Artículo

Ciberinteligencia vs Cibersabiduría

BDO

Desde su inicio en 2004, cuando Estados Unidos designó octubre como el mes de la Concientización sobre la Seguridad Cibernética, esta campaña ha ganado impulso global. Su misión: protegernos en el entorno digital. Con el tiempo, más países se han unido, promoviendo una cultura mundial de ciberseguridad.

¿Por qué es vital? En un mundo donde los ciberataques son cada vez más avanzados, este mes nos recuerda la importancia de estar informados y preparados. Empresas, gobiernos y usuarios individuales colaboran para compartir buenas prácticas, concientizar sobre nuevas amenazas y fomentar la cooperación internacional.

Proyecciones de Ciberinteligencia

Data estadística sobre ciberinteligencia en Latinoamérica:

- **Aumento de ciberataques:** En 2024, el 30% de las organizaciones en América Latina han reportado al menos un incidente de seguridad (existen compañías que no lo reportan). Además, el 23% de las empresas sufrió intentos de ataque de ransomware en los últimos dos años.
- **Tipos de amenazas:** Los ataques más comunes en la región incluyen el phishing, que sigue siendo el ciberataque más frecuente con aproximadamente 3.400 millones de correos spam diarios. También se destacan los exploits para vulnerabilidades antiguas en algunas herramientas, que representaron el 81% de los ataques en 2023.
- **Impacto financiero:** El costo promedio de una violación de datos en 2022 fue de 4,35 millones de dólares a nivel mundial. En América Latina, las pérdidas financieras debido a ciberataques han sido significativas, con un aumento del 38% en los ciberataques en 2021.
- **Preparación y respuesta:** A pesar de la creciente amenaza, el 62% de las organizaciones en América Latina considera insuficiente su presupuesto destinado a ciberseguridad. Sin embargo, el 86% de las empresas encuestadas no estaría dispuesta a negociar el pago de un rescate en caso de un ataque de ransomware.

Ciberinteligencia

Estas estadísticas demuestran la importancia de fortalecer las medidas de ciberinteligencia en la región para proteger los activos digitales y mitigar los riesgos.

Pero, ¿qué es ciberinteligencia? Se refiere a la recopilación y análisis de información para identificar, rastrear y predecir las actividades de actores hostiles en el ciberespacio. Este proceso permite a las organizaciones anticiparse a las amenazas, mitigar riesgos y tomar decisiones informadas para proteger sus activos digitales.

Aspectos clave de la ciberinteligencia

- Anticipación de amenazas y mitigación de riesgos,
- Gobierno de ciberseguridad actualizado y efectivo,
- Herramientas digitales y dispositivos SOC (Security Operations Center),
- Proveedor para implementar controles de ciberseguridad,
- Concientización al personal y al público en materia de ciberseguridad,
- Automatización (RPA) e Inteligencia artificial (IA),
- Ecosistema de control interno en la nube.

En términos generales se ha puesto en práctica algunas prácticas de ciberinteligencia, pero, si los ciberataques han aumentado e impactan cada vez en mayor escala a las organizaciones, si cada vez más las compañías sufren ataques de ransomware, si el número de víctimas de phishing se prolifera constantemente, si las pérdidas financieras producto de ciberdelitos incrementan gradual y ágilmente y si la mayoría de las empresas no tienen un presupuesto óptimo para ciberdefensa y ciberrespuesta, entonces... ¿qué falta?

Cibersabiduría

Cibersabiduría es la integración avanzada y contemporánea de conocimiento profundo de tecnología y ciberamenazas, prácticas efectivas de ciberinteligencia, vasta experiencia en la seguridad y protección de la información y juicio prudente en el ciberespacio. La cibersabiduría permite no solo la identificación y mitigación de amenazas cibernéticas, sino también la aplicación de estrategias informadas y éticas para la gestión, confidencialidad, privacidad y optimización de la información, recursos y costos en el entorno digital.

Aspectos clave de la cibersabiduría:

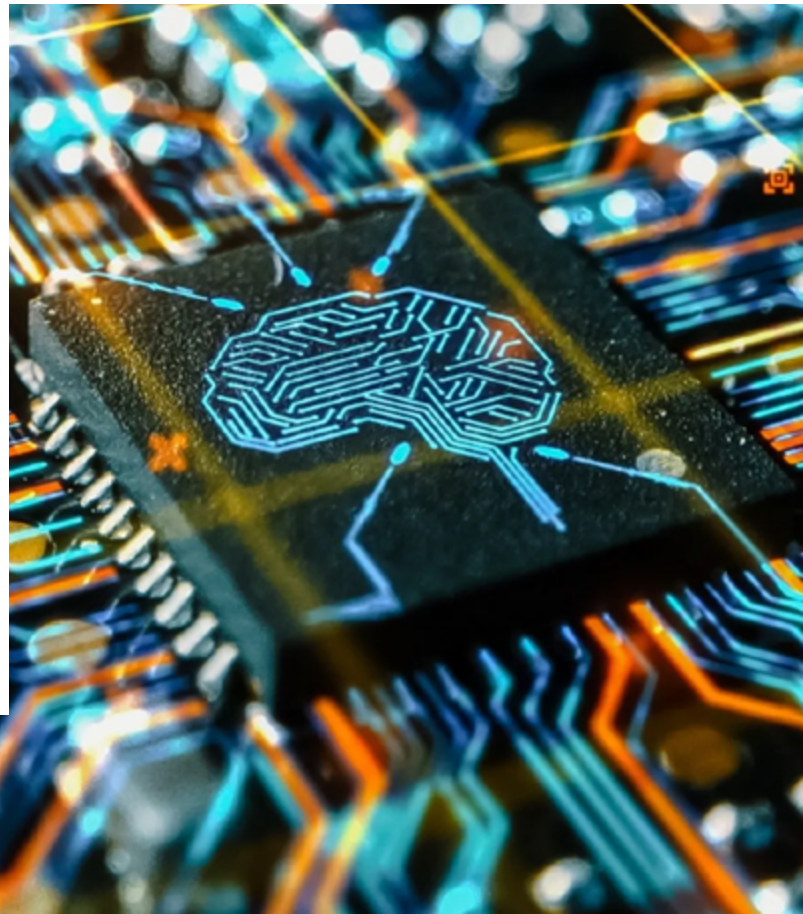
- Inversión dinámica y orgánica en ciberseguridad a la medida.
- Cultura de riesgo de ciberseguridad.
- Ciberresiliencia activa.
- Implementación medible de marcos de referencia de buenas prácticas internacionales.
- Controles preventivos para reducir los costos financieros ante ciberincidentes.
- Contratar un proveedor de implementación de ciberseguridad; sí, pero auditado por SOC (Service Organization Controls).
- Contratar una compañía consultora para la emisión de un informe SOC 2 tipo 2.
- Obtención de un informe SOC de ciberseguridad.
- Contratar un proveedor de primer nivel y de marca mundial de servicios de Aseguramiento de TI sobre la eficiencia del control interno y la integración efectiva de ciberseguridad en:
  - Inteligencia artificial (IA)
  - Sostenibilidad (impacto ESG)
  - Gestión de Riesgo de Terceros (TPRM)
  - Escepticismo y Zero Trust
  - Efecto y resultados de las campañas de concientización
  - Optimización de los costos de cumplimiento
  - Satisfacción del cliente y la comunidad de negocios
  - Riesgo reputacional, confianza al público e imagen de la marca
  - Diferenciación de su oferta de servicios y aporte de valor adicional

Conclusión

La ciberinteligencia y la cibersabiduría son pilares fundamentales en la lucha contra las crecientes amenazas cibernéticas. La ciberinteligencia nos permite anticipar y mitigar riesgos mediante la recopilación y análisis de datos, mientras que la cibersabiduría integra este conocimiento con experiencia, estrategia, juicio prudente y aplicación ética para gestionar y proteger la información digital de manera efectiva mediante una toma de decisiones informada.

La combinación de estas dos disciplinas es esencial para crear un entorno digital seguro y resiliente. La creciente sofisticación de los ciberataques y el impacto financiero significativo que estos pueden tener enfatizan la necesidad de una estrategia integral que no solo se enfoque en la prevención, sino también en la respuesta y recuperación.

En **BDO**, comprendemos muy bien la relevancia de proteger sus activos digitales y garantizar la continuidad de su negocio. Ofrecemos servicios de Aseguramiento de TI en materia de Evaluación de Riesgos de Ciberseguridad e Informes SOC, diseñados para ayudarle a identificar, evaluar y mitigar las amenazas cibernéticas y generar confianza. Póngase en contacto con nosotros hoy mismo para saber cómo podemos ayudarle a proteger su información y asegurar el futuro de su organización en el entorno digital mediante nuestro equipo de especialistas en ciberintelingencia y cibersabiduría.



CONTACTO

DARÍO GONZÁLEZ
Socio Líder de Auditoría y Aseguramiento

dario.gonzalez@bdo.com.pa

CARLOS PINTO
Socio de Auditoría y Aseguramiento

carlos.pinto@bdo.com.pa

VIDALINA CANDANEDO
Socia de Auditoría y Aseguramiento

vidalina.candanedo@bdo.com.pa

CONTENIDO PREPARADO POR:

MARVIN CABEZAS
Gerente Senior de Auditoría en Sistemas

marvin.cabezas@bdo.com.pa

www.bdo.com.pa