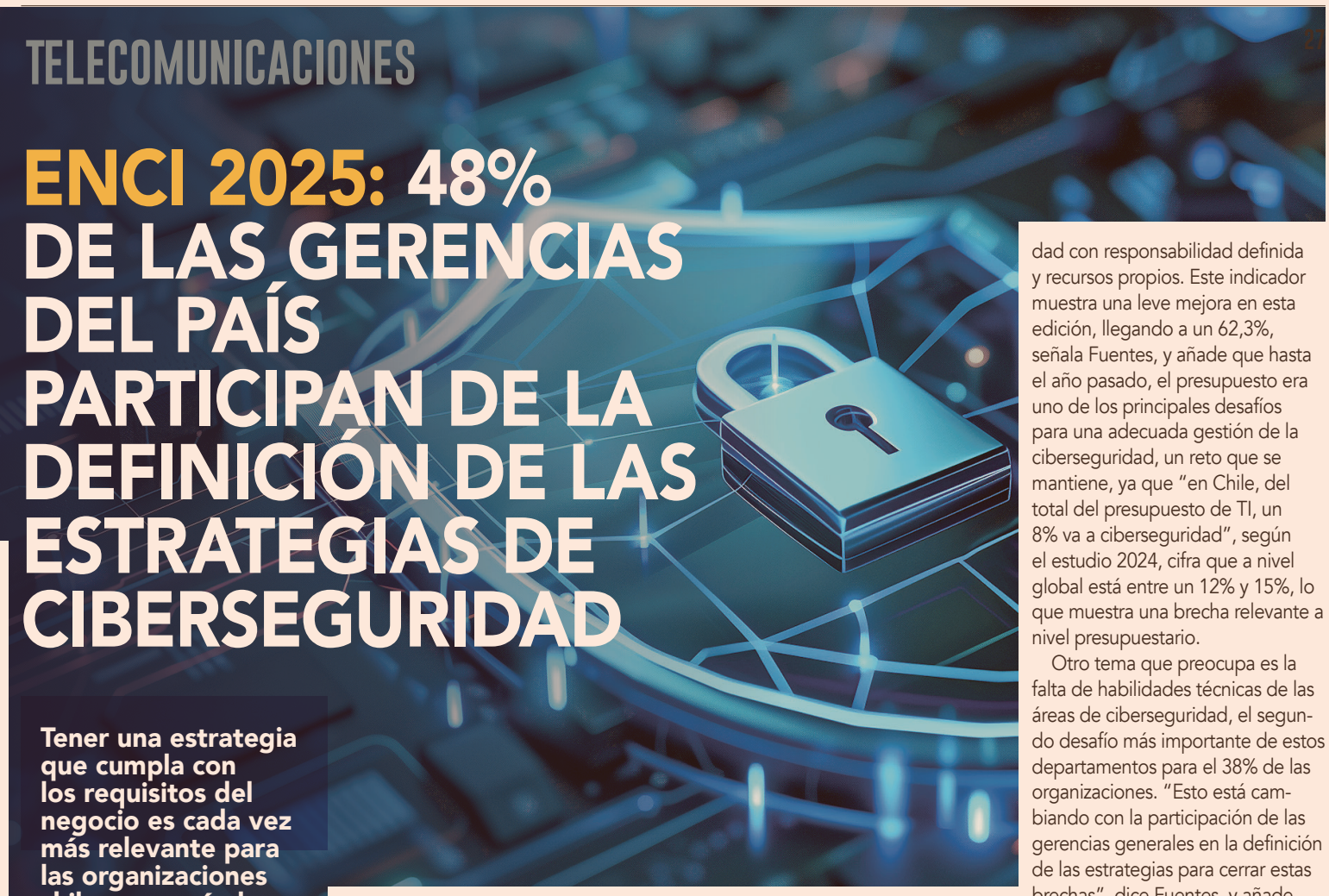
DF
DIARIO FINANCIERO®
SUPLEMENTO
SANTIAGO DE CHILE
MARTES 26 DE AGOSTO DE 2025

ENCI 2025: 48% DE LAS GERENCIAS DEL PAÍS PARTICIPAN DE LA DEFINICIÓN DE LAS ESTRATEGIAS DE CIBERSEGURIDAD



Tener una estrategia que cumpla con los requisitos del negocio es cada vez más relevante para las organizaciones chilenas, según los primeros resultados del Estudio Nacional de Ciberseguridad 2025, elaborado por CETIUC.

POR ANDREA CAMPILLAY

En un mundo interconectado, contar con un área de ciberseguridad definida y usuarios capacitados en este ámbito, se ha vuelto cada vez más importante para las organizaciones chilenas. Así lo constatan los resultados preliminares del Estudio Nacional de Ciberseguridad (ENCI) 2025, desarrollado por el Centro de Estudios de Tecnologías de la Información de la Pontificia Universidad Católica de Chile (CETIUC), que revela que, de las 50 organizaciones que participaron en esta edición, en un 48% de los casos la gerencia general participa de la definición de la estrategia de ciberseguridad.

"Eso es muy importante porque quiere decir que el tema de la ciberseguridad, y principalmente la definición de una estrategia que cumpla con los requisitos del negocio, está siendo cada vez más importante", afirma el director de estudios y tecnología en CETIUC, Matías Fuentes.

Una de las nuevas dimensiones de esta versión del estudio es el impacto que han tenido los ciberataques en las organizaciones, donde un 72% señaló que el principal impacto ha sido la interrupción de operaciones, y en segundo lugar la pérdida de confianza en la tecnología.

En 2024, los resultados revelaron que un 61% de las organizaciones contaba con un área de ciberseguridad con responsabilidad definida y recursos propios. Este indicador muestra una leve mejora en esta edición, llegando a un 62,3%, señala Fuentes, y añade que hasta el año pasado, el presupuesto era uno de los principales desafíos para una adecuada gestión de la ciberseguridad, un reto que se mantiene, ya que "en Chile, del total del presupuesto de TI, un 8% va a ciberseguridad", según el estudio 2024, cifra que a nivel global está entre un 12% y 15%, lo que muestra una brecha relevante a nivel presupuestario.

Otro tema que preocupa es la falta de habilidades técnicas de las áreas de ciberseguridad, el segundo desafío más importante de estos departamentos para el 38% de las organizaciones. "Esto está cambiando con la participación de las gerencias generales en la definición de las estrategias para cerrar estas brechas", dice Fuentes, y añade que también "hay un brecha importante en la educación y cultura de los usuarios de TI", dimensión que un 76% de los encuestados señaló como un punto a mejorar.

Los resultados finales de esta medición serán liberados a fin de año, adelanta Fuentes.

PUBLIRREPORTAJE

Mainsoft®

MAINSOFT, único Partner Elite en Ciberseguridad - DARKTRACE en Latinoamérica

Únicos en Latinoamérica y destacados por CETIUC

La multinacional Inglesa de **Ciberseguridad DARKTRACE**, líder especialista en Network Detection & Response (NDR), recientemente nombró a **MAINSOFT como Partner categoría Elite** para la venta de sus Soluciones y Servicios, siendo el único en esta categoría en la región.

Esta categoría avala el más alto nivel de experiencia y capacidad en el ecosistema de DARKTRACE y se otorga al demostrar un completo dominio de la tecnología, un historial de implementaciones exitosas y un compromiso absoluto con la satisfacción del cliente. MAINSOFT cuenta con más de **30 clientes en Chile, Argentina y Perú** que pueden acreditar esta condición.

Este logro lo refrenda también la destacada Encuesta Nacional de Ciberseguridad (ENCI) 2025, elaborada por **CETIUC**, que evalúa muy bien a MAINSOFT en las categorías de Consultoría en Ciberseguridad y Servicios Administrados de Ciberseguridad. El **Estudio ENCI** reúne la opinión de más de **100 CIO´s** y **CISO´s** de grandes empresas y organismos del país, quienes evaluaron a sus proveedores.

Innovación para la ciberseguridad

DARKTRACE y MAINSOFT se distinguen por un enfoque pionero en la **Ciberseguridad impulsada por la Inteligencia Artificial**. A diferencia de las soluciones tradicionales, DARKTRACE junto al **SOC Cognitivo** de MAINSOFT utilizan IA de autoaprendizaje para comprender el "patrón de vida" único de cada organización, esto les permite detectar y neutralizar amenazas sofisticadas en tiempo real, sin depender de firmas o reglas predefinidas.

Los ingenieros de MAINSOFT certificados en DARKTRACE utilizan la innovación de las soluciones de DARKTRACE para mejorar la capacidad de análisis, detección y respuesta ante los desafíos de Ciberseguridad que demanda la constante evolución de amenazas a las que las empresas se ven afectadas.



Innovación e IA las claves del compromiso de MAINSOFT con la seguridad de sus clientes.

DARKTRACE y CETIUC reconocen la calidad y profesionalismo de MAINSOFT en la provisión de servicios de ciberseguridad.

Los clientes nuestro foco principal

Este reconocimiento de DARKTRACE avala más de 8 años de trabajo de nuestro equipo, el cual cuenta con la **certificación más avanzada** en sus soluciones, lo que nos permite diseñar, implementar y gestionar proyectos de **Ciberseguridad** con la máxima eficiencia para nuestros clientes. Esta experiencia se complementa con el ofrecimiento de nuevos servicios en nuestro Centro de Operaciones de Seguridad **(SOC – MDR)**, especializados para DARKTRACE, lo que nos **permite monitorear, detectar y responder a incidentes** de forma precisa y proactiva.

DÉFICIT DE TALENTO Y ALZA DE ATAQUES TENSIONAN LA CIBERSEGURIDAD LOCAL



Ante el sostenido aumento de ataques informáticos y en medio de una fuerte escasez de especialistas, los proveedores refuerzan sus servicios y ajustan estrategias de defensa. Aquí, actores de la industria lo analizan. POR MACARENA PACULL M.

Los crecientes incidentes informáticos en Chile han posicionado a la ciberseguridad como una prioridad estratégica para organizaciones públicas y privadas. De acuerdo con el informe Kaspersky IT Security Economics, publicado a principios de agosto, en los últimos meses las grandes empresas chilenas experimentaron la mayor tasa de incidentes de seguridad de red, a pesar de contar con las medidas de protección más completas. El *ransomware* es la principal amenaza mundial y regional, según el Reporte Ciberseguridad 2025 de Entel Digital, y tiene a Chile como uno de sus blan-

PUBLIRREPORTAJE

SOCIO ESTRATÉGICO PARA CIBERDEFENSA

Plataforma de Widefense diagnostica el estado de ciberseguridad para tener una hoja de ruta efectiva

Evaluar en qué nivel de ciberseguridad está una empresa permite verificar su capacidad de protección, identificar las acciones que pueden mejorarla y tomar acción sobre las que más impactan.

Con una trayectoria de más de cuatro décadas, Widefense es testigo de la falta de madurez de las empresas en su relación con la ciberseguridad. No solo se invierte poco, sino que la mayor parte del tiempo las acciones son reactivas. "Hoy los desafíos apuntan no solo a resguardar a la organización de ciberataques, sino también a cumplir las nuevas normativas de protección de datos y ciberseguridad, lo que no deja de ser complejo, en términos de establecer controles, disponer de tecnología y personal especializado, entre otras demandas", indica Marcelo Carvajal, subgerente de Consultoría.

Así, en su calidad de socio estratégico para ciberdefensa Widefense ofrece, entre muchos otros servicios, una plataforma que le permite a las empresas cuantificar en qué estado se encuentra su ciberseguridad y establecer las bases para una estrategia de seguridad exitosa y medible.



Marcelo Carvajal, subgerente de Consultoría.

"Con nuestra experiencia y las mejores prácticas internacionales, desarrollamos esta plataforma que, a través de una evaluación basada en estándares como CIS, NIST y CMMI, permite a las organizaciones simplificar el diagnóstico y tener recomendaciones accionables", explica el especialista y agrega que a diferencia de auditorías parciales, esta plataforma da un contexto integral que abarca desde el análisis técnico y los procesos hasta la gobernanza, ofreciendo una evaluación 360 de su postura de ciberseguridad.

De esta manera Widefense acompaña a cada organización para establecer una estrategia de ciberdefensa y definir la ruta crítica para implementarla, midiendo el impacto de las iniciativas y planes de inversión, además de entregar visibilidad para iniciar un proceso de mejora continua.

"Hoy todas las empresas están expuestas a un ataque, el desafío está en cómo lo enfrentamos, qué hacemos al ser atacados. De eso depende la continuidad del negocio y qué tanto puede impactar un ataque, nuestro objetivo es ayudarles a estar mejor preparadas y maximizar el beneficio de una estrategia personalizada de ciberseguridad", afirma Marcelo Carvajal.

Escanea el QR para conocer más sobre la plataforma o accede directamente a http://www.widefense.com/wsc



cos preferidos: es el cuarto país más afectado con esta modalidad de ataque.

En este escenario, los proveedores locales han encontrado una oportunidad y han ganado terreno para desarrollar y ofrecer soluciones que van desde centros de operaciones de seguridad (SOC) y arquitecturas *zero trust*, hasta plataformas de detección de *phishing* y servicios avanzados de protección de datos.

A juicio del jefe CSIRT en ITQ Latam, Sebastián Ávila, la industria local de ciberseguridad está en auge, pero tiene desafíos, especialmente de capital humano. El experto explica que la digitalización y el avance de los ataques cibernéticos revelaron un problema no menor: falta talento para enfrentar esta situación. Apunta que, para este año, se estima una falta de más de 7 mil profesionales del rubro en Chile, lo que se refleja en salarios más exigentes y afecta a las pymes de manera directa.

Un hito positivo que resalta Ávila es la entrada en vigencia, a principios de año, de la Ley Marco de Ciberseguridad. "Establece una institucionalidad y reglas claras, impulsando a las empresas a dedicarse, a invertir y profesionalizarse en esta materia, más aún en la actualidad, ya que las organizaciones se enfrentan a desafíos importantes como la brecha y fuga de talento; la creciente sofisticación de los ataques, impulsados por tecnologías como la inteligencia artificial", sostiene.

El *ransomware* es la principal amenaza mundial y regional, según el Reporte Ciberseguridad 2025 de Entel Digital, y tiene a Chile como uno de sus blancos preferidos: es el cuarto país más afectado con esta modalidad de ataque.

La gerenta general para la Región Sur de América Latina de Kaspersky, Andrea Fernández, dice que el país es el más avanzado en ciberseguridad en Latinoamérica por su madurez, adopción de leyes y la creación de entidades para hacerse cargo del tema a nivel nacional. "Muchos países en la región no tienen ni uno, ni otro. En el caso de los ataques y vulnerabilidades, podemos decir que Chile no se destaca por la creación de ciberataques, sino que es blanco de amenazas extranjeras, principalmente troyanos desarrollados en Brasil, ataques de ransomware internacionales e *infostealers*", acota.

Soluciones

Los expertos coinciden en que no hay una estrategia estandarizada para que las empresas estén más protegidas. Las firmas que proveen estos servicios así lo han entendido, y por eso la oferta es variada. En este escenario, la adopción del enfoque *zero trust* toma fuerza. Desde Mainsoft explican que en los últimos cuatro años, muchas empresas empezaron a planificar cómo implementarlo. Una tendencia que se debe, sobre todo, al auge de tecnologías *cloud* y a las nuevas modalidades de trabajo remoto, dicen desde la firma.

Ávila destaca los sistemas de detección y respuesta ante incidentes, y explica que los EDR/XDR permiten automatización defensiva frente amenazas en tiempo real. Resalta el uso de plataformas de Gestión de Identidad y Acceso (IAM), con soluciones como la implementación de dos o más tipos de verificación de identidad, o la administración de accesos y permisos de los colaboradores de forma centralizada. Dice que otra solución clave está en los Centros de Operaciones de Seguridad (SOC), una unidad centralizada y externa responsable de supervisar y administrar la seguridad de una organización.

A juicio del gerente general de Widefense, Kenneth Daniels, los SOC locales tienen una ventaja que los internacionales no tienen: el idioma, la cercanía, el conocimiento del entorno normativo y del mercado, lo que les da una capacidad de respuesta más ágil y personalizada. Acota que los internacionales, en cambio, "atienden a miles de empresas y principalmente a grandes corporaciones".

"Los SOC locales somos más personalizados en la atención y nos enfocamos en mantener un acompañamiento cercano y permanente", plantea.

PUBLIRREPORTAJE

Netprovider destaca en estudio CETI UC en Ciberseguridad

NETPROVIDER
KEEPING YOU ONLINE

"Es un orgullo ver cómo el esfuerzo constante y consciente por alcanzar la excelencia operacional se refleja en este tipo de reconocimientos. Que sean nuestros propios clientes quienes nos evalúan y destacan, nos motiva a seguir mejorando día a día y a mantenernos firmes en la senda de crecimiento y liderazgo en ciberseguridad", indica Alberto Castañeda Rojas, gerente general.

Como líder de ciberseguridad Netprovider busca consolidar y mantener la calidad técnica que entrega en cada proyecto a sus clientes. "El mercado enfrenta un escenario complejo por la constante evolución de las amenazas en ciberseguridad, en un entorno marcado por la adopción de la IA. Frente a ello, seguiremos evolucionando nuestros servicios para anticiparnos y responder de manera efectiva a estos nuevos riesgos", explica el gerente.

Asimismo, las nuevas normativas — Ley Marco de Ciberseguridad y Ley de Protección de Datos— exigen a las organizaciones avanzar en materia de gobernanza, gestión de riesgos y cumplimiento. "Nuestro desafío es estar a la altura de ese contexto, acompañando y guiando a nuestros clientes de manera oportuna para que fortalezcan sus controles y mantengan la confianza en sus operaciones", señala Alberto Castañeda.

Enfoque, agilidad y compromiso

Con operaciones en Santiago, Lima y Bogotá, Netprovider integra ciberseguridad avanzada y capacidades de observabilidad para asegurar la continuidad operativa de organizaciones en sectores estratégicos de Chile y América Latina.

De esa manera, empresas en sectores críticos confían en Netprovider para fortalecer su operación, principalmente por su enfoque que logra reducir incidentes, mejorar la eficiencia y cumplir con exigentes normativas en tiempo récord.

"Nuestra propuesta de valor se enfoca en ayudar a que nuestros clientes eleven de manera continua su madurez en ciberseguridad, fortaleciendo así la resiliencia y continuidad de sus operaciones", asegura el gerente general.

www.netprovider.com



"Buscamos empoderar a las empresas en su evolución digital, afirma Alberto Castañeda Rojas, gerente general.

Datos de interés

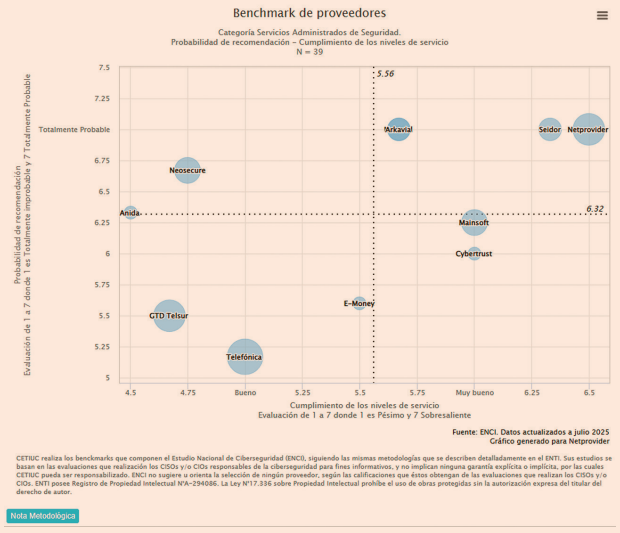
95% Satisfacción general de clientes LATAM

80% Reducción de incidentes críticos

70% Mejora en eficiencia operativa gracias a monitoreo avanzado

Propuesta de Valor

- Netprovider ofrece servicios personalizados, diseñados en función de las particularidades de cada industria y de los riesgos específicos que enfrentan.
- Busca integrarse a su cadena de valor, lo que refuerza la confianza mutua y su compromiso a ser un socio confiable en su protección y crecimiento.
- Ayuda a las empresas a elevar de manera continua su madurez en ciberseguridad, fortaleciendo así la resiliencia y continuidad de sus operaciones.



Fuente: ENCI. Datos actualizados a julio 2025
Gráfico generado para Netprovider

CETIUC realiza los benckmarks que componen el Estudio Nacional de Ciberseguridad (ENCI), siguiendo las mismas metodologías que se describen detalladamente en el ENTI. Sus estudios se basan en las evaluaciones que realizacion los CISOs y/o CIOs responsables de la ciberseguridad para fines informativos, y no implican ninguna garantía explícita o implícita, por las cuales CETIUC pueda ser responsabilizado. ENCI no sugiere u orienta la selección de ningún proveedor, según las calificaciones que éstos obtengan de las evaluaciones que realizan los CISOs y/o CIOs. ENTI posee Registro de Propiedad Intelectual N°A-294086. La Ley N°17.336 sobre Propiedad Intelectual prohibe el uso de obras protegidas sin la autorización expresa del titular del derecho de autor.

Nota Metodológica

CHILE AVANZA EN CIUDADES INTELIGENTES, PERO LA INCLUSIÓN DIGITAL SIGUE SIENDO UN DESAFÍO



Aunque el país lidera en despliegue de 5G y fibra óptica en la región, las brechas territoriales y sociales, junto con la falta de coordinación regulatoria, siguen limitando la consolidación de *smart cities* inclusivas y sostenibles, advierten expertos.

POR VALENTINA CÉSPEDES

Chile ha sido pionero en Latinoamérica en el despliegue de fibra óptica y 5G, tecnologías que se han convertido en la base habilitante para la transformación hacia ciudades inteligentes. Según el último Informe del Sector de Telecomunicaciones de la Subtel, el país alcanzó 6,5 millones de conexiones 5G en marzo de 2025, lo que representa un crecimiento de 53,4% respecto al año anterior. Sin embargo, las brechas territoriales, sociales y regulatorias todavía limitan la consolidación de urbes inclusivas y eficientes.

El presidente de la Cámara Chilena de Infraestructura Digital, Rodrigo Ramírez, explica que "el despliegue de 5G y fibra óptica, más capacidad analítica en el borde y en la nube, constituyen en Chile la base habilitante de cualquier ecosistema de ciudad inteligente". La fibra óptica asegura transporte de datos a gran escala con baja latencia, mientras el 5G otorga movilidad y capilaridad para aplicaciones en tiempo real.

Estos avances, añade, "están permitiendo que los municipios y gobiernos regionales comiencen a ensayar plataformas convergentes de *smart cities*, como inteligencia artificial para la seguridad pública, sensores urbanos, gestión eficiente de energía y agua, y sistemas de participación ciudadana digital".

Pero el desarrollo no es uniforme. El deputy country manager de Xiaomi Chile, Martín Castro, advierte que mientras Santiago y otras ciudades como Valparaíso, Concepción y Antofagasta avanzan con proyectos de *smart cities*, muchas zonas rurales tienen acceso limitado a redes de alta velocidad. "También existe una brecha social, donde la adopción de nuevas tecnologías depende del nivel socioeconómico y la brecha de inversión en infraestructura digital puede ralentizar la masificación del 5G", dice.

Ramírez coincide en que estas limitaciones "se traducen en una consolidación desigual de las ciudades inteligentes". A sus ojos, urge avanzar a un modelo donde comunas pequeñas o rurales "no queden rezagadas y evitar una ciudadanía de primera y segunda categoría en lo digital".

La cofundadora de Fundación Datos Protegidos, Jessica Mattus, complementa el análisis advirtiendo que Chile "necesita una ley marco de ciudades inteligentes que defina principios de inclusión, sostenibilidad y participación". En esa línea, Ramírez sostiene que los desafíos se concentran en tres planos: estratégico, regulatorio y sustentable. En lo estratégico, señala que el país requiere un plan de transformación digital al 2030 que entregue una visión nacional de ciudades inteligentes y evite depender solo de proyectos piloto. En lo regulatorio, plantea que se requiere agilizar permisos y coordinar normas entre distintos organismos. Y en lo sustentable, integrar criterios de eficiencia energética y economía circular, de modo que las *smart cities* no solo sean competitivas, sino también resilientes e inclusivas.

PUBLIRREPORTAJE

Netline aumenta en 300% su cobertura en el territorio nacional

La compañía expande su presencia a nivel nacional, llevando tecnología de punta en conectividad a las regiones con un uptime de 99,98%, infraestructura inalámbrica antivandálica y velocidades de hasta 10Gb, disponible en solo 24 horas.

Con más de 28 años de trayectoria, Netline vuelve a marcar un hito en la industria de las telecomunicaciones: un crecimiento de 300% en su cobertura nacional. Esta expansión no solo implica mayor alcance territorial, sino también la disponibilidad de capacidades de conectividad que hasta hace poco estaban reservadas exclusivamente para grandes capitales.

"Hoy la conectividad empresarial no puede depender únicamente de la fibra óptica. Nuestro modelo inalámbrico dedicado permite llevar Internet de alta disponibilidad a cualquier punto del país, tanto como enlace principal como respaldo estratégico para operaciones críticas", afirma Joel Bendersky, Gerente General de Netline.

Tecnología de nueva generación, en tiempo récord

La propuesta de Netline se basa en una infraestructura inalámbrica dedicada, inmune al vandalismo y diseñada para entregar continuidad operativa incluso en entornos de alta exigencia. Su servicio se instala en menos de 24 horas y ofrece un uptime de 99,98%, asegurando estabilidad y confianza en cada conexión. Además, alcanza velocidades de hasta 10Gb, con una calidad que supera los estándares de la industria.

Respaldo para la fibra y acceso en todo el territorio

El salto de cobertura permite que esta tecnología —tradicionalmente concentrada en zonas metropolitanas— esté ahora disponible en casi todo Chile. Empresas de regiones, industrias estratégicas y polos productivos podrán acceder a la misma conectividad de alto nivel que antes solo se encontraba en Santiago u otras grandes ciudades.

La solución no solo responde a las necesidades de conectividad primaria: también se ha consolidado como el mejor respaldo para enlaces de fibra óptica, garantizando continuidad en caso de cortes o incidentes. Esto la convierte en una herramienta clave para la continuidad de negocios, especialmente en sectores donde cada minuto de interrupción significa pérdidas económicas significativas.



Joel Bendersky, Gerente General de Netline.

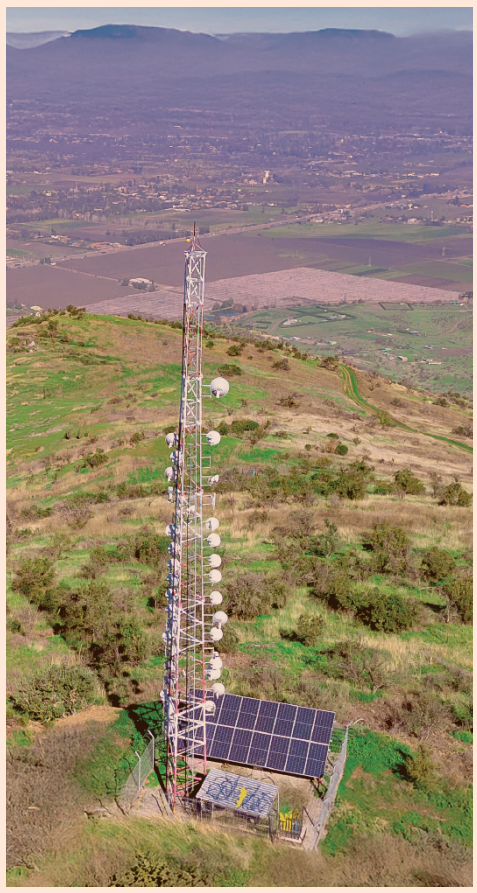
Un futuro más competitivo y resiliente

Para Netline, la conectividad es mucho más que velocidad: es resiliencia, continuidad y competitividad. "Nuestro compromiso es claro: democratizar el acceso a Internet empresarial de calidad, eliminando barreras de infraestructura y permitiendo que ninguna organización quede fuera del mundo digital", subraya Bendersky.

Con esta expansión, Netline reafirma su visión de futuro: un país más conectado, resiliente y preparado para los desafíos de la era digital.

Datos de Interés

Cobertura 300% mayor, conectividad de alto nivel en todo el territorio.
Instalación en 24 horas, enlace dedicado inmune al vandalismo con 99,98% uptime.



La expansión de Netline impulsa un futuro donde la conectividad de alta disponibilidad llega a cada rincón, asegurando continuidad y competitividad en la era digital.

CENTROS DE DATOS: CHILE ACELERA LIDERAZGO Y SE CONSOLIDA COMO POLO TECNOLÓGICO DE LA REGIÓN

El país ya suma 33 centros en operación y 34 proyectos en desarrollo, con inversiones que superan los US$ 4 mil millones hacia 2030. La conectividad, la energía limpia y la estabilidad institucional refuerzan su atractivo. POR VALENTINA CÉSPEDES



La industria de data centers en Chile continúa expandiéndose con fuerza. Estas instalaciones, claves para albergar grandes cantidades de servidores y sistemas informáticos que almacenan, procesan y distribuyen información digital, están consolidando al país como un hub tecnológico en América Latina y, de hecho, el último informe de GPS Property evidenció que ya es el segundo país en la región con mayor capacidad instalada, una posición estratégica que el Plan Nacional de Data Centers busca fortalecer.

Para la gerenta general de Chile Data Centers, Catalina Achermann, el sector ha vivido un auge sin precedentes, en gran parte por el aumento de la demanda asociada a la inteligencia artificial (IA). "Hoy contamos con 33 centros de datos en funcionamiento y 34 proyectos en desarrollo, lo que refleja un dinamismo pocas veces visto en otro sector ligado a la infraestructura en tan poco tiempo", afirma.

En esa línea, el gerente general de Entersoft, Rodrigo Acevedo, plantea que "Chile se está posicionando como un polo estratégico para la economía digital en la región, con beneficios en inversión, empleo y competitividad".

La fuerte inversión extranjera, como la anunciada en mayo pasado por AWS -US$ 4 mil millones en 15 años-, también ha sido decisiva para ampliar la infraestructura tecnológica y acelerar la adopción de servicios en la nube. El country manager de AWS Chile, Felipe Ramírez, subraya que la estabilidad política, la energía renovable, la conectividad robusta y el talento local calificado han permitido que "más empresas e instituciones accedan a infraestructura digital de clase mundial, lo que acelera la transformación en sectores clave como la banca, salud, educación y el retail".

En el ámbito de conectividad, el managing director de Equinix Chile & Perú, Francisco Basoalto, resalta que "hoy tenemos más de 60 mil kilómetros de fibra óptica desplegada y una red creciente de cables submarinos que nos conecta con Estados Unidos, Europa y próximamente Asia-Pacífico". Además, cerca del 60% de la matriz eléctrica nacional proviene de fuentes limpias, lo que asegura operaciones alineadas con compromisos globales de carbono neutralidad.

De cara al futuro, Achermann detalla que los 34 proyectos en desarrollo "implican más de US$ 4 mil millones de inversión" hasta 2030, consolidando a Chile como habilitador del desarrollo de IA, servicios en la nube y transformación digital para el Estado y las empresas.

Sin embargo, Acevedo advierte que el país enfrenta retos en infraestructura eléctrica y transmisión, procesos de permisología complejos, un déficit de talento especializado en TI y ciberseguridad, y la presión por avanzar en sostenibilidad y reducir el consumo de agua y energía. "Chile tiene ventajas competitivas claras, pero debe enfrentar estos desafíos para mantener su liderazgo regional", agrega.

GRUPO DF
DF DFLIVE DFMAS DFSUDI SEÑAL DF CAPITAL ED ED

Director: José Tomás Santa María / **Subdirectora:** Paula Vargas / **Gerente Comercial:** José Ignacio De la Cuadra / **Editora:** Claudia Marín / **Director Creativo y Arte:** Rodrigo Aguayo
Coordinadora: Marcia Aguilar / **Dirección** Edificio Fundadores, Badajoz 45, piso 10, Las Condes, Fono: 2 23391000 / e-mail: buzondf@df.cl / **Impreso por** Gráfica Andes Limitada, que sólo actúa como impresor.
Se prohíbe la reproducción total o parcial de los contenidos de la publicación.

PUBLIRREPORTAJE

AERMEC SOUTH AMERICA

AERMEC SOUTH AMERICA

Soluciones de climatización world class para centros de datos de misión crítica

Con más de 70 años de trayectoria, la compañía ha suministrado más de 100MW de enfriamiento a los centros de datos en Europa en los últimos 3 años.

El crecimiento continuo de las aplicaciones tecnológicas demanda el buen funcionamiento de los centros de datos con potencias cada vez más elevadas, lo cual conlleva a la necesidad de sistemas de climatización y enfriamiento eficientes, modulares, flexibles, sustentables y con un robusto servicio postventa.

Las soluciones para centros de datos de misión crítica de Aermec incluyen enfriadoras que combinan el freecooling con el enfriamiento adiabático, enfriadores de freecooling avanzado que incorporan el exclusivo Dynamic Set Point de Aermec, así como una amplia gama de climatizadores de precisión y unidades in-row, junto con unidades de booster bajo suelo para el enfriamiento localizado.

"Contamos con todas las certificaciones más importantes a nivel mundial y el laboratorio de pruebas más grande de Europa, con la capacidad de soportar cargas de enfriamiento de hasta 2MW. Además, nos preocupamos de establecer relaciones de largo plazo, fortalecer nuestro departamento de servicios, contar con la mejor infraestructura y capacitar de manera permanente a nuestro equipo técnico para entregar el mejor servicio post venta", afirma Ramón Morales, Director Regional Sudamericana.



Una climatización eficiente y de alta calidad es fundamental para resguardar los centros de datos y asegurar la continuidad operativa en proyectos críticos.

contacto@aermec.cl
https://global.aermec.com/es/data-centres/
Redhill Data Centre S140
Redhill (Gran Bretaña)
Centros de datos

