las amenazas de esta naturaleza representaron, en 2023, el 17.21% de las actividades maliciosas registradas. Desafortunadamente, muchas empresas mexicanas no cuentan aún con el nivel de madurez suficiente para detectarlas, e incluso no dimensionan el nivel de riesgo que representan. Los creadores de APTs se caracterizan por estudiar a detalle el negocio de la organización, su cadena de suministro, su estructura tecnológica, y coludirse con insiders para estructurar un ataque APT efectivo. Botnets. Los botnets, que toman el control de los equipos críticos de la organización de manera remota, conformaron el 10.5% de las amenazas, colocándolos en el tercer lugar del grupo. Impacto y cifras  El impacto de estas amenazas no es mínimo, y exige acciones concretas y más efectivas para combatirlas. Si bien hay industrias más reguladas, como la financiera, donde el marco normativo exige implementar mecanismos de protección y ciberseguridad bastante estrictos, y que tardarán en permear a otros, esta no debería ser una condición para implementar controles de protección robustos y adaptados a la realidad de cada sector. El Cybersecurity Defense Center recopiló información sobre los vectores de ataque más utilizados por los ciberdelincuentes para penetrar en la organización, y los resultados han sido los siguientes: Con el 44%, el phishing fue uno de los vectores de ataque mediante los cuales se comprometieron los activos de las organizaciones mexicanas, con una tasa de éxito cercana al 100%. La explotación de vulnerabilidades no conocidas ocupó la segunda posición con 24.13% como el vector utilizado con mayor frecuencia en México. Los grandes fabricantes de software se esfuerzan por minimizar las vulnerabilidades; sin embargo, las empresas no actualizan ni aplican los parches que se les proporciona, lo que deja abierta la puerta a los atacantes para materializar sus amenazas. El 10.34% de los intentos de ciberataques utilizó software malicioso en sus distintas formas. De los más populares fueron los troyanos. A diferencia de hace dos décadas, este malware no penetra un equipo a través de un medio extraíble; hoy lo hace usando aplicaciones descargables, muchas de ellas gratuitas, que son aprovechadas por los delincuentes para acceder, mediante saltos laterales, a los activos de la organización. Lockbit, MarioLocker, Black Hat SEO y Lazarus son grupos dedicados al desarrollo de ataques de campañas de software que aprovechan las amenazas y vectores mencionados anteriormente. Se trata de grandes agrupaciones con alcance global y fondeo internacional, cuyo poder de captación de nuevos recursos tecnológicos, humanos y aliados al interior de las empresas crece exponencialmente. El Cybersecurity Defense Center ha recopilado algunas cifras que dan una dimensión más amplia del entorno actual de amenazas en el que operan las empresas mexicanas. A lo largo de 2023 se detectaron: Más de 153,000 campañas de ransomware Más de 25 campañas de botnets Más de 41 campañas de APT 13 campañas de phishing Más de 2,621 vulnerabilidades detectadas, de las cuales el 50% fueron de alto riesgo y el 15% fueron críticas. Microsoft reportó 877 vulnerabilidades. Navegadores web, como Chrome, Firefox y Edge identificaron 423 vulnerabilidades Linux, Oracle y Red Hat tuvieron 292, 219 y 212 vulnerabilidades, respectivamente. En un contexto de transformación digital acelerada, las amenazas cibernéticas no dan tregua. La colaboración entre empresas, proveedores de servicios y desarrolladores es esencial para crear un entorno de protección efectivo. La realidad en México refleja la situación global, donde la ciberseguridad se vuelve imperativa. No bajar la guardia y adaptarse a las lecciones aprendidas es crucial para salvaguardar la integridad de las organizaciones en el paisaje digital actual.

**Datos de contacto:**

Gabriela Medina Guerrero

AB Estudio de Comunicación

5539663493

Nota de prensa publicada en: [https://www.mexicopress.com.mx/minsait-comparte-las-lecciones-aprendidas-en](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: Inteligencia Artificial y Robótica Software Ciberseguridad Estado de México Ciudad de México Digital



[**http://www.mexicopress.com.mx**](http://www.notasdeprensa.es)