Publicado en CDMX el 02/02/2023

# [5 factores clave del crecimiento de ciberataques en América Latina: Hillstone Networks](http://www.notasdeprensa.es)

## El incremento de amenazas se mantendrá implacable en 2023 incluyendo ataques a las cadenas de suministro, filtraciones de datos a gran escala, incremento en amenazas de ransomware y malware de criptominado, así como nuevas vertientes de ataques de ingeniería social

 Hillstone Networks comparte los 5 factores preponderantes por los cuales los ciberataques seguirán creciendo a ritmos impresionantes en América Latina. Monetización: Los ciberdelincuentes han logrado obtener cuantiosas ganancias de sus ataques, lo cual los motiva a seguir buscando brechas y nuevos métodos que les permita seguir incrementando sus ingresos.   Presupuestos limitados: Los presupuestos asignados a ciberseguridad por las empresas y organizaciones son limitados en comparación con los recursos que tienen los cibercriminales para buscar nuevos vectores o mejorar sus ataques. Además, la falta de profesionales especializados se ha convertido en un reto con el que deben lidiar las empresas para enfrentar las amenazas.   Inversión no prioritaria: Algunas entidades gubernamentales no ven la tecnología como un habilitador de mejores servicios para la comunidad, por consiguiente, no realizan las inversiones necesarias en estrategias de ciberseguridad.   Infraestructura crítica: La integración de la infraestructura crítica a las redes de TI ha hecho que los cibercriminales la ubiquen como su nuevo objetivo, debido al impacto que puede tener en la sociedad.   Frágiles obligaciones de cumplimiento: A pesar de que la cultura de la ciberseguridad ha crecido y las empresas se están apegando cada vez más a estándares, el hecho de no tener la obligación de cumplir con algunas regulaciones de ciberseguridad hace que muchas instituciones de gobierno queden vulnerables. Bajo este panorama, Manuel Acosta, Director General para México en Hillstone Networks, comenta que durante este año serán recurrentes los ataques a las cadenas de suministro, filtraciones de datos a gran escala, incremento en amenazas de ransomware y malware de criptominado, así como nuevas vertientes de ataques de ingeniería social. "Hoy en día el malware es tan avanzado que permite a los usuarios seguir utilizando sus dispositivos mientras trabajan en segundo plano; una vez establecido busca moverse en la red para crear botnets y robar recursos importantes como bases de datos, credenciales, etc. En ocasiones el Ransomware es una de las últimas acciones que realizan los atacantes para borrar los rastros de sus crímenes", explicó Acosta. Por esta razón, las estrategias de ciberseguridad que solo contemplan un modelo de prevención ya no son eficientes. El uso de firewalls, antivirus, antispam, entre otras soluciones, no ha servido para detener a los cibercriminales, por eso es importante integrar las nuevas tecnologías de Visibilidad de Amenazas y Automatización. "Las soluciones de Detección y Remediación Extendida (XDR) ahora permiten integrar los diferentes dispositivos de ciberseguridad con el objetivo de tener la visibilidad del estado de ciberseguridad de la organización en una sola pantalla y automatizar las respuestas ante los Indicadores de Compromiso detectados por las diferentes soluciones que componen la infraestructura de ciberseguridad de la empresa", destacó Manuel Acosta. Además, ante el incremento de los servicios en la nube y del trabajo remoto, las organizaciones deben adoptar arquitecturas basadas en ZTNA (Zero Trust Network Access), SD-WAN, así como considerar la microsegmentación de cargas de trabajo virtualizadas o contenerizadas.

**Datos de contacto:**

Carlos Soto

Comunicación en Movimiento

5532322068

Nota de prensa publicada en: [https://www.mexicopress.com.mx/5-factores-clave-del-crecimiento-de\_1](http://www.notasdeprensa.es/educalivecom-disfruta-de-cursos-presenciales-y-clases-particulares-a-traves-de-internet)

Categorías: E-Commerce Ciberseguridad Otros Servicios



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