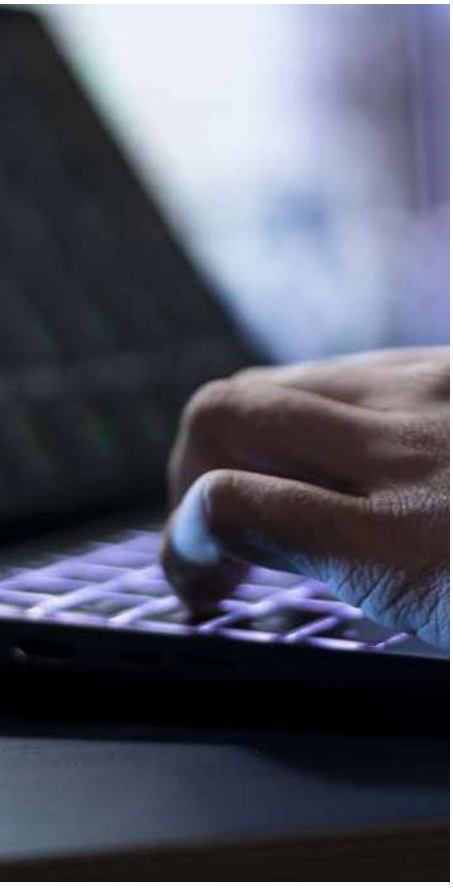
www.mexis.net

2025:

¿DIRIGIR O NAUFRAGAR EN LA SEGURIDAD DIGITAL?

mexis aggity



En 2025, las amenazas digitales serán más sofisticadas que nunca. Desde "stealers" y ransomware hasta ataques potenciados por inteligencia artificial, las empresas deberán priorizar la ciberseguridad como un pilar estratégico. Explora cómo prepararte para este desafiante panorama.

Imagine que su empresa es un barco navegando en un mar que, a simple vista, parece tranquilo. Desde la superficie, todo luce bajo control, pero bajo las aguas acechan remolinos y corrientes inesperadas que podrían poner en riesgo la operación o incluso volcar la embarcación. Así es el mundo de la seguridad digital: un entorno dinámico y lleno de amenazas ocultas.

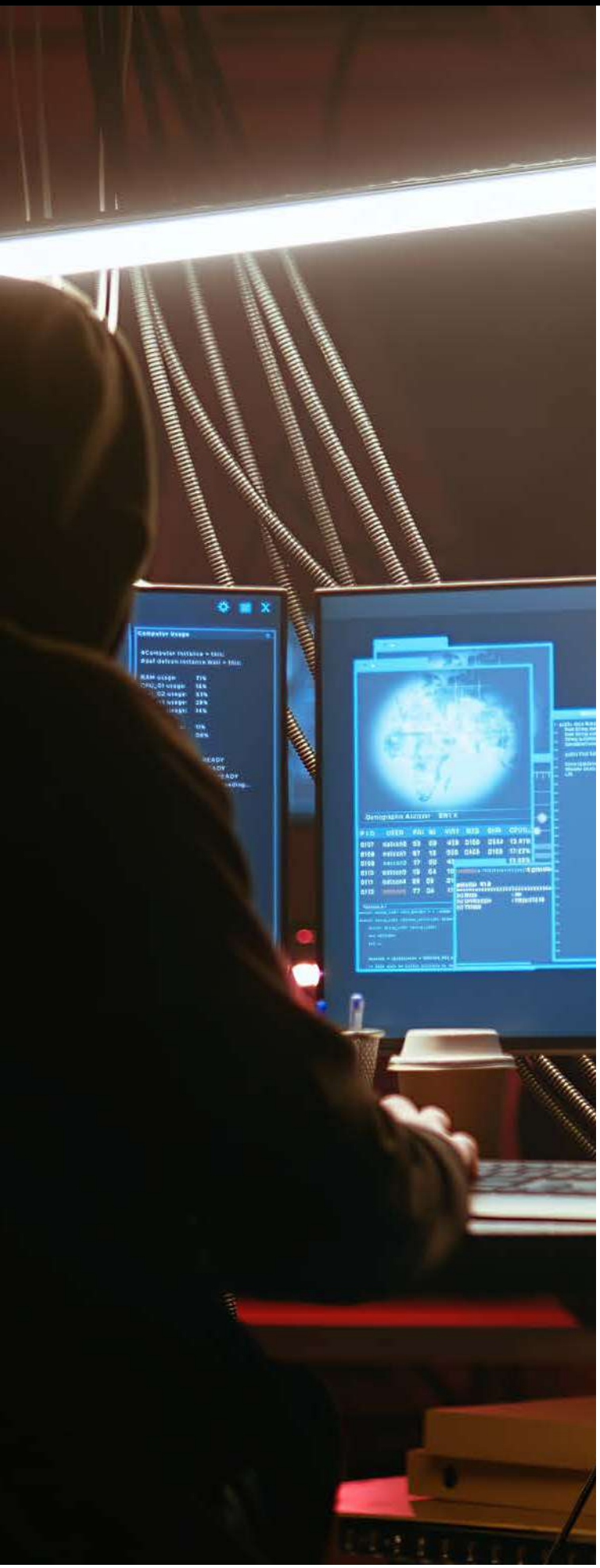
En este mar digital lleno de incertidumbres, **la ciberseguridad no debe ser vista como un simple salvavidas al que se recurre en momentos de crisis; debe ser el timón que guíe a las empresas hacia un futuro seguro y exitoso,** integrándose de forma proactiva en cada aspecto de la operación empresarial. Cuando se implementa desde el inicio, permite navegar con confianza incluso en las aguas más turbulentas, evitando riesgos innecesarios y asegurando una dirección clara hacia el crecimiento.

Las cifras del **Panorama de Amenazas Corporativas** de especialistas son un recordatorio contundente: **en 2024, más de 268 millones de ataques digitales fueron bloqueados en la región, liderados por el phishing, el ransomware y los troyanos bancarios.** Estos ataques no solo han aumentado en volumen, sino también en sofisticación, apuntando a sectores clave como el gobierno, la manufactura, la salud y la educación, entre otros.

Hablemos de 2025. En este año, las amenazas digitales evolucionarán y exigirán que las empresas den un paso adelante. Por ejemplo, los “stealers” serán una preocupación importante. **Estos programas maliciosos están diseñados para robar información valiosa, como credenciales de acceso y datos confidenciales de clientes o empleados.** Esa información robada puede ser utilizada directamente para cometer fraudes o vendida en mercados clandestinos, alimentando otras actividades del cibercrimen organizado. Proteger estos datos ya no es opcional, es esencial.

También veremos a los bancos centrales y a las plataformas de banca abierta bajo el foco de los atacantes. Estos sistemas dependen de tecnologías como las API para funcionar, pero esas mismas conexiones pueden ser aprovechadas por los ciberdelincuentes para acceder a información sensible.
El ransomware también evolucionará. Ya no se trata solo de bloquear el acceso a datos para pedir un rescate, sino de alterar información crítica, lo que puede dejar a las empresas en situaciones aún más complicadas como la perdida de información valiosa o incluso la quiebra; y con la llegada de nuevas tecnologías como la computación cuántica, algunos ataques podrían hacerse casi imposibles de contrarrestar.

Otra tendencia es el uso de la inteligencia artificial tanto para proteger como para atacar. Los defensores podrán usarla para detectar amenazas rápidamente y anticiparse a los problemas, pero los atacantes también están aprovechando estas herramientas para crear estrategias más sofisticadas. Por ejemplo, en el año pasado, el 21% de los correos de phishing ya eran generados por IA, logrando evadir incluso medidas de seguridad robustas.



Y es que este tipo de amenaza sigue siendo una de las tácticas más comunes y efectivas, con más de 721,000 intentos diarios bloqueados en la región durante 2024, según el mismo reporte. De hecho, estas herramientas permiten eludir la autenticación biométrica mediante la manipulación de videos, imágenes y datos filtrados, lo que representa un desafío significativo para los sistemas de seguridad corporativos, e incluso para las compañías que aún no capacitan a sus empleados para detectar este tipo de amenazas.

El crimen cibernético también se está globalizando. **Grupos internacionales están expandiendo sus operaciones hacia nuevos mercados, afectando sectores como la salud, la educación y las finanzas,** a lo que se le suma que el cumplimiento normativo está siendo usado como una herramienta de extorsión. Algunos atacantes buscan explotar esta presión, manipulando datos para generar violaciones regulatorias y forzar a las empresas a pagar rescates. Esta es una señal clara de que la seguridad debe ser parte del corazón del negocio.

Como un barco que necesita mapas y una tripulación preparada, las empresas requieren estrategias sólidas para enfrentar ciberamenazas cada vez más sofisticadas. Muchas organizaciones, especialmente pequeñas y medianas, subestiman estos riesgos, creyendo que no serán objetivos por su tamaño. Sin embargo, estas “tormentas digitales” afectan a todas por igual.

La ciberseguridad no es solo un escudo; es una ventaja estratégica en un entorno donde se valora la confianza y la resiliencia. Invertir en ciberseguridad garantiza continuidad y competitividad; ya no hablamos de un gasto sino de una inversión.

Recién zarpamos en esta aventura llamada 2025, y **este inicio de año es un gran momento para que las empresas revisen sus estrategias y adopten un enfoque proactivo para enfrentar este panorama.** Esto implica capacitación constante para los colaboradores, actualizaciones regulares de software, implementación de tecnologías avanzadas de detección y respuesta, y la creación de una cultura organizacional que valore la seguridad como un pilar fundamental del negocio. En este viaje, el rumbo es tan importante como la embarcación misma.

Fuente de información: impactotic