LITORALPRESS

Fecha: 26-01-2026
Medio: La Estrella de Arica
Supl. : La Estrella de Arica
Tipo: Noticia general
Título: **Resiliencia digital: ¿ estamos preparados para proteger la operación y los datos?**

Pág. : 6
Cm2: 253,7

Tiraje: 7.300
Lectoría: 21.900
Favorabilidad: No Definida

DINOS QUE PIENSAS

opinion@estrellaarica.cl
@EstrelladeArica La Estrella de Arica

Resiliencia digital: ¿estamos preparados para proteger la operación y los datos?

Durante los últimos años, la conversación sobre ciberseguridad ha estado marcada por la preocupación y la urgencia. Ataques, filtraciones y caídas de sistemas ocupan titulares y generan una sensación permanente de vulnerabilidad. Sin embargo, es importante hacer una distinción clave: que existan amenazas no significa que estemos indefensos. Hoy, las organizaciones cuentan con la tecnología, el conocimiento y las metodologías necesarias para proteger su operación, resguardar los datos y asegurar la continuidad de sus servicios.

La transformación digital avanzó a gran velocidad y, con ella, aumentó la superficie de exposición. Este escenario exige un cambio de enfoque: pasar de una lógica reactiva a una estrategia de resiliencia digital. Hablamos de la capacidad de anticipar incidentes, resistirlos cuando ocurren, recuperarse rápidamente y aprender para fortalecer los sistemas. Esa resiliencia ya no es un ideal teórico, sino una capacidad concreta que puede diseñarse, medirse y gestionarse.

En Chile, este desafío adquiere una dimensión adicional. La entrada en vigor del Marco de Ciberseguridad y el avance de la nueva Ley de Protección de Datos Personales establecen obligaciones claras para las organizaciones, entre ellas la notificación de incidentes relevantes a la Agencia Nacional de Ciberseguridad (ANCI).

Este componente de obligatoriedad no solo eleva el estándar, sino que también fortalece el Sistema Nacional de Ciberseguridad, promoviendo mayor transparencia, coordinación y aprendizaje colectivo frente a amenazas cada vez más sofisticadas.

Desde el punto de vista tecnológico, hoy existen arquitecturas maduras y probadas que permiten enfrentar eventos críticos sin afectar el negocio. Modelos de escalabilidad elástica, servicios distribuidos en la nube, segmentación inteligente de cargas, redundancia geográfica y mecanismos automáticos de mitigación ante ataques —como los DDoS— forman parte del estándar disponible. Estas soluciones hacen posible absorber picos de demanda, contener incidentes y sostener la operación activa incluso en escenarios de alta presión.

No obstante, la tecnología por sí sola no es suficiente. La resiliencia digital también se construye a través de la preparación y la capacitación. Pruebas periódicas, test de estrés y simulaciones de escenarios críticos ayudan a anticipar el comportamiento real de la infraestructura y de los equipos humanos. En un contexto regulatorio más exigente, esta preparación resulta clave para responder de forma oportuna, cumplir con las obligaciones de reporte y minimizar impactos operacionales, comerciales y reputacionales.

Otro elemento prioritario es el monitoreo continuo. Contar con centros especializados de operación de seguridad, vigilancia 24/7, herramientas avanzadas de detección y planes claros de recuperación facilita la identificación temprana de anomalías y la acción antes de que un incidente escale. Esta combinación de prevención, detección y respuesta convierte a la ciberseguridad en un habilitador del negocio y de la confianza pública.

La experiencia demuestra que las organizaciones que no planifican terminan asumiendo costos mucho mayores: interrupciones de servicio, procesos de recuperación complejos y pérdida de credibilidad. En cambio, aquellas que integran la resiliencia digital como parte de su estrategia —y alineadas con el marco normativo chileno— alcanzan mayor estabilidad, continuidad y confianza frente a clientes, usuarios y ciudadanos.

La ciberseguridad no debe entenderse desde el miedo, sino desde la preparación. Hoy estamos en condiciones de proteger la operación y los datos de forma efectiva. La diferencia no está en evitar todos los incidentes, sino en cuán preparados estamos para responder, informar y recuperarnos con rapidez, contribuyendo así a un ecosistema digital más resiliente para el país.

Pablo Álvarez, gerente de Negocios y Ciberseguridad de Entelgy Chile