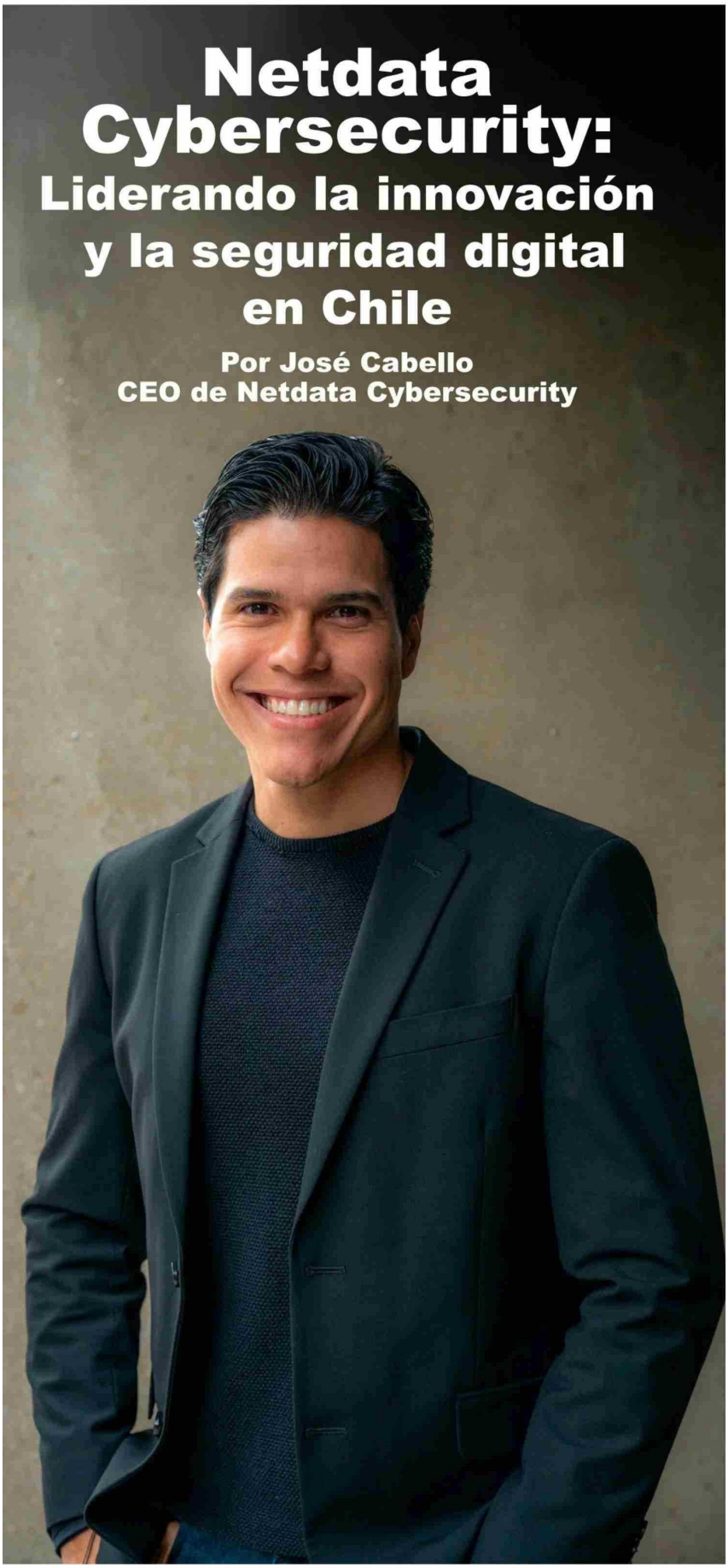
LITORALPRESS

Fecha: 06-01-2025
Medio: Revista TrendTIC
Supl. : Revista TrendTIC
Tipo: Noticia general
Título: **Netdata Cybersecurity: Liderando la innovación y la seguridad digital en Chile**

Pág. : 18
Cm2: 564,6
VPE: $ 0

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida



Desde nuestra llegada a Chile en 2021, en Netdata Cybersecurity nos hemos enfocado en algo fundamental: mostrar a las empresas de la región un enfoque diferente para abordar la ciberseguridad.

Con más de 15 años de experiencia en América Latina, sabemos que no solo es el tiempo lo que importa, sino las historias detrás de cada proyecto. Durante este tiempo en Chile hemos logrado varios hitos significativos: más de 90 implementaciones exitosas en 28 clientes de sectores como el bancario, el farmacéutico, el petrolero y el industrial, alcanzando un 95.3% de satisfacción.

También hemos aprendido que la confianza no se gana con promesas, sino con resultados. Y eso es lo que ofrecemos: resultados concretos, medibles y alineados con las necesidades de cada organización.

De cara a los desafíos que nos plantea el futuro, como la Ley Marco de Ciberseguridad en 2025 y la nueva Ley de Protección de Datos, nuestro rol es claro: ser un socio estratégico para ayudar a las compañías a cumplir con las nuevas regulaciones gubernamentales. Sabemos que la normativa es un camino necesario, pero también es un desafío si no se implementa correctamente. Por eso, no sólo operamos la tecnología, sino que trabajamos codo a codo con nuestros clientes para asegurar procesos robustos, auditorías efectivas y un cumplimiento que va más allá de lo exigido.

En Netdata siempre hemos tenido claro que la tecnología por sí sola no es suficiente. Son las personas quienes marcan la diferencia. Nuestro equipo no solo está altamente capacitado, sumando más de 1,400 certificaciones técnicas, también está comprometido con una misión: entregar soluciones que protejan y generen valor real. Invertimos en la formación continua de nuestro personal porque entendemos que, en un mundo tan cambiante, el conocimiento debe estar al servicio de nuestros clientes.

Como CEO de Netdata, siempre he creído que la ciberseguridad no es solo un desafío técnico: es un habilitador de crecimiento, confianza y transformación. No estamos aquí solo para responder a ataques; estamos para anticiparnos a ellos, construir relaciones de largo plazo y asegurar que nuestros clientes puedan crecer en un entorno protegido.

Con esto en mente, hemos desarrollado soluciones como Sentria, una plataforma impulsada por Inteligencia Artificial y Machine Learning que permite detectar amenazas

LITORALPRESS

Fecha: 06-01-2025
Medio: Revista TrendTIC
Supl. : Revista TrendTIC
Tipo: Noticia general
Título: Netdata Cybersecurity: Liderando la innovación y la seguridad digital en Chile

Pág. : 19
Cm2: 481,4
VPE: $ 0

Tiraje: Sin Datos
Lectoría: Sin Datos
Favorabilidad: No Definida

en menos de 20 minutos y responder en menos de 2 horas, lo cual no solo transforma los tiempos de respuesta, sino que también entrega algo invaluable: mayor tranquilidad para nuestros clientes.

Netdata Cybersecurity es más que un proveedor de soluciones. Somos un socio estratégico que entiende la realidad local, los desafíos globales y, sobre todo, el valor de la confianza. Nuestro compromiso es claro: proteger el presente para construir juntos un futuro digital más seguro para Chile.

Tendencias de Ciberseguridad para el 2025

El 2025 está a la vuelta de la esquina, y en un mundo hiperconectado, las amenazas cibernéticas no solo evolucionan, sino que lo hacen con una rapidez sin precedentes. Desde Netdata Cybersecurity, observamos que el panorama actual exige una mentalidad ágil, innovadora y predictiva para enfrentar los desafíos de la ciberseguridad en la región y el mundo.

Por esta razón, queremos compartir las principales tendencias que marcarán la pauta para el próximo año:

1. Inteligencia Artificial y Machine Learning

El uso de la IA generativa por parte de los ciberatacantes alcanzará niveles sin precedentes este 2025. Desde campañas de phishing hiperpersonalizadas hasta malware adaptativo que aprende y evade defensas, la IA empezará a jugar un papel protagónico en la creación de amenazas.

Sin embargo, aunque la IA pueda parecer un peligro, también será una gran ventaja para las organizaciones que la implementen dentro de su esquema de ciberseguridad. Soluciones como Cortex y servicios como Sentria han demostrado que la inteligencia artificial permite detectar patrones invisibles, identificar amenazas en tiempo real y automatizar respuestas. La clave estará en la adopción rápida y ética de esta tecnología por parte de las organizaciones.

2. Seguridad de Zero Trust

El modelo Zero Trust, basado en el principio de "no confiar en nada y verificarlo todo", se consolidará como el estándar definitivo en ciberseguridad durante los próximos años. De acuerdo con Mike Wilson, miembro del consejo de Forbes, se proyecta que el mercado de esta arquitectura crezca exponencialmente, pasando de 31.450 millones de dólares en 2024 a 95.220 millones para 2030, lo que refleja su adopción acelerada a nivel global.

No obstante, el reto más urgente es el manejo de identidades comprometidas, hoy en día el vector de ataque más común. Aquí es donde soluciones avanzadas como Identity Threat Detection and Response (ITDR) resultan imprescindibles por su capacidad de detectar anomalías basados en el comportamiento de usuarios y detener movimientos laterales antes de que escalen y comprometan la red.

El éxito en 2025 dependerá de una estrategia integrada que combine visibilidad completa, segmentación dinámica y control constante, asegurando que ningún acceso sea otorgado sin una validación rigurosa.

3. Seguridad en la Nube

La seguridad en la nube en 2025 enfrentará el reto de la adopción de ambientes multicloud cada vez más sofisticados. El aumento de APIs mal configuradas y el uso de inteligencia artificial para automatizar las brechas de la nube, hará que las empresas deban pasar de un enfoque centrado en la remediación y migrar a una estrategia más preventiva, en la que identifiquen y neutralicen las amenazas antes de que generen daños.

La velocidad y sofisticación de los ataques exigirá que las empresas construyan soluciones integrales de Cloud Security Posture Management (CSPM) junto con tecnologías predictivas que proporcionen visibilidad total y refuercen el control de las configuraciones. Además, el uso de plataformas unificadas permitirán una respuesta mucho más ágil y eficiente, optimizando recursos y reduciendo tiempos críticos en la detección y mitigación de incidentes.

4. Amenazas a la Cadena de Suministro

Históricamente, las empresas han buscado consolidar el número de proveedores y herramientas de seguridad. Sin embargo, tras el incidente de CrowdStrike en 2024, persiste una creciente desconfianza en depender de un único proveedor.

Ante este panorama, es previsible una transición hacia un Cybersecurity Mesh o arquitectura de malla, que permita a las organizaciones minimizar puntos únicos de fallo, equilibrar riesgos y centralizar sus operaciones en un solo lugar.

5. Brecha de talento

De aquí a 2025, la creciente escasez de profesionales en ciberseguridad impactará profundamente la capacidad de las organizaciones para defenderse frente a amenazas cada vez más complejas.

La dependencia de múltiples proveedores, sin contar con la experiencia interna necesaria, dejará a las empresas vulnerables, dificultando la gestión de sus plataformas y reduciendo su eficacia. Como resultado, las empresas estarán cada vez más expuestas a incidentes de seguridad, filtración de datos y pérdidas financieras significativas.

Es fundamental que las organizaciones no solo inviertan en talento especializado, sino también en herramientas y estrategias que les permitan simplificar el manejo de su arquitectura de seguridad.

6. Mayores exigencias normativas

Las empresas se enfrentarán a una creciente presión normativa cómo la Ley Marco de Ciberseguridad, la Ley de Protección de Datos, el Reglamentos de la Unión Europea sobre IoT, las Normas de Divulgación de Ciberseguridad de la SEC, la Ley de Resiliencia Operativa Digital (DORA) y la Directiva NIS2. Esto incrementará aún más la necesidad de que las compañías cuenten con estrategias integradas que faciliten el cumplimiento, mitiguen los riesgos y aseguren la continuidad operativa en un entorno cada vez más demandante.

Como podemos ver, en 2025 el panorama de la ciberseguridad pondrá nuevos retos sobre la mesa, haciendo que las empresas tengan que adoptar enfoques y estrategias más integrales, que les permitan garantizar la seguridad de sus operaciones mediante la implementación de soluciones proactivas para anticiparse a las amenazas y mantener la visibilidad de su infraestructura tecnológica en todo momento.

En Netdata Cybersecurity, impulsamos soluciones innovadoras para cubrir cada uno de los frentes mencionados y permitir a las organizaciones mantenerse protegidas frente a este entorno tan desafiante.