Perú- “Amenazas cibernéticas en América Latina: un llamado al compliance empresarial”

Alejandra Guevara, la subject matter expert of cybersecurity for compliance assurance en HSBC US, nos da a conocer las nuevas amenazas cibernéticas y la importancia del cumplimiento normativo para proteger a las organizaciones en la región.

Link de la noticia
Fuente: https://lacamara.pe/

“Es crucial que los líderes de la organización demuestren un compromiso visible con la ciberseguridad para establecer el tono desde arriba. Establezcan políticas y procedimientos claros de ciberseguridad, así como fomentar la colaboración entre diferentes departamentos para abordar la ciberseguridad de manera integral”, resalta, entre otras acciones.

A lo que se añade que las organizaciones deben asignar presupuestos adecuados para la ciberseguridad, demostrando su compromiso con una cultura de cumplimiento.

También teniendo en cuenta que América Latina es particularmente susceptible a la ingeniería social, las organizaciones deben crear conciencia sobre estas vulnerabilidades culturales específicas y cómo pueden ser explotadas por los ciberdelincuentes.

“En las organizaciones, esto se traduce en programas de capacitación continua y actualizados para todos los niveles, desde empleados hasta altos ejecutivos”, menciona.

Con respecto a cómo crear en las organizaciones una cultura de compliance de la ciberseguridad, Alejandra Guevara, destaca que se debe desarrollar una cultura de cumplimiento de la ciberseguridad en las organizaciones latinoamericanas es un desafío complejo pero crucial, y para ello es necesario la educación y la concientización continua.

IMPACTO DEL COMPLIANCE

Pero también el compliance es importante para proteger la información personal y cumplir con las leyes de protección de datos y para ayudar a mitigar el riesgo del impacto reputacional, al demostrar un compromiso con la seguridad y la protección de datos, añade.

“La diversidad en la regulación de países latinoamericanos hace que el compliance sea complejo pero crucial, ya que las empresas deben navegar diferentes marcos legales, especialmente si operan en múltiples países de la región”, destaca.

Y un gran aliado de la ciberseguridad es el compliance, el conjunto de buenas prácticas que asumen las empresas con el fin de evitar, gestionar, mitigar los riesgos empresariales, a través de mecanismos, algunos exigidos por ley y otros recomendados por estándares.

En este contexto, destaca la subject matter expert of cybersecurity for compliance assurance en HSBC US, que la ciberseguridad en el mundo digital ha adquirido mucha importancia, debido a que se presenta como un pilar fundamental para el desarrollo digital seguro de América Latina, crucial para proteger la información, la infraestructura crítica, la economía y los derechos de los ciudadanos en un mundo cada vez más conectado y vulnerable a amenazas cibernéticas sofisticadas.

IMPORTANCIA DE LA CIBERSEGURIDAD

“México se encuentra entre los 10 países más atacados del mundo, con 85 000 millones de intentos de ciberataques solo en el primer semestre de 2024. Esto subraya la magnitud del desafío que enfrentan las organizaciones en la región. Además, la falta de preparación y respuesta adecuada ante estos ataques, como se evidencia en casos recientes como el ataque al Poder Judicial de la Ciudad de México, que revela deficiencias en estrategias, presupuesto y ciber-resiliencia a nivel institucional”, señala.

A lo que se añade el cibercrimen organizado y el hacktivismo; ataques sofisticados con IA; las amenazas móviles, con el aumento de la penetración de Internet móvil en la región; ataques de suplantación de marcas (brand Impersonation).

Además, están los ataques de infraestructuras críticas en la que sectores como energía, salud y servicios básicos son blancos frecuentes, con implicaciones potencialmente graves para la seguridad nacional.

En cuanto a las nuevas modalidades de ataques cibernéticos a las que están expuestas las organizaciones en la región, detalla que algunas de las principales amenazas más comunes y persistentes incluyen al phishing y ataques de ingeniería social, que aprovechan las vulnerabilidades del usuario final. Asimismo, está el ransomware, dirigido específicamente a empresas e instituciones, que se ha vuelto cada vez más sofisticado y dañino.

MODALIDADES DE ATAQUES CIBERNÉTICOS

Ante este panorama el compliance en ciberseguridad empresarial es de vital importancia, destaca Alejandra Guevara, subject matter expert of cybersecurity for compliance assurance en HSBC US, que participará en el ‘VIII Congreso Internacional de Compliance y Lucha Anticorrupción’, organizado por la Cámara de Comercio de Lima (CCL) junto a la World Compliance Association (WCA) y que se realizará los próximos 9 y 10 de setiembre, en la sede institucional del gremio empresarial.

Las organizaciones en América Latina enfrentan una evolución constante en las amenazas cibernéticas, con nuevas modalidades de ataques que reflejan las vulnerabilidades regionales, y que impactan en sus costos financieros directos e indirectos, incluyen daños reputacionales y pérdida de confianza en las plataformas digitales y servicios en línea