EL HERALDO
Fecha: 16/04/2026 Audiencia: 6.000 Sección: OPINION
Vpe: $753.875 Tirada: 3.000 Frecuencia: 0
Vpe pág: $1.850.000 Difusión: 3.000
Vpe portada: $1.850.000 Ocupación: 40,75%

Ciberseguridad: las pymes bajo amenaza

En un escenario marcado por la acelerada digitalización, la ciberseguridad ha dejado de ser un tema exclusivo de grandes corporaciones para convertirse en una prioridad ineludible para las pequeñas y medianas empresas (pymes). Si bien la adopción de tecnologías digitales ha abierto oportunidades para mejorar la eficiencia, optimizar procesos y ampliar mercados, también ha incrementado de manera significativa los riesgos asociados a las amenazas informáticas.

Persistir en la idea de que las pymes no son un objetivo atractivo para los ciberdelincuentes es, hoy en día, un error estratégico. Los ataques ya no son necesariamente dirigidos, sino masivos y automatizados, lo que implica que cualquier empresa conectada a internet puede convertirse en un blanco potencial. En este contexto, la vulnerabilidad no depende del tamaño de la organización, sino de la solidez de sus medidas de protección.

Las consecuencias de un incidente de ciberseguridad pueden ser devastadoras. El robo de información sensible- como datos de clientes, registros financieros o documentos internos- no solo compromete la operación diaria, sino que también puede generar pérdidas económicas relevantes y un deterioro profundo de la confianza por parte de clientes y socios. En muchos casos, el daño reputacional resulta incluso más difícil de revertir que el impacto financiero inmediato.

Un aspecto especialmente preocupante es que una gran proporción de estos incidentes tiene su origen en errores humanos. Acciones aparentemente simples, como abrir un archivo adjunto malicioso o hacer clic en un enlace fraudulento, pueden desencadenar brechas de seguridad importantes.

Por ello, fomentar una cultura organizacional de ciberseguridad se vuelve fundamental. La capacitación continua de los colaboradores no debe entenderse como un gasto, sino como una inversión clave para la sostenibilidad del negocio. Reconocer amenazas, aplicar buenas prácticas digitales y adoptar una actitud preventiva son habilidades que deben reforzarse de manera permanente, especialmente considerando que las tácticas de los ciberdelincuentes evolucionan con rapidez.

Carol Alarcón, Head of Marketing de NOVARED – www.novared.net

En esta línea, enfoques como el modelo Zero Trust adquieren cada vez mayor relevancia. La premisa de no confiar automáticamente en ninguna solicitud y verificar cada acceso permite reducir significativamente los riesgos, especialmente en entornos donde el trabajo remoto y el uso de múltiples dispositivos son cada vez más comunes.

A esto se suma un desafío emergente como lo es el empleo de inteligencia artificial por parte de actores maliciosos. Hoy es posible generar correos fraudulentos altamente convincentes, imitar estilos de comunicación e incluso automatizar ataques a gran escala, lo que eleva el nivel de sofisticación de las amenazas.

En definitiva, la ciberseguridad ya no puede ser vista como un aspecto técnico secundario, sino como un pilar estratégico para la continuidad y el crecimiento de las pymes. Invertir en protección digital no solo reduce riesgos, sino que fortalece la confianza, asegura la operación y posiciona a las empresas de mejor manera.