LITORALPRESS

Fecha: 27-05-2026
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: **Identidad, el nuevo perímetro de la ciberseguridad**

Pág. : 7
Cm2: 252,9

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

CONTROL DE ACCESO:

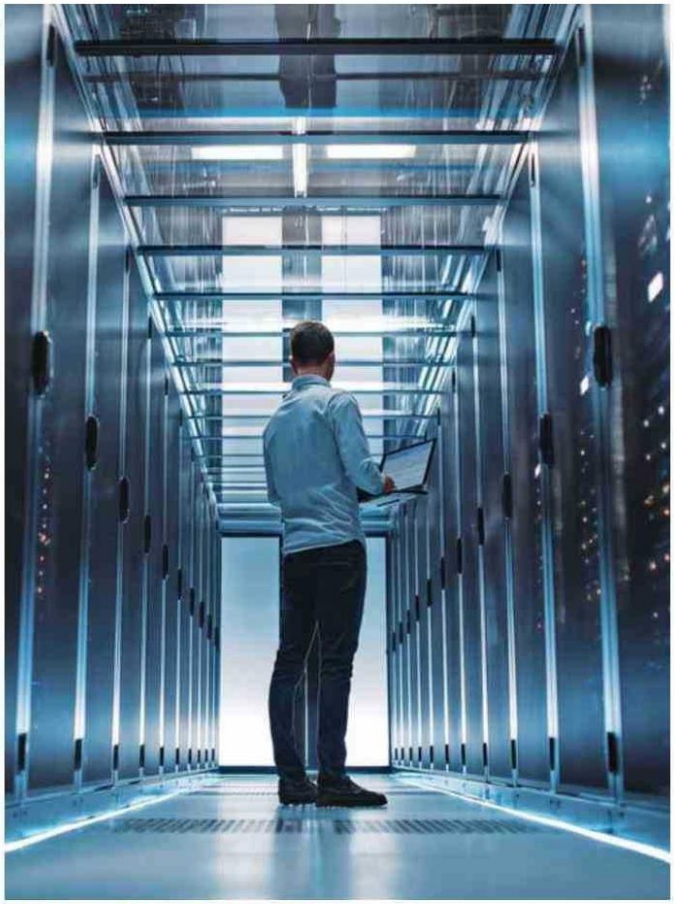
Identidad, el nuevo perímetro de la ciberseguridad

La autentificación se ha convertido en el principal punto de defensa ante el aumento de ataques con credenciales robadas y el explosivo crecimiento de entes no humanos.

IVÁN SILVA I.

Los ataques cibernéticos cada vez más complejos están obligando a las organizaciones a replantear sus estrategias de seguridad. Por ende, el perímetro tradicional basado en redes ha perdido relevancia frente a las identidades.

"La mayoría de los ataques ya no empieza con una vulnerabilidad técnica, sino con una identidad comprometida. En un entorno donde las identidades humanas y no humanas se multiplican exponencialmente, el control de accesos se convierte en el principal punto de defensa", señala Juan Carlos Beltrán, CTO del Centro de Excelencia en Ciberseguridad de Gtd.



DE ACUERDO CON VERIZON DBIR, cerca del 38% de las brechas globales involucran credenciales robadas.

UN PROBLEMA QUE ESCALA CON LOS DATOS

De acuerdo con Verizon DBIR, cerca del 38% de las brechas globales involucran credenciales robadas. Y mientras Ponemon Institute dice que en América Latina, el 54% de las organizaciones ha sufrido brechas por este vector, Check Point estima que el 65% de los ataques exitosos utilizó métodos basados en identidad.

Solo en la primera mitad de 2025 se registraron 1.800 millones de credenciales robadas en el mundo, un 160% más que en el mismo período del año anterior.

EL NUEVO ROSTRO DEL RANSOMWARE

El modelo *Ransomware as a Service* ha profesionalizado el cibercrimen. Los atacantes combinan ingeniería social, credenciales robadas y movimiento lateral. Con frecuencia, las credenciales se comprometen en dispositivos personales antes de ingresar a las redes corporativas. Una vez dentro, escalan privilegios, se desplazan lateralmente y buscan persistencia.

Y la IA ha elevado la sofisticación de estos ataques. Según el Fortinet Threat Intelligence Report 2025, el 45% de los ataques de ingeniería social utilizó inteligencia artificial para crear mensajes más creíbles.

Al respecto, Beltrán sostiene que "la IA está eliminando muchas de las señales tradicionales de fraude. Los ataques hoy son más personalizados, más creíbles y mucho más difíciles de detectar".

Un factor crítico ha sido el crecimiento de identidades no humanas. Por cada usuario humano, las empresas gestionan entre 10 y 45 identidades automatizadas (API, *bots* y agentes de IA) con altos privilegios.

EL CAMINO A SEGUIR EN CHILE

En nuestro país, donde la banca, el *retail*, la minería y los servicios públicos avanzan en materia de digitalización, gestionar identidades se ha vuelto un desafío estratégico.

Por ello, se recomienda adoptar un modelo *Identity-Centric Security* basado en *zero trust*, que incluye autenticación multifactor (MFA), gestión de identidades y accesos (IAM), control de accesos privilegiados (PAM) y monitoreo con IA.

"El enfoque *zero trust* reconoce que el perímetro desapareció. Actualmente, el control está en la identidad; es decir, en quién accede, con qué privilegios y en qué condiciones. Si no gestionamos eso de forma continua, la organización queda expuesta", subraya Beltrán.