Informe sobre Tendencias en Ciberseguridad, Ciberdelito y Riesgos para 2025

Introducción

La ciberseguridad se ha convertido en un elemento crítico para la protección de datos y sistemas en el contexto de una digitalización acelerada. Con el aumento del uso de tecnologías emergentes, la evolución constante del ciberdelito y un paisaje normativo cambiante es vital entender las tendencias que marcarán el futuro cercano. Este informe explora las principales tendencias esperadas en ciberseguridad, ciberdelito y los riesgos asociados para 2025.

1. Tendencias en Ciberseguridad

La inteligencia artificial será un pilar fundamental para mejorar las capacidades defensivas frente a amenazas cibernéticas. Las herramientas basadas en IA ayudarán a detectar patrones inusuales y responder automáticamente a incidentes, reduciendo así el tiempo de respuesta ante ataques.

El modelo Zero Trust se volverá estándar entre las organizaciones debido al aumento del trabajo remoto y la necesidad de asegurar datos más allá del perímetro tradicional. Este enfoque implica no confiar automáticamente en ninguna entidad dentro o fuera de la red.

Mientras que las tecnologías basadas en “blockchain” proporcionarán soluciones innovadoras para garantizar la integridad de los datos y autenticar identidades digitales sin depender completamente de entidades centralizadas.

Las normativas relacionadas con protección de datos seguirán evolucionando con regulaciones más estrictas como las leyes de Protección de Datos ampliándose globalmente, lo que obligará a las empresas a fortalecer sus prácticas e inversiones en ciberseguridad y enfoques basados en GRC.

2. Tendencias en Ciberdelito

Ataques cada día más sofisticados. Los ciberdelincuentes utilizan técnicas avanzadas como el "deepfake", la manipulación de IA y el ransomware de doble extorsión, lo que dificulta la detección y respuesta a incidentes.

Se espera que el ransomware siga siendo una amenaza predominante, con grupos criminales cada vez más sofisticados utilizando tácticas como "ransomware-as-a-service" (RaaS). Las organizaciones deben prepararse no solo para pagos sino también para posibles filtraciones públicas como forma adicional presión.

Con el aumento del trabajo remoto y la movilidad laboral, las amenazas internas se volverán más comunes. Es probable que empleados descontentos o descuidados filtren información sensible, lo que representa un riesgo significativo para la seguridad empresarial.

Además los ciberdelincuentes dirigirán sus esfuerzos hacia infraestructuras críticas como sistemas de energía, transporte y salud. Estos ataques pueden tener repercusiones catastróficas y serán utilizados como herramienta para ejercer presión política o extorsión financiera.

Las técnicas de ingeniería social se sofisticarán aún más con el uso de inteligencia artificial para personalizar ataques (phishing) y manipulaciones psicológicas (pretexting), haciendo que los individuos sean un eslabón débil en la cadena de seguridad.

3. Evaluación de Riesgos Asociados desde un enfoque GRC

Como tendencia para 2025 se destaca la necesidad de un enfoque GRC proactivo y adaptable para abordar los riesgos emergentes. Las organizaciones deben fortalecer sus capacidades de gobierno, gestión de riesgos y cumplimiento para proteger su reputación, activos financieros y la confianza de sus partes interesadas en un entorno digital cada vez más complejo y amenazante.

Los incidentes cibernéticos pueden dañar gravemente la reputación organizacional, afectando no solo aspectos financieros sino también relaciones con clientes, socios comerciales e inversores.

Paralelamente el costo promedio por incidente cibernético seguirá aumentando debido al crecimiento en demandas por compensaciones, multas por incumplimiento normativo y gastos relacionados con recuperación post-incidente.

La paralización de operaciones debido a un ataque puede resultar en pérdidas de ingresos, retrasos en la producción y daños a la cadena de suministro.

El incumplimiento de regulaciones sobre protección de datos y privacidad puede acarrear multas elevadas y sanciones legales.

A medida que las regulaciones se vuelven más estrictas, las organizaciones enfrentarán riesgos legales elevados si no cumplen con los requisitos establecidos en materia de protección y gestión adecuada del dato personal o sensible.

Conclusiones

Las organizaciones deberían considerar la implementación de tecnologías avanzadas como IA y “blockchain”. Adoptar estrategias robustas bajo el modelo Zero Trust.

Formar planes sólidos contra ransomware e ingeniería social.

Desarrollar una cultura organizacional centrada en la seguridad para mitigar riesgos internos por medio de una estrategia GRC implementando herramientas como AURIGA® para una gestión integral y eficiente, que permita la identificación, evaluación, monitoreo y tratamiento de los riesgos, así como el mapeo de procesos y la generación de informes para una toma de decisiones más informada."

Mantenerse actualizado sobre estos cambios será esencial para navegar el peligroso campo actual del ciberespacio donde tanto oportunidades como amenazas están en constante evolución. La colaboración entre sectores público y privado también jugará un papel crucial al abordar desafíos globales relacionados con el ciberdelito y asegurar una infraestructura digital resiliente frente a futuros ataques cibernéticos.