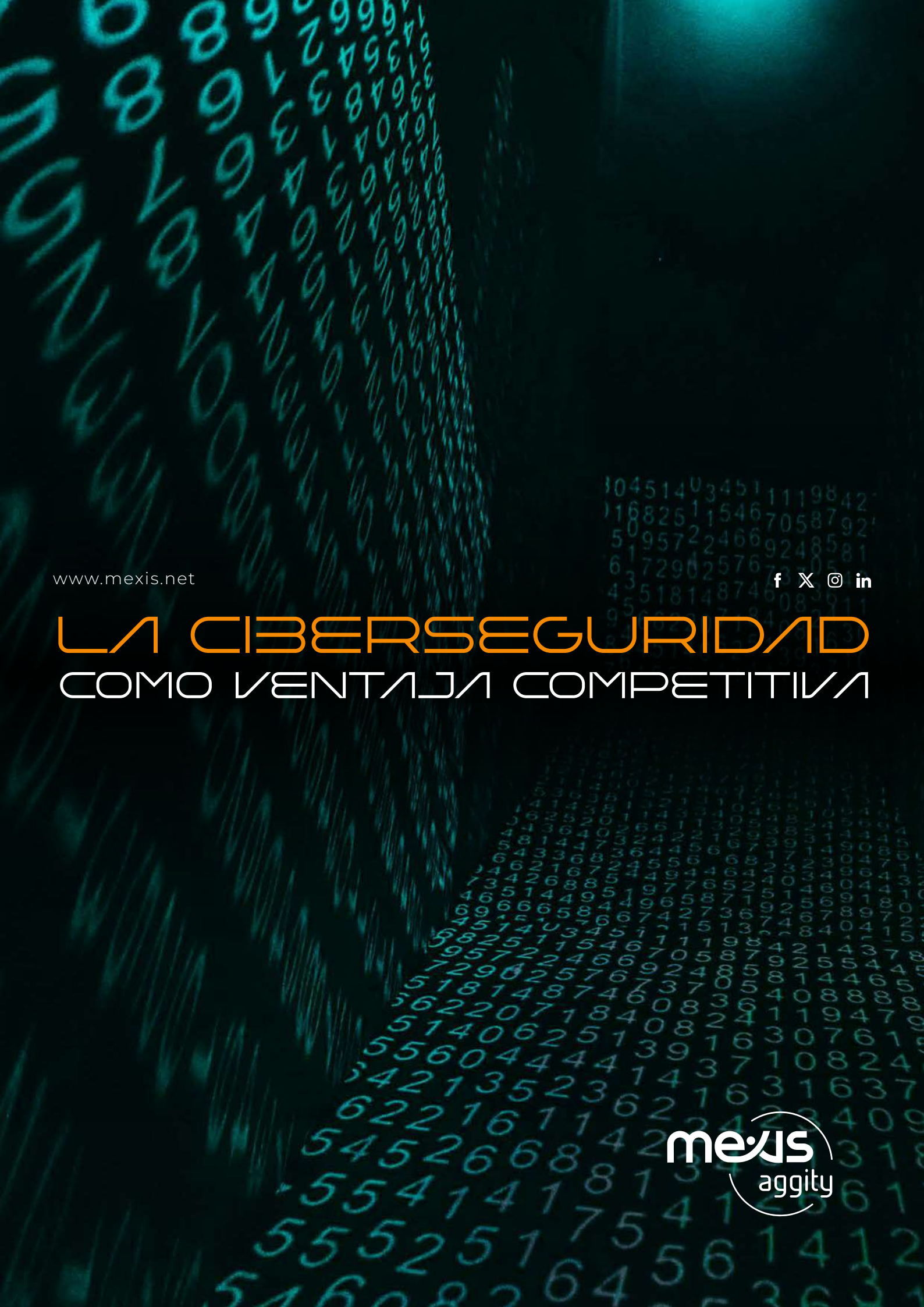


www.mexis.net

LA CIBERSEGURIDAD
COMO VENTAJA COMPETITIVA

mexis aggity

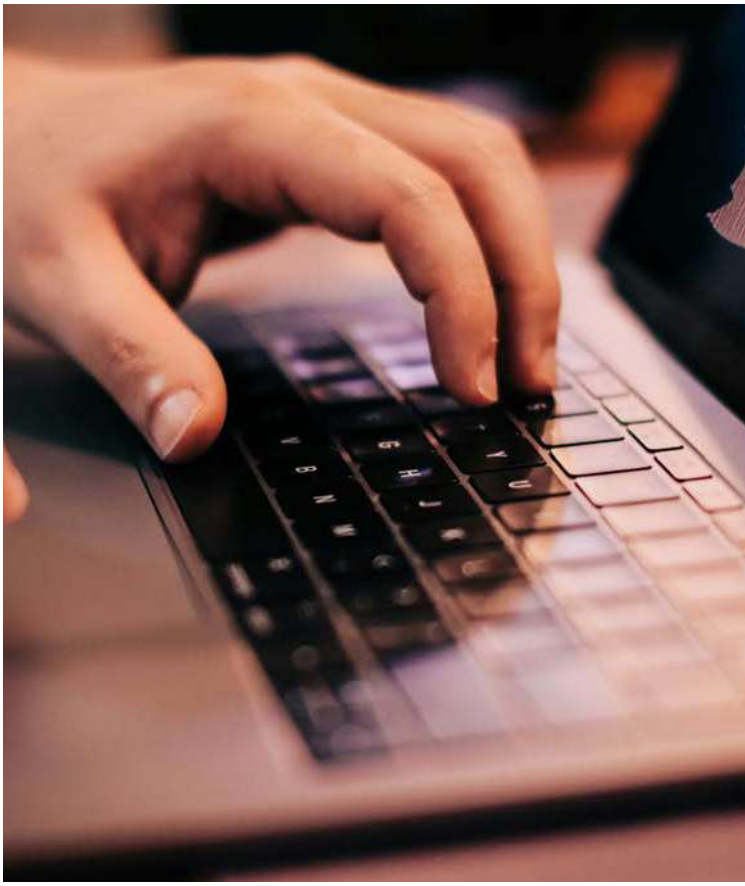
El costo de ignorar la ciberseguridad es inmenso, aunque es importante entender que ningún sistema es completamente infalible.

Las empresas que adoptan un enfoque proactivo en ciberseguridad no solo defienden sus sistemas, sino que también ganan un lugar privilegiado en el mercado. Priorizar la ciberseguridad genera confianza en los clientes, refuerza la cadena de suministro y, a largo plazo, protege el valor de la marca y la reputación corporativa.

El costo de ignorar la ciberseguridad es inmenso, aunque es importante entender que ningún sistema es completamente infalible. Grandes organizaciones como Target, Equifax y Marriott, que contaban con fuertes medidas de ciberseguridad, han sufrido ataques devastadores que comprometieron los datos personales de millones de clientes, lo que erosionó su reputación. Según KPMG, **se estima que el 84% de los consumidores no volvería a comprar de una empresa que ha sufrido una violación de datos si cree que su información personal está en riesgo.** Estos incidentes no solo afectan las operaciones inmediatas, sino que tienen un impacto duradero en la confianza y lealtad de los clientes.

Aunque muchas empresas afirman tener proyectos de ciberseguridad en marcha, esto no necesariamente implica que estén trabajando de manera proactiva o que cuenten con una estrategia sólida. Un enfoque reactivo se centra en responder a incidentes y hallazgos después de que ya han ocurrido, mientras que la proactividad implica anticiparse a los problemas. Para ser verdaderamente proactivos, las empresas deben integrar la ciberseguridad en su cultura organizacional, esto incluye la identificación continua de riesgos tecnológicos y la implementación de marcos de referencia que permitan gestionar estos riesgos, además de auditorías periódicas para verificar que todo funcione de manera correcta.

La concientización es un elemento clave de este enfoque proactivo. No es suficiente con que el equipo de TI o ciberseguridad entienda los riesgos; toda la organización debe estar alineada y comprometida con la ciberseguridad. **Esto implica capacitar a los empleados sobre prácticas seguras, como la detección de correos de phishing o el uso de contraseñas robustas.** Además, los líderes de la organización deben ser un ejemplo a seguir, asegurándose de que sus procesos tecnológicos estén alineados con las políticas de ciberseguridad y de compartirlos con el equipo de ciberseguridad para evitar riesgos que puedan comprometer a la organización.



En muchas empresas, no existe un inventario adecuado de tecnología o de datos, lo que dificulta reaccionar eficientemente ante un incidente. Esto revela que no se está priorizando la información clave que sustenta al negocio. **Un enfoque proactivo también incluye el cumplimiento de protocolos avanzados, como la gestión de vulnerabilidades, la realización de pruebas de penetración periódicas para identificar debilidades, la aplicación de parches de ciberseguridad de manera oportuna y el monitoreo continuo de la red.** Estas acciones permiten a las empresas adelantarse a los problemas, reducir el tiempo de respuesta y mitigar el impacto de posibles ataques.

Cada vez más organizaciones, tanto clientes como proveedores, están exigiendo evidencia de la madurez en las prácticas de ciberseguridad de sus socios. Esto se ha vuelto esencial en los procesos de evaluación de la cadena de suministro, ya que **cualquier eslabón débil puede poner en riesgo a toda la red.** Las empresas que demuestran cumplir con los estándares más altos no solo protegen sus propios activos, sino que también ofrecen garantías a sus clientes y socios, fortaleciendo las relaciones comerciales y asegurando la continuidad operativa.

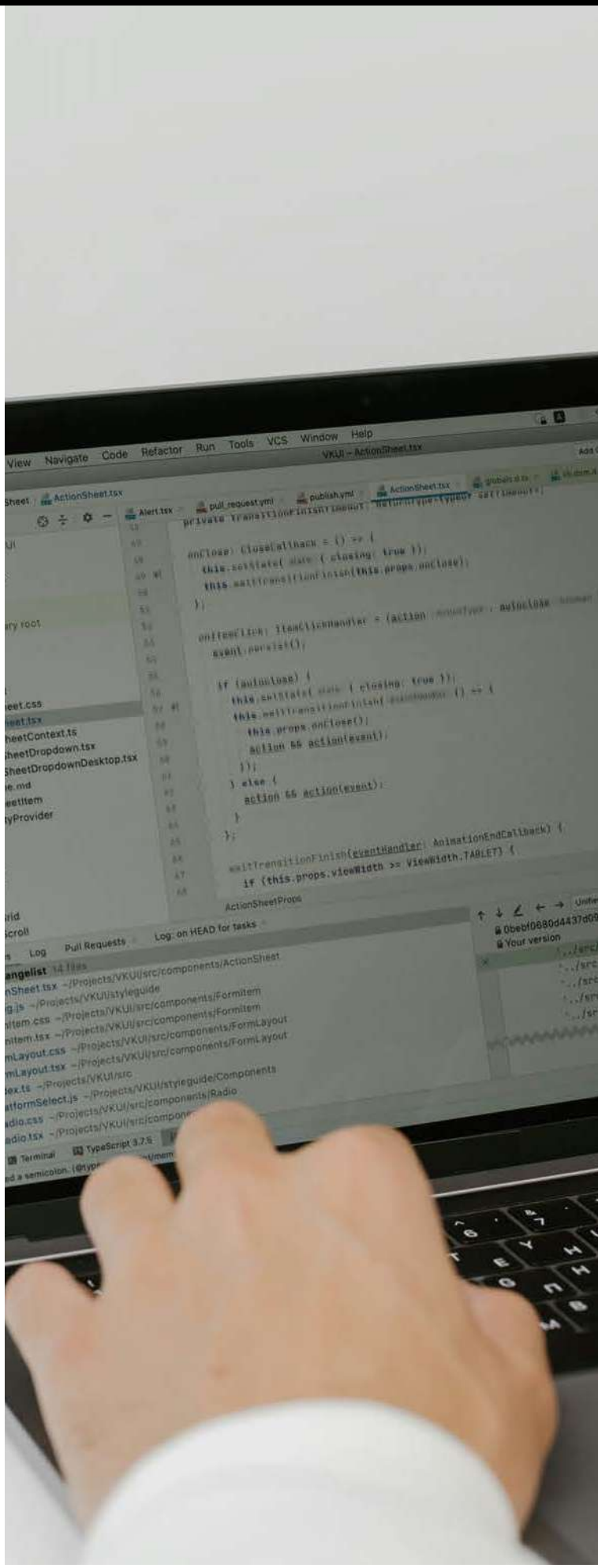
Adoptar un enfoque proactivo en ciberseguridad también proporciona una ventaja competitiva frente a aquellas empresas que solo reaccionan ante los incidentes. **Los consumidores son cada vez más conscientes de los riesgos de los ciberataques y prefieren hacer negocios con organizaciones que demuestran un compromiso sólido con la protección de datos.** Comunicar claramente las políticas de ciberseguridad y cómo se protegen los datos sensibles no solo genera confianza, sino que también fortalece las relaciones con los clientes.

Desde la perspectiva del cumplimiento regulatorio, las organizaciones que invierten en ciberseguridad están mejor preparadas para cumplir con las normativas cada vez más estrictas en torno a la protección de datos. **El Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA) son ejemplos de cómo los reguladores están adoptando medidas más estrictas para garantizar la privacidad.** Aunque en América Latina aún no se han implementado regulaciones tan estrictas, es cuestión de tiempo para que las empresas deban cumplir con normas similares. Cumplir con estos requisitos no solo evita multas, sino que también refuerza la imagen de la empresa como una organización responsable y comprometida con la protección de la privacidad.

Finalmente, **las organizaciones que toman en serio la ciberseguridad están mejor preparadas para recuperarse rápidamente de incidentes.** No se trata solo de proteger la infraestructura tecnológica; la resiliencia también implica la capacidad de mantener las operaciones en marcha incluso durante un ciberataque. **Las empresas que pueden continuar operando sin interrupciones durante un incidente se destacan frente a la competencia**, ganan la confianza de los clientes y minimizan el impacto financiero.

La ciberseguridad es mucho más que un requisito técnico: es una inversión estratégica. Aquellas empresas que adopten un enfoque proactivo estarán mejor protegidas contra las amenazas actuales y tendrán una ventaja competitiva ante los demás, fortaleciendo la confianza de sus clientes y asegurando la resiliencia a largo plazo.

Las organizaciones que comprendan esto estarán mejor posicionadas para liderar en un entorno cada vez más digital y vulnerable.



Autor: Andrés Velázquez
Fuente de información: cybernews.com