LITORALPRESS

Fecha: 30-05-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Migración cloud: ¿De quién esla responsabilidad sobre la seguridad de los datos?**

Pág. : 6
Cm2: 345,0

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

MODELOS DE GESTIÓN Y GOBERNANZA

Migración *cloud*: ¿De quién es la responsabilidad sobre la seguridad de los datos?

La protección de la información y servicios que una empresa tenga en plataformas en la nube es una tarea compartida, indican los expertos; el proveedor garantiza controles de seguridad, pero estos dependerán de los criterios que los clientes deben definir.

NOEMÍ MIRANDA

Se estima que, para 2027, el 90% de las organizaciones a nivel mundial utilizará una nube híbrida, conformada por el uso de nubes públicas, privadas y la propia infraestructura local, según Gartner. Sus usos van desde almacenamiento y análisis de grandes volúmenes de datos, hasta el desarrollo, testeo y puesta en marcha de servicios y soluciones tecnológicas.

Este panorama genera preocupaciones por la seguridad de los datos contenidos y la continuidad operativa de los servicios, temas que fueron abordados en el panel "Despejando la nube: Seguridad, escalabilidad y *data science*", realizado durante el Cybertech South America 2025.

FYPO PHOTOS

EDUARDO OLIVARES, editor de Economía y Negocios, moderó la conversación entre Cuky Pérez, Marcelo Díaz, Ernesto Tachoires y Luis Elola.

ÁMBITOS DE PROTECCIÓN

Ernesto Tachoires, director corporativo de Desarrollo de Negocios de Ciberseguridad de SONDA, destaca que existen al menos dos ámbitos de protección: el primero se refiere a los servicios en la nube tal como se les conoce en la industria; el segundo, a veces menos evidente, son las acciones que llevamos a cabo día a día, como compartir documentos, hojas de cálculo o carpetas. Si en esa conexión se genera una brecha por la que ingresa un *malware*, un equipo comprometido puede terminar afectando a toda la organización.

"Existe una falsa sensación de seguridad en las organizaciones; migrar a la nube no significa que la responsabilidad de seguridad se le transfiere al proveedor", dijo Tachoires. Es un modelo de responsabilidad compartida, en que la empresa proveedora entrega a su cliente ciertos controles, y otros resguardos son deber de los usuarios corporativos que utilizan el servicio.

"No se trata tan solo de poner mis servicios a nivel *cloud* y dejarlos ahí; tengo que incorporar niveles y capas de seguridad", resaltó Marcelo Díaz, socio del Área de Ciberseguridad de Deloitte Chile. Estos involucran el manejo de vulnerabilidades, control de identidades y monitoreo de configuraciones, entre otros, que deben ser incluidos en los modelos de gestión y gobernanza, definiendo los puntos clave de la seguridad, en el entendido de que todos los servicios que se manejan en la nube puedan convivir de manera segura.

Esto cobra mayor relevancia en un contexto cada vez más desafiante, comentó Luis Elola, *cybersecurity product & advisor manager* de Servicios de Ciberseguridad de Entel, cuyos reportes permanentes arrojan que los principales problemas son la configuración de la seguridad y, luego, la exfiltración (exposición involuntaria de información).

Por ello, las empresas deben tener una política de gobernanza de datos y una estrategia clara de administración. Cuky Pérez, experta en *data science*, advirtió que una compañía que lleva sus datos y procesos a la nube debe definir asuntos clave como qué tipo de información se mantendrá en estas plataformas, cuán estratégica es y cuánto valor agrega al negocio. Además, debe tener clara la trazabilidad de la información, considerando las normativas que así lo exigen.

Pérez advirtió sobre otro frente crítico y emergente: ante la vorágine tecnológica, los equipos de desarrollo y prueba pueden crear y compartir código o descargar programas de contrapartes en apariencia seguras, pero que pueden introducir vulnerabilidades. Por ende, ninguna área debe quedar fuera de la estrategia de seguridad.

PANEL 4