Ciberseguridad: Cinco tips para proteger tu empresa de ciberataques

Los ataques cibernéticos han seguido aumentando en la región Hispanoamérica este año, en especial en países como México, Colombia, Perú y Argentina, siendo los ataques por malware y las variantes de ransomware los más habituales.

Si bien según la encuesta Nivel de Adopción Digital Corporaciones Hispam 2021, realizada por Movistar Empresas, más de la mitad de las corporaciones en la región han implementado soluciones de ciberseguridad para el equipamiento y protección de sus redes, los especialistas estiman que los ciberataques seguirán causando daños económicos y reputacionales si no se tiene una estrategia de seguridad para 2023.

“La pandemia aceleró aún más la preocupación por invertir en soluciones de ciberseguridad. La nueva realidad exige a las corporaciones aumentar su presupuesto en soluciones digitales. Creemos que es posible forjar un ecosistema digital más seguro, en la medida que se considere a las herramientas de ciberseguridad como una inversión y no un gasto”, explica Antuanet Rivas Plata, Gerente Comercial y de Producto de Telefónica Tech.

En el Día Mundial de la Ciberseguridad, celebrado cada 30 de noviembre, las organizaciones deben reforzar sus medidas para evitar fraudes, filtración de datos y robos de información.

Según Fortinet, en la primera mitad de 2022, América Latina y el Caribe sufrieron 137.000 millones de intentos de ciberataques, un aumento del 50% en comparación con el mismo período de 2021. México fue el país más atacado de la región (con 85.000 millones), mientras que Perú ocupó el cuarto lugar antes que Argentina y Brasil.

En ese sentido, la especialista de Telefónica Tech Perú, Antuanet Rivas Plata, brinda cinco claves para incorporar la ciberseguridad en los negocios y no improvisar en el momento que suceda una contingencia:

1. Prevención

El trabajo remoto abrió las puertas a amenazas cibernéticas que no eran tan peligrosas cuando los equipos estaban en la oficina. Muchos usuarios son conducidos a enviar datos confidenciales o abrir enlaces sospechosos y, por ello, es clave implementar sistemas de seguridad avanzados que lo eviten. De hecho, el 95% de los problemas de ciberseguridad se originan en errores humanos, según el Foro Económico Mundial.

2. Es tarea de todos

Como principal riesgo de ciberseguridad que deben gestionar las empresas, el error humano no solo es responsabilidad exclusiva de los equipos de TI, sino que recorre a toda la organización, y hay que ser conscientes de que todos manejamos el activo más valioso de una empresa: la información. Por ello, es importante respetar las recomendaciones de seguridad implementadas o consultar si hay alguna anomalía que puede resultar en amenaza.

3. Capacitación constante

La empresa debe animar a los empleados a adoptar una postura de prevención frente a las ciberamenazas y ser consciente de las buenas prácticas de seguridad y animar a los empleados.

4. Políticas de seguridad

Es importante elaborar un plan de seguridad basado en el funcionamiento y las necesidades del negocio. Este reglamento permitirá proteger información sensible y limitar su acceso para evitar el riesgo de pérdida, deterioro o acceso no autorizado por parte de posibles vulnerabilidades y amenazas de ciberdelincuentes.

5. Adquirir herramientas de seguridad

Implementar soluciones de Firewalls y otras para analizar y prevenir ataques exteriores a las redes de la empresa, así como la protección de la red WI- FI que suele ser una de los ingresos preferidos por los cibercriminales para obtener la información sensible, así como los ataques del tipo Ransomware.

Frente a este escenario de ciberamenazas en 2023, Telefónica Tech seguirá impulsando la prevención y capacitación, con cada vez mejores tiempos de respuesta de las empresas.