

• AMENAZAS • REGULACIÓN • RESPUESTA

Panorama de Ciberseguridad

Amenazas, regulación y respuesta en Chile durante el primer semestre de 2026.

La identidad fue el hilo del semestre

El primer semestre de 2026 confirmó que la ciberseguridad dejó de ser un asunto técnico para volverse una preocupación estratégica. El hilo que conectó al semestre fue la identidad: la mayoría de los incidentes no comenzó con un exploit sofisticado, sino con una credencial robada o un dispositivo de borde expuesto.

A nivel global, la inteligencia artificial se consolidó como el principal motor de cambio, potenciando por igual a atacantes y defensores, el ransomware operó como industria y el robo de credenciales se afianzó como el combustible del acceso inicial. Ese patrón aterrizó en las plataformas más masificadas: Fortinet concentró una secuencia de eventos, de la cadena de bypass de enero a la campaña "FortiBleed" de junio, que expuso credenciales de cerca de la mitad de los firewalls FortiGate alcanzables desde internet, no por debilidad del producto, sino porque su ubicuidad maximiza el retorno del atacante.

En el plano local, el país muestra una cara doble: el ransomware retrocedió de forma sostenida desde 2023, favorecido por el avance regulatorio, pero las filtraciones de datos siguen creciendo en la región y el fraude por mensajería (smishing) se instaló como la manifestación que sienten el ciudadano y el cliente. La respuesta regulatoria marca la agenda: la Ley 21.719 de protección de datos entra en plena vigencia el 1 de diciembre de 2026 y la Ley 21.663 de ciberseguridad ya fiscaliza.

El mensaje para el liderazgo es claro y constructivo: **la ventaja competitiva estará en las organizaciones que traten la ciberseguridad como una capacidad estratégica, gobernanza, identidad y preparación, antes de que el plazo regulatorio y la exposición técnica las alcancen.**

EL SEMESTRE EN CINCO CIFRAS

13%

organizaciones "muy preparadas" para la Ley 21.719 · PwC / FGE

+210%

aumento de data breach en LATAM 2025 vs 2024 · CCI Entel

~50%

FortiGate expuestos alcanzados por FortiBleed · CISA / NCSC

45%

uso de IA entre trabajadores, desde 15% en un año · DBIR 2026

73%

conoció a alguien afectado por fraude digital en 2025 · WEF

Las 10 conversaciones que definieron la agenda

Ordenadas por impacto para organizaciones chilenas (impacto empresarial + frecuencia + presencia en informes + importancia estratégica).

#	CONVERSACIÓN	PRIORIDAD
1	Protección de datos personales, Ley 21.719	● CRÍTICA
2	Explotación de dispositivos de borde, caso Fortinet	● ALTA
3	IA: oportunidad y gobernanza del dato (Shadow AI)	● ALTA
4	Identidad como perímetro, credenciales / infostealers	● ALTA
5	Filtraciones y recirculación de datos en Chile	● ALTA
6	Fraude digital y smishing	● ALTA
7	Ransomware como industria (RaaS, doble extorsión)	● MEDIA-ALTA
8	Infraestructura crítica, Ley 21.663 / ANCI	● ALTA
9	Resiliencia, gestión de terceros y ciberseguros	● MEDIA
10	Geopolítica y amenazas APT a infraestructura crítica	● MEDIA

Escala de prioridad (identidad de marca): ● Crítica ● Alta ● Media-alta ● Media

Aceleración, IA y fragmentación

El primer semestre de 2026 confirmó un cambio de naturaleza más que de volumen: la ciberseguridad dejó de ser un asunto técnico para consolidarse como preocupación estratégica y económica. El Global Cybersecurity Outlook 2026 del Foro Económico Mundial (WEF), con Accenture (enero 2026; 800+ líderes en 92 países), ordena el año en torno a tres fuerzas: la IA acelerando la carrera armamentista, la fragmentación geopolítica y una creciente "inequidad cibernética" entre organizaciones preparadas y rezagadas.

La IA es señalada como el principal motor de cambio por el 94% de los encuestados, y opera en ambos bandos: fortalece la defensa (detección, respuesta, automatización del SOC) y escala el ataque (ingeniería social, automatización de la explotación, menor barrera de entrada). El punto crítico es la brecha entre adopción y gobernanza. En amenazas concretas, el ransomware se industrializó, Fortinet reportó 7.831 víctimas confirmadas, +389% interanual, y el robo de credenciales vía infostealers (RedLine, Lumma, Vidar) se consolidó como el principal combustible del acceso inicial. El DBIR 2025 de Verizon registró un alza de 34% en la explotación de vulnerabilidades, ya responsable del 20% de las brechas.

Dos señales relevantes para el lector chileno. Primero, el fraude habilitado digitalmente pasó a ser la principal preocupación de los CEO, desplazando al ransomware, con phishing, vishing y smishing como métodos más comunes; el 73% declaró que alguien de su entorno fue víctima durante 2025. Segundo, la inequidad tiene rostro regional: en América Latina y el Caribe solo el 13% confía en la capacidad de su país para proteger infraestructura crítica, y el 69% de los CEO admite carecer de las competencias para cumplir sus metas de ciberseguridad.

Para las empresas, la resiliencia, la gobernanza y las competencias, no solo la tecnología, separan a quienes absorben un incidente de quienes lo sufren.

El caso Fortinet: cuando la ubicuidad se vuelve el blanco



Si las tendencias globales explican el "qué", Fortinet fue el "dónde" del semestre. La lectura correcta no es que el producto sea deficiente, sino económica: los atacantes buscan el mayor retorno por unidad de tiempo, y lo obtienen apuntando a plataformas masificadas en el perímetro de red. Fortinet, uno de los firewalls más desplegados del mundo y con fuerte presencia en la infraestructura chilena, concentró una secuencia de eventos que la industria siguió mes a mes.

En **enero**, Fortinet divulgó CVE-2026-24858 (CVSS 9.4), un bypass de autenticación en FortiCloud SSO explotado antes de un parche estable. En **mayo**, una falla en FortiClient EMS (CVE-2026-35616) distribuyó un infostealer disfrazado de actualización oficial. Y en **junio**, la campaña "FortiBleed" expuso credenciales de decenas de miles de firewalls FortiGate en 194 países, cerca de la mitad de los alcanzables desde internet, no por un zero-day nuevo, sino por reutilización de credenciales antiguas y cracking de hashes legados.

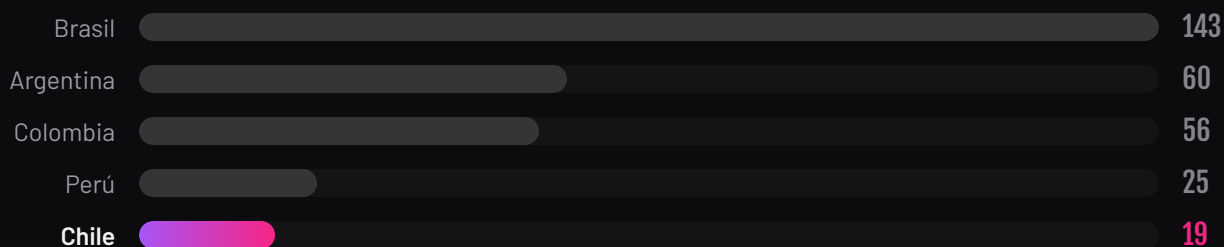
El patrón lo enmarca Verizon: el borde se explota el día de su divulgación mientras el parcheo tarda una mediana de 30 días, y no se puede instalar un EDR en un firewall. Para Chile la consecuencia es directa: por su alta penetración de FortiGate, la exposición es de base. La decisión no es cambiar de marca, sino de higiene operativa: sacar las interfaces de administración de internet, forzar MFA en administración y VPN, rotar credenciales y migrar hashes, y no confiar en "parchado = seguro".

Si el incidente compromete datos personales, puede activar, además, las obligaciones de notificación de la Ley 21.719.

Entre el avance y el riesgo latente

Bajando el foco al país, el semestre mostró un Chile que es, a la vez, un caso de avance y de riesgo latente. En ransomware el país es un outlier regional: el Reporte 2026 del Centro de Ciberinteligencia (CCI) de Entel Digital lo ubica quinto en Latinoamérica, con una disminución sostenida desde 2023 que atribuye a las nuevas leyes, la creación de agencias y una mayor conciencia institucional. Es una buena noticia con letra chica: el reporte advierte "cifras grises" por incidentes no divulgados, de modo que la caída medida probablemente subestima el riesgo real.

VÍCTIMAS DE RANSOMWARE · LATINOAMÉRICA 2025 (CCI ENTEL DIGITAL)



Chile: 5º lugar regional, con descenso sostenido desde 2023.

Ese piso no es estable, y el dato que lo confirma está en las filtraciones: en Latinoamérica los eventos de data breach crecieron un 210% en 2025 respecto de 2024, en parte por una mejor detección de la venta de accesos de los Initial Access Brokers. Los casos públicos del período comparten un patrón nítido: doble extorsión, explotación de servicios cloud y SaaS, en especial Microsoft 365, y accesos iniciales vía VPN o credenciales débiles. El episodio de mayo aporta el matiz más útil: la ANCI aclaró que el "hacking masivo" a organismos públicos no fue un ataque nuevo, sino recirculación de datos ya filtrados. La lección: el dato filtrado en el pasado sigue siendo munición para el fraude futuro.

Smishing: la cara ciudadana del dato filtrado

Corriente abajo de las filtraciones, el fraude por mensajería fue el fenómeno que el ciudadano y el cliente sintieron de forma directa. La PDI, a través de su Brigada del Cibercrimen, alertó en marzo por el aumento del smishing, SMS que suplantando a bancos, empresas e instituciones para inducir a la víctima a entregar claves y códigos mediante enlaces fraudulentos. El SERNAC reporta que durante eventos como CyberDay los reclamos por estafas digitales superan en más de 200% el promedio mensual.

El fenómeno se industrializó: investigaciones atribuyen buena parte de las campañas dirigidas a Chile a redes de "crimen como servicio" (como la Smishing Triad), que venden kits listos para operar, suplantando marcas nacionales de correo y retail para capturar datos de tarjetas.



CÓMO EL DATO FILTRADO SE CONVIERTE EN FRAUDE

Dato filtrado (nombre, RUT, tarjeta)



SMS que suplanta una marca



Enlace fraudulento



Captura de credencial

El punto que más interesa al directorio es la relación entre filtraciones y fraude. A nivel de mecanismo está documentada, el SERNAC y la ABIF describen que vishing y smishing se apoyan en datos reales obtenidos de filtraciones previas, pero atribuir una ola específica de fraude a una filtración puntual sigue siendo una hipótesis salvo evidencia concluyente. Para las organizaciones, el fraude es sobre todo un riesgo reputacional y de confianza en el canal digital: las decisiones pasan por concientización sostenida, autenticación resistente a la ingeniería social y protección de marca.

El doble frente regulatorio

Frente a este panorama, Chile responde elevando el estándar regulatorio, y ese fue el hilo que dominó la conversación ejecutiva del semestre. Dos leyes complementarias marcan el nuevo piso: una gobierna el dato, la otra la seguridad del sistema que lo contiene. Para el directorio, la clave es que son **dos leyes, dos agencias y dos relojes**: un incidente que exponga datos personales puede gatillar ambos reportes a la vez.

ASPECTO	Ley 21.719 • Datos personales	Ley 21.663 • Ciberseguridad
QUÉ PROTEGE	Los datos personales de las personas; actualiza la Ley N° 19.628.	La seguridad de los sistemas e infraestructura crítica del país.
AGENCIA	Agencia de Protección de Datos Personales (APDP).	Agencia Nacional de Ciberseguridad (ANCI) + CSIRT Nacional.
SUJETOS	Todo responsable de tratamiento de datos personales.	Servicios Esenciales y Operadores de Importancia Vital (OIV).
PLAZOS	Notificación de brechas dentro de 72 horas.	Alerta temprana en 3 h y reporte completo en 72 h.
MULTAS	Parten desde las 5.000 UTM y pueden llegar hasta las 20.000 UTM.	Hasta 40.000 UTM.
VIGENCIA	Plena vigencia el 1 dic 2026 (transición de 24 meses).	Ya vigente; 2026 es su primer año de fiscalización completa.

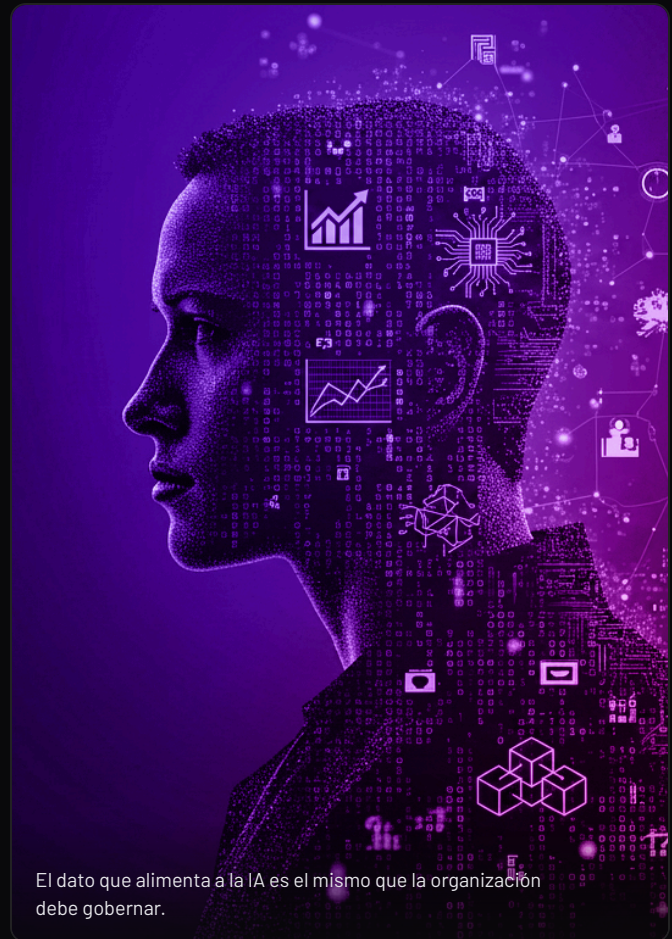
El dato de preparación es el más revelador: según PwC Chile y la Fundación Generación Empresarial, solo el 13% de las organizaciones se considera muy preparada y un 33% se reconoce poco preparada. La brecha no es de desconocimiento, sino de subestimación del esfuerzo. La decisión es tratar el cumplimiento como un proyecto transversal, legal, TI, compliance y RRHH, y documentar el avance, porque la buena fe temprana opera como atenuante.

La oportunidad y el dilema de gobernanza del dato

Cerrando el arco del dato, la IA fue la conversación que más rápido escaló en el semestre, y no principalmente como amenaza técnica, sino como dilema de gobernanza. El WEF la identificó como el principal motor de cambio para el 94% de los líderes, y en las salas de directorio el temor concreto no fue el ataque, sino la fuga: los CEO señalaron la exposición de datos propios como su principal riesgo asociado a la IA generativa.

Según el DBIR 2026 de Verizon, el uso de IA entre trabajadores saltó de 15% a 45% en un solo año, y el "Shadow AI" se convirtió en la tercera acción interna no maliciosa más común en los registros de fuga de datos, con dos tercios de los usuarios accediendo mediante cuentas no corporativas.

Lo que más sale por esa puerta es código fuente, seguido de documentación técnica y datos de negocio. El problema de fondo es de visibilidad: los controles tradicionales no fueron diseñados para inspeccionar un texto pegado en el navegador.



El dato que alimenta a la IA es el mismo que la organización debe gobernar.

EL TRILEMA QUE ENFRENTA TODO COMITÉ EJECUTIVO

Bloquear

Elimina el riesgo en el papel, pero empuja al uso clandestino: riesgo sin control ni trazabilidad. El peor mundo.

Habilitar con restricciones

Herramientas corporativas, clasificación del dato, DLP y registro de uso. Equilibra valor y control.

Habilitar con criterio

Suma la formación del juicio del usuario. Más de la mitad no ha recibido ninguna capacitación de riesgos.

El dilema era claro: "bloquear la IA y arriesgarme a quedar fuera de una de las revoluciones más importantes de la década, o usarla con responsabilidad y mirada corporativa". La idea es fomentar el uso responsable bajo un criterio corporativo, no dejarlo librado al criterio individual de cada colaborador.

De la defensa perimetral a la resiliencia

El semestre no solo trajo amenazas; consolidó una respuesta. La conversación corporativa se desplazó de "cómo evito el ataque" a "cómo sigo operando cuando ocurra", y ese giro hacia la resiliencia, anticipar, resistir, responder y recuperar, es el marco que ordena las decisiones dispersas en los bloques anteriores.



Identidad como perímetro

Zero Trust pasó de aspiración a estándar: MFA, gestión de identidades y segmentación como base.



Riesgo de terceros

La seguridad de una organización es tan fuerte como la de su proveedor más débil: auditorías y estándares mínimos.



Capacidades gestionadas

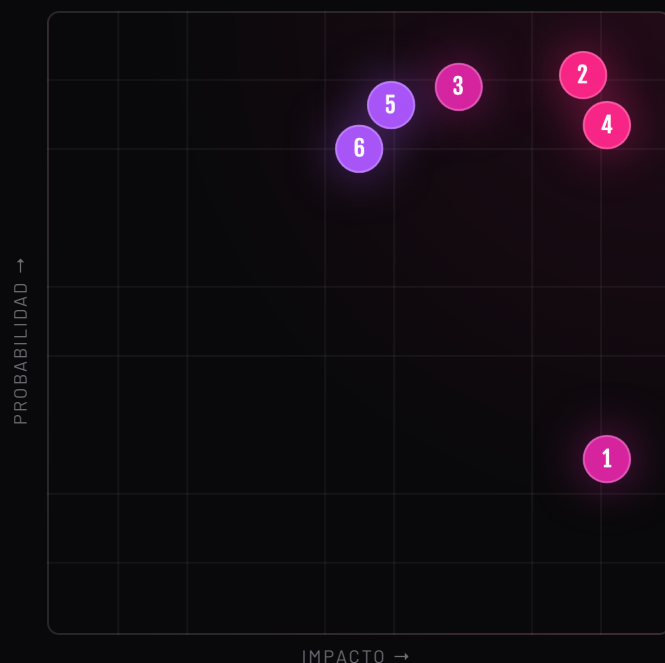
MDR/SOC 24/7 cubren el punto ciego; las aseguradoras condicionan pólizas a seguridad gestionada.

La evidencia local acompaña la tendencia. Deloitte, que sitúa a Chile como el cuarto país más atacado del continente, reporta que el 57% de las compañías aumentará su presupuesto de ciberseguridad, aunque solo la mitad de los altos ejecutivos confía en la capacidad actual de su organización. Ese desajuste entre inversión y confianza es el dato más honesto del semestre: se está gastando más, pero la madurez todavía no alcanza, y las organizaciones con mayor madurez obtienen **2,4 veces más resultados positivos**.

La ciberseguridad dejó de ser un gasto técnico para volverse una capacidad estratégica del negocio, medible, transversal y cada vez más exigida por reguladores, aseguradoras y clientes como condición para operar y competir.

Hacia el segundo semestre: Chile y Sudamérica

MATRIZ DE RIESGO · PROBABILIDAD × IMPACTO



- 1 APT en infraestructura crítica (OT/ICS)
- 2 Incumplimiento Ley 21.719
- 3 Fuga de datos a IA no gobernada (Shadow AI)
- 4 Exposición del parque de borde (FortiGate)
- 5 Filtraciones / Initial Access Brokers (+210%)
- 6 Fraude digital y smishing

CHILE

Tres riesgos ganan tracción: el **preposicionamiento silencioso de actores estatales** (Volt/Salt Typhoon, Sandworm, Lazarus) en infraestructura crítica, baja probabilidad, alto impacto sobre OT/ICS; el **incumplimiento regulatorio** de la Ley 21.719 con solo 13% de organizaciones preparadas; y la **fuga de datos hacia la IA no gobernada** (Shadow AI), sobre una exposición estructural del parque de dispositivos de borde.

SUDAMÉRICA

El riesgo se concentra y profesionaliza. Brasil, Argentina y Colombia absorben el grueso del ransomware, pero la economía de accesos iniciales distribuye el riesgo por toda la cadena de suministro (+210% de filtraciones). Lo agravan la brecha de talento (69%) y la baja confianza en proteger infraestructura crítica (13%), mientras la IA ofensiva y los deepfakes de voz y video bajan la barrera del fraude dirigido.

● CONCLUSIONES ESTRATÉGICAS

Seis decisiones que toda organización debe adoptar

La ciberseguridad se consolidó como una capacidad estratégica del negocio, medible y exigible. Para el liderazgo, seis decisiones concentran el mayor retorno.

1 Identidad como nuevo perímetro

MFA en toda cuenta crítica, gestión de identidades y hoja de ruta hacia Zero Trust.

3 Endurecer la higiene de credenciales y el borde

Asumir explotación el mismo día de la divulgación; sacar administración de internet.

5 Invertir en resiliencia operacional

Gestión de terceros y evaluación de la superficie de ataque; ciberseguros con controles reales.

2 Cerrar la brecha regulatoria antes de diciembre

Inventario de datos, DPO, contratos con encargados y notificación de brechas en 72 h.

4 Postura explícita frente a la IA

Habilitarla con criterio y control para que el Shadow AI no decida por omisión.

6 Sostener la concientización

El factor humano sigue siendo el vector y la primera defensa.

La evidencia es clara: las organizaciones con mayor madurez obtienen **2,4 veces más resultados positivos**. La ventaja competitiva será de quienes actúen antes de que el plazo regulatorio y la exposición técnica las alcancen.

BIBLIOGRAFÍA

Internacional: WEF, Global Cybersecurity Outlook 2026 (con Accenture); Verizon, DBIR 2025 y 2026; Fortinet / FortiGuard Labs, Global Threat Landscape 2026; Gartner; Deloitte, The Future of Cyber / Cyber Icon Chile; Zscaler ThreatLabz; Palo Alto Networks; National Cybersecurity Alliance; Microsoft Purview; NIST AI RMF. · Vulnerabilidades / borde: CISA, CVE-2026-24858 y FortiBleed; NCSC (UK); Cloud Security Alliance; Bitsight; Qualys; SOCRadar; Recorded Future; Arctic Wolf; Team Cymru; Amazon Threat Intelligence. · Chile: BCN, Ley 21.719 y 21.663; Secretaría de Gobierno Digital; ANCI, DS 295/2024 e instrucciones 2026; PwC Chile + Fundación Generación Empresarial; CCI Entel Digital, Reporte 2026; IAPP; SERNAC; ABIF; PDI, Brigada del Cibercrimen; Garrigues.

● DE LA EVALUACIÓN A LA IMPLEMENTACIÓN

La ciberseguridad es hoy una capacidad estratégica del negocio

El primer semestre de 2026 dejó una conclusión transversal: la ciberseguridad ya no es un gasto técnico, sino una capacidad estratégica del negocio. Identidad, gobernanza del dato y preparación regulatoria son los ejes que separan a las organizaciones resilientes de las expuestas. En vCISO acompañamos ese camino, de la evaluación a la implementación.

SERVICIOS VCISO

- **Diagnóstico e Implementación Ley 21.719**
Servicio principal · Protección de Datos Personales
- **Ethical Hacking**
Pruebas ofensivas controladas
- **Desarrollo Seguro de Aplicaciones**
Seguridad en el ciclo de vida
- **Seguridad Endpoint & Perimetral**
Protección del borde y estaciones
- **Detección de Brechas en la Superficie de Ataque**
Reconocimiento y exposición externa



CONVERSEMOS

WEB

vciso.cloud

CORREO

consultor@vciso.cloud

TELÉFONO

+56 9 9308 7797

LINKEDIN

[/company/vciso-cloud](https://company/vciso-cloud)