Ciberseguridad en la óptica, una tarea todavía pendiente

El número de ciberataques está al alza y ninguna compañía está libre de sufrirlos, tampoco las pequeñas y medianas empresas, que necesitan poner en práctica algunas recomendaciones para estar más protegidas.

En el contexto de la era digital, la transformación tecnológica ha revolucionado la manera en que interactuamos, trabajamos y nos comunicamos. Este avance, sin embargo, también ha traído consigo nuevos desafíos; en este escenario, la ciberseguridad emerge como una cuestión crítica que es imprescindible abordar.

El número de ciberataques está al alza y nadie está libre de sufrirlos. Tampoco las pequeñas y medianas empresas, como puede ser una óptica. Antes los delincuentes ponían el ojo en grandes corporaciones con ataques muy sofisticados, pero ahora la *ransomware*, el *phising* y, en general, la ingeniería social hacen que todo el mundo esté en el punto de mira. Y ahí también entran en juego las empresas más pequeñas.

Según un estudio de Sage, las pymes españolas se enfrentan diariamente a retos en el ámbito de la ciberseguridad. Con presupuestos reducidos, dificultad para formar a sus empleados, complicaciones para acceder a las herramientas e innovaciones adecuadas y falta de orientación y asesoramiento, navegar en la complejidad de la ciberseguridad e impulsar sus negocios continúa siendo un reto para las pequeñas empresas.

A pesar de que las pymes españolas tienen muy presente su ciberseguridad, existe una confianza implícita, posiblemente equivocada, en cómo la gestionan. En concreto, siete de cada 10 pymes españolas (71%) indica que la ciberseguridad forma parte de su cultura corporativa y hasta el 82% se muestran confiadas respecto a su gestión de la ciberseguridad. Sin embargo, la realidad es que casi tres cuartas partes de ellas (73%) reconocen no hablar de ella con regularidad.

Esto es lo que se desprende del estudio "Ciberseguridad para pymes: navegar por la complejidad y crear resiliencia", publicado por Sage. La compañía ha realizado un análisis global para investigar las percepciones de las pequeñas y medianas empresas sobre la ciberseguridad y los principales obstáculos a los que se enfrentan en este ámbito. A través de él, Sage pretende desmitificar la ciberseguridad y cambiar la percepción de esta, pasando de un reto desalentador, a una herramienta de empoderamiento para que las

DESAFÍOS CLAVE

Una de las principales preocupaciones de las pymes es mantener o ampliar sus oportunidades de negocio y hacerlo de forma segura. Para lograr este objetivo, deben tener en cuenta a la evolución del panorama de las ciberamenazas. Entre los principales retos relacionados con la ciberseguridad de las pymes figuran aspectos como el factor humano, la falta de cualificación y competencia o la inversión.

En lo relativo a la inversión merece la pena recordar que el 93% de las pymes son microempresas, con menos de 10 empleados y sin personal dedicado a las TI o la seguridad. Hacerles ver que invertir en este ámbito es crucial para su supervivencia desde los comienzos puede ser una tarea complicada que abordar, pero sin duda es necesaria. Se debe poner fin a las situaciones en las que las empresas se dan cuenta de la necesidad de la ciberseguridad sólo después de un incidente importante, evidentemente cuando ya es demasiado tarde.

Por otro lado, cabe mencionar que las pymes se enfrentan a dificultades para acceder a profesionales de la seguridad capacitados para un asesoramiento a medida sobre la integración de la ciberseguridad en sus operaciones. Según un estudio del ISC2 *Cybersecurity Workforce Study 2022*, en Europa faltaban más de 300.000 especialistas en ciberseguridad (60.000 de ellos en España). Todo ello conlleva una mayor responsabilidad para los directivos y empleados de las pymes de mantenerse al día en un escenario de ciberseguridad complejo y en constante cambio.

pymes puedan centrarse en hacer crecer su negocio, desarrollar sus equipos y ofrecer una experiencia de cliente excepcional.

En cuanto a cómo afrontar los retos que supone la ciberseguridad, España se diferencia del resto del mundo en relación con sus prioridades y cómo atajar estas preocupaciones. De forma global, las pymes encuestadas muestran una visión transversal y a largo plazo, enfocada en asegurar que los empleados entienden lo que se espera de ellos respecto a seguridad (45%), educarlas acerca de cómo protegerse (44%) y entender las necesidades reales de seguridad de la empresa (43%).

Por su parte, las pymes españolas mantienen una cultura más centrada en el ahora y en la ayuda externa, en lugar de enfocarse en sus actuales empleados. Los retos que preocupan a las pymes españolas pasan por estar al día de las nuevas amenazas (51%), entender sus necesidades reales de seguridad (44%) y contratar a personas con habilidades en ciberseguridad (44%).

El estudio, además, revela que casi la mitad de las pymes a nivel global (48%) han sufrido un incidente de ciberseguridad en el último año y el 25%, más de uno. En el caso de las españolas son el 32% las que han sufrido múltiples ciberataques en los últimos meses.

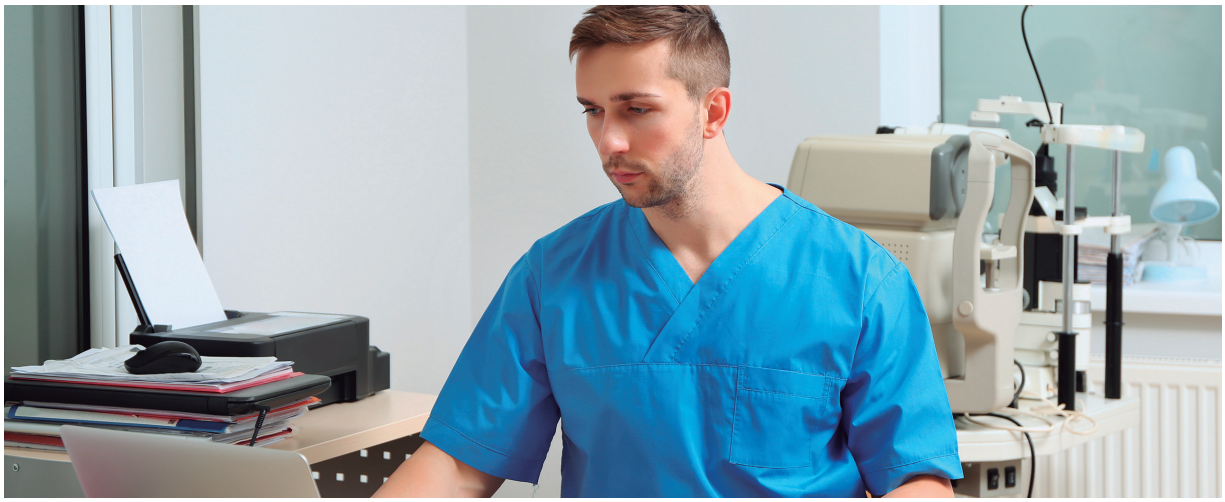
Por otro lado, el 70% de las pymes españolas tiene copias de seguridad de sus datos y solo un 21% confían su protección en controles básicos (antivirus). En cuanto a la protección del teletrabajo, el 82% de las pymes ha adoptado algún tipo de control de seguridad, aunque solo el 57% lo supervisa de cerca. En el caso de España, aunque ocho de cada 10 pymes (82%) dispone de un proceso para gestionar los riesgos de los trabajadores a distancia, el 33% confiesa que no se cumple de forma generalizada.

Con la multiplicación de las ciberamenazas, saber qué es importante, por dónde empezar y superar las barreras del coste es fundamental para las pymes que quieren reforzar su ciberresiliencia. En España, el 46% de las pymes españolas reclama más servicios de emergencia para que puedan informar sobre incidentes y el 45%, más apoyo en educación y formación. De manera global, más de la mitad también reclama más apoyo en educación y formación. Sin embargo, el 45% atribuye la responsabilidad de actuar a los gobiernos y el 43% a los partners tecnológicos de confianza.

Medidas prácticas a adoptar

Según el manual de supervivencia contra las ciberamenazas impulsado por la Universidad de León,

LAS PYMES ESPAÑOLAS SE ENFRENTAN DIARIAMENTE A RETOS EN EL ÁMBITO DE LA CIBERSEGURIDAD, CON PRESUPUESTOS REDUCIDOS Y DIFICULTAD PARA FORMAR A SUS EMPLEADOS



existen cuatro medidas clave que deben tenerse en cuenta a la hora de crear una estrategia de seguridad y que pueden ayudar a las pymes a minimizar riesgos. Por un lado, identificar los procesos y recursos críticos de la empresa, las amenazas a la seguridad, las vulnerabilidades y los riesgos. Por otro lado, implantar medidas de seguridad, como un estricto control de acceso, concienciación y formación, gestión de vulnerabilidades y parches, y procesos de copia de seguridad y recuperación de datos. Además, potenciar el uso de procedimientos actualizados *antimalware*, de detección de incidentes de seguridad y de notificación al personal y a los usuarios. Por último, mantener los planes de recuperación ante incidentes y catástrofes y establecer las estructuras de comunicación adecuadas para interactuar con las partes interesadas.

Los tipos más comunes de ataques a las pymes incluyen *malware, phishing*, ataques basados en web, *ransomware* y denegación de servicio distribuido (DDoS). Para evitarlo, los expertos aconsejan poner en práctica estas recomendaciones:

1. Control de acceso estricto: gestión de contraseñas

Más del 60% de las violaciones de la ciberseguridad afectan a las credenciales de los usuarios. Las prácticas deficientes y débiles en materia de contraseñas suponen un riesgo real para la ciberseguridad. Utilizar una contraseña fuerte y única con al menos 12 caracteres y letras, números y símbolos puede ser de gran utilidad. Según la guía, se recomienda "encarecidamente" utilizar un gestor de contraseñas para generarlas, gestionarlas y almacenarlas de forma cifrada. Aplicar y activar la autenticación multifactor (AMF) para las aplicaciones y sistemas que las pymes utilizan o ponen a su disposición también resulta vital.

2. Gestión de vulnerabilidades

Corresponde a las pymes garantizar que se identifican y mitigan las vulnerabilidades de sus productos. Los parches para vulnerabilidades y las medidas de mitigación para los productos/servicios que utilizan (señalados por los proveedores o las autoridades nacionales) deben aplicarse oportunamente. La instalación y el mantenimiento adecuado de distintos sistemas antivirus es un paso esencial para proteger los sistemas operativos y las aplicaciones de las pymes de otras amenazas.

3. Copia de seguridad de datos

Copia de seguridad de los datos esenciales para las actividades empresariales en, al menos, dos ubicaciones fuera de la red corporativa. Podrán utilizar el cifrado completo de disco para garantizar que, en caso de pérdida o robo de un disco duro, los datos permanezcan seguros. Las claves de cifrado también deberán protegerse de forma segura.

4. Instalación y mantenimiento de cortafuegos

Instalar un cortafuegos para mejorar la seguridad aislando una red confiable de otra que no lo es puede suponer un valor diferencial. Parchear y reforzar el cortafuegos también. Las pymes deberán utilizar un enfoque de listas blancas (denegación por defecto) para permitir únicamente el tráfico específico que requieren los servicios utilizados por la empresa. Actualizar periódicamente el software del cortafuegos y, en la medida de lo posible, automatizar el proceso.

5. Inalámbrico / Acceso Wi-Fi protegido (WPA)

El manual recomienda emplear WPA3 siempre que sea posible y una contraseña única y segura con cifrado de red Wi-Fi que contenga al menos 20 letras, números y caracteres especiales.

6. Red privada virtual (VPN)

Una VPN robusta puede proporcionar un acceso remoto seguro a una red y sus aplicaciones.

7. Mantener un plan de recuperación de incidentes y catástrofes

Definir y mantener un plan de recuperación ante incidentes y catástrofes para responder a las violaciones de seguridad, de modo que las pymes puedan recuperar el control de sus operaciones y datos empresariales.