LITORALPRESS

Fecha: 16-01-2025
Medio: El Mercurio
Supl. : El Mercurio - FINANZAS & TECNOLOGÍA
Tipo: Noticia general
Título: Los pilares para construir una estrategia de ciberseguridad

Pág. : 3
Cm2: 266,7

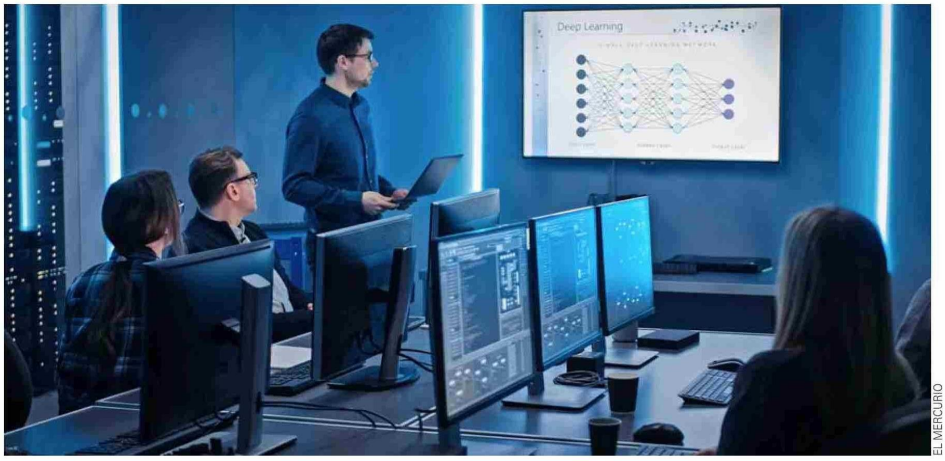
Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

INVOLUCRA DESDE LA TOMA DE DECISIONES HASTA LA FORMACIÓN CONSTANTE:

Los pilares para construir una estrategia de ciberseguridad

NOEMÍ MIRANDA G.

La protección digital de una empresa debe ser abordada integralmente, a todos los niveles y desde todas las áreas. Entender que es un tema transversal y no solo técnico es un paso clave.



EL MERCURIO

En las últimas dos décadas, casi el 20% de los ciberataques a nivel global tuvieron como blanco al sector financiero, causando pérdidas por más de US$ 12.000 millones, reportó en 2024 el Fondo Monetario Internacional. Y si bien hasta ahora estos incidentes —capaces de amenazar la resiliencia de las operaciones de las entidades financieras— no han sido sistémicos, con la vertiginosa transformación tecnológica este riesgo crece radicalmente.

Es por eso que toda institución que posee un capital digital debe construir una base sólida a escala técnica y humana para hacer frente a dicha amenaza.

¿Cuáles deben ser los pilares de una estrategia en este sentido?

Decisiones a conciencia

Un error común es creer que la ciberseguridad es un asunto solamente técnico e ignorar a las personas. "Datos del Foro Económico Mundial indican que en el 95% de las brechas de ciberseguridad influye el factor humano. Por ende, la gestión del cambio y la generación de conciencia son fundamentales para una estrategia exitosa", dice Romina Garrido, directora de Protección de Datos y Ciberseguridad en Prieto Abogados, y subdirectora del GobLab de la Universidad Adolfo Ibáñez.

Por ello, y considerando las exigencias legales, se debe partir abordando la ciberseguridad a nivel de directorio y/o de los dueños de una empresa: lo peor es delegar este desafío en otras personas y esperar que las decisiones y soluciones simplemente aparezcan, indica Bernardo Siu, ingeniero y cofundador de la *fintech* de pagos electrónicos ETpay. Estima que tomar la decisión al nivel más alto es el primer paso: "La seguridad de la información y el resguardo ante un potencial fraude a sus clientes debe ser un eje fundamental".

Equipos y cultura

"Se debe definir un equipo o un comité de ciberseguridad, compuesto por roles clave como el Chief Information Security Officer (CISO) u otro responsable; ingenieros especializados en seguridad informática y redes, y representantes de áreas críticas, como tecnología, operaciones y legal o *compliance*. En el caso de empresas pequeñas, esto se podría externalizar con un proveedor especializado y un seguimiento interno", detalla Vicente Cruz Infante, CEO de The Sheriff, *fintech* especializada en evaluación de riesgo crediticio de personas y empresas.

Además, estima indispensable definir políticas y procedimientos claros sobre manejo de datos, control de accesos y respuesta ante incidentes. "Es fundamental, por lo mismo, crear una cultura de seguridad, sensibilizando a todo el personal, desde directivos hasta operadores, sobre la importancia de la ciberseguridad mediante capacitaciones continuas", advierte.

También se requiere un equipo transversal que monitoree el avance y el grado de madurez que se va adquiriendo en ciberseguridad, y que vele por el cumplimiento de la estrategia.

Definir áreas críticas

Romina Garrido indica que es clave diagnosticar los puntos más vulnerables y el capital crítico a proteger, desde datos personales hasta dinero: "El análisis de riesgo es fundamental para orientar la inversión y, dentro del riesgo, están las pérdidas económicas, las reputacionales y las sanciones legales de órganos reguladores. Esto es lo que viene en el área de datos personales; fuertes multas por no implementar medidas de seguridad suficientes".

En materia de datos, "siempre es bueno hacer un inventario de activos, sea información u otros, que indica qué proteger y a qué costo. Si se trata de un proyecto nuevo o servicio, hay que partir pensando para qué se guarda cierta información", comenta Bernardo Siu.

Por su parte, Cruz Infante destaca que es clave "asegurar que los datos personales, financieros o transaccionales estén encriptados en reposo y en tránsito. El cumplimiento de normativas como la GDPR de EE.UU. o la Ley de Protección de Datos chilena es crítico". También se deben implementar controles de acceso estrictos (como autenticación multifactor) y políticas de privilegios mínimos, realizar análisis de vulnerabilidades y pruebas periódicas para identificar puntos débiles. Junto con esto, hay que "contar con un plan de respuesta a incidentes que incluya medidas inmediatas, responsables designados y protocolos de recuperación, y monitorear y auditar los sistemas y accesos de proveedores externos que manejen datos críticos o interactúan con la infraestructura de la empresa".

Errores frecuentes

"El área más crítica en la ciberseguridad son las personas; tener colaboradores internos y externos conscientes de los riesgos y amenazas a los que están expuestos es crucial. Sin eso, no hay herramientas o productos que den garantías de un adecuado nivel de ciberseguridad", advierten desde la Cámara de Comercio de Santiago.

Otro error frecuente es no capacitar al personal en temas básicos, como la detección de *phishing* y otros fraudes digitales, o caer en la confianza excesiva. "Aunque los sistemas de seguridad son importantes, no reemplazan la necesidad de procesos robustos y monitoreo constante. Muchas empresas crean planes de ciberseguridad pero nunca los prueban. Esto las deja vulnerables ante incidentes reales. Lo mismo sucede si es que delegan servicios críticos a terceros sin auditar su seguridad. Finalmente, las empresas que no planifican cómo volver a operar tras un ataque tienden a enfrentar mayores pérdidas financieras y de confianza", advierte Cruz Infante.