Centro de experiencia

ECIJA COLOMBIA & PERÚ | Advisory

Tips organizacional No. 1

Ciberataques en el sector público y privado: Estrategias de Control Interno

En esta era digital, las compañías del sector público y privado se enfrentan a una amenaza constante: los ciberataques. Estos ataques informáticos pueden tener un impacto devastador en la estrategia, la reputación y la continuidad del negocio. En este artículo, ECIJA explora desde su experiencia, cómo afectan estos ciberataques a las organizaciones, qué medidas deben tomar para prevenirlos, detectarlos y responder de manera oportuna, y cómo las compañías especializadas pueden desempeñar un papel crucial en la prevención de riesgos cibernéticos, y la protección y continuidad del negocio.

1. Impacto de los Ciberataques en la Estrategia de las Compañías

Los ciberataques pueden socavar significativamente la estrategia de una compañía de varias formas:

- **Daño a la Reputación**

  Cuando una organización sufre un ciberataque, su reputación puede verse gravemente dañada. La pérdida de la confianza de los clientes y socios comerciales puede ser difícil de recuperar. Los clientes pueden dudar en compartir información confidencial o hacer negocios con una empresa que ha experimentado una brecha de seguridad.

► **Pérdida de Datos Sensibles**

Los ciberataques a menudo resultan en la pérdida o el robo de datos sensibles, como información financiera, propiedad intelectual o datos personales de clientes y empleados. Esto no solo puede tener implicaciones legales o económicas, sino que también puede afectar la ventaja competitiva de la empresa.

► **c. Interrupción de Operaciones**

Los ciberataques pueden paralizar las operaciones comerciales o de servicios vitales en un país o en una compañía. Los ataques de ransomware, por ejemplo, pueden bloquear el acceso a sistemas críticos, lo que lleva a una interrupción costosa y a la pérdida de ingresos. Varias compañías y entidades públicas que han sido victimas de estos ataques han tenido inmensas dificultades para recuperar el 100% de la información secuestrada.

2. Medidas para Prevenir, Detectar y Responder a Ciberataques

Para protegerse contra los ciberataques y minimizar su impacto en la estrategia empresarial, las organizaciones deben implementar un enfoque integral de control interno que ayude a la prevención, detección y respuesta a los mismos. A continuación unas sugerencias:

a. Prevención

- **Seguridad de la Información**: debe incluir e implementar políticas y procedimientos de seguridad de la información robustos, incluyendo la educación continua de los colaboradores sobre las mejores prácticas de seguridad.
- **Actualización y Parcheo:** que permita mantener sistemas y software actualizados con los últimos parches de seguridad para cerrar vulnerabilidades conocidas.
- **Firewalls y Antivirus:** que sean confiables para bloquear amenazas conocidas.

b. Detección

- **Monitoreo Continuo:** donde se Implemente sistemas de detección de intrusiones y de monitoreo de manera constante el tráfico de red en busca de actividades inusuales.
- **Análisis de Logs:** que permita revisar y analizar regularmente los registros de actividad para detectar patrones o comportamientos sospechosos.
- **Pruebas de Penetración:** donde se realice pruebas de penetración regulares para identificar debilidades en la seguridad (Ethical Hacking).

c. Respuesta

- **Plan de Respuesta a Incidentes:** donde se vislumbre un plan claro y escalable para responder a los ciberataques. Esto incluye la asignación de roles y responsabilidades, la comunicación efectiva y la recuperación de datos.

- **Formación en Respuesta a Incidentes:** donde se capaciten a los equipos de respuesta para manejar situaciones de crisis de manera efectiva.

3. El Papel de Compañías Especializadas y la Continuidad del Negocio

Las compañías especializadas en seguridad cibernética pueden desempeñar un papel crucial en la protección y la continuidad del negocio, donde ofrecen una visión del negocio diferenciadora, diferente de lo que ven sus colaboradores internos:

- **Servicios de Consultoría en Ciberseguridad:** donde ayudan a las organizaciones a evaluar sus vulnerabilidades, desarrollar estrategias de seguridad y fortalecer sus defensas.
- **Monitoreo y Detección Gestionados:** donde proporcionan servicios de monitoreo continuo y respuesta a incidentes para detectar y mitigar amenazas en tiempo real.
- **Recuperación de Desastres:** ayudan en la recuperación de datos y sistemas después de un ataque, minimizando el tiempo de inactividad.

En conclusión, los ciberataques representan una amenaza constante para las compañías del sector público y privado, con un impacto significativo en su estrategia y operaciones. La prevención, detección y respuesta efectivas son fundamentales para mitigar estos riesgos. Al colaborar con compañías especializadas en ciberseguridad, las organizaciones pueden fortalecer sus defensas y garantizar la continuidad del negocio en un entorno digital cada vez más peligroso.

Contacto ECIJA

Colombia & Perú

Simón Guzman G.
Advisory Partner
Cel. + 57 313 8170765
E-mail: sguzman@ecija.com

Andrés Velasco P.
Senior Manager
Cel. + 57 313 4782260
E-mail: avelasco@ecija.com

https://ecija.com/presencia-global/colombia/