LITORALPRESS

Fecha: 16-06-2025
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: **AdvanSolution y EFE comparten estrategia para blindar una infraestructura crítica**

Pág. : 29
Cm2: 264,0
VPE: $ 2.339.693

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

CASO DE ÉXITO:

AdvanSolution y EFE comparten estrategia para blindar una infraestructura crítica

Luis Egaña, líder de Ciberseguridad en EFE, responde cinco claves sobre cómo blindar una infraestructura crítica, como el ferrocarril, frente a amenazas cada vez más sofisticadas.

¿Qué debe hacer un CISO para blindar su organización frente a los ciberataques?

- En EFE una figura como un CISO debe liderar una estrategia integral de ciberseguridad que proteja tanto la infraestructura TI como los sistemas operativos ferroviarios (OT). Esto incluye evaluar riesgos, aplicar estándares de seguridad TI como OT, segmentar redes críticas, fortalecer la detección y respuesta ante incidentes, y capacitar al personal. La clave es blindar la continuidad operacional del transporte frente a amenazas cada vez más sofisticadas.

¿Cómo justificar el presupuesto de ciberseguridad?

- En EFE, justificamos el presupuesto de ciberseguridad porque protegemos una infraestructura crítica para el país. Un ciberataque puede interrumpir el servicio ferroviario, afectar señales, trenes y la seguridad de nuestros pasajeros y trabajadores. Invertir en ciberseguridad es prevenir riesgos operacionales, cumplir con la Ley Marco de Ciberseguridad y proteger tanto nuestros sistemas tecnológicos (TI) como los operativos (OT). Además, es clave para asegurar una transformación digital segura y confiable en el transporte público.

¿Vale la pena tercerizar un SOC?

- En EFE, tercerizar un SOC sí vale la pena, especialmente por la necesidad de vigilancia 24/7, detección temprana de amenazas y respuesta rápida ante incidentes en infraestructuras críticas. Un SOC externo aporta experiencia especializada, herramientas avanzadas y escalabilidad, lo que complementa nuestras capacidades internas. Sin embargo, debe ser un modelo híbrido y supervisado, donde EFE mantenga el control estratégico y la visión de seguridad, asegurando que se protejan tanto los entornos TI como OT con conocimiento del negocio ferroviario.

Luis Egaña, líder de ciberseguridad de EFE.

¿Qué tan importante es capacitar a los colaboradores?

- En EFE, capacitar a los colaboradores en ciberseguridad es fundamental. La mayoría de los ciberataques comienzan por errores humanos, como abrir un correo malicioso. Por eso, formar a nuestro personal tanto administrativo como operacional es clave para proteger los sistemas críticos que mueven los trenes y garantizar la continuidad del servicio. La ciberseguridad no es solo un tema técnico, es una responsabilidad compartida.

¿Cómo se mide el retorno de la inversión (ROI) en ciberseguridad?

- En EFE, medimos el retorno de la inversión en ciberseguridad no solo en términos económicos, sino en continuidad operativa y reducción de riesgos. Invertir en protección evita interrupciones del servicio ferroviario, sanciones por incumplimientos normativos y daños a la reputación. El ROI se refleja en incidentes evitados, tiempos de respuesta más rápidos y mayor confianza de usuarios y autoridades. En una empresa como la nuestra, la ciberseguridad es una inversión para mantener el país en movimiento, no un gasto.