BRANDEFENSE COUNTRY REPORT · CHILE 2026

Brandefense Informe del panorama de ciberamenazas de Chile 2026

Identidad, afirmaciones de extorsión y continuidad de servicios esenciales

Odin by Brandefense
Periodo de investigación: 1 de enero–22 de noviembre de 2026
Versión 1.0 · Edición pública de investigación · TLP:CLEAR · 8–22 de noviembre de 2026

98 de 250
organizaciones seleccionadas tenían una credencial anunciada a la venta al comprobarse

6
expedientes detallados de afirmaciones, no seis intrusiones confirmadas

41
publicaciones chilenas de ransomware en el periodo de observación

25
dominios seleccionados de banca, pagos e inversión, no un censo bancario

CONTENIDO

Contenido

Translated with AI

Esta edición se ha traducido con IA a partir del texto original en inglés. En caso de diferencia, prevalece la edición en inglés.

01	Resumen ejecutivo	05
	Mapa del informe	09
02	Contexto digital y de seguridad de Chile	10
03	Exposición nacional: una cartera de dominios seleccionados	15
04	Evidencia clandestina e interpretación de afirmaciones	23
05	Incidentes, afirmaciones y decisiones de respuesta por sector	38
06	Hacktivismo, DDoS y disponibilidad de servicios	54
07	Actores de amenazas y relaciones respaldadas	58
08	La economía del fraude	68
09	Banca y servicios financieros	73
10	Regulación y respuesta nacional	78
11	Perspectivas y planificación condicional	85
12	Plan de acción	89
A	Anexo A. Alcance y límites de evidencia	97
B	Anexo B. Registro de evidencia	100
C	Anexo C. Fuentes	102
D	Anexo D. Glosario	106
	Acerca de este informe	108

Directorio y ejecutivos	01 05 11 12
CISO y delegado	03 04 05 10 12
Inteligencia y SOC	04 06 07 B
Fraude y atención al cliente	05 08 09
Asesoría jurídica y privacidad	05 10 A

Sobre esta edición

Traducido con IA. La edición en inglés prevalece en caso de discrepancia.

Elaborado con asistencia de IA. Las evidencias y sus límites acompañan a los hallazgos.

Las señales de Chile muestran abuso de cuentas, afirmaciones sobre datos, engaño financiero y servicios interrumpidos; valide la exposición específica y preserve la función esencial.

27,891

observaciones de volumen de publicaciones asociadas a Chile; no es un recuento de incidentes

400

observaciones de volumen de publicaciones del 8–22 de noviembre; no son nuevas intrusiones

41

filas de publicaciones de ransomware sobre Chile; afirmaciones delictivas

250

dominios de organizaciones seleccionados; no es un censo nacional

Las poblaciones de volumen de publicaciones, entradas de ransomware y dominios seleccionados son distintas. Sus recuentos no deben sumarse. La evidencia narrativa se limita al material conservado y los relatos de fuentes descritos en cada capítulo. [S1][S2][S5]

Contenido y rutas de lectura

Capítulo	Pregunta para decidir	Primer lector
1 Resumen ejecutivo	¿Qué decisiones necesitan un responsable de inmediato?	Dirección y CISO
2 Contexto	¿Qué condiciones nacionales cambian la respuesta?	CISO y equipo jurídico
3 Exposición de dominios seleccionados	¿Qué mediciones están disponibles y qué sigue sin conocerse?	Seguridad e infraestructura
4 Evidencia de mercados clandestinos	¿Qué permiten establecer realmente los anuncios?	Inteligencia y respuesta
5 Casos por sector	¿Qué consecuencias requieren distintos responsables?	Equipos de servicios, privacidad y fraude
6 DDoS y disponibilidad	¿Qué distingue una interrupción de un acceso establecido?	Operaciones y comunicaciones
7 Actores y relaciones	¿Qué fuente respalda cada proposición sobre actores?	Inteligencia y dirección
8 Economía del fraude	¿Cómo deben los equipos interrumpir un engaño creíble?	Fraude, tesorería y atención
9 Servicios financieros	¿Qué preguntas institucionales y de clientes deben mantenerse separadas?	Seguridad financiera y cumplimiento
10 Regulación	¿Qué obligación, condición y plazo de notificación corresponden?	Equipo jurídico y delegado
11 Perspectivas	¿Qué señales deben cambiar el plan?	Dirección y riesgos
12 Plan de acción	¿Quién ejecuta y qué demuestra su cumplimiento?	Responsables designados
Anexos A–D	¿Cuáles son los límites de la evidencia, las fichas, las fuentes y los términos?	Todos los lectores

La dirección puede comenzar por los capítulos 1, 5, 11 y 12. Los equipos de respuesta pueden seguir los capítulos 3, 4, 6 y 7. Fraude, asesoría jurídica y atención al cliente pueden usar los capítulos 8–10 junto al caso sectorial correspondiente.

Las etiquetas de evidencia son **observación**, **afirmación**, **versión oficial reportada** e **inferencia del analista**. Un anuncio observado sigue siendo una afirmación sobre su contenido. Una limitación de servicio confirmada puede dejar sin resolver el acceso a datos, la identidad del actor y la vía de entrada.

CAPÍTULO 01

Resumen ejecutivo

01

ESTE CAPÍTULO RESPONDE

¿Qué justifica hacer primero la evidencia de Chile y cómo debe la dirección verificar la respuesta?

4

decisiones de dirección con responsables designados

Cuatro decisiones para la dirección 07

El año en cifras 07

CAPÍTULO 01

Resumen ejecutivo

EN RESUMEN

La evidencia de Chile respalda validar identidades, recuperar servicios esenciales, proteger clientes y preparar notificaciones. Las publicaciones delictivas anuncian archivos de proveedores, accesos privilegiados, registros educativos e información de salud. No confirman intrusiones. Las versiones oficiales y organizacionales reportadas distinguen acceso con cuentas válidas, republicación histórica, posible extracción e interrupciones. Asigne un responsable a cada señal pertinente, verifique la cuenta o función afectada y ensaye la decisión de notificar antes de que comience el breve plazo legal.

Este informe combina material clandestino y entradas de ransomware conservados por Brandefense con observaciones pasivas de dominios y fuentes públicas. Mantiene separadas las poblaciones, fechas y limitaciones de confianza. Ninguna publicación, entrada, dominio seleccionado o aviso público se convierte automáticamente en un incidente nacional único. [S1][S2][S3][S5]

El periodo de incidentes es del 1 de enero–22 de noviembre de 2026. La quincena final, del 8–22 de noviembre, se destaca por separado. La fecha de publicación no establece la fecha de intrusión. Parte del material recién divulgado es histórico; una actualización puede referirse a una interrupción iniciada meses antes.

1. La evidencia de cuentas exige una respuesta más acotada que un titular sobre filtraciones. La actualización de mayo de ANCI identificó acceso no autorizado con credenciales válidas y lo distinguió de ataques a la infraestructura. Su posterior aviso sobre datos históricos atribuyó otra alerta a material antiguo. Valide finalidad, vigencia, permisos y actividad actual de la cuenta antes de decidir el alcance de la contención. [S7][S8]

2. Los anuncios de proveedores e instituciones siguen siendo afirmaciones sobre accesos y archivos. Seis expedientes clandestinos detallados abarcan archivos cargados a un proveedor, material de consultoría, un portal administrativo vinculado a un banco, datos educativos, datos escolares históricos y registros de salud. El texto establece ofertas y afirmaciones. No establece las cantidades anunciadas, ventas realizadas ni un incidente separado en cada cliente mencionado. [S1]

3. La extorsión visible se concentra, pero la preparación debe abarcar más de dos etiquetas. Ransompedia registra 41 filas de publicaciones sobre Chile, distribuidas entre 13 etiquetas. Qilin y The Gentlemen reúnen 26, o el 63.4%. Las 15 restantes llevan otras etiquetas. Las entradas justifican preparar recuperación y divulgación, pero no cuentan cifrados o robos confirmados. [S2]

4. Las consecuencias operacionales difieren incluso dentro de los servicios esenciales. Las noticias hospitalarias distinguen la interrupción de reservas de horas de la atención clínica mantenida. Los registros eléctricos describen la indisponibilidad continuada de una instalación generadora. Una actualización posterior de un comercio agrega interrupciones logísticas y de canales de venta. La recuperación necesita la aceptación del responsable del servicio, no solo una declaración general sobre sistemas restablecidos. [S34][S53][S86][S52]

5. Las obligaciones vigentes de notificación y los cambios propuestos requieren tratamientos distintos. El máximo aplicable para la alerta temprana de la Ley 21.663 es de tres horas. El documento de ANCI sobre MFA de noviembre sigue en consulta. La aprobación parlamentaria de una postergación de la ley de datos no establece su promulgación y publicación. Conserve el instrumento jurídico, la entidad aplicable y el momento de conocimiento que respaldan cada decisión. [S13][S15][S31][S50]

Cuatro decisiones para la dirección

1. **Asegure que la evidencia pertinente llegue a un responsable.** Pruebe la entrega y el escalamiento de alertas. Luego valide las señales actuales de identidad y servicios con evidencia de la propia organización. Registre conclusiones como actuales, históricas, ajenas o sin resolver.
1. **Demuestre el servicio mínimo y una recuperación segura.** Pida al responsable de negocio que complete la tarea esencial durante la degradación. Restaure los registros y concilie el trabajo interrumpido antes de aceptar que el servicio se recuperó.
1. **Coordine la respuesta de proveedores, clientes y fraude.** Obtenga una versión acotada del proveedor y facilite una vía independiente para verificar contactos sospechosos. No cierre la protección al cliente solo porque el servicio técnico se haya restablecido.
1. **Ensaye la decisión de notificación aplicable.** Confirme el alcance legal, la condición de OIV, los contactos y la cronología de conocimiento. Pruebe un evento fuera de horario con asesoría jurídica, el delegado de ciberseguridad y el responsable operacional correspondiente.

El año en cifras

27,891

Observaciones de volumen de publicaciones asociadas a Chile en el periodo solicitado

QUÉ NO MIDE

Ataques confirmados o víctimas únicas

400

Observaciones recientes de volumen de publicaciones del 8–22 de noviembre

QUÉ NO MIDE

Intrusiones iniciadas en esa quincena

41

Filas de publicaciones chilenas de ransomware

QUÉ NO MIDE

Intrusiones confirmadas de manera independiente

39

Cadenas distintas de nombres de organizaciones en esas filas

QUÉ NO MIDE

Organizaciones jurídicas independientes validadas

19 / 7 / 15

Filas de Qilin / The Gentlemen / otras etiquetas

QUÉ NO MIDE

Operadores, rescates pagados o pérdidas totales

250

Dominios de organizaciones seleccionados en diez grupos sectoriales

QUÉ NO MIDE

Prevalencia nacional o una clasificación por ingresos

98 / 250

Organizaciones seleccionadas con una credencial anunciada a la venta al comprobarse

QUÉ NO MIDE

Intrusiones confirmadas o ventas completadas

58/100 (B)

Cifra principal nacional de Atlas para la cartera seleccionada

QUÉ NO MIDE

Porcentaje de brechas o calificación sectorial

324

Reportes de incidentes significativos recibidos por ANCI en enero–junio

QUÉ NO MIDE

Un recuento hasta noviembre o de organizaciones afectadas únicas

Fuentes: observaciones conservadas, agregados de publicaciones e instantánea de exposición de Brandefense [S1][S2][S5][S210], y reportes del primer semestre de ANCI [S9][S10].

De 250 organizaciones seleccionadas, 98 tenían una credencial anunciada a la venta al comprobarse. La cifra principal nacional de Atlas es 58/100 (B). 795,641 asociaciones de dispositivos y 2,999,478 asociaciones de registros de credenciales requieren validaciones separadas de cuentas y dispositivos. Estas observaciones superpuestas no establecen prevalencia nacional ni intrusiones confirmadas. [S210]

La evidencia de la quincena final merece atención sin exagerar su novedad. Una oferta de datos escolares abarca expresamente años anteriores. Otra afirmación sobre educación y fotografías, y una sobre datos electorales, tienen procedencia sin resolver. Esta última no establece una intrusión actual en sistemas electorales ni efectos sobre elección alguna. [S1]

Si está gestionando un evento actual, comience por el caso que corresponda a la evidencia, no solo por el nombre del sector. Un mismo sector puede enfrentar uso indebido de cuentas, servicios indisponibles, información custodiada por proveedores y suplantación. Cada situación exige una validación y una prueba de cierre distintas.

CONCLUSIONES CLAVE

01

Valide la proposición específica sobre identidad, datos o servicios detrás de una afirmación.

02

Mantenga separadas las publicaciones, las entradas de ransomware, los casos públicos y las observaciones de dominios seleccionados.

03

Exija decisiones con responsables y capacidad demostrada para servicios, clientes y notificaciones.

Mapa del informe

Comience por la decisión que le corresponde y siga la evidencia, su límite y la prueba de cumplimiento.

Directorio y ejecutivos	¿Puede la organización proteger su función esencial y decidir a tiempo?	01 05 11 12
CISO y delegado	¿Qué observaciones justifican validar o contener?	03 04 05 10 12
Inteligencia y SOC	¿Qué declaraciones son observadas, afirmadas o corroboradas?	04 06 07 B
Fraude y atención al cliente	¿Cómo puede usarse información creíble para inducir una acción perjudicial?	05 08 09
Asesoría jurídica y privacidad	¿Qué entidad, fuente, fecha y condición respaldan la decisión?	05 10 A

Línea de evidencia	Qué respalda	Qué no establece
Texto clandestino conservado	Existe una oferta, afirmación de publicación o solicitud	Posesión, actualidad, venta o impacto
Publicación delictiva	Existe una publicación de quien hace la afirmación	Cifrado, robo o una organización única
Versión pública	El evento y la posición reportados por la fuente citada	Detalles técnicos o de atribución no expresados
Observación pasiva	Un resultado de configuración fechado para un dominio evaluado	Seguridad de aplicaciones o eficacia nacional de controles
Inferencia del analista	Una interpretación acotada con alternativas	Una relación verificada o probabilidad de ataque futuro

CAPÍTULO 02

Contexto digital y de seguridad de Chile

02

ESTE CAPÍTULO RESPONDE

¿Qué condiciones nacionales cambian las decisiones que debe tomar un defensor en Chile?

324

reportes de incidentes significativos recibidos por ANCI en el primer semestre

2.1 La conectividad amplía la relevancia de las decisiones sobre identidad y servicios 11

2.2 Los reportes nacionales describen otra población 11

2.3 Las cuentas válidas cambian la pregunta de contención 12

2.4 Los servicios esenciales crean una obligación operacional 12

2.5 El fraude financiero cruza los límites institucionales 13

2.6 La atribución y las fechas de publicación necesitan evidencia separada 13

2.7 Las fechas regulatorias requieren verificar su estado actual 13

CAPÍTULO 02

Contexto digital y de seguridad de Chile

EN RESUMEN

La evidencia pública de Chile reúne seguridad de identidad, continuidad de servicios esenciales y fraude financiero en un mismo panorama operacional. Los reportes de ANCI, las divulgaciones públicas y los anuncios delictivos describen poblaciones diferentes. No pueden sumarse como un total nacional de ataques. La designación regulatoria crea obligaciones sin implicar que una organización sufrió un incidente. Identifique las cuentas, servicios, proveedores y obligaciones de notificación de su organización y pruebe su respuesta conjunta.

2.1 La conectividad amplía la relevancia de las decisiones sobre identidad y servicios

La edición Digital 2027 Chile de DataReportal se publicó el 5 de noviembre de 2026. Su observación de octubre de 2026 estima 19.1 millones de usuarios de internet y una penetración poblacional del 95.6%. El título de la edición no convierte esas cifras en una previsión para 2027. [S85]

Estas estimaciones describen conectividad, sin medir prevalencia de ciberataques ni eficacia de controles. Respaldan la atención a servicios accesibles para clientes, ciudadanía y trabajadores. No aportan un denominador para las publicaciones delictivas ni los incidentes organizacionales de este informe.

2.2 Los reportes nacionales describen otra población

ANCI informó 324 reportes de incidentes significativos en enero–junio de 2026. Su evaluación de amenazas de octubre y su anuncio del Mes de la Ciberseguridad presentan la misma cifra semestral. No es un recuento hasta noviembre ni un total de organizaciones afectadas únicas. [S9][S10]

Una noticia posterior cita una respuesta de transparencia de ANCI que registra 566 reportes de incidentes de efecto significativo del 1 de enero al 15 de octubre. Es otro periodo y una respuesta oficial reportada, sin abarcar hasta la fecha de corte de este informe. [S71]

La misma noticia señala que la notificación comenzó en marzo de 2025 y que su adopción puede influir en las comparaciones. No respalda interpretar el cambio como un aumento equivalente de los ataques subyacentes. Conserve el universo de reportes y el periodo al presentar la cifra. [S71]

Las siguientes poblaciones respaldan decisiones distintas.

Población	Unidad	Uso adecuado	Límite
Reportes a ANCI	Reportes de incidentes significativos en un periodo definido	Comprender la carga de casos reportada por la autoridad	No es un censo nacional completo de incidentes
Divulgaciones públicas	Declaraciones e incidentes reportados	Comparar decisiones de respuesta y consecuencias respaldadas	Las fechas de publicación e intrusión pueden diferir
Publicaciones clandestinas	Mensajes, ofertas y afirmaciones	Validar indicios pertinentes para activos propios	No verifican posesión ni acceso logrado
Entradas de ransomware	Publicaciones delictivas	Preparar la respuesta a extorsión y continuidad	No confirman robo ni cifrado
Dominios seleccionados	Observaciones asociadas a organizaciones	Investigar señales específicas de exposición	No representan prevalencia nacional ni entidades jurídicas independientes

2.3 Las cuentas válidas cambian la pregunta de contención

Las declaraciones de mayo de ANCI muestran por qué el acceso con credenciales exige una evaluación específica. Su aviso inicial describió una investigación de publicaciones de datos reportadas. Una actualización identificó accesos no autorizados con credenciales válidas, probablemente obtenidas de filtraciones anteriores o malware de robo de información. [S6][S7]

La agencia distinguió esos hallazgos de un ataque a la infraestructura subyacente. No respaldó una afirmación general de acceso al Estado como un solo entorno. Por ello, la respuesta debe comenzar por la identidad afectada y el servicio al que podía acceder. [S7]

Ante una alerta de cuenta, la titularidad, vigencia y permisos preceden a una conclusión sobre la red más amplia. Una contraseña encontrada en material histórico exige una respuesta distinta de la evidencia de uso de una cuenta privilegiada actual. Una etiqueta única como filtración de datos oculta esa diferencia.

2.4 Los servicios esenciales crean una obligación operacional

El aviso de designación de julio de ANCI informó un total combinado de 1,154 operadores de importancia vital, u OIV, en el primer proceso. Describe responsabilidades reforzadas: delegado de ciberseguridad, capacitación, gestión de seguridad y planificación de continuidad. La designación es una condición regulatoria, sin constituir evidencia de incidente. [S11]

La unidad práctica es la entidad jurídica designada y sus servicios pertinentes. Un grupo empresarial no debe asumir que la condición de una entidad se aplica igual a todas sus filiales. Tampoco debe inferirla de la etiqueta sectorial o de la lista de dominios seleccionados de este informe.

El delegado de ciberseguridad necesita acceso a quienes pueden tomar decisiones operacionales. Un equipo técnico puede evaluar una cuenta afectada. El responsable del servicio debe juzgar la función mínima aceptable y las consecuencias de restringir el acceso. Los equipos jurídicos y de cumplimiento determinan qué obligaciones de notificación corresponden.

2.5 El fraude financiero cruza los límites institucionales

En agosto, Fiscalía describió una mesa nacional de coordinación con el Ministerio Público y nueve organismos financieros públicos y privados. El aviso identifica fraude por correo empresarial, phishing, malware, fraude de pagos, estafas de inversión y falsas ofertas laborales entre las variantes pertinentes. [S29]

La advertencia de ANCI sobre cuentas bancarias de septiembre ilustra el problema. Describe a estafadores que provocan un bloqueo y después suplantan al banco para pedir un código o autorización. La aparente coincidencia entre el problema de cuenta y la llamada posterior forma parte del engaño. [S21]

2.6 La atribución y las fechas de publicación necesitan evidencia separada

Noticias de telecomunicaciones de agosto describieron una investigación con información de autoridades estadounidenses y actividad observada desde 2024. La fecha de publicación no establece que la actividad comenzó en 2026. Las descripciones de actores y vínculos estatales siguen siendo evaluaciones de las fuentes citadas. [S45]

El caso de servicio público de noviembre contiene versiones contrapuestas del mecanismo técnico. La evidencia no respalda resolver esa discrepancia mediante especulaciones sobre un operador. Mantenga separados el impacto de servicio, el acceso, la cronología y la atribución. [S36]

2.7 Las fechas regulatorias requieren verificar su estado actual

Dos novedades requieren tratamientos distintos. CMF dice que su norma de autenticación reforzada entró plenamente en vigor el 1 de agosto de 2026. El documento de ANCI sobre MFA de noviembre seguía en consulta pública al corte. Un proyecto de estándar no es una obligación ya vigente. [S27][S15][S16]

El calendario de datos personales también requiere cuidado. La ley original fijaba su entrada en vigor para el 1 de diciembre de 2026. Un aviso parlamentario del 20 de noviembre dice que el proyecto de postergación pasó a promulgación. La aprobación legislativa no establece una nueva fecha promulgada y publicada. [S30][S31][S32]

CONCLUSIONES CLAVE

01

Conserve el periodo y la unidad al comparar reportes nacionales con publicaciones delictivas.

02

Asigne identidades y servicios esenciales a responsables operacionales y jurídicos.

03

Trate la atribución política y la entrada en vigor legal como preguntas de cada fuente que necesitan evidencia propia.

CAPÍTULO 03

Exposición nacional: una cartera de dominios seleccionados

ESTE CAPÍTULO RESPONDE

¿Qué observaciones de exposición requieren validación en la cartera seleccionada?

98 de 250

organizaciones seleccionadas tenían una credencial anunciada a la venta al comprobarse

3.1 Ficha del universo 16
3.2 Anuncios vigentes y cifra principal nacional 17
3.3 Dispositivos y credenciales requieren contexto 18
3.4 Resultados pasivos y sus límites 21
3.5 Titularidad y evidencia de cumplimiento 22

CAPÍTULO 03

Exposición nacional: una cartera de dominios seleccionados

EN RESUMEN

De 250 organizaciones seleccionadas, 98 tenían una credencial anunciada a la venta al comprobarse. La cifra principal nacional de Atlas es 58/100 (B). La cartera contiene 795,641 asociaciones de dispositivos y 2,999,478 asociaciones de registros de credenciales. Pueden superponerse y no establecen validez actual de cuentas ni prevalencia nacional. Valide los anuncios vigentes, determine el contexto de trabajadores o clientes y asigne responsables de identidad, dispositivos o fraude.

3.1 Ficha del universo

Elemento	Definición
Población seleccionada	250 registros de dominios principales en diez grupos sectoriales fusionados
Selección sectorial	25 registros por grupo, según relevancia institucional y de servicios
Unidad	Asociación seleccionada entre organización y dominio; un dominio por sí solo no establece identidad jurídica independiente ni titularidad
Población con resolución	225 dominios seleccionados en la observación pasiva fechada
Población sin resolución	25 dominios seleccionados; la falta de resolución no es un veredicto de seguridad
Fecha de exposición	22 de noviembre de 2026; dispositivos, credenciales, documentos y anuncios describen los registros disponibles en esa fecha, no solo eventos iniciados en 2026
Mediciones pasivas	Observaciones fechadas de DNS, políticas de correo y HTTPS con sus denominadores evaluados
Mediciones de exposición	Observaciones de dispositivos, dispositivos de trabajadores, registros de credenciales, documentos y anuncios vigentes de credenciales
Calificación nacional	Cifra principal de Atlas para la cartera seleccionada: 58/100 (B)

La muestra describe servicios seleccionados, sin medir prevalencia nacional. Empresas relacionadas pueden compartir control y una organización puede operar varios dominios. Valide la asociación antes de atribuir un hallazgo a una entidad jurídica. [S5]

La instantánea de exposición y el periodo de incidentes tienen bases temporales distintas. Credenciales históricas y anuncios repetidos pueden seguir visibles tras la corrección. La fecha de observación no establece cuándo ocurrió la actividad subyacente. [S210]

3.2 Anuncios vigentes y cifra principal nacional

En la cartera seleccionada, 98 de 250 organizaciones tenían una credencial anunciada a la venta al comprobarse. Las asociaciones de registros de credenciales abarcan 238 dominios seleccionados; las de dispositivos, 238; y las de dispositivos de trabajadores, 200. Estas poblaciones pueden superponerse. [S210]

La cifra principal nacional de Atlas es 58/100 (B). Los valores mayores indican mayor exposición observada en esta cartera seleccionada. La calificación no es un porcentaje de brechas, una probabilidad de intrusión ni una certificación de eficacia de controles. [S210]

Solo se publica la calificación nacional. Las filas sectoriales presentan recuentos de señales y sus denominadores. No proporcionan calificaciones de seguridad por sector ni por organización.

Los anuncios vigentes de credenciales abarcan dominios seleccionados de distintos sectores



Anuncios vigentes de credenciales por sector (coral); denominadores de dominios seleccionados. Sin calificaciones sectoriales de riesgo. Fuente: instantánea de exposición de Brandefense, 22 de noviembre de 2026 [S5][S210]. 250 dominios seleccionados; asociaciones acumuladas y solapadas, no personas únicas ni intrusiones confirmadas.

Sector	Dominios	Anuncios vigentes	Documentos
Administración nacional	25	2	5,285
Organismos públicos y municipalidades	25	6	1,426
Banca, pagos e inversiones	25	17	2,359
Seguros y pensiones	25	17	185
Universidades e investigación	25	8	4,601

Sector	Dominios	Anuncios vigentes	Documentos
Salud y ciencias de la vida	25	8	133
Energía, agua y servicios básicos	25	13	359
Minería, manufactura y agricultura	25	1	135
Transporte, puertos y logística	25	7	450
Comercio, comunicaciones y medios	25	19	2,212

La columna de documentos suma 17,145 asociaciones en 149 dominios seleccionados. Una asociación documental no establece confidencialidad, acceso ilícito ni posesión por un adversario. Documentos públicos y material repetido siguen siendo explicaciones posibles. [S210]

98 / 250

Organizaciones seleccionadas con una credencial anunciada a la venta al comprobarse

58/100 (B)

Cifra principal nacional de Atlas para la cartera seleccionada

149 / 250

Dominios seleccionados con asociaciones de documentos

3.3 Dispositivos y credenciales requieren contexto

La cartera contiene 795,641 asociaciones de dispositivos, incluidas 23,676 asociaciones de dispositivos de trabajadores. También contiene 2,999,478 asociaciones de registros de credenciales. La tabla siguiente conserva unidades separadas. [S210]

Sector	Dominios	Dispositivos	Dispositivos de trabajadores	Registros de credenciales
Administración nacional	25	49,507	430	61,050
Organismos públicos y municipalidades	25	55,505	748	127,556
Banca, pagos e inversiones	25	151,575	1,151	249,271

Sector	Dominios	Dispositivos	Dispositivos de trabajadores	Registros de credenciales
Seguros y pensiones	25	124,175	431	67,612
Universidades e investigación	25	51,929	15,703	2,022,142
Salud y ciencias de la vida	25	13,420	278	22,281
Energía, agua y servicios básicos	25	53,087	584	63,078
Minería, manufactura y agricultura	25	4,326	1,068	88,617
Transporte, puertos y logística	25	73,813	432	36,538
Comercio, comunicaciones y medios	25	218,304	2,851	261,333
Total	250	795,641	23,676	2,999,478

Los totales de dispositivos son asociaciones observadas. Las asociaciones pueden superponerse entre dominios. Las asociaciones de dispositivos de trabajadores figuran dentro de la vista de dispositivos y no deben sumarse. Ninguna población cuenta dispositivos nacionales únicos.

Universidades e investigación reúne 2,022,142 asociaciones de registros de credenciales. La visibilidad histórica y las poblaciones de servicios pueden influir en la concentración. Esto no establece la tasa actual de compromiso del sector ni el número de personas afectadas. [S210]

Un dominio de servicio al cliente puede aparecer en un dispositivo del cliente. Esa asociación no establece que el operador del servicio sea dueño del dispositivo. Los registros tampoco establecen sistema de origen, validez actual ni intrusión interna.

Las poblaciones sectoriales de dispositivos y credenciales difieren en escala y significado

Asociaciones de dispositivos de trabajadores Otras asociaciones de dispositivos

Asociaciones de dispositivos (subconjunto de trabajadores entre paréntesis)



Asociaciones de registros de credenciales (escala separada)



Asociaciones de documentos (escala separada)



Fuente: instantánea de exposición de Brandefense, 22 de noviembre de 2026 [S5][S210]. 250 dominios seleccionados; asociaciones acumuladas y solapadas, no personas únicas ni intrusiones confirmadas.

3.4 Resultados pasivos y sus límites

Las observaciones de controles pasivos conservan un denominador separado por resultado

	DMARC	SPF	DKIM	DNSSEC DS	TLS válido	HSTS
Administración nacional	17/24	21/24	19/24	1/24	15/19	8/12
Organismos públicos y municipalidades	19/21	21/21	18/21	1/21	16/17	6/15
Banca, pagos e inversiones	16/21	20/21	16/21	2/21	18/19	7/8
Seguros y pensiones	21/23	20/23	18/23	0/23	19/21	18/19
Universidades e investigación	10/24	24/24	22/24	0/24	19/20	12/23
Salud y ciencias de la vida	6/23	16/23	15/23	0/23	15/17	7/13
Energía, agua y servicios básicos	15/18	17/18	16/18	2/18	14/15	8/9
Minería, manufactura y agricultura	16/23	21/23	20/23	1/23	18/22	7/16
Transporte, puertos y logística	16/23	22/23	20/23	0/23	19/22	11/17
Comercio, comunicaciones y medios	15/25	24/25	20/25	4/25	24/24	10/17

Fuente: observaciones pasivas fechadas [S5]. Cada resultado conserva su denominador evaluado. Una política observada no demuestra aplicación ni eficacia de controles.

Observación de control	Observados	Población evaluada
DMARC con cuarentena o rechazo	151	225
Registro SPF observado	206	225
Registro DKIM observado	184	225
Registro DS de DNSSEC observado	11	225
Validación positiva de certificado TLS	177	196
Cabecera HSTS observada	94	149

Una observación de política de correo respalda revisar la configuración. No establece autenticación ni aplicación por receptores para cada mensaje legítimo. Valide remitentes autorizados y necesidades de entrega antes de cambiar políticas en producción. [S3]

Un registro DKIM no observado no establece que nunca se firmen correos. Un registro relacionado con DNSSEC no establece una cadena validada para cada servicio. Un resultado TLS válido no establece seguridad de aplicaciones.

La revisión pasiva abarcó 225 dominios con resolución. Los resultados TLS fueron concluyentes para 196 y hubo observaciones de cabeceras HTTP para 149. Los resultados no concluyentes siguen desconocidos; la falta de resolución no evidencia controles ausentes. [S3]

3.5 Titularidad y evidencia de cumplimiento

Función	Responsabilidad	Evidencia de cumplimiento
Responsable del dominio	Confirmar organización, servicio y responsabilidad administrativa	Registro aprobado de titularidad y servicio
Mensajería	Validar remitentes autorizados y autenticación prevista	Prueba controlada de entrega y revisión de política
Infraestructura	Evaluar observaciones pertinentes de DNS y HTTPS	Resultado local fechado y decisión de corrección
Identidad y dispositivos	Validar actualidad, privilegios, contexto laboral y sesiones de cuentas	Resolución como actual, histórica, no relacionada o sin resolver
Fraude y protección al cliente	Validar por separado la pertinencia de dispositivos de clientes y tarjetas	Evaluación de fraude con responsable, sin presumir intrusión institucional

CONCLUSIONES CLAVE

01

Valide las 98 asociaciones de anuncios vigentes con cuentas y servicios propios.

02

Mantenga dispositivos, dispositivos de trabajadores, registros de credenciales y documentos como poblaciones separadas que pueden superponerse.

03

Asigne responsables de identidad, dispositivos, fraude y configuración con evidencia fechada de cumplimiento.

CAPÍTULO 04

Evidencia clandestina e interpretación de afirmaciones

04

ESTE CAPÍTULO RESPONDE

¿Qué establecen los anuncios asociados a Chile y qué afirmaciones merecen validación con un responsable?

6

expedientes detallados de afirmaciones, no seis intrusiones confirmadas

4.1 Ficha del universo 24
4.2 Volumen mensual y quincena final 25
4.3 Los principales tipos de afirmación requieren verificaciones distintas 27
4.4 Expedientes detallados de afirmaciones 28
4.5 Otras ofertas específicas y afirmaciones recientes 35
4.6 Qué cambia la decisión de un defensor 37

CAPÍTULO 04

Evidencia clandestina e interpretación de afirmaciones

EN RESUMEN

El material conservado anuncia archivos de proveedores, código de consultoría, accesos privilegiados, información educativa y registros de salud. Seis expedientes conservan afirmaciones, cronología, alternativas y límites. Las publicaciones recientes incluyen una oferta escolar histórica, otra afirmación educativa y material electoral de procedencia sin resolver. Ninguna establece un total verificado de personas afectadas ni una venta realizada. Valide la afirmación pertinente para sus cuentas o registros antes de decidir contención, notificación o atención al cliente.

4.1 Ficha del universo

La población de volumen de publicaciones y la evidencia narrativa tienen alcances distintos. Las cifras de volumen describen observaciones asociadas a Chile en el periodo solicitado. Las fichas narrativas incluyen material pertinente conservado fuera de esa población. No se presentan como un subconjunto estricto de su recuento. [S1]

Elemento	Significado
Periodo	Publicaciones fechadas del 1 de enero–22 de noviembre de 2026
Observaciones de volumen	27,891 en los totales mensuales asociados
Volumen reciente	400 observaciones fechadas del 8–22 de noviembre
Contenido pertinente	Rango analítico de 9,725–10,368 publicaciones entre las 27,890 conservadas de la población de volumen
Evidencia narrativa	Ofertas y afirmaciones conservadas con contexto específico de fuente
Límite del recuento	Las publicaciones no son incidentes, personas, conjuntos de datos ni ventas realizadas
Límite de fecha	Las fechas de publicación no establecen fechas de extracción o intrusión
Límite de relaciones	La similitud de texto o cantidades no establece por sí sola posesión u operación común

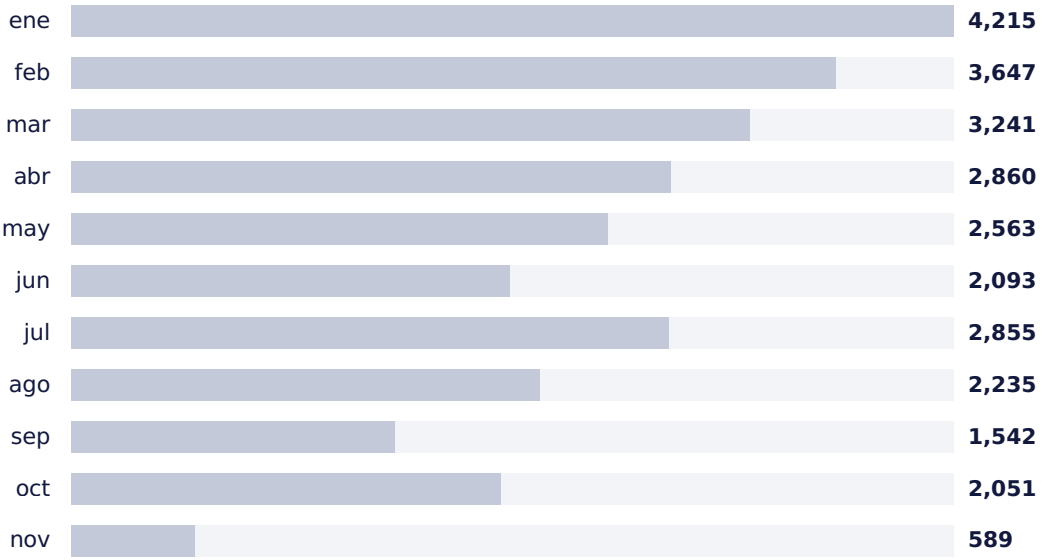
La asociación con un país también es más acotada que la selección de objetivos. Un mensaje puede mencionar Chile dentro de una oferta o solicitud más amplia. Su presencia no establece que el autor operó en Chile ni dirigió una intrusión contra una institución chilena.

4.2 Volumen mensual y quincena final

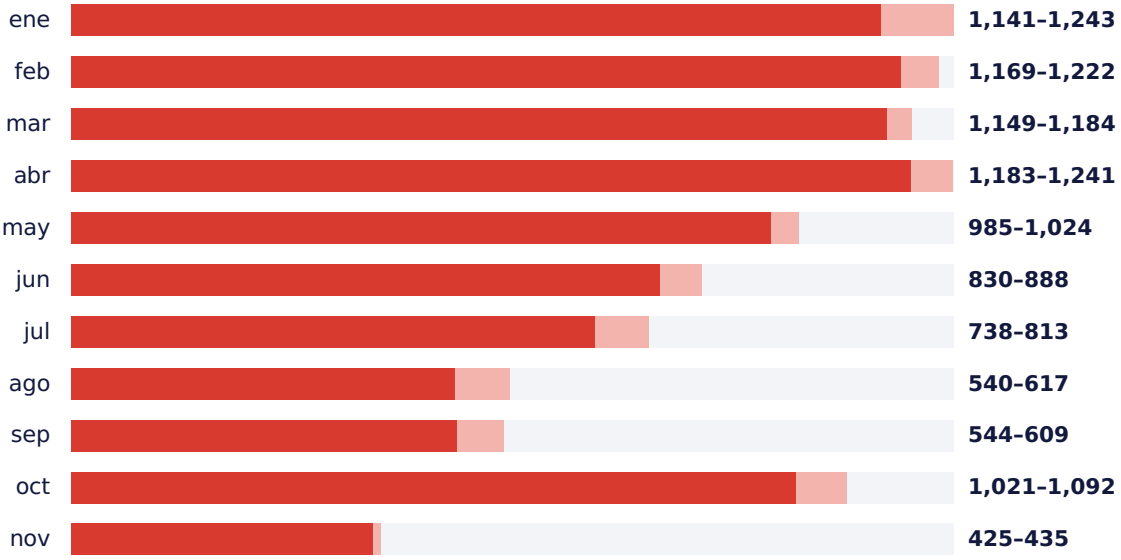
La serie mensual muestra el volumen de publicación observado. Los cambios pueden reflejar tanto la población de fuentes como la actividad. El último mes es parcial y la serie no establece una tendencia comparable de intrusiones logradas. [S1]

El volumen observado cae desde enero, mientras noviembre sigue siendo parcial

Observaciones de volumen de publicaciones



Rango de publicaciones pertinentes (escala separada)



Fuente: observaciones de Brandefense, 1 de enero–22 de noviembre de 2026; noviembre parcial [S1]. Las observaciones de volumen y los temas solapados no son incidentes confirmados.

Mes	Observaciones de volumen	Mes	Observaciones de volumen
Enero	4,215	Julio	2,855
Febrero	3,647	Agosto	2,235
Marzo	3,241	Septiembre	1,542
Abril	2,860	Octubre	2,051
Mayo	2,563	Noviembre hasta el corte	589
Junio	2,093	Total	27,891

La quincena final tiene 400 observaciones de volumen. La cifra describe publicaciones, sin establecer actividad iniciada en ese periodo. Un conjunto escolar recién publicado puede abarcar muchos años anteriores, y una afirmación electoral puede tener procedencia pública o histórica sin resolver.

Las observaciones de plataforma describen mensajes, sin establecer nacionalidad del actor



Fuente: observaciones de Brandefense, 1 de enero–22 de noviembre de 2026; noviembre parcial [S1]. Las observaciones de volumen y los temas solapados no son incidentes confirmados.

Población	Recuento observado	Significado
Telegram	27,578	Publicaciones de la población conservada asociada al país
Foro	284	Publicaciones de la población conservada asociada al país
Sitio de textos	24	Publicaciones de la población conservada asociada al país
Discord	4	Publicaciones de la población conservada asociada al país

Telegram reúne 27,578 de las 27,890 publicaciones conservadas en la población de volumen correspondiente, o el 98.9%. Los casos narrativos de foros no representan esa distribución por plataforma. Se omiten los recuentos por idioma porque las categorías disponibles no permiten una comparación inequívoca. [S1]

4.3 Los principales tipos de afirmación requieren verificaciones distintas

El rango analítico es de 9,725–10,368 publicaciones pertinentes entre las 27,890 conservadas de la población de volumen. Es un rango analítico, sin constituir un intervalo estadístico de confianza ni una estimación de actividad nacional. [S1]

Los casos narrativos abarcan productos supuestamente distintos: archivos cargados a proveedores, código fuente, accesos privilegiados y registros institucionales. No pueden sumarse como si midieran un único tipo de pérdida. Una fila de base de datos, una persona, un volumen de archivos y un permiso de acceso son unidades distintas.

Los temas conservados se superponen y requieren responsables distintos para validarlos



Fuente: observaciones de Brandefense, 1 de enero–22 de noviembre de 2026; noviembre parcial [S1]. Las observaciones de volumen y los temas solapados no son incidentes confirmados.

Tema	Rango de publicaciones	Límite
Contenido relacionado con ransomware	93–93	Temas de contenido superpuestos, no incidentes
Afirmaciones sobre datos y bases de datos	2,909–2,975	Temas de contenido superpuestos, no incidentes
Ofertas de documentos de identidad	2,002–2,125	Temas de contenido superpuestos, no incidentes
Ofertas de acceso	105–106	Temas de contenido superpuestos, no incidentes
Material de malware de robo de información	119–124	Temas de contenido superpuestos, no incidentes

Tema	Rango de publicaciones	Límite
Paquetes de credenciales	410–426	Temas de contenido superpuestos, no incidentes
Material de tarjetas de pago	3,912–4,046	Temas de contenido superpuestos, no incidentes
Ofertas de cuentas financieras	2,001–2,101	Temas de contenido superpuestos, no incidentes
Phishing y fraude	1,058–1,112	Temas de contenido superpuestos, no incidentes
Contenido relacionado con interrupciones	8–8	Temas de contenido superpuestos, no incidentes
Material de malware y vulnerabilidades	197–199	Temas de contenido superpuestos, no incidentes

Los temas del gráfico describen mensajes, sin constituir categorías de incidentes mutuamente excluyentes. Un anuncio puede combinar código fuente, credenciales y registros de clientes. Su presencia en varios temas no crea varias intrusiones ni demuestra que exista cada componente anunciado.

Los recuentos temáticos sobre tarjetas de pago describen publicaciones que tratan ese material. Están separados de la población de registros de tarjetas distintos de la sección 8.5. Un mensaje puede hablar de tarjetas sin establecer una tarjeta utilizable, una transacción realizada o el origen de la exposición.

4.4 Expedientes detallados de afirmaciones

A

CASO A

Archivos cargados a un proveedor y posterior anuncio de venta (B01, B02)

Servicios tecnológicos

Afirmación delictiva; sin verificar

AFIRMACIÓN	Una oferta citada afirmó 6.1 TB de archivos de clientes y código fuente de aplicaciones asociados a un proveedor de software empresarial y alojamiento. Una publicación posterior anunció su disponibilidad para venta. [S1]
CRONOLOGÍA	Una respuesta de foro del 4 de abril contiene la oferta citada. Un seguimiento del 15 de abril en el mismo hilo dice que el material está a la venta. La fecha del texto anterior no establece el momento de extracción.
ESTABLECIDO	La respuesta y el seguimiento conservados contienen publicidad relacionada. Los nombres de clientes de una oferta no son confirmación independiente de que cada cliente sufrió un incidente.

ALTERNATIVA	La oferta podría exagerar el volumen, combinar archivos antiguos o usar una lista de clientes para aumentar la presión. La publicidad relacionada no establece que los archivos ofrecidos sean auténticos o completos.
LÍMITE	No se establecen posesión, extracción, alcance específico por cliente, venta realizada, eliminación ni recuperación del material. Las dos publicaciones no justifican una red de actores más amplia.
RESPUESTA	Solicite una versión del proveedor vinculada a sus servicios y registros. Revise accesos administrativos, actividad de los entornos de clientes y credenciales compartidas pertinentes cuando la evidencia interna respalde la preocupación.

En definitiva

Solicite una versión del proveedor vinculada a sus servicios y registros. Revise accesos administrativos, actividad de los entornos de clientes y credenciales compartidas pertinentes cuando la evidencia interna respalde la preocupación.

Ficha de evidencia B01 — 4 abr 2026

Reservado darkforums.su Forum ['EN']

ORIGINAL

we obtained 6.1TB of customer uploads

TRADUCCIÓN

obtuvimos 6.1TB de archivos cargados por clientes

Lo que consta

La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta

La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B02 — 15 abr 2026

Reservado darkforums.su Forum ['EN']

ORIGINAL

Data is now for sale

TRADUCCIÓN

Los datos ya están a la venta

Lo que consta

Un seguimiento conservado en el mismo hilo de foro dice que los datos están a la venta.

Lo que no consta

Que se realizara una venta. Que existiera todo el material ofrecido.

Noticias de junio describen la versión de un cliente minero sobre un evento en un proveedor externo de plataforma. La empresa dijo que sus sistemas corporativos y la continuidad productiva no estaban afectados. Su estimación preliminar de datos asociados difería de alegaciones mayores y de una afirmación más amplia sobre la plataforma. [S44]

El proveedor también aparece en el contexto de fuentes del Caso A. Esa coincidencia no establece que las publicaciones y la respuesta empresarial se refieran al mismo evento o archivos. La respuesta pública aporta contexto; no se cuenta como otra intrusión independiente.

Para un cliente, la solicitud adecuada es una evaluación acotada del proveedor. Identifique el servicio, la información y los accesos involucrados. No sustituya la pérdida medida de un cliente por una cantidad afirmada para toda una plataforma.

B

CASO B

Archivos de consultoría anunciados con lenguaje de rescate

Ficha de evidencia B04 | 5 abr 2026 | spear.cx | Servicios tecnológicos

Afirmación delictiva; sin verificar

AFIRMACIÓN	Un vendedor alegó una interrupción del sitio web y anunció código fuente de aplicaciones y una base descrita como de 40,081 filas. La oferta incluía un plazo de pago y lenguaje de rescate. [S1]
CRONOLOGÍA	La publicación está fechada el 5 de abril. Esa fecha no establece cuándo supuestamente ocurrieron el acceso o la extracción.
ESTABLECIDO	El texto conservado combina una oferta de archivos relacionada con una consultoría y lenguaje de extorsión. El número de filas no es un total verificado de trabajadores, clientes o personas afectadas.
ALTERNATIVA	Respaldos antiguos o un conjunto menor de datos del sitio podrían describirse como un evento corporativo más amplio. El texto por sí solo no resuelve esa posibilidad.
LÍMITE	No se establecen interrupción web, código actual, secretos utilizables ni consecuencias para clientes. No se atribuye una familia de ransomware por la redacción de la publicación.
RESPUESTA	Revise integridad web, acceso a respaldos y cambios en aplicaciones pertinentes. Evalúe secretos expuestos con evidencia propia antes de rotarlos o atribuir un incidente a un cliente.

En definitiva

Revise integridad web, acceso a respaldos y cambios en aplicaciones pertinentes. Evalúe secretos expuestos con evidencia propia antes de rotarlos o atribuir un incidente a un cliente.

C

CASO C

Oferta de un portal administrativo relacionado con un banco

Ficha de evidencia B03 | 6 mar 2026 | breachforums.as | Banca

Afirmación delictiva; sin verificar

AFIRMACIÓN	Un autor de foro ofreció usuarios de un portal administrativo, puntos de conexión y claves API a un postor. El rol afirmado corresponde a un banco chileno. [S1]

CRONOLOGÍA	La oferta está fechada el 6 de marzo. Otra respuesta la califica de estafa. Ni la oferta ni la acusación establecen validez del acceso.
ESTABLECIDO	La conversación conservada contiene un anuncio de acceso y una disputa de credibilidad. No establece control actual de cuentas ni una transacción realizada.
ALTERNATIVA	El autor podría reciclar identificadores, simular permisos o hacer una oferta fraudulenta. La objeción sigue siendo la evaluación de un participante del foro.
LÍMITE	No se establecen credenciales válidas, claves utilizables, intrusión institucional lograda ni consecuencias para clientes. Una etiqueta bancaria no demuestra acceso a la infraestructura bancaria subyacente.
RESPUESTA	Valide cuentas privilegiadas, actividad API y cambios de sesiones pertinentes mediante el proceso controlado de incidentes del banco. Revoque accesos cuando la evidencia propia lo justifique.

En definitiva

Valide cuentas privilegiadas, actividad API y cambios de sesiones pertinentes mediante el proceso controlado de incidentes del banco. Revoque accesos cuando la evidencia propia lo justifique.

Las fichas B04 y B03 respaldan los Casos B y C, respectivamente. Sus afirmaciones y límites distintos permanecen separados.

Ficha de evidencia B04 — 5 abr 2026

Reservado | spear.cx | Forum | ['EN']

ORIGINAL

The ransom price will double in 48 hours.

TRADUCCIÓN

El precio del rescate se duplicará en 48 horas.

Lo que consta

La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta

La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B03 — 6 mar 2026

Reservado | breachforums.as | Forum | ['EN']

ORIGINAL

I have endpoints and API keys.

TRADUCCIÓN

Tengo puntos de conexión y claves API.

Lo que consta

La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta

La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

CASO D

D

Afirmación de publicación de datos de administración educativa (B06, B07)

Educación

Afirmación delictiva; sin verificar

AFIRMACIÓN	Publicaciones en español afirmaron información sobre 3,046,248 estudiantes y apoderados. Una versión posterior dijo que el material no estaba a la venta ni se cobraba rescate. [S1]
CRONOLOGÍA	Las publicaciones estrechamente relacionadas están fechadas el 4 y 5 de octubre. Usan la misma población afirmada y descripciones similares. Esto respalda un expediente de datos supuestamente comunes, sin confirmar dos incidentes.
ESTABLECIDO	El texto describe estudiantes o apoderados y afirma una extracción. Este informe establece que los autores hicieron esa afirmación, sin establecer que la extracción ocurrió.
ALTERNATIVA	Las publicaciones podrían volver a presentar información antigua, repetir publicidad copiada o describir material de acceso público como obtenido por intrusión. La redacción de la fuente no permite elegir entre esas posibilidades.
LÍMITE	No se establecen autenticidad, integridad, fecha de extracción, recuento de personas únicas ni acceso logrado al servicio. Un total afirmado de registros no es una población afectada contada de manera independiente.
RESPUESTA	Revise actividad de cuentas educativas y exportaciones masivas pertinentes. Si se valida internamente la exposición, prepare una vía de atención que aborde la suplantación de apoderados y estudiantes.

En definitiva

Revise actividad de cuentas educativas y exportaciones masivas pertinentes. Si se valida internamente la exposición, prepare una vía de atención que aborde la suplantación de apoderados y estudiantes.

Ficha de evidencia B06 — 5 oct 2026

Reservado | updap.com | Forum | ['ES']

ORIGINAL

extraído información de 3,046,248 estudiantes y tutores.

TRADUCCIÓN

extraído información de 3,046,248 estudiantes y apoderados.

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B07 — 4 oct 2026

Reservado | updap.com | Forum | ['ES']

ORIGINAL

extraido informacion de 3,046,248 estudiantes y tutores.

TRADUCCIÓN

extraído información de 3,046,248 estudiantes y apoderados.

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

E

CASO E

Oferta de una red escolar que abarca años anteriores

Ficha de evidencia B08 | 12 nov 2026 | bf.st | Educación

Afirmación delictiva; sin verificar

AFIRMACIÓN	Una publicación del 12 de noviembre anuncia datos asociados a cinco colegios y fechados en 2010–2026. Afirma 107,781 filas y 23,240 personas únicas. [S1]
CRONOLOGÍA	La publicación pertenece a la quincena final. Su periodo histórico declarado impide tratar cada registro anunciado como una nueva adquisición de 2026.
ESTABLECIDO	El autor distingue filas anuales de una supuesta cantidad de personas únicas. Ambas cifras siguen siendo afirmaciones del vendedor y no se suman.
ALTERNATIVA	Un directorio histórico o conjunto reutilizado podría haberse presentado como una nueva extracción. La extracción atribuida al propio autor no se establece de manera independiente.
LÍMITE	La autenticidad, unicidad, mecanismo de extracción e intrusión reciente siguen sin verificarse. La oferta no demuestra un incidente separado en cada colegio mencionado.
RESPUESTA	Revise el acceso a datos archivados y las exportaciones masivas. Verifique la procedencia antes de tratar el anuncio como un incidente actual o identificar personas afectadas.

En definitiva

Revise el acceso a datos archivados y las exportaciones masivas. Verifique la procedencia antes de tratar el anuncio como un incidente actual o identificar personas afectadas.

CASO F

F

Afirmación de publicación de datos de varios prestadores de salud

Afirmación delictiva; sin verificar

Ficha de evidencia B05 | 29 oct 2026 | darkforums.su | Salud

AFIRMACIÓN	Una publicación de foro del 29 de octubre afirma una divulgación gratuita de registros atribuidos a varias organizaciones de salud. Se refiere a material de 2026. [S1]
ESTABLECIDO	El texto conservado contiene roles de objetivos médicos y lenguaje de divulgación. La lista de nombres no constituye un conjunto de incidentes institucionales confirmados.
ALTERNATIVA	La publicación podría combinar información antigua de salud o material disponible públicamente. Su relato no establece de manera independiente el origen de la información ni la identidad del autor.
LÍMITE	No se establecen autenticidad, integridad, acceso actual ni incidentes separados en los prestadores mencionados. La etiqueta de fecha del autor no fecha los registros de manera independiente.
RESPUESTA	Valide coincidencias de registros mediante canales internos controlados. Revise exportaciones pertinentes de datos de pacientes y prepare atención focalizada si la evidencia de la organización establece exposición.

En definitiva

Valide coincidencias de registros mediante canales internos controlados. Revise exportaciones pertinentes de datos de pacientes y prepare atención focalizada si la evidencia de la organización establece exposición.

No se establece una conexión entre esta afirmación y los incidentes hospitalarios del capítulo 5. Compartir un rol del sector salud no basta para vincular eventos. Cada afirmación necesita su propia evaluación de procedencia, cronología y consecuencias.

Las fichas B08 y B05 respaldan los Casos E y F, respectivamente. Su presentación conjunta no establece un evento compartido.

Ficha de evidencia B08 12 nov 2026

Reservado bf.st Forum ['EN']

ORIGINAL

I am selling a database from a network of 5 schools in Chile

TRADUCCIÓN

Vendo una base de datos de una red de 5 colegios en Chile

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B05 29 oct 2026

Reservado darkforums.su Forum ['EN']

ORIGINAL

full data free

TRADUCCIÓN

todos los datos gratis

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

4.5 Otras ofertas específicas y afirmaciones recientes

Las fichas adicionales conservan afirmaciones que merecen atención sin exagerar su valor probatorio. No se cuentan como más intrusiones confirmadas.

Ficha	Publicación	Rol	Afirmación conservada y límite
B11	2 de febrero	Plataforma de administración de propiedades	Anuncia 724,000 registros de usuarios; procedencia, actualidad y alcance sin verificar
B12	14 de enero	Servicio de registros públicos	Anuncia 9,200,000 líneas; no se establecen fecha de recopilación ni una nueva intrusión de 2026
B09	20 de noviembre	Organización educativa	Afirma datos y fotografías de menores; no se establecen autenticidad ni conexión con otras afirmaciones educativas
B10	22 de noviembre	Registros electorales	Afirma material de seis millones de electores; disponibilidad pública, antigüedad y nueva intrusión sin resolver

Fuente: material de publicaciones conservado [S1]. Las cantidades pertenecen a las afirmaciones de los autores. Un registro, una línea, una referencia a elector y una persona afectada única no son unidades intercambiables.

Ficha de evidencia B11 — 2 feb 2026

Reservado | breachforums.bf | Forum | ['EN']

ORIGINAL

724,000 Chilean user records

TRADUCCIÓN

724,000 registros de usuarios chilenos

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B12 — 14 ene 2026

Reservado | breachforums.bf | Forum | ['EN']

ORIGINAL

total lines 9 200 000

TRADUCCIÓN

líneas totales 9 200 000

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B09 — 20 nov 2026

Reservado | darkforums.su | Forum | ['EN']

ORIGINAL

faces and names of minors

TRADUCCIÓN

rostros y nombres de menores

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación.

Ficha de evidencia B10 — 22 nov 2026

Reservado | darkforums.su | Forum | ['EN']

ORIGINAL

have electoral data for 6 million voters

TRADUCCIÓN

tengo datos electorales de 6 millones de votantes

Lo que consta
La publicación conservada contiene el anuncio citado o la afirmación de divulgación.

Lo que no consta
La autenticidad, vigencia, integridad o utilidad de los datos o accesos anunciados. Que la fecha de publicación sea la de intrusión o recopilación. Una intrusión asociada a la elección actual. Si los datos electorales subyacentes ya eran públicos.

La afirmación educativa del 20 de noviembre es distinta de la oferta de la red escolar y del expediente de administración educativa. El informe no establece datos u operador comunes. La sensibilidad del asunto justifica validación y atención cuidadosas, sin inferir una campaña contra instituciones relacionadas.

La afirmación de datos electorales del 22 de noviembre exige especial cautela. La fuente no establece si la información ya era pública, cuándo se obtuvo ni su integridad. No establece una intrusión actual en sistemas electorales, motivo político ni efectos sobre una elección.

Una afirmación de foro del 23 de marzo anuncia 10,000 registros de sitio web atribuidos a una universidad. La descripción menciona nombres y códigos de usuario. No se establecen autenticidad, actualidad, procedencia no pública ni acceso utilizable a cuentas. Las filas afirmadas no son un recuento confirmado de personas afectadas. [S1]

Otra afirmación universitaria de marzo anuncia 70,000 registros de un sitio. Su retransmisión describe información y fotografías de estudiantes. La afirmación original y su retransmisión no establecen corroboración independiente ni otra intrusión. Autenticidad y actualidad de los datos siguen sin resolverse. [S1]

Estas afirmaciones universitarias conservan sus aseveraciones separadas sobre objetivos y conjuntos de datos. No se establece intrusión compartida, archivos subyacentes comunes ni operador común verificado.

Otra oferta del sector público describe datos relacionados con transparencia. La disponibilidad pública y la fecha de recopilación siguen sin resolverse. Ese límite impide convertir un gran volumen anunciado en prueba de robo de información gubernamental no pública. [S1]

4.6 Qué cambia la decisión de un defensor

Para ofertas de acceso, compruebe estado, permisos y actividad de cuentas. Para archivos, establezca procedencia y sensibilidad por canales controlados de la organización. Para afirmaciones sobre proveedores, solicite una evaluación vinculada al servicio propio de la organización en lugar de una lista global de clientes.

La evidencia de cierre es una conclusión fechada, con responsable y fundamento. Registre qué proposición se estableció, contradijo o dejó sin resolver. Un restablecimiento o aviso a clientes debe seguir esa evaluación y el procedimiento de incidentes, sin depender del lenguaje de presión del anuncio.

CONCLUSIONES CLAVE

01

Las publicaciones conservadas establecen afirmaciones y ofertas, sin verificar posesión, nuevas intrusiones o ventas realizadas.

02

Conserve las unidades, fechas y alternativas distintas dentro de cada expediente.

03

Valide la evidencia propia pertinente antes de actuar sobre cuentas, proveedores, privacidad o clientes.

CAPÍTULO 05

Incidentes, afirmaciones y decisiones de respuesta por sector

ESTE CAPÍTULO RESPONDE

¿Qué versiones públicas establecen un problema operacional y qué debe verificar primero cada sector?

Separe

acceso, publicación de datos y disponibilidad del servicio

5.1 Lea el caso antes de contar el incidente 39
5.2 Afirmaciones de mayo sobre servicios públicos y comunicaciones 40
5.3 Información de salud y continuidad clínica 41
5.4 Las operaciones energéticas requieren una evaluación de impacto distinta 43
5.5 Un incidente de servicio público con versiones técnicas contrapuestas 44
5.6 Actividad reciente: 8–22 de noviembre de 2026 44
5.7 Las advertencias financieras requieren su propia población de casos 46
5.8 Qué respalda la evidencia sectorial 46
5.9 Recuperación del comercio minorista y límites de una declaración inicial 47
5.10 Versiones sobre proveedores, redes y acceso administrativo 48
5.11 Servicios jurídicos y cuentas de publicación de contenidos 51
5.12 Más contexto de fuentes sin un recuento adicional de incidentes 53
5.13 Exclusiones importantes y avisos que no son incidentes 53

CAPÍTULO 05

Incidentes, afirmaciones y decisiones de respuesta por sector

EN RESUMEN

Las versiones públicas de Chile distinguen uso no autorizado de cuentas válidas, datos históricos presentados como nuevos, exposición de información hospitalaria e interrupciones. Avisos recientes agregan indisponibilidad hospitalaria, interrupción energética continuada y versiones contrapuestas de un incidente de servicio público. Son estados de evidencia distintos. La advertencia de un regulador no es otra intrusión confirmada. Comience por la función afectada y el hallazgo real de la fuente; asigne después la respuesta de identidad, privacidad, fraude o continuidad correspondiente.

5.1 Lea el caso antes de contar el incidente

Los casos siguientes distinguen una declaración primaria de autoridad de las noticias sobre la versión de una organización. Los nombres siguen expresados como roles cuando no se cumplen las condiciones para publicarlos. Un rol genérico no significa que el aviso subyacente carezca de un sujeto específico.

Un caso es un expediente que explica una decisión. No equivale automáticamente a una intrusión confirmada. Los avisos de mayo sobre accesos abarcan varias afirmaciones reportadas. La corrección sobre datos históricos interpreta una alerta. Los avisos hospitalarios describen episodios reportados distintos. Ninguno debe sumarse mecánicamente a las publicaciones delictivas.

La tabla presenta el estado de evidencia y la primera función responsable.

Estado de evidencia	Conclusión respaldada	Primer responsable	Pregunta inicial
La autoridad identifica acceso con cuentas válidas	Las cuentas afectadas requieren investigación	Identidad y respuesta	¿Qué cuentas y permisos se usaron?
La autoridad identifica material histórico	Una nueva publicación no implica necesariamente una nueva intrusión	Inteligencia y privacidad	¿La evidencia coincide con un evento conocido?
La prensa informa una denuncia penal	La denuncia reportada describe un incidente	Respuesta y asesoría jurídica	¿Qué establece realmente la versión oficial?
La organización reporta una interrupción	La función de servicio indicada fue afectada	Responsable del servicio	¿Qué tareas esenciales siguen funcionando?
El regulador advierte sobre sospechas de fraude	Los clientes necesitan una vía confiable de verificación	Fraude y atención al cliente	¿Qué solicitud o pago necesita validación?
Un actor publica una entrada de extorsión	Existe una afirmación delictiva	Respuesta y comunicaciones	¿Hay evidencia independiente de acceso o impacto?

5.2 Afirmaciones de mayo sobre servicios públicos y comunicaciones

CASO G

G

Acceso con cuentas válidas dentro de un relato más amplio de filtraciones

Administración pública

Versión de fuente: límites conservados

REPORTE INICIAL	El 1 de mayo, ANCI dijo que investigaba publicaciones de datos reportadas sobre operadores de comunicaciones y servicios públicos. Aún no se habían corroborado autenticidad y alcance. [S6]
HALLAZGO ACTUALIZADO	El 8 de mayo, ANCI identificó acceso no autorizado con credenciales válidas. Consideró probables fuentes las filtraciones anteriores o el malware de robo de información y reportó ausencia de evidencia de ataques a infraestructura. [S7]
LÍMITE	La actualización no establece acceso a cada organización mencionada en las afirmaciones anteriores. Tampoco respalda tratar al Estado como una sola red afectada.
ALTERNATIVA	Un anuncio delictivo puede combinar un evento real de cuenta con material histórico o ajeno. Cada fuente y vía de acceso afirmadas requiere su propia evidencia.
RESPUESTA	Valide las cuentas coincidentes, revise permisos y sesiones actuales y delimite los registros accesibles. Use contención focalizada cuando la evidencia lo justifique, sin tratar toda credencial anunciada como una intrusión institucional actual.

En definitiva

Valide las cuentas coincidentes, revise permisos y sesiones actuales y delimite los registros accesibles. Use contención focalizada cuando la evidencia lo justifique, sin tratar toda credencial anunciada como una intrusión institucional actual.

CASO H

H

Una nueva alerta sobre material atribuido a una filtración antigua

Datos de identidad

Evaluación de datos históricos

AFIRMACIÓN REPORTADA	Una alerta de mayo describió más de seis millones de registros chilenos. Esa cantidad pertenece a la alerta, sin constituir una población verificada de un nuevo incidente en este informe. [S8]

EVALUACIÓN DE LA AUTORIDAD	El aviso de ANCI del 20 de mayo atribuyó el material a una filtración de una plataforma social de 2019, en vez de una intrusión reciente en infraestructura nacional. [S8]
LÍMITE	El origen histórico no establece que los datos sean inocuos, actuales o exactos. Tampoco establece un nuevo acceso cuando el material vuelve a anunciarse.
RESPUESTA	Compruebe si las cuentas afectadas ya fueron remediadas y si la información aún permite suplantaciones. Corrija la cronología del incidente y mantenga atención proporcional para quienes enfrentan nuevos contactos.

En definitiva

Compruebe si las cuentas afectadas ya fueron remediadas y si la información aún permite suplantaciones. Corrija la cronología del incidente y mantenga atención proporcional para quienes enfrentan nuevos contactos.

5.3 Información de salud y continuidad clínica

CASO I

Noticias de septiembre sobre acceso y publicación de registros de imagenología

Denuncia reportada; alcance incierto

Salud

VERSIÓN OFICIAL REPORTADA	T13 informó que un hospital presentó una denuncia penal sobre acceso no autorizado a registros de imagenología y publicación en línea. La versión siguió a una notificación de ANCI del 20 de septiembre. [S33]
ALCANCE	La noticia no estableció la población afectada total. La versión de la denuncia no valida una cantidad afirmada en una publicación de extorsión anterior.
LÍMITE DE EVIDENCIA	Este caso se basa en noticias sobre la denuncia. Aquí no se adopta atribución de actor, vía de entrada ni total final de pacientes.
RESPUESTA	Asigne responsables de datos clínicos para identificar los registros y evaluar consecuencias para pacientes. Distinga la investigación de privacidad de la disponibilidad de los sistemas clínicos.

En definitiva

Asigne responsables de datos clínicos para identificar los registros y evaluar consecuencias para pacientes. Distinga la investigación de privacidad de la disponibilidad de los sistemas clínicos.

La información de imagenología puede tener una sensibilidad distinta de una lista de contactos. Los equipos deben establecer qué revelan los registros y quién necesita apoyo. Una referencia amplia a un hospital no permite inferir afectación de cada paciente, departamento o sistema.

La respuesta a pacientes también necesita una vía de contacto confiable. El personal debe explicar qué se conoce, qué sigue en revisión y cómo reportar contactos posteriores sospechosos. Conocer un detalle médico no basta para autenticar a quien llama.

CASO J

J

Interrupción de servidores hospitalarios en noviembre con atención clínica mantenida

Salud

Incidente de servicio reportado

EVENTO REPORTADO	T13 informó la declaración del hospital el 16 de noviembre, seguida de cobertura de BioBioChile. La versión describe un incidente iniciado el 14 de noviembre, interrupción de reservas y canales de apoyo, atención clínica mantenida y coordinación técnica con ANCI. [S56][S34]
LÍMITE	La exposición de datos de pacientes seguía sin resolverse en la versión citada. No se asigna una familia de ransomware ni se vincula el evento al episodio de septiembre por fecha o tipo institucional.
DISTINCIÓN OPERACIONAL	Mantener atención clínica no establece que todos los recorridos administrativos o de pacientes funcionaran normalmente. La interrupción de reservas tampoco establece acceso a sistemas de tratamiento.
RESPUESTA	Pruebe alternativas de agendamiento, priorice solicitudes clínicamente urgentes y concilie el trabajo acumulado durante la interrupción. Evalúe el acceso a datos por separado de la decisión de restablecimiento del servicio.

En definitiva

Pruebe alternativas de agendamiento, priorice solicitudes clínicamente urgentes y concilie el trabajo acumulado durante la interrupción. Evalúe el acceso a datos por separado de la decisión de restablecimiento del servicio.

Para la dirección clínica, una unidad en funcionamiento es un hito, no la recuperación completa. Los pacientes aún pueden tener dificultades para agendar, obtener información o confirmar una visita. El responsable del servicio debe identificar esas tareas y proporcionar una alternativa confiable.

ANCI y CENS anunciaron recomendaciones para sistemas de información de salud en agosto. La publicación aporta un recurso sectorial pertinente. Este informe no atribuye controles detallados a la guía sin basarse en su texto sustantivo. [S38]

5.4 Las operaciones energéticas requieren una evaluación de impacto distinta

CASO K

K

Desconexión prolongada de una instalación generadora

Energía

Causa reportada por el operador

REGISTRO OPERACIONAL	El registro del coordinador eléctrico del 27 de agosto presenta una instalación solar y baterías desconectadas, con ciberataque como causa reportada por el operador. Los registros del 9 y 15 de noviembre aún indican 0% de disponibilidad. Noticias posteriores describen la desconexión continuada. [S53] [S54][S86][S35]
LÍMITE	El informe no establece actor, vía de entrada ni causa común con problemas de control remoto en otras instalaciones. La desconexión continuada no establece una interrupción más amplia del suministro eléctrico.
PREGUNTA OPERACIONAL	Una instalación puede estar indisponible para despacho mientras otras generadoras cubren la demanda. Las consecuencias para esa instalación y para el sistema nacional requieren evidencias distintas.
RESPUESTA	Verifique la función operacional afectada con el ingeniero responsable. Documente recuperación segura, controles de acceso remoto y aceptación del responsable operacional antes de reconectar un servicio.

En definitiva

Verifique la función operacional afectada con el ingeniero responsable. Documente recuperación segura, controles de acceso remoto y aceptación del responsable operacional antes de reconectar un servicio.

La misma cautela se aplica a reportes simultáneos. La cercanía de fechas puede justificar investigar una relación. No establece operador, vulnerabilidad o campaña comunes sin una conexión concreta.

Una solicitud parlamentaria de noviembre pregunta por conocimiento, notificación y respuesta a los incidentes eléctricos. La solicitud no establece sus propias respuestas. Mantiene expresamente incertidumbre sobre orígenes, sistemas afectados y vínculos entre eventos. [S60]

5.5 Un incidente de servicio público con versiones técnicas contrapuestas

CASO L

L

Una investigación sin mecanismo de entrada establecido

Servicios públicos

Versiones distintas

ALEGACIONES DE PRENSA	Noticias de noviembre citaron versiones anónimas que alegaban phishing y malware persistente en un organismo de servicio público. Son alegaciones atribuidas, sin constituir hallazgos adoptados por este informe. [S36]
RESPUESTAS OFICIALES REPORTADAS	La organización dijo que había análisis forense en curso. ANCI indicó al medio que investigaba y sospechaba DDoS. No había sido informada del supuesto mecanismo de malware ni había aplicado multas. [S36]
LÍMITE	La evidencia no resuelve mecanismo de entrada, persistencia, ventas de datos ni identidad del actor. Un evento sospechado de disponibilidad no establece acceso a los registros subyacentes.
RESPUESTA	Separe el monitoreo de disponibilidad de la investigación de acceso. Conserve las versiones contrapuestas, obtenga evidencia del responsable del servicio y comunique qué proposición cambia con cada actualización.

En definitiva

Separe el monitoreo de disponibilidad de la investigación de acceso. Conserve las versiones contrapuestas, obtenga evidencia del responsable del servicio y comunique qué proposición cambia con cada actualización.

5.6 Actividad reciente: 8–22 de noviembre de 2026

La quincena final incluye eventos recién reportados, actualizaciones de interrupciones anteriores, advertencias de fraude y novedades normativas. La tabla conserva esos tipos. No es un recuento de nuevas intrusiones.

Publicación	Tipo	Novedad respaldada	Implicación para defensores
9 de noviembre	Registro operacional continuado	El coordinador eléctrico aún indica 0% de disponibilidad para las unidades afectadas [S54]	Conservar las consecuencias por instalación y la aceptación operacional
10 de noviembre	Advertencia de concientización	ANCI describe errores o verificaciones falsas que inducen acciones inseguras [S18]	Dar al personal una vía de apoyo confiable ante instrucciones inesperadas

Publicación	Tipo	Novedad respaldada	Implicación para defensores
11 de noviembre	Noticias de incidente	Las versiones de servicio público difieren sobre el mecanismo técnico [S36]	Mantener la incertidumbre y verificar servicio y acceso por separado
12 de noviembre	Orientación de respuesta	ANCI distingue recibir un mensaje de ingresar credencia- les o información bancaria [S19]	Determinar qué hizo realmente la persona
15 de noviembre	Observación operacional continuada	El coordinador eléctrico vuelve a registrar 0% de disponibilidad para las mismas unidades [S86]	Prolonga el evento existente, sin constituir uno nuevo
17 de noviembre	Nuevo evento reportado	Autoridades hospitalarias describen el incidente en servidores del 14 de noviembre y las reservas interrumpidas [S34]	Mantener alternativas clínicas y administrativas
17 de noviembre	Consulta	CMF propone cambios en definiciones e información de reportes bancarios de ciberincidentes [S87]	Conservar su condición de propuesta y seguir el instrumento final
18 de noviembre	Interrupción continuada	Noticias señalan que continuó una desconexión energética de agosto [S35]	Exigir un estado de recuperación aceptado operacionalmente
18 de noviembre	Consulta parlamentaria	Una solicitud oficial pregunta por continuidad y preparación hospitalaria [S57]	Las preguntas no establecen hallazgos forenses
18 de noviembre	Advertencia de fraude	CMF advierte sobre cobros de aplicaciones de crédito y sospechas de usura [S25]	Derivar reportes de cobro coercitivo a atención capacitada e investigación
18 de noviembre	Advertencia de fraude	CMF describe ofertas de préstamos con pago anticipado y una denuncia [S26]	Verificar al proveedor sin usar su aprobación afirmada como autenticación
18 de noviembre	Advertencia de concientización	ANCI aborda ofertas laborales no solicitadas que buscan información, dinero o códigos de recuperación [S20]	Informar a reclutamiento y al personal de atención
19 de noviembre	Consulta	ANCI abre consulta sobre requisitos propuestos de MFA [S15][S16]	Revisar la propuesta conservando su condición de proyecto

Publicación	Tipo	Novedad respaldada	Implicación para defensores
19 de noviembre	Orientación de seguridad	ANCI aborda ataques asistidos por IA sin anunciar una campaña nacional confirmada [S17]	Evaluar conducta y exposición propia, no solo la etiqueta de IA
20 de noviembre	Novedad legislativa	La Cámara informa que la postergación de la ley de datos pasó a promulgación [S31][S32]	Confirmar promulgación y publicación antes de cambiar el plazo legal

El evento energético continuado no debe recontarse como intrusión de noviembre. La fecha de publicación de la noticia hospitalaria no debe sustituir la fecha de evento reportada. Las denuncias de CMF describen presuntas conductas indebidas y actuaciones regulatorias, sin constituir condenas.

5.7 Las advertencias financieras requieren su propia población de casos

El aviso de CMF de junio se refirió a trece aplicaciones de crédito no reguladas. El de noviembre, a tres aplicaciones. Ambos describen cobros extorsivos y sospechas de usura. Esos recuentos corresponden a aplicaciones en avisos, no a incidentes de ransomware, deudores o grupos delictivos separados. [S28][S25]

Otras advertencias sobre préstamos describen pagos solicitados antes de entregar créditos que no se concretaron. El aviso de marzo se refiere a ocho entidades; el de abril, a cuatro. El de noviembre describe otra oferta reportada. No se suman como total de víctimas únicas o pérdidas financieras. [S42][S43][S26]

5.8 Qué respalda la evidencia sectorial

La principal lección común es distinguir las consecuencias. El uso indebido de identidad exige validar cuentas y sesiones. La posible exposición de registros exige evaluar privacidad con alcance definido. Una interrupción necesita alternativas utilizables y aceptación de negocio. Las sospechas de fraude al cliente necesitan una vía confiable de verificación.

Estas lecciones se aplican entre sectores sin establecer una clasificación nacional por riesgo. Las prácticas de divulgación pública difieren y algunos incidentes no se hacen públicos. Los casos descritos aquí no representan la frecuencia de todos los incidentes en salud, energía, gobierno o finanzas.

5.9 Recuperación del comercio minorista y límites de una declaración inicial

CASO M

M

Una actualización posterior cambia el panorama operacional de un comercio

Comercio minorista

Divulgación oficial

DIVULGACIÓN INICIAL	Un hecho esencial del 16 de septiembre dice que un comercio conoció un incidente el 15 de septiembre. Algunos sistemas estaban afectados, se activaron respuesta y trabajo forense, y los efectos financieros seguían sin resolverse. [S51]
ACTUALIZACIÓN POSTERIOR	La declaración del 6 de octubre describe retrasos logísticos, de distribución y reposición de tiendas, además de interrupciones digitales y mayoristas. Las tiendas seguían abiertas. La empresa aún no establecía el impacto financiero. [S52]
LÍMITE	Las declaraciones empresariales no establecen grupo de ransomware ni robo de datos confirmado. La posición de septiembre debe conservar su fecha, sin convertirse en garantía permanente sobre todas las consecuencias posibles.
RESPUESTA	Evalúe tiendas físicas, ventas digitales, pedidos mayoristas y reposición como recorridos de servicio distintos. Concilie pedidos acumulados y movimientos de inventario antes de considerar las tiendas abiertas como recuperación completa.

En definitiva

Evalúe tiendas físicas, ventas digitales, pedidos mayoristas y reposición como recorridos de servicio distintos. Concilie pedidos acumulados y movimientos de inventario antes de considerar las tiendas abiertas como recuperación completa.

5.10 Versiones sobre proveedores, redes y acceso administrativo

Contexto de fuente: incidente de proveedor de un cliente minero

- **Versión empresarial reportada.** Una noticia de junio reproduce la respuesta del cliente minero: el evento concernía a un proveedor externo de plataforma y no a sus sistemas corporativos. La empresa dijo que la continuidad productiva no estaba afectada. [S44]
- **Límite de cantidades.** La estimación preliminar del cliente sobre datos asociados difería de una alegación mayor y de una afirmación más amplia del atacante sobre la plataforma. Las cantidades describen afirmaciones y alcances distintos.
- **Límite.** La respuesta citada no establece una intrusión separada en la red corporativa del cliente. Un incidente de proveedor puede afectar información de clientes sin convertirse en una intrusión independiente en cada cliente.
- **Respuesta.** Obtenga una evaluación del proveedor específica para el cliente e identifique información y accesos involucrados. Registre por separado consecuencias productivas y de privacidad. No use la afirmación global del proveedor como pérdida medida del cliente.

Este proveedor también aparece en el contexto de fuentes del Caso A. Los registros no establecen el mismo evento o archivos, por lo que esta versión no se cuenta como otra intrusión independiente.

La declaración de una empresa de que sus sistemas no fueron afectados acota una proposición. No resuelve automáticamente la información custodiada en otros lugares. El registro de respuesta debe conservar la distinción, sin forzar una sola etiqueta de ausencia o totalidad de afectación.

CASO O

Investigación de telecomunicaciones con actividad histórica

Telecomunicaciones

Investigación reportada

INVESTIGACIÓN REPORTADA	Noticias de agosto dicen que PDI y Fiscalía investigaron actividad en redes de telecomunicaciones tras recibir información de autoridades estadounidenses. Aluden a malware y una etiqueta de actor, con actividad observada desde 2024. [S45]
LÍMITE DE ATRIBUCIÓN	Las descripciones del actor y sus asociaciones estatales pertenecen a las fuentes citadas. Este informe no infiere una conexión gubernamental, una entrada nueva en 2026 ni una relación con políticas de infraestructura.
LÍMITE DE ALCANCE	El informe no establece una población confirmada de datos de usuarios finales. Investigar actividad de red no equivale a contar cada abonado o dispositivo del servicio.

RESPUESTA	Conserve el periodo observado de la fuente y valide evidencia pertinente de red y administradores. Evalúe por separado consecuencias para proveedores o clientes. Distinga la actividad histórica de la fecha en que la investigación se hizo pública.

En definitiva

Conserve el periodo observado de la fuente y valide evidencia pertinente de red y administradores. Evalúe por separado consecuencias para proveedores o clientes. Distinga la actividad histórica de la fecha en que la investigación se hizo pública.

P

CASO P

Mensajes no autorizados y breve interrupción de un servicio público

Servicios públicos

Versión de fuente: límites conservados

VERSIÓN DEL ORGANISMO REPORTADA	Una noticia de agosto cita a un organismo de servicio público que describió un incidente no autorizado con interrupción temporal de 05:00 a 09:00. También describe mensajes masivos no solicitados. [S46]
LÍMITE	Esos hechos no establecen acceso a todos los registros, operador identificado ni motivo político. El restablecimiento del servicio no establece el alcance de un posible acceso a datos.
RESPUESTA	Revise la autoridad de mensajería afectada y los permisos pertinentes. Confirme que los destinatarios reconocen comunicaciones legítimas posteriores y que funciona la tarea del servicio público restablecido.

En definitiva

Revise la autoridad de mensajería afectada y los permisos pertinentes. Confirme que los destinatarios reconocen comunicaciones legítimas posteriores y que funciona la tarea del servicio público restablecido.

El contenido del mensaje es innecesario para el hallazgo defensivo. El problema es el uso no autorizado de un canal confiable y la interrupción reportada. El informe no reproduce imágenes políticas ni adopta una interpretación de su ideología.

Q

CASO Q

Posible extracción de información de salud con atención mantenida

Salud

Posible extracción

DECLARACIÓN PRIMARIA	Una declaración de un servicio de salud describe la detección, el 4 de mayo, de posible extracción no autorizada de información tras una alerta externa. Dice que sistemas y atención no estaban afectados entonces. [S63]

MECANISMO SIN RESOLVER	El origen seguía bajo análisis y no se había descartado el uso indebido de credenciales. Ninguna posibilidad debe convertirse en un mecanismo de acceso establecido.
LÍMITE	La declaración se refiere a una posible extracción, sin verificar un volumen final ni concluir sobre todos los registros. Su versión de sistemas y atención no afectados permanece vinculada a esa fecha.
RESPUESTA	Conserve la alerta externa, identifique responsables de los datos pertinentes y evalúe el uso de cuentas. Mantenga la atención mientras la pregunta sobre acceso a información recibe una conclusión propia y acotada.

En definitiva

Conserve la alerta externa, identifique responsables de los datos pertinentes y evalúe el uso de cuentas. Mantenga la atención mientras la pregunta sobre acceso a información recibe una conclusión propia y acotada.

R

CASO R

Un incidente multinacional con una consecuencia chilena reportada

Manufactura

Versión forense reportada

EVENTO REPORTADO	Noticias de agosto describen un incidente de ransomware de marzo en un grupo manufacturero multinacional. Señalan que también se cifró almacenamiento en la operación chilena. [S64]
LÍMITE DE ATRIBUCIÓN	El artículo atribuye su evaluación del actor a una investigación forense reportada. Este informe no adopta de manera independiente esa atribución ni un volumen de datos afirmado.
LÍMITE GEOGRÁFICO	La cronología comenzó fuera de Chile. La consecuencia local reportada no convierte todo el incidente multinacional en un evento exclusivamente nacional.
RESPUESTA	Mapee dependencias compartidas de identidad, almacenamiento y soporte entre entidades del grupo. Pruebe cómo la operación chilena restaura su servicio necesario cuando no está disponible un recurso controlado por el grupo.

En definitiva

Mapee dependencias compartidas de identidad, almacenamiento y soporte entre entidades del grupo. Pruebe cómo la operación chilena restaura su servicio necesario cuando no está disponible un recurso controlado por el grupo.

CASO S

S

Evento de cuenta administrativa en un organismo público regional

Noticias locales

Administración regional

VERSIÓN REPORTADA	Noticias de marzo describen un evento del 1 de marzo con una cuenta administrativa, un cambio de contraseña y acceso a servicios institucionales. También reportan una denuncia penal. [S65]
LÍMITE	Esta versión se basa en las noticias regionales citadas. La ubicación de una dirección de origen no establece la identidad del operador.
LÍMITE DE IMPACTO	Una cantidad pequeña de datos reportada no establecería por sí sola consecuencias bajas. Permisos, sensibilidad y continuidad del acceso requieren evaluaciones separadas.
RESPUESTA	Revise permisos, sesiones y configuración de recuperación de la cuenta. Confirme qué servicios institucionales eran accesibles y conserve la cronología que respalda la denuncia.

En definitiva

Revise permisos, sesiones y configuración de recuperación de la cuenta. Confirme qué servicios institucionales eran accesibles y conserve la cronología que respalda la denuncia.

5.11 Servicios jurídicos y cuentas de publicación de contenidos

CASO T

T

Denuncia de ransomware y versión de recuperación de una firma jurídica

Denuncia reportada

Servicios jurídicos

EVENTO REPORTADO	Un artículo de mayo fecha un mensaje de extorsión el 22 de abril. Describe un informe interno y una denuncia sobre información cifrada o eliminada y sistemas indisponibles. La firma confirmó denuncia y recuperación con especialistas externos. [S70]
VERSIÓN OPERACIONAL	La firma dijo que la actividad jurídica normal continuaba. Esa declaración posterior tiene un alcance distinto de los efectos de sistemas reportados antes y debe conservar su fecha.

LÍMITE DE ATRIBUCIÓN	Las amenazas usaban la identidad Akira. Este informe la trata como el nombre reportado de quien hizo la afirmación, sin determinar de manera independiente identidad del operador, origen o vínculo con otro caso.
RESPUESTA	Pruebe la restauración de registros de asuntos jurídicos, comunicaciones esenciales y acceso a documentos de trabajo. Conserve las evaluaciones de acceso privilegiado e información de clientes separadas de una declaración de continuidad profesional.

En definitiva

Pruebe la restauración de registros de asuntos jurídicos, comunicaciones esenciales y acceso a documentos de trabajo. Conserve las evaluaciones de acceso privilegiado e información de clientes separadas de una declaración de continuidad profesional.

U

CASO U

Exposición de cuentas de publicación con servicios principales excluidos

Servicios públicos

Versión oficial reportada

DECLARACIÓN REPORTADA	Dos noticias de mayo recogen la misma respuesta institucional a una alerta de cuentas. La declaración limita el asunto a cuentas de publicación de noticias y dice que los servicios operacionales principales no estaban afectados. [S83][S84]
RESPUESTA DESCRITA	La institución reportó protección adicional de autenticación y acciones legales. La alerta y la declaración posterior pertenecen a un caso de cuentas, sin ser dos incidentes por aparecer en dos medios.
LÍMITE	La declaración citada no es una evaluación forense independiente de cada medio. No respalda extender el evento a todos los sistemas institucionales ni inferir la identidad del operador.
RESPUESTA	Revise permisos de publicación, acceso delegado, recuperación de cuentas y estado de sesiones. Confirme la integridad de comunicaciones públicas y evalúe por separado los servicios principales.

En definitiva

Revise permisos de publicación, acceso delegado, recuperación de cuentas y estado de sesiones. Confirme la integridad de comunicaciones públicas y evalúe por separado los servicios principales.

5.12 Más contexto de fuentes sin un recuento adicional de incidentes

Noticias de enero sobre una distribuidora energética describen un acceso reconocido a almacenamiento interno, notificación a autoridades y monitoreo reforzado. La empresa dijo que los datos personales de clientes, las contraseñas de acceso y las operaciones no estaban afectados. Las afirmaciones delictivas de robo seguían sin resolverse. La divulgación de enero no fecha la intrusión. [S74][S75]

Una respuesta de mayo de una organización del sector salud describe una anomalía contenida en sistemas institucionales y afirma ausencia de interrupción asistencial o extracción de información personal. Es su posición fechada. Debe leerse junto a la versión posterior de ANCI, sin demostrar que toda afirmación más amplia fuera falsa. [S77][S7]

Instructure, un proveedor global de plataforma educativa, también confirma eventos de seguridad de abril y mayo y mitigaciones posteriores. Su versión no identifica clientes chilenos ni establece acceso a información específica de Chile. De esa declaración global no se infiere ninguna institución local ni otra intrusión chilena. [S76]

5.13 Exclusiones importantes y avisos que no son incidentes

Un caso de estudio manufacturero de septiembre dice que el evento ocurrió en Nochebuena sin establecer el año. La fecha de publicación no basta para clasificarlo como nuevo incidente de 2026. Queda fuera de recuentos de incidentes fechados en 2026. [S49]

Una noticia de agosto sobre respuesta preventiva de ANCI ante una situación de cadena de suministro también requiere cautela. La agencia describió exposición potencial y notificaciones a instituciones posiblemente afectadas. Distinguió expresamente esa posición de un incidente confirmado de impacto significativo en ese momento. [S48]

La noticia que retransmite una afirmación de extorsión sobre un asegurador de salud describe una publicación de actor sin confirmación empresarial o de autoridad. Su alcance afirmado no se adopta como incidente de salud verificado. La población del capítulo 7 sigue separada de los casos organizacionales reportados antes. [S37]

Un anuncio de persecución penal es otra población distinta. Noticias de septiembre describen a Fiscalía y PDI investigando presuntos accesos ilícitos, uso de credenciales, agregación y venta de datos. Continuaban investigación y examen de dispositivos. Una acusación no es condena ni prueba que todas las afirmaciones públicas anteriores pertenecieran al caso. [S47]

CONCLUSIONES CLAVE

01

Distinga acceso real a cuentas, republicación histórica, posible exposición de datos e interrupción del servicio.

02

La actividad reciente incluye orientaciones e interrupciones continuadas, además de eventos nuevos reportados.

03

Asigne a identidad, privacidad, fraude y recuperación operacional responsables y evidencias de cumplimiento separados.

CAPÍTULO 06

Hacktivismo, DDoS y disponibilidad de servicios

ESTE CAPÍTULO RESPONDE

¿Qué distingue una afirmación sobre disponibilidad de un acceso establecido o daño operacional?

3

preguntas separadas: estado del servicio, acceso a datos y atribución

6.1 Una afirmación necesita más que comprobar una página caída 55

6.2 Cronología de versiones públicas y contexto de respuesta 55

6.3 Afirmación frente a versión oficial 56

6.4 Las consecuencias operacionales requieren evidencia propia 56

6.5 Prepare una declaración pública acotada 57

6.6 Evidencia de cumplimiento para preparación de disponibilidad 57

CAPÍTULO 06

Hacktivismo, DDoS y disponibilidad de servicios

EN RESUMEN

Una afirmación sobre disponibilidad no establece acceso a registros, presencia persistente ni operador identificado. El caso reciente de servicio público ilustra versiones técnicas contrapuestas, sin una campaña nacional establecida. Las noticias de salud y energía también muestran consecuencias operacionales distintas por servicio. Verifique la tarea esencial del usuario, conserve la investigación de acceso y prepare una declaración que describa solo el impacto respaldado actualmente.

6.1 Una afirmación necesita más que comprobar una página caída

La noticia de noviembre sobre un servicio público es un ejemplo útil. Versiones anónimas alegaron phishing y malware persistente. ANCI indicó al medio que investigaba y sospechaba DDoS; la organización dijo que continuaba el análisis forense. La fuente no resuelve el mecanismo técnico. [S36]

6.2 Cronología de versiones públicas y contexto de respuesta

La cronología distingue declaraciones de fuentes y novedades reportadas. No conecta las filas en una sola campaña.

1 may 2026	**ANCI** Investiga publicaciones de datos reportadas; autenticidad y alcance sin resolver [S6]
8 may 2026	**ANCI** Identifica acceso con cuentas válidas y lo distingue de ataques a infraestructura [S7]
4 jul 2026	**Noticias de radio** Retransmiten una afirmación no confirmada sobre un organismo de servicio público; impacto y mecanismo no establecidos [S82]
27 ago 2026	**Coordinador eléctrico** El registro operacional indica desconexión de una instalación con ciberataque como causa reportada por el operador; ningún actor establecido [S53]
9 nov 2026	**Coordinador eléctrico** El registro operacional fechado aún indica 0% de disponibilidad para las unidades afectadas [S54]
11 nov 2026	**Noticias de prensa** La investigación de un servicio público contiene versiones contrapuestas de phishing, malware y sospecha de DDoS [S36]
15 nov 2026	**Coordinador eléctrico** El registro actualizado vuelve a indicar 0% de disponibilidad para las mismas unidades; evento existente [S86]

17 nov 2026 **Noticias de prensa**
Autoridades hospitalarias describen interrupción de reservas y atención clínica mantenida [S34]

18 nov 2026 **Noticias de prensa**
Reportan la desconexión continuada de la instalación energética [S35]

Los avisos de mayo tratan afirmaciones de acceso, sin demostrar un evento DDoS. Las filas de energía y hospitales corresponden a funciones operacionales distintas. Su inclusión muestra por qué el tipo de evidencia y la consecuencia deben permanecer visibles en una cronología de respuesta.

6.3 Afirmación frente a versión oficial

El panel siguiente separa las afirmaciones controvertidas del servicio público de lo respaldado por las noticias. No reproduce una cita directa de un actor.

Pregunta	Alegación reportada	Versión oficial reportada	Evaluación
Vía de entrada	Fuentes anónimas alegaron phishing [S36]	Había análisis forense en curso [S36]	No se adopta una vía de entrada establecida
Acceso persistente	Fuentes anónimas alegaron persistencia de malware [S36]	ANCI no había sido informada de ese mecanismo alegado [S36]	La persistencia sigue sin establecerse
Causa de indisponibilidad	La versión contiene explicaciones contrapuestas [S36]	ANCI dijo que sospechaba DDoS e investigaba [S36]	Una sospecha no es un hallazgo técnico final
Ventas de datos	Una interrupción puede acompañarse de especulación	La versión citada no establece una venta verificada	No inferir posesión, transferencia ni entrega comercial
Actuación regulatoria	Las alegaciones citadas no establecen una sanción verificada	ANCI dijo que no había aplicado multas [S36]	Conservar la posición declarada por la agencia en esa fecha

6.4 Las consecuencias operacionales requieren evidencia propia

La noticia hospitalaria distingue interrupción de reservas de atención clínica mantenida. Eso respalda pruebas separadas de continuidad administrativa y clínica. No establece que todos los procesos de pacientes estuvieran intactos ni que se preservara la confidencialidad de datos. [S34]

La versión energética describe una instalación y baterías que siguen desconectadas. No establece un apagón nacional. Su respuesta requiere aceptación operacional, no una instrucción genérica de reconectar equipos cuando un problema de red parece resuelto. [S35]

6.5 Prepare una declaración pública acotada

Una primera declaración útil identifica la función afectada, la alternativa actual y la hora de próxima actualización. Puede reconocer una investigación sin elegir un mecanismo de entrada no verificado. Debe separar una limitación confirmada del servicio de una posible consecuencia de privacidad.

6.6 Evidencia de cumplimiento para preparación de disponibilidad

Responsable	Ejercicio	Evidencia de cumplimiento
Responsable del servicio	Completar la tarea esencial de clientes o ciudadanía durante la degradación	Resultado presenciado e instrucciones utilizables de alternativa
Infraestructura	Activar la ruta acordada de respuesta de disponibilidad	Registro fechado de ejercicio de escalamiento y mitigación
Identidad y respuesta	Evaluar si la interrupción coincide con uso no autorizado de cuentas	Conclusión separada sobre acceso e incertidumbre restante
Operaciones	Aceptar el estado del servicio físico o clínico correspondiente	Aprobación operacional autorizada y lista de excepciones
Comunicaciones	Emitir una actualización limitada por la evidencia	Declaración aprobada con función afectada y próxima actualización
Asesoría jurídica	Revisar condiciones de notificación según hechos establecidos	Decisión registrada y cronología de conocimiento conservada

CONCLUSIONES CLAVE

01

Una afirmación publicada sobre disponibilidad no establece acceso persistente, ventas de datos ni identidad del actor.

02

Pruebe por separado el servicio esencial y el acceso.

03

Exija evidencia del responsable del servicio y una actualización pública acotada antes de declarar recuperación.

CAPÍTULO 07

Actores de amenazas y relaciones respaldadas

07

ESTE CAPÍTULO RESPONDE

¿Qué observaciones sobre actores están respaldadas y qué miden realmente las entradas?

41

publicaciones chilenas de ransomware en el periodo de observación

7.1 Las etiquetas describen una población de publicaciones 59
7.2 Las comparaciones regionales aportan contexto, sin clasificar seguridad 61
7.3 La fecha de publicación no es la fecha de intrusión 62
7.4 Relaciones respaldadas sin inferir un operador común 64
7.5 Las investigaciones y la persecución penal no completan la atribución 66
7.6 Prepárese para capacidades y conserve la incertidumbre sobre actores 66
7.7 Un ejemplo global de vulnerabilidad sin afirmar explotación en Chile 66

CAPÍTULO 07

Actores de amenazas y relaciones respaldadas

EN RESUMEN

Ransompedia registra 41 entradas chilenas con 13 etiquetas de quienes hacen las afirmaciones. Qilin y The Gentlemen reúnen 26, o el 63.4%. Son publicaciones delictivas, sin confirmar intrusiones ni organizaciones jurídicas únicas. Las noticias públicas también describen investigaciones y persecución penal sin establecer un operador común entre casos. Prepárese para extorsión y uso indebido de identidad, y mantenga cada etiqueta de actor vinculada a la fuente específica que la respalda.

7.1 Las etiquetas describen una población de publicaciones

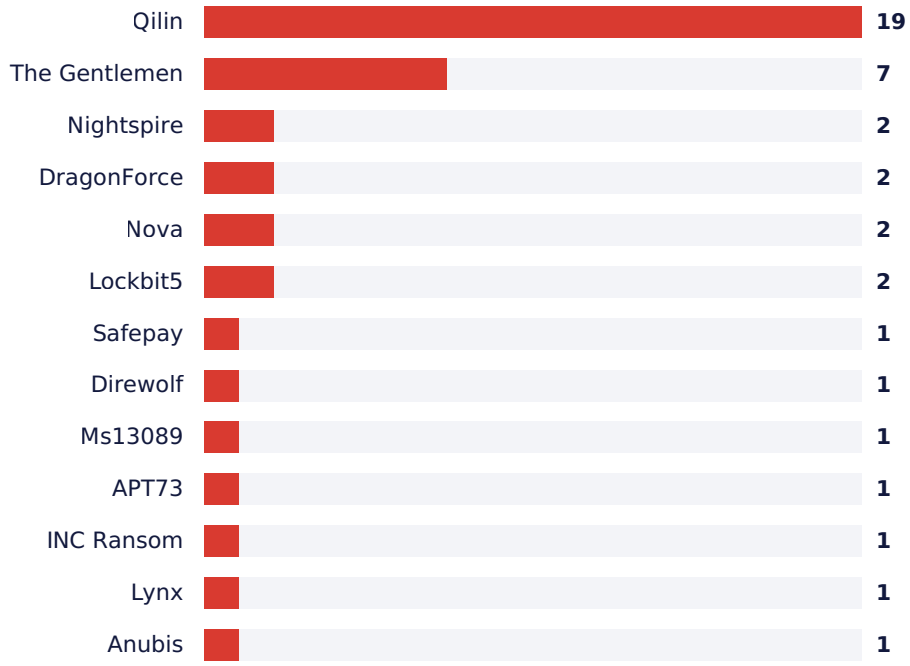
La población chilena conservada contiene 41 filas de entradas fechadas y 39 cadenas distintas de nombres de organizaciones. Ninguna medida establece un recuento de organizaciones jurídicas validado de manera independiente. Nombres repetidos, estructuras de grupos y afirmaciones delictivas subyacentes necesitan evaluación separada. [S2]

Una etiqueta de ransomware identifica el nombre usado en la fuente de la entrada. No demuestra que cada fila usara el mismo afiliado, vía de acceso o malware. Una entrada tampoco establece cifrado, información copiada, pago ni magnitud del daño.

Las etiquetas principales son Qilin y The Gentlemen. Su participación conjunta muestra concentración en esta población conservada. No mide su participación en todos los incidentes de Chile ni la probabilidad de que el lector enfrente a alguno de los grupos. [S2]

El gráfico y la tabla siguientes distinguen las etiquetas principales del resto de la población.

Qilin y The Gentlemen reúnen 26 de 41 entradas chilenas



Fuente: Brandefense Ransompedia, 1 de enero-22 de noviembre de 2026; noviembre parcial [S2]. Las filas son afirmaciones delictivas, no intrusiones confirmadas ni una clasificación nacional de riesgo.

Etiqueta	Entradas	Participación	Significado
Qilin	19	46.3%	Publicaciones con esta etiqueta de quien afirma
The Gentlemen	7	17.1%	Publicaciones con esta etiqueta de quien afirma
Otras 11 etiquetas	15	36.6%	Resto de etiquetas combinadas
Total	41	100.0%	Filas chilenas de entradas en el periodo de observación

Qilin

Etiqueta de entrada de extorsión | No se evalúa atribución estatal

EN CHILE, 2026

2026

19 entradas etiquetadas como Chile en el periodo del informe

OBJETIVOS REIVINDICADOS

Solo la población conservada de entradas etiquetadas por país; nombres de víctimas reservados

EN FUENTES PÚBLICAS

[S2] Ransompedia registra 19 entradas etiquetadas como Chile bajo esta etiqueta.

NUESTRA VALORACIÓN

Una entrada es una afirmación. No establece cifrado, extracción de datos, pago realizado ni un operador común entre todas las entradas.

CONFIANZA

Alta para el recuento conservado de la etiqueta; las afirmaciones subyacentes de incidentes siguen sin verificarse

The Gentlemen

Etiqueta de entrada de extorsión | No se evalúa atribución estatal

EN CHILE, 2026

2026

7 entradas etiquetadas como Chile en el periodo del informe

OBJETIVOS REIVINDICADOS

Solo la población conservada de entradas etiquetadas por país; nombres de víctimas reservados

EN FUENTES PÚBLICAS

[S2] Ransompedia registra 7 entradas etiquetadas como Chile bajo esta etiqueta.

NUESTRA VALORACIÓN

Use una entrada pertinente para validar datos propios y continuidad de servicio. La etiqueta no identifica a un operador individual ni establece un incidente consumado.

CONFIANZA

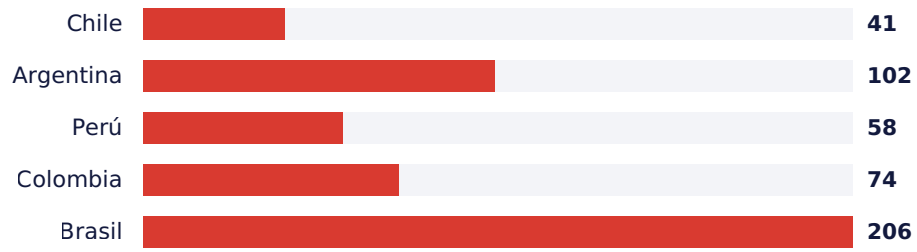
Alta para el recuento conservado de la etiqueta; las afirmaciones subyacentes de incidentes siguen sin verificarse

7.2 Las comparaciones regionales aportan contexto, sin clasificar seguridad

Argentina, Perú, Colombia y Brasil aportan comparación regional para el mismo periodo solicitado. Sus totales se muestran junto a Chile con la misma cautela sobre afirmaciones delictivas. Aquí no se controlan escala económica, poblaciones de organizaciones ni prácticas de divulgación. [S2]

Los países de comparación se seleccionaron como ejemplos únicamente para aportar contexto; su elección no implica una clasificación ni una valoración política.

Chile tiene 41 entradas conservadas frente a 58–206 de los cuatro países comparados



Fuente: Brandefense Ransompedia, 1 de enero–22 de noviembre de 2026; noviembre parcial [S2]. Las filas son afirmaciones delictivas, no intrusiones confirmadas ni una clasificación nacional de riesgo.

País	Filas de entradas	Interpretación
Chile	41	Población de entradas asociada al país
Argentina	102	Comparación regional sin ajuste poblacional
Perú	58	Comparación regional sin ajuste poblacional
Colombia	74	Comparación regional sin ajuste poblacional
Brasil	206	Comparación regional sin ajuste poblacional

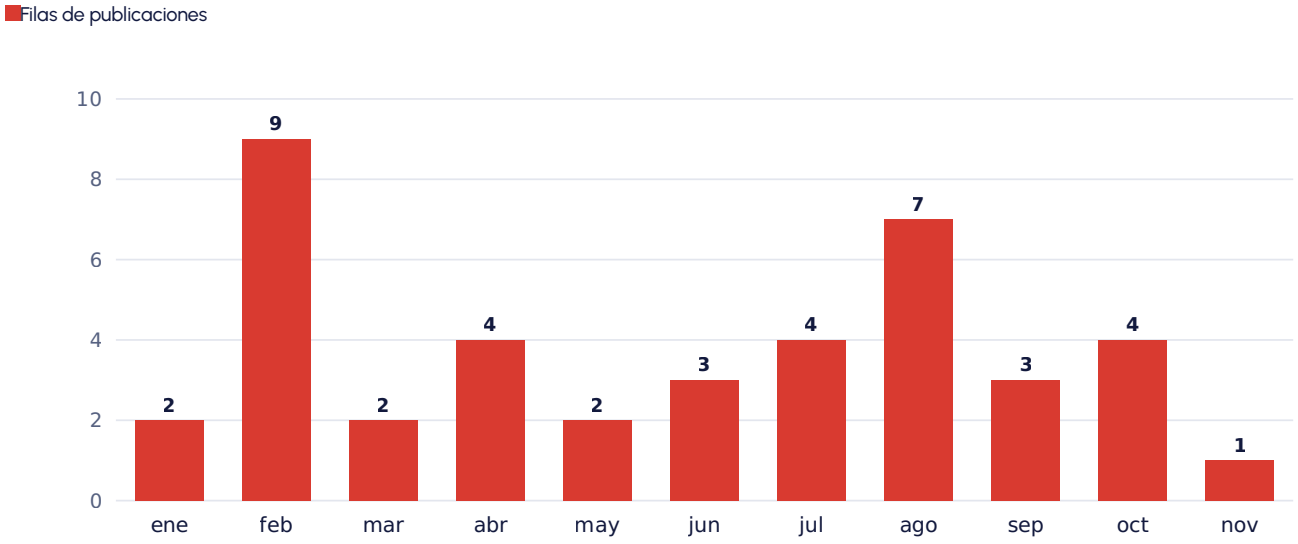
Los cuatro países tienen más filas conservadas que Chile. Eso no establece que las organizaciones chilenas sean más seguras ni que sus controles sean más eficaces. La tabla no aporta denominador de organizaciones comparables ni una tasa de éxito verificada de manera independiente.

El total chileno del año completo anterior es de 21 para 2025. Las 41 filas del periodo actual superan ese total anual. Se compara un año parcial con uno completo, por lo que no es una tasa de crecimiento de periodos equivalentes. [S2]

7.3 La fecha de publicación no es la fecha de intrusión

La serie mensual describe la fecha de los registros. No establece cuándo ocurrió el acceso inicial ni cuándo la organización descubrió un evento. Noviembre es un mes parcial al corte del informe. [S2]

La publicación de entradas varía por mes, sin filas conservadas en la quincena final



Fuente: Brandefense Ransompedia, 1 de enero-22 de noviembre de 2026; noviembre parcial [S2]. Las filas son afirmaciones delictivas, no intrusiones confirmadas ni una clasificación nacional de riesgo.

Mes	Entradas chilenas	Mes	Entradas chilenas
Enero	2	Julio	4
Febrero	9	Agosto	7
Marzo	2	Septiembre	3
Abril	4	Octubre	4
Mayo	2	Noviembre hasta el corte	1
Junio	3	Total	41

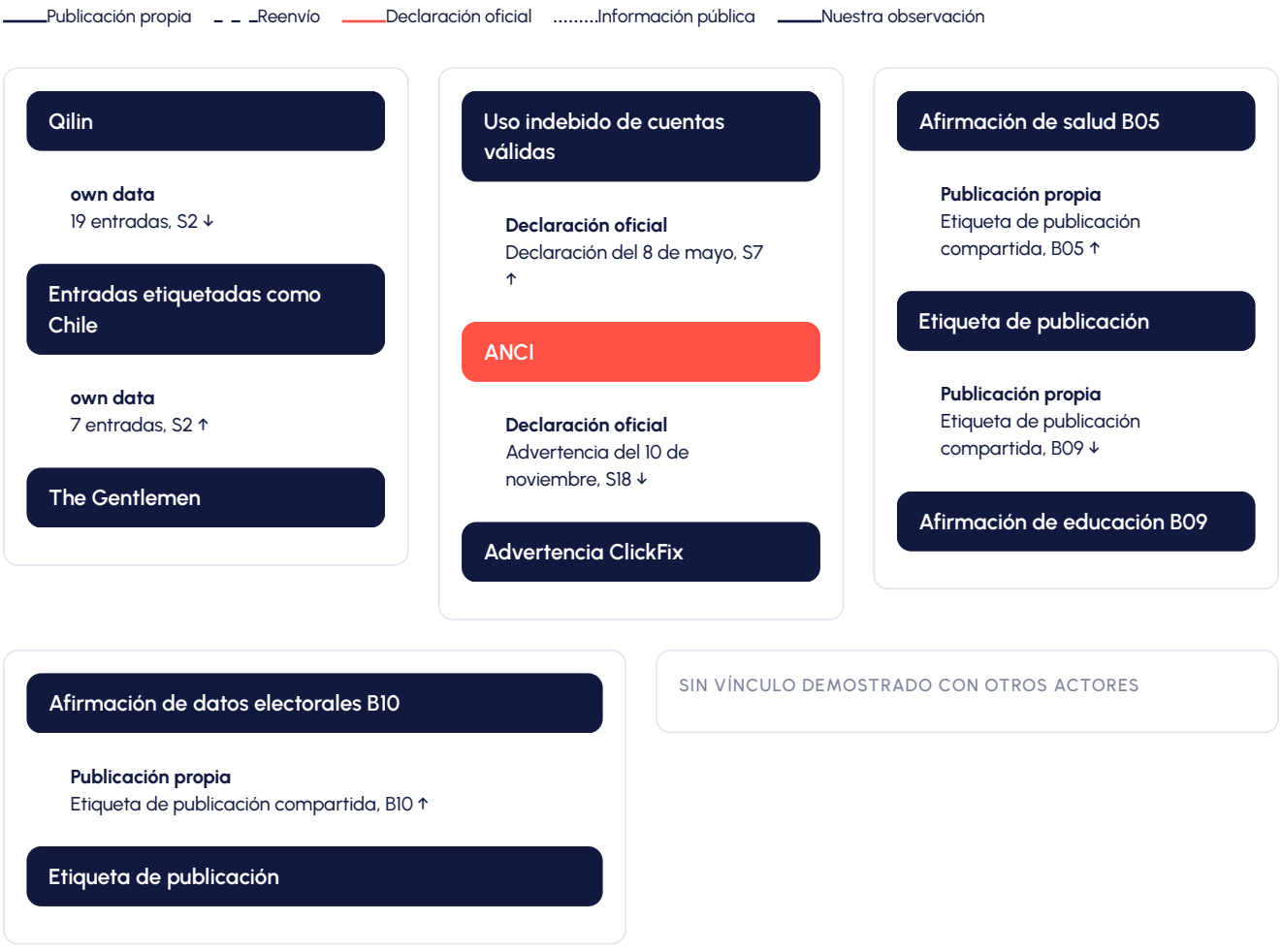
La única fila de noviembre está fechada el 2 de noviembre y lleva la etiqueta Qilin. Ninguna fila conservada cae en el 8–22 de noviembre. Es una declaración sobre esta población de fuentes, sin demostrar ausencia de actividad de ransomware en Chile durante la quincena final. [S2]

Una retransmisión pública también describe una afirmación Qilin no verificada sobre un asegurador de salud. Esa versión carecía de confirmación empresarial o de autoridad y de alcance técnico. La retransmisión no se convierte en confirmación independiente de la afirmación delictiva subyacente. [S37]

Otras retransmisiones públicas describen una entrada sobre una financiera en septiembre y una afirmación sobre una empresa marítima en abril. No establecen incidentes confirmados por empresas ni consecuencias operacionales verificadas. Sus fechas describen visibilidad de entradas o afirmaciones, sin establecer independientemente fechas de intrusión. [S72][S73]

7.4 Relaciones respaldadas sin inferir un operador común

El mapa relaciona una fuente con la proposición que respalda. No conecta actores separados mediante una etiqueta nacional compartida, una técnica similar o un tema político común.



Las relaciones de fuentes también pueden leerse en una tabla.

Fuente	Relación respaldada	Qué no establece
Ransompedia	Las etiquetas Qilin y The Gentlemen aparecen en la población chilena [S2]	Operador común en cada entrada o intrusión confirmada
Actualización de ANCI de mayo	Se identificó acceso con cuentas válidas en las afirmaciones investigadas [S7]	Actor identificado o acceso a todo el Estado
Noticias de investigación de telecomunicaciones	Autoridades investigaron actividad de red con información de autoridades estadounidenses [S45]	Atribución estatal propia de este informe o total de datos de usuarios finales
Noticias de persecución penal de septiembre	Fiscalía y PDI persiguieron presuntos accesos ilícitos y comercio de datos [S47]	Condena o vínculo con cada anuncio anterior
Noticias de servicio público	Las versiones técnicas diferían mientras seguía la investigación [S36]	Vía de entrada establecida, acceso persistente o venta verificada

Las relaciones de Ransompedia son de datos propios en este informe. Las declaraciones oficiales y las noticias siguen siendo tipos de fuente distintos. Su cercanía en el diagrama no implica acuerdo sobre un actor ni que describan el mismo evento.

La publicación de salud B05, la de educación y fotografías B09 y la de datos electorales B10 comparten la misma etiqueta visible de publicación en el material conservado. Esto respalda una asociación de publicaciones, sin establecer que una persona verificada operara la etiqueta. [S1]

Etiqueta de publicación entre sectores

Alias reservado

Asociación a nivel de fuente | No se evalúa atribución política ni estatal

EN CHILE, 2026

2026-10-29
B05 afirmación conservada

2026-11-20
B09 afirmación conservada

2026-11-22
B10 afirmación conservada

OBJETIVOS REIVINDICADOS

Roles de salud, educación y datos electorales en anuncios separados no verificados

EN FUENTES PÚBLICAS

[S1] La misma etiqueta de publicación aparece en B05, B09 y B10.

NUESTRA VALORACIÓN

Esto respalda una asociación entre anuncios conservados. No establece un solo operador humano, intrusión compartida, archivos idénticos ni infraestructura afectada común.

CONFIANZA

Alta para la asociación observada de etiqueta de publicación; las afirmaciones subyacentes de datos y acceso siguen sin verificarse

La asociación no establece datos comunes, intrusión compartida, infraestructura común ni motivo político. La autenticidad, procedencia y consecuencias afirmadas de cada publicación permanecen separadas. Se reserva la etiqueta y no se reproduce ninguna vía de contacto.

7.5 Las investigaciones y la persecución penal no completan la atribución

Noticias de telecomunicaciones de agosto mencionan malware y una etiqueta de actor al describir una investigación de PDI y Fiscalía. Parte de la actividad observada data de 2024. La fecha de noticia no debe convertirse en una nueva fecha de entrada. La atribución permanece vinculada a la fuente. [S45]

Noticias de septiembre describen detención e investigación formal por acceso ilícito, uso de credenciales, agregación y venta de datos. Continuaban examen y correlación de dispositivos. Aquí no se identifica a ningún imputado y una acusación no se trata como condena. [S47]

7.6 Prepárese para capacidades y conserve la incertidumbre sobre actores

Un mensaje pertinente de quien hace una afirmación debe llegar a un responsable de respuesta. Este debe evaluarla con evidencia propia y la versión del responsable del servicio. Registre si queda corroborada, contradicha, histórica o sin resolver.

7.7 Un ejemplo global de vulnerabilidad sin afirmar explotación en Chile

El siguiente ejemplo de control está separado de las afirmaciones chilenas sobre actores y acceso. El registro de NVD y el aviso del proveedor tratan una vulnerabilidad de soporte remoto. No establecen instalación del producto afectado ni explotación en una organización chilena seleccionada. [S68][S69]

Referencia	Alcance afectado	Corrección verificada	Límite
CVE-2026-1731	Proveedor: Remote Support 25.3.1 y anteriores; Privileged Remote Access 24.3.4 y anteriores	Parches de rama BT26-02-RS / BT26-02-PRA; Remote Support 25.3.2 o posterior; la orientación de mitigación de PRA indica 25.1.1 o posterior	Seguir las instrucciones admitidas del proveedor para la rama instalada

NVD describe un límite de configuración de PRA anterior a 25.1; la mitigación del proveedor indica 25.1.1 o posterior. Conserve esa diferencia, sin inventar una versión intermedia corregida. Actualizar un producto tampoco establece de manera independiente si hubo acceso no autorizado previo. [S68][S69]

Las ramas de parches del proveedor cubren Remote Support 21.3–25.3.1 y PRA 22.1–24.X. Las versiones antiguas sin soporte necesitan una actualización admitida, sin asumir un parche. Siga las instrucciones del proveedor para la versión instalada. [S68]

La oferta bancaria del Caso C no tiene conexión establecida con esta vulnerabilidad. Un registro global aporta contexto de control, sin completar la vía de entrada o atribución que faltan.

CONCLUSIONES CLAVE

01

Qilin y The Gentlemen encabezan la población conservada, sin constituir un censo nacional verificado de incidentes.

02

Los recuentos regionales y fechas mensuales de publicación no establecen seguridad comparativa ni momento de intrusión.

03

Separe las relaciones entre fuente y proposición de la atribución de operador común.

CAPÍTULO 08

La economía del fraude

ESTE CAPÍTULO RESPONDE

¿Cómo puede la información creíble apoyar el engaño y qué respuesta puede interrumpirlo?

Verifique

un detalle plausible no autentica una solicitud

8.1 Información y monetización son proposiciones separadas 69
8.2 Ofertas de préstamos y cobros coercitivos 69
8.3 El contexto real no autentica 70
8.4 Suplantación de organismos y avisos inseguros 70
8.5 Material de tarjetas de pago: una observación acotada 70
8.6 La persecución penal es una población de evidencia separada 71
8.7 Evidencia de cumplimiento para protección contra fraude 71

CAPÍTULO 08

La economía del fraude

EN RESUMEN

Las advertencias públicas describen ofertas de préstamos, cobros coercitivos, suplantación bancaria, mensajes de reservas y empleos falsos. Los casos clandestinos anuncian información y acceso sin demostrar transacciones realizadas. La pregunta defensiva común es si una persona puede verificar una solicitud plausible por una vía confiable. Mantenga separadas ofertas, reportes de clientes, alegaciones delictivas y pagos validados; capacite a los equipos de atención y aprobación correspondientes.

8.1 Información y monetización son proposiciones separadas

Archivos de proveedores, registros escolares, información de salud y anuncios de acceso pueden generar preocupaciones distintas. El lenguaje comercial de una publicación no establece posesión ni venta realizada. Una afirmación de divulgación gratuita no establece autenticidad ni elimina la posible consecuencia de privacidad. [S1]

Lo siguiente es un **modelo analítico** para planificar. Conecta información, contacto creíble, una acción solicitada y un posible pago. No establece que el mismo operador controlara esas etapas en los casos chilenos.

Etapa	Abuso posible	Interrupción defensiva
Hay información disponible	El contexto personal hace convincente un mensaje	Establecer categorías afectadas y atención adecuada
Se inicia el contacto	Una llamada o mensaje imita un servicio confiable	Proporcionar una vía de contacto verificada de forma independiente
Se solicita una acción	Se pide un código, pago o aprobación de recuperación	Explicar el proceso legítimo y el escalamiento
Se intenta un pago	Un destino cambiado o anticipo desvía dinero	Aplicar controles de pago y fraude de la organización
Continúa el contacto	El contexto anterior respalda otro acercamiento	Vincular reportes respaldados y actualizar la advertencia

8.2 Ofertas de préstamos y cobros coercitivos

Los avisos de CMF de marzo y abril describen denuncias sobre ocho y cuatro entidades, respectivamente, que ofrecieron créditos tras anticipos sin entregar los préstamos. El aviso de noviembre describe otra oferta en línea reportada y una denuncia. Son versiones regulatorias atribuidas, sin constituir condenas. [S42][S43][S26]

CMF también advirtió sobre trece aplicaciones de crédito en junio y tres en noviembre, con cobros extorsivos y sospechas de usura. Los recuentos de aplicaciones no son de deudores, grupos delictivos o incidentes de ransomware. Los avisos no aportan denominador nacional de pérdidas financieras. [S28][S25]

8.3 El contexto real no autentica

La advertencia de ANCI sobre bloqueos bancarios describe a un estafador que provoca un bloqueo y después suplanta al banco para pedir un código o autorización. Un problema de cuenta coincidente puede, por tanto, formar parte del engaño. [S21]

Su advertencia sobre reservas explica que detalles reales pueden hacer creíble una solicitud maliciosa de pago. Esos detalles no establecen control del servicio legítimo por el remitente ni acceso a su infraestructura subyacente. [S22]

En noviembre, ANCI advirtió sobre empleos falsos que buscan información personal, pagos o códigos de recuperación de aplicaciones de mensajería. Recursos humanos y atención al cliente deben saber derivar a procesos auténticos de postulación o soporte. No autentique el contacto mediante el remitente sospechoso. [S20]

8.4 Suplantación de organismos y avisos inseguros

La advertencia tributaria de ANCI describe mensajes fraudulentos que imitan servicios públicos relacionados con impuestos. Su ejemplo de correo de febrero imita una empresa estatal. Suplantar una institución no establece acceso a sus sistemas. [S23][S24]

La advertencia ClickFix describe avisos falsos de error o verificación humana que persuaden a seguir instrucciones inseguras. El mensaje defensivo pertinente es detenerse y usar una vía confiable de soporte. Este informe no reproduce comandos ni un flujo ofensivo. [S18]

La orientación de ANCI tras un clic distingue recibir un mensaje de ingresar credenciales o datos bancarios. La respuesta empresarial también debe establecer qué hizo realmente la persona y qué servicio estuvo involucrado. No prescriba la misma acción disruptiva para cada reporte. [S19]

8.5 Material de tarjetas de pago: una observación acotada

ALCANCE DE LAS CIFRAS DE TARJETAS

Estas cifras describen una población observada limitada de material de tarjetas de pago. No establecen la prevalencia nacional, la posibilidad de uso actual, transacciones realizadas ni pérdidas por fraude.

El material conservado contiene 288 registros distintos de tarjetas de pago asociados a Chile. Es una observación acotada de material publicado, sin constituir un censo de emisores chilenos ni medir uso actual posible. No se infiere una transacción fraudulenta realizada ni un total de pérdidas. [S4]

Fuente: observaciones acotadas de tarjetas de pago basadas en publicaciones [S4]. El material publicado no establece de manera independiente uso actual posible, pago fraudulento realizado ni origen de exposición. No se reproduce ningún identificador personal o de tarjeta de pago.

8.6 La persecución penal es una población de evidencia separada

Noticias de septiembre describen a Fiscalía y PDI persiguiendo presuntos accesos ilícitos, credenciales, agregación y venta. El examen y la correlación de dispositivos continuaban. La versión no demuestra que existiera cada conjunto anunciado ni que toda afirmación anterior perteneciera a la investigación. [S47]

El aviso de coordinación de Fiscalía de agosto identifica variantes de fraude financiero y una mesa nacional de cooperación. Respalda atender la coordinación entre instituciones. Los totales históricos del aviso no se adoptan como incidencia nacional de 2026. [S29]

Las advertencias de CMF de enero y febrero sobre plataformas de inversión tratan registro y autorización legal para prestar servicios regulados. La falta de autorización no es por sí sola condena por fraude. El lector debe verificar la condición del proveedor por la vía oficial competente. [S40][S41]

Una medida judicial de agosto se refiere a un empleado acusado de vender información de una investigación. Es una alegación investigada, sin constituir condena ni evidencia de intrusión externa. El contexto respalda revisar accesos privilegiados y manejo de información sin vincularlo a incidentes separados de publicación de cuentas. [S78]

8.7 Evidencia de cumplimiento para protección contra fraude

Responsable	Capacidad	Evidencia de cumplimiento
Atención al cliente	Reconocer suplantación y coerción plausibles	Ejercicio de personal y registro de escalamiento
Tesorería	Verificar instrucciones modificadas por una vía confiable	Registro aprobado de verificación de pago
Fraude	Evaluar autorizaciones y transacciones pertinentes	Decisión acotada con evidencia de respaldo
Privacidad	Identificar información útil para contactos posteriores	Evaluación de categorías de datos y advertencia adecuada
Seguridad	Distinguir un mensaje de un evento de cuenta o dispositivo	Conclusión de respuesta fechada

CONCLUSIONES CLAVE

01

El contexto personal exacto y la aprobación regulatoria afirmada no autentican una solicitud.

02

Mantenga separados los productos anunciados, las denuncias regulatorias y las consecuencias financieras validadas.

03

Dé al personal y los clientes una vía confiable de verificación que haya sido probada.

CAPÍTULO 09

Banca y servicios financieros

ESTE CAPÍTULO RESPONDE

¿Qué observaciones financieras requieren acciones sobre cuentas, clientes o continuidad?

25

dominios seleccionados de banca, pagos e inversión, no un censo bancario

9.1 Conserve los denominadores financieros 74
9.2 Una oferta administrativa no establece acceso a todo un banco 75
9.3 Una declaración de continuidad tiene alcance fechado 75
9.4 Acceso institucional y fraude al cliente necesitan responsables paralelos 76
9.5 Las obligaciones de autenticación requieren evaluar cada recorrido 76
9.6 Dependencias de proveedores y evidencia de cumplimiento 76

CAPÍTULO 09

Banca y servicios financieros

EN RESUMEN

Los servicios financieros enfrentan preguntas separadas sobre acceso institucional, engaño a clientes, proveedores y autenticación. La cartera de banca, pagos e inversión tiene 25 dominios; otros 25 abarcan seguros y pensiones. Las observaciones pasivas no establecen intrusiones bancarias ni exposición actual de clientes. Un anuncio de acceso privilegiado sigue sin verificarse. Valide la cuenta específica, mantenga una verificación confiable para clientes y pruebe en paralelo las decisiones aplicables de autenticación y notificación.

9.1 Conserve los denominadores financieros

El grupo financiero seleccionado incluye bancos, servicios de pago y organizaciones de inversión. Sus 25 dominios no son 25 bancos validados de manera independiente. Seguros y pensiones forman otro conjunto de 25 dominios seleccionados, con servicios y poblaciones de cuentas distintos. [S5]

Sector seleccionado	Dominios evaluados	Política DMARC	Cabecera HSTS
Banca, pagos e inversiones	21	16 / 21	7 / 8 respuestas
Seguros y pensiones	23	21 / 23	18 / 19 respuestas

La columna DMARC cuenta políticas observadas que solicitan cuarentena o rechazo. No demuestra aplicación efectiva para cada mensaje legítimo. Los recuentos HSTS conservan el denominador menor de respuestas HTTPS disponibles. [S3]

El grupo de 25 dominios de banca, pagos e inversión contiene 151,575 asociaciones de dispositivos, incluidas 1,151 asociaciones de dispositivos de trabajadores. Tiene 249,271 asociaciones de registros de credenciales, 17 dominios con anuncios vigentes y 2,359 asociaciones documentales. Son observaciones superpuestas, no intrusiones bancarias confirmadas. [S210]

Seguros y pensiones contiene 124,175 asociaciones de dispositivos, incluidas 431 asociaciones de dispositivos de trabajadores. Tiene 67,612 asociaciones de registros de credenciales, 17 dominios con anuncios vigentes y 185 asociaciones documentales. No se publican calificaciones institucionales, sectoriales ni por grupo. [S210]

La vista de bancos emisores abarca 10 dominios emisores dentro de la cartera bancaria seleccionada. Contiene 112,293 asociaciones de dispositivos no vinculadas a empleados, 940 asociaciones de trabajadores y 10 dominios con anuncios vigentes. Las asociaciones no vinculadas a empleados no establecen identidad del cliente ni titularidad bancaria del dispositivo. [S210]

ALCANCE DE LAS CIFRAS DE TARJETAS

Estas cifras describen una población observada limitada de material de tarjetas de pago. No establecen la prevalencia nacional, la posibilidad de uso actual, transacciones realizadas ni pérdidas por fraude.

La misma vista de bancos emisores contiene 136 asociaciones de tarjetas entre 6 emisores. Esta vista seleccionada es distinta de los 288 registros únicos de tarjetas asociados a Chile del capítulo 8. No establece un evento de exposición común ni una clasificación de seguridad bancaria. [S4][S210]

10

Dominios emisores dentro de la cartera bancaria seleccionada

112,293

Asociaciones de dispositivos no vinculadas a empleados en la vista de bancos emisores

940

Asociaciones de dispositivos de trabajadores en la vista de bancos emisores

El alcance de tarjetas anterior también rige la interpretación de la vista de bancos emisores. El material de tarjetas, los registros de credenciales y un anuncio de acceso no establecen origen común, validez actual ni pago fraudulento completado.

9.2 Una oferta administrativa no establece acceso a todo un banco

El Caso C contiene un anuncio de un portal administrativo vinculado a un banco. El autor afirmó tener usuarios, puntos de conexión y claves API. Otro participante cuestionó la credibilidad. Ninguna publicación establece acceso utilizable, permisos actuales ni transacción realizada. [S1]

La validación pertinente corresponde al proceso controlado de respuesta de la institución. Confirme la titularidad del servicio afirmado, la vigencia de la cuenta o clave y los permisos que podría ejercer. Revise actividad pertinente antes de decidir el alcance de contención.

9.3 Una declaración de continuidad tiene alcance fechado

Una declaración oficial de una institución financiera del 2 de mayo dice que sus plataformas y servicios funcionaban normalmente, ante reportes sobre datos personales del sector público. Es una declaración atribuida de continuidad, sin confirmar una intrusión bancaria. [S55]

9.4 Acceso institucional y fraude al cliente necesitan responsables paralelos

La advertencia de ANCI sobre bloqueo bancario describe un engaño que aprovecha un problema real de cuenta para respaldar un contacto fraudulento. El cliente puede enfrentar una solicitud convincente sin intrusión demostrada en la infraestructura bancaria. [S21]

9.5 Las obligaciones de autenticación requieren evaluar cada recorrido

CMF dice que la autenticación reforzada de clientes bajo NCG 538 entró plenamente en vigor el 1 de agosto. Su aviso se centra principalmente en transferencias y enrolamiento digital, con excepciones definidas sobre mecanismos de datos impresos. No convierta esa descripción en prohibición universal de cada mecanismo. [S27]

Cumplimiento debe identificar la transacción y norma pertinentes. Producto y arquitectura deben demostrar cómo el cliente autoriza la acción prevista. Fraude debe evaluar el engaño en ese recorrido, sin tratar una autenticación exitosa como prueba de intención legítima.

La propuesta de estándar MFA de ANCI abarca servicios esenciales y OIV, y sigue en consulta al corte. Las instituciones deben evaluar preparación conservando esa condición legal. Una propuesta y una obligación vigente de CMF no deben compartir una fecha de vigencia sin distinciones. [S15][S16]

9.6 Dependencias de proveedores y evidencia de cumplimiento

Pruebe si el proveedor puede explicar servicio afectado, periodo y categorías de datos mientras persiste la incertidumbre. Conserve momentos de conocimiento y la decisión de la institución receptora. Notificación, gestión de fraude y restablecimiento pueden necesitar responsables separados aunque compartan hechos.

Responsable	Pregunta	Evidencia de cumplimiento
Seguridad financiera	¿Está afectada una cuenta o servicio institucional pertinente?	Conclusión acotada de identidad y actividad
Fraude y atención	¿Puede el cliente verificar independientemente una solicitud sospechosa?	Vía de contacto probada y respuesta del personal
Producto y cumplimiento	¿Cumple el recorrido pertinente su obligación de autenticación?	Evaluación del recorrido, evidencia y excepciones
Responsable del proveedor	¿Puede apoyar la decisión propia de incidente de la institución?	Ejercicio conjunto de notificación y versión acotada
Continuidad de negocio	¿Pueden los clientes completar la tarea financiera esencial?	Prueba presenciada del servicio y su alternativa

CONCLUSIONES CLAVE

01

Las observaciones de dominios financieros, afirmaciones de acceso privilegiado y tarjetas de pago tienen poblaciones separadas.

02

Valide en paralelo acceso institucional y engaño al cliente con sus responsables correspondientes.

03

Pruebe autenticación, notificación de proveedores y recorridos esenciales según sus obligaciones reales.

CAPÍTULO 10

Regulación y respuesta nacional

10

ESTE CAPÍTULO RESPONDE

¿Qué obligaciones ya son aplicables y qué propuestas de noviembre necesitan verificar su estado?

3 horas

máximo legal de alerta temprana bajo la obligación pertinente del artículo 9

10.1 Distinga el instrumento de su estado actual 79
10.2 El artículo 9 requiere una cronología de conocimiento utilizable 80
10.3 La contención OIV es más específica que una instrucción genérica de restablecer contraseñas 81
10.4 Los límites sancionatorios no son estimaciones de pérdidas 83
10.5 La autenticación financiera es un requisito vigente 83
10.6 El documento MFA de ANCI de noviembre sigue siendo propuesta 83
10.7 La entrada en vigor de datos personales sigue siendo relevante 84
10.8 Haga operativas las vías nacionales de respuesta 84

CAPÍTULO 10

Regulación y respuesta nacional

EN RESUMEN

La Ley 21.663 establece un plazo breve de alerta temprana y deberes separados de actualización e informe final. La condición OIV agrega responsabilidades y puede acortar la actualización si se afecta el servicio esencial. La autenticación reforzada de CMF ya rige; el estándar MFA de ANCI de noviembre sigue en consulta. La postergación de la ley de datos requiere verificar promulgación. Asigne alcance legal, momentos de conocimiento, responsables y canales de notificación antes de un incidente.

Este capítulo apoya la planificación operacional. No sustituye asesoría jurídica sobre obligaciones de una entidad, modificaciones, normas sectoriales aplicables o hechos de un incidente específico.

10.1 Distinga el instrumento de su estado actual

La tabla siguiente separa los instrumentos principales de la evidencia citada.

Instrumento	Estado al corte	Obligación o novedad pertinente	Función responsable
Ley 21.663	Marco legal publicado	Notificación de incidentes del artículo 9; responsabilidades OIV reforzadas y tramos legales de sanciones [S13]	Asesoría jurídica, delegado de ciberseguridad y respuesta
Designación OIV	ANCI reportó el cierre de su primer proceso	1,154 entidades designadas en el proceso combinado; la designación no es un incidente [S11]	Responsable de entidad jurídica y cumplimiento
Instrucción General 4	Publicada en diciembre de 2025; ANCI explicó deberes en junio de 2026	Contención OIV, credenciales administrativas afectadas y controles de administración remota [S12][S14]	Delegado, identidad y operaciones
NCG 538 de CMF	CMF informa vigencia plena desde el 1 de agosto de 2026	Autenticación reforzada de clientes, principalmente para transferencias y enrolamiento digital, con excepciones definidas [S27]	Cumplimiento financiero, fraude y responsables de producto
Propuesta CMF de reportes bancarios	Consulta abierta el 17 de noviembre	Definiciones propuestas de ciberincidentes y alertas e información de reportes; comentarios hasta el 15 de diciembre [S87]	Cumplimiento financiero y respuesta

Instrumento	Estado al corte	Obligación o novedad pertinente	Función responsable
Estándar MFA de ANCI	Consulta pública abierta el 19 de noviembre	Requisitos propuestos para servicios esenciales y OIV, sin ser estándar final [S15][S16]	Arquitectura de seguridad y asesoría jurídica
Calendario de la Ley 21.719	Deben distinguirse la entrada en vigor original y un proyecto posterior	Fecha original 1 de diciembre de 2026; postergación en etapa de promulgación el 20 de noviembre [S30][S31][S32]	Responsable de privacidad y asesoría jurídica

El artículo 53 identifica organismos sujetos a regímenes especiales fuera de la regulación, fiscalización y supervisión de ANCI. Deben acordar mecanismos de notificación de incidentes y coordinación de respuesta. Asesoría jurídica debe establecer el régimen aplicable antes de tratar la secuencia ordinaria de ANCI como uniforme entre organismos públicos. [S209]

10.2 El artículo 9 requiere una cronología de conocimiento utilizable

Para las instituciones comprendidas en el artículo 4, el artículo 9 exige reportar ciberataques o incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27. Deben considerarse los regímenes especiales aplicables. [S209]

La ley original exige reportar lo antes posible, con un máximo de tres horas desde el conocimiento para la alerta temprana. Después exige actualización dentro de 72 horas. Para un OIV con prestación de servicios esenciales afectada, el periodo indicado de actualización es de 24 horas. El plazo del informe final se mide desde la alerta temprana. [S13]

Por eso, cada plazo pertinente necesita una entrada separada en el registro de incidentes.

Etapa	Máximo legal en el texto citado	Referencia del plazo	Responsable operacional	Evidencia operacional
Alerta temprana	3 horas	Conocimiento del incidente pertinente	Responsable de respuesta	Momento de conocimiento registrado, decisión sobre obligación y comprobante de envío
Actualización del incidente	72 horas	Conocimiento, según la secuencia pertinente del artículo 9	Responsable de respuesta	Alcance, impacto y respuesta actualizados
Actualización OIV por servicio afectado	24 horas	Conocimiento, cuando está afectada la prestación del servicio esencial	Delegado de ciberseguridad	Condición OIV y conclusión documentada de impacto al servicio

Etapa	Máximo legal en el texto citado	Referencia del plazo	Responsable operacional	Evidencia operacional
Plan de acción OIV	Adoptar dentro de 7 días corridos; informar al CSIRT Nacional tan pronto se adopte	Conocimiento del incidente	Delegado de ciberseguridad, con responsable de respuesta	Momentos de conocimiento y adopción registrados, plan adoptado y comprobante de envío
Informe final o de situación	15 días corridos	Envío de alerta temprana	Responsable de respuesta, con revisión jurídica	Informe final; si el incidente sigue en curso, lo reemplaza un informe de situación
Informe final tras un incidente continuado	15 días corridos	Se ha gestionado el incidente	Responsable de respuesta, con revisión jurídica	Fecha de gestión registrada, informe final y comprobante de envío

Si el incidente sigue en curso, presente un informe de situación en lugar del informe final inicial. Presente el informe final dentro de quince días corridos desde que se haya gestionado el incidente. No asuma que investigar asuntos sin resolver permite guardar silencio hasta conocer todos los hechos. Los responsables jurídicos y de respuesta deben preparar una versión acotada de hechos establecidos e incertidumbres pendientes. [S13]

10.3 La contención OIV es más específica que una instrucción genérica de restablecer contraseñas

La Instrucción General 4 establece los siguientes deberes OIV ante incidentes. Los responsables y registros de cumplimiento sugeridos permiten aplicarlos; estos cargos son recomendaciones. [S14]

Deber	Activación y alcance	Acción obligatoria	Responsable sugerido	Evidencia de cumplimiento
Contraseñas administrativas, artículo 2	Incidente que afecte confidencialidad, integridad de información o uso legítimo de recursos; sistemas afectados o sospechosos	Cambiar inmediatamente todas las contraseñas de cuentas con permisos totales o parciales de administración, dentro de tres horas desde el conocimiento. Informar a ANCI las cuentas modificadas en la alerta temprana.	Responsables de identidad e infraestructura	Horas de conocimiento y cambio; lista de cuentas y comprobante de envío

Deber	Activación y alcance	Acción obligatoria	Responsable sugerido	Evidencia de cumplimiento
Eliminación de cuentas administrativas, artículo 2	Misma activación y sistemas del artículo 2	Eliminar inmediatamente cuentas genéricas y las no asociadas a funcionarios o proveedores activos, dentro de tres horas desde el conocimiento. Crear antes una cuenta administrativa personal si no existe. Informar las cuentas eliminadas en la alerta temprana.	Responsables de identidad e infraestructura	Revisión de cuentas, creación de cuenta personal cuando corresponda, horas de eliminación y comprobante de envío
Accesos expuestos públicamente, artículo 3(a)	Cualquier incidente de ciberseguridad detectado; accesos remotos o administrativos expuestos públicamente a Internet	Revisar si existen accesos expuestos. Informar a ANCI los detectados en la alerta temprana y bloquearlos o darlos de baja dentro de tres horas desde el conocimiento.	Responsable de infraestructura, con responsable de respuesta	Revisión de exposición, horas de restricción y comprobante de envío
Acceso remoto durante incidentes, artículo 3(b–d)	Sistemas de acceso remoto expuestos a Internet y acceso remoto utilizado durante la gestión del incidente	Permitir acceso solo por la VPN institucional. Si no está disponible, restringir a segmentos o direcciones IP específicas indispensables; bloquear y registrar otros intentos de conexión. Usar credenciales aleatorias y MFA si resulta inmediatamente factible. Deshabilitar el acceso remoto al completar su tarea durante el incidente.	Responsables de infraestructura e identidad	Reglas de acceso, registros de conexión, configuración de autenticación y registro de deshabilitación

El artículo 2 exige además aplicar preventivamente las medidas de revisión y eliminación de cuentas de su segundo párrafo al menos cada seis meses. Los deberes ante incidentes se activan cuando concurren sus supuestos; los ejercicios programados de preparación del capítulo 12 no los postergan. [S14]

Ese requisito no es una instrucción universal de cambiar contraseñas en tres horas ante cualquier rumor u organización. Importan el alcance legal, la identidad afectada y los hechos aplicables. El equipo debe conocer las credenciales administrativas y sistemas sobre los que puede actuar bajo la obligación pertinente.

10.4 Los límites sancionatorios no son estimaciones de pérdidas

La ley original fija multas máximas distintas según gravedad y condición OIV. Son topes legales en UTM, sin predecir la sanción de un caso ni medir pérdidas cibernéticas. [S13]

Clasificación	Máximo general	Máximo OIV
Leve	5,000 UTM	10,000 UTM
Grave	10,000 UTM	20,000 UTM
Gravísima	20,000 UTM	40,000 UTM

La evaluación jurídica determina clasificación y procedimiento aplicables. La noticia de servicio público del capítulo 6 citó a ANCI diciendo que no había aplicado multas en ese caso. No convierta controversias, investigación o un titular de prensa en sanción concluida. [S36]

10.5 La autenticación financiera es un requisito vigente

El aviso de CMF del 31 de julio dice que NCG 538 entró plenamente en vigor el 1 de agosto de 2026. Destaca autenticación reforzada para transferencias y enrolamiento digital. Describe excepciones definidas de mecanismos de datos impresos, sin respaldar que todos quedaran universalmente prohibidos. [S27]

La advertencia de ANCI sobre cuentas bancarias refuerza la distinción. Una llamada puede aprovechar un bloqueo real para pedir un código o autorización. El problema real del cliente no autentica a quien llama. Proporcione una vía confiable de verificación independiente del contacto sospechoso. [S21]

Otra consulta de CMF, abierta el 17 de noviembre, trata archivos de reportes bancarios: definiciones de ciberincidentes y alertas e información usada para describir incidentes. Acepta comentarios hasta el 15 de diciembre. Es una propuesta, sin constituir un cambio final de las obligaciones de notificación vigentes. [S87]

10.6 El documento MFA de ANCI de noviembre sigue siendo propuesta

El 19 de noviembre, ANCI abrió una consulta de 30 días sobre un estándar propuesto de MFA y prevención de incidentes para servicios esenciales y OIV. El proyecto aborda cuentas humanas, administración remota y acceso a tecnología operacional. Su publicación no hace vigente cada disposición propuesta. [S15][S16]

Los considerandos del proyecto tratan accesos con credenciales válidas en incidentes significativos reportados desde marzo de 2025 hasta la fecha del documento. Ese periodo difiere del informe. El considerando no debe convertirse en participación nacional de incidentes de enero–noviembre de 2026 ni en estadística de publicaciones de Brandefense. [S16]

10.7 La entrada en vigor de datos personales sigue siendo relevante

La historia legislativa de BCN registra publicación de la Ley 21.719 el 13 de diciembre de 2024 y entrada en vigor original el 1 de diciembre de 2026. El aviso de la Cámara del 20 de noviembre dice que la postergación pasó a promulgación. La fecha sustitutiva prevista es el 15 de octubre de 2027. [S30][S31]

El informe de comisión identifica el boletín 18.623-07 y describe el cambio de fecha propuesto. El seguimiento oficial registra que el proyecto se encuentra en trámite de aprobación presidencial y fue despachado al Ejecutivo. Ninguno es una modificación promulgada. El avance parlamentario citado no establece promulgación y publicación en el Diario Oficial al corte del informe. [S32][S50]

El responsable jurídico debe verificar ese paso final de inmediato y nuevamente antes del 1 de diciembre de 2026. Mantenga el plazo original salvo que una modificación publicada y verificada lo cambie. Registre instrumento, publicación y vigencia comprobados. No revise un cronograma de proyecto solo porque los legisladores aprobaron una postergación.

La misma distinción se aplica a la futura autoridad de protección de datos. Una propuesta parlamentaria sobre su composición no evidencia que ya opere bajo el marco modificado. No infiera de esa propuesta un regulador activo, una vía de notificación o una sanción. [S31]

10.8 Haga operativas las vías nacionales de respuesta

El anuncio de ANCI de octubre describe reportes ciudadanos y un primer ejercicio nacional de ciberseguridad. El aviso de Fiscalía de agosto describe coordinación nacional contra fraude financiero. Son funciones distintas. Una organización debe identificar contactos apropiados de incidentes y fraude antes de asumir que una notificación satisface toda necesidad. [S10][S29]

CONCLUSIONES CLAVE

01

Conserve el plazo de alerta de tres horas y los requisitos separados de actualización e informe final.

02

Aplique deberes OIV y financieros a la entidad, servicio y transacción pertinentes.

03

Confirme el estado jurídico final de MFA y ley de datos antes de presentar propuestas como normas vigentes.

CAPÍTULO 11

Perspectivas y planificación condicional

11

ESTE CAPÍTULO RESPONDE

¿Qué preparaciones se desprenden de la evidencia y qué cambiaría esas prioridades?

6

juicios de planificación acotados con señales explícitas de revisión

11.1 Seis juicios y sus límites 86

11.2 Escenarios condicionales para el siguiente ciclo de planificación 87

11.3 Qué no puede predecir este informe 87

CAPÍTULO 11

Perspectivas y planificación condicional

EN RESUMEN

Prepárese para uso indebido de identidad, suplantación convincente, afirmaciones de extorsión e interrupción de servicios. Los avisos oficiales de Chile respaldan esas preguntas sin establecer probabilidades de ataque futuro. Los datos históricos pueden seguir sirviendo a estafadores y los servicios recuperados dejar preguntas de privacidad pendientes. El calendario regulatorio también necesita verificación continua. Asigne a cada juicio un responsable, una señal de revisión y una prueba de cumplimiento; reevalúe cuando cambie la evidencia.

11.1 Seis juicios y sus límites

La confianza se refiere a la proposición expresada, sin predecir que una organización individual sufrirá un incidente. Un mecanismo documentado puede justificar preparación aunque se desconozca su frecuencia nacional. La tabla mantiene juntos el respaldo y la limitación.

Juicio	Confianza	Base	Límite	Señal de revisión
El uso indebido de cuentas actuales merece validación temprana	Alta para la necesidad documentada de respuesta	La actualización de ANCI de mayo identifica acceso con credenciales válidas [S7]	Sin probabilidad nacional ni censo de cuentas afectadas	Evidencia de cuenta pertinente activa, privilegiada o usada recientemente
Los datos históricos pueden generar nuevo trabajo contra suplantación	Media para la implicación de planificación	ANCI distingue material histórico de un nuevo evento de infraestructura [S8]	No se establece utilidad continuada de cada registro	Contacto posterior verificado que usa la información
La continuidad necesita aceptación de negocio	Alta para la distinción	Versiones hospitalarias y energéticas describen consecuencias operacionales distintas [S34] [S35]	Los casos no establecen causa común ni frecuencia sectorial	Falla de una tarea crítica o restricción operacional pendiente
El fraude financiero requiere contacto confiable e independiente	Alta para el mecanismo documentado	Advertencias de bloqueo bancario, anticipos y aplicaciones de crédito [S21][S25] [S26]	Las advertencias no son estimaciones nacionales de pérdidas	Evidencia del cliente sobre autorización o solicitud de pago sospechosa

Juicio	Confianza	Base	Límite	Señal de revisión
Una etiqueta de IA por sí sola es un desencadenante débil de respuesta	Alta para la orientación de la autoridad	ANCI enfatiza conducta maliciosa y exposición innecesaria [S17]	No se infiere una campaña chilena de IA confirmada	Evidencia de activo o identidad afectados o acción perjudicial específica
La preparación jurídica debe seguir el estado final del instrumento	Alta para la necesidad de verificar	Consulta MFA y avance parlamentario de la ley de datos [S15] [S31][S32]	Las fechas propuestas no son fechas promulgadas	Publicación de estándar o modificación finales

Estos juicios no clasifican sectores por seguridad. Identifican capacidades respaldadas por la evidencia pública conservada. Cada organización debe priorizarlas según sus servicios reales, exposiciones validadas y obligaciones.

11.2 Escenarios condicionales para el siguiente ciclo de planificación

Los siguientes escenarios son ejercicios, sin constituir pronósticos ni hallazgos de una operación delictiva compartida.

Escenario	Condición	Primera decisión	Evidencia de preparación
Una credencial anunciada coincide con una cuenta privilegiada activa	Validación de cuenta propia y evidencia actual pertinente	Decidir contención con responsables de identidad y servicio	Revocación de sesiones, revisión de acceso y alternativa de negocio probadas
Clientes reciben solicitudes plausibles de pago tras un incidente de datos	Reportes conservados contienen contexto coincidente del incidente	Coordinar atención antifraude y una advertencia confiable	Ejercicio de personal, vía verificada de contacto y vinculación de casos
Un servicio crítico está indisponible con causa discutida	El responsable confirma una tarea esencial fallida	Activar alternativa e investigar acceso por separado	Prueba presenciada de tarea y plantilla de comunicación acotada
Un instrumento regulatorio final cambia la obligación aplicable	Se verifica promulgación o publicación oficial	Actualizar registro de obligaciones y responsable de implementación	Evaluación jurídica fechada y plan de controles revisado

Ningún escenario asume que el mismo actor obtiene información, contacta al cliente y recibe ganancias. Esa cadena sería un modelo analítico hasta establecer sus vínculos con evidencia. El ejercicio prueba puntos de interrupción sin afirmar una cadena delictiva completa de suministro.

11.3 Qué no puede predecir este informe

Los volúmenes de publicaciones no establecen la probabilidad de ataque a una organización chilena. Las entradas delictivas no establecen pérdidas futuras, eficacia de controles ni frecuencia nacional de cifrado exitoso. Los patrones de divulgación pública no aportan denominador completo para comparar sectores.

El informe tampoco pronostica resultados políticos ni atribuye una campaña futura a una decisión gubernamental. Un anuncio nuevo de actor debe evaluarse frente a activos propios y consecuencias corroboradas. Por sí solo no cambia el perfil técnico de riesgo del país.

Revise los juicios cuando un incidente relevante, una exposición validada o un instrumento jurídico final cambie la evidencia. Registre brevemente qué cambió y por qué el responsable modificó la respuesta. Eso crea un ciclo de planificación con responsabilidades, en vez de una clasificación estática de amenazas.

CONCLUSIONES CLAVE

01

Prepárese para mecanismos documentados sin convertirlos en probabilidades de ataque futuro.

02

Revise prioridades cuando cambie la evidencia de cuentas, clientes, servicios o normas.

03

Asigne a cada escenario un responsable de decisión y una prueba demostrada de cumplimiento.

CAPÍTULO 12

Plan de acción

12

ESTE CAPÍTULO RESPONDE

¿Qué deben entregar los equipos en 30, 60 y 90 días y cómo lo verificará la dirección?

21

acciones de planificación con responsables y evidencia de cumplimiento

12.1 Plan de 30/60/90 días 90
12.2 Equipos de identidad y dispositivos 93
12.3 Responsables de negocio y operaciones 93
12.4 Fraude, tesorería y operaciones de clientes 93
12.5 Asesoría jurídica, privacidad y comunicaciones 94
12.6 Un tablero de directorio basado en evidencia 94
12.7 Use el informe como registro entre evidencia y decisión 94

CAPÍTULO 12

Plan de acción

EN RESUMEN

Asegure primero que las alertas pertinentes lleguen a un responsable. Valide cuentas actuales, preserve plazos de notificación y establezca el servicio mínimo que debe continuar. Luego pruebe avisos de proveedores, autenticación, verificación de clientes y alternativas operacionales. Al día 90, demuestre recuperación y un ejercicio conjunto de incidentes ante la dirección. Son metas de planificación, sin autorizar retrasos de respuesta urgente. Asigne cada acción y conserve evidencia de que funciona la capacidad prevista.

12.1 Plan de 30/60/90 días

El plan convierte la evidencia del informe en un programa. Aplique cada fila a servicios reales y exposición validada de la organización. Un incidente actual relevante entra de inmediato al proceso de respuesta, cualquiera sea el periodo de planificación.

1 Inmediato; repetir antes del 1 de diciembre de 2026

Verificar el estado de la ley de datos; mantener el plazo original salvo modificación publicada y verificada [S30][S50]

RESPONSABLE

Asesoría jurídica y responsable de privacidad

EVIDENCIA DE CUMPLIMIENTO

Dos verificaciones fechadas de publicación, instrumento revisado y plazo operativo de cumplimiento

2 Días 1–30

Confirmar que alertas pertinentes de identidad, datos y servicios llegan a una persona responsable

RESPONSABLE

CISO y mesa de ayuda

EVIDENCIA DE CUMPLIMIENTO

Entrega probada, suplente y registro de escalamiento

Validar ofertas actuales coincidentes de credenciales contra cuentas propias

RESPONSABLE

Identidad y respuesta a incidentes

EVIDENCIA DE CUMPLIMIENTO

Evaluación fechada de cuenta, permisos, actualidad y sesiones

Investigar evidencia pertinente de dispositivos de trabajadores sin asumir que los demás son de clientes

RESPONSABLE

Equipos de dispositivos e identidad

EVIDENCIA DE CUMPLIMIENTO

Finalidad de cuenta determinada y decisión de respuesta documentada

Mapear tarea esencial, responsable y alternativa de cada servicio crítico

RESPONSABLE

Negocio y operaciones

EVIDENCIA DE CUMPLIMIENTO

Mapa aprobado de servicios y vía alternativa demostrada

Confirmar alcance de entidad jurídica, condición OIV y secuencia aplicable de reportes

RESPONSABLE

Asesoría jurídica y delegado de ciberseguridad

EVIDENCIA DE CUMPLIMIENTO

Registro de obligaciones, fuentes verificadas y aprobador identificado

Probar la decisión de alerta temprana fuera del horario normal

RESPONSABLE

Respuesta, asesoría jurídica y delegado

EVIDENCIA DE CUMPLIMIENTO

Cronología de conocimiento, envío de práctica y registro de brechas

Establecer una vía confiable para reportar pagos y contactos sospechosos

RESPONSABLE

Fraude, tesorería y atención al cliente

EVIDENCIA DE CUMPLIMIENTO

Proceso de verificación publicado e información al personal

3Días 31–60

Probar notificación con un proveedor que custodie registros sensibles o accesos críticos

RESPONSABLE

Responsable del proveedor y asesoría jurídica

EVIDENCIA DE CUMPLIMIENTO

Aviso de ejercicio con hechos acotados, horas y contactos

Revisar sesiones privilegiadas activas, métodos de recuperación y accesos delegados

RESPONSABLE

Identidad y arquitectura de seguridad

EVIDENCIA DE CUMPLIMIENTO

Pruebas presenciadas de revocación y recuperación con excepciones

Evaluar autenticación de recorridos pertinentes de clientes y administración remota

RESPONSABLE

Producto, arquitectura y cumplimiento

EVIDENCIA DE CUMPLIMIENTO

Evaluación específica, norma aplicable y responsable de corrección

Validar remitentes legítimos y autenticación de comunicaciones importantes

RESPONSABLE

Mensajería y responsables de dominios

EVIDENCIA DE CUMPLIMIENTO

Inventario aprobado de remitentes y prueba controlada de entrega

Ensayar alternativas de reservas, atención ciudadana u operaciones según corresponda

RESPONSABLE

Responsable del servicio y operaciones

EVIDENCIA DE CUMPLIMIENTO

Prueba completada de tarea esencial y aceptación de negocio

Ejercitar atención al cliente frente a suplantación con contexto exacto

RESPONSABLE

Fraude y operaciones de clientes

EVIDENCIA DE CUMPLIMIENTO

Ejercicio de personal y resultado de verificación independiente

Revisar el estado del estándar MFA propuesto

RESPONSABLE

Asesoría jurídica y arquitectura de seguridad

EVIDENCIA DE CUMPLIMIENTO

Verificación fechada de consulta y publicación, con decisión sobre la obligación aplicable

4Días 61–90

Restaurar un servicio crítico y validar registros y tareas esenciales

RESPONSABLE

Infraestructura y responsable de negocio

EVIDENCIA DE CUMPLIMIENTO

Restauración aislada, pruebas de integridad y resultado operacional aceptado

Ensayar interrupción de servicio y posible exposición de datos simultáneas

RESPONSABLE

Respuesta, operaciones, privacidad y comunicaciones

EVIDENCIA DE CUMPLIMIENTO

Decisiones separadas de servicio, acceso, notificación y comunicación

Probar restricción de acceso remoto operacional cuando corresponda

RESPONSABLE

Responsable OT e ingeniero autorizado

EVIDENCIA DE CUMPLIMIENTO

Procedimiento seguro, cambio aprobado y verificación operacional independiente

Revisar contactos de clientes relacionados con el incidente tras recuperación técnica	
RESPONSABLE	EVIDENCIA DE CUMPLIMIENTO
Atención al cliente y fraude	Revisión acotada de seguimiento y conclusión de reportes validados
Reevaluar exposición histórica y anuncios repetidos	
RESPONSABLE	EVIDENCIA DE CUMPLIMIENTO
Inteligencia, identidad y privacidad	Conclusión actual, histórica, ajena o sin resolver para cada indicio pertinente
Informar resultados, excepciones y dependencias pendientes a la dirección	
RESPONSABLE	EVIDENCIA DE CUMPLIMIENTO
CISO y ejecutivos responsables de negocio	Registro del directorio con responsables, vencimientos y evidencia presenciada

12.2 Equipos de identidad y dispositivos

Comience por la finalidad real de la cuenta. Confirme que dominio y servicio pertenecen a la organización, establezca si sigue activa y revise permisos en riesgo. Las credenciales históricas y el uso actual no autorizado requieren decisiones distintas.

Cuando corresponda contener, considere sesiones, métodos de autenticación agregados, accesos delegados y recuperación junto con la contraseña. La prueba de cumplimiento es un estado controlado de cuenta con responsable designado. No debe depender solo de que el usuario acuse recibo de un correo de restablecimiento.

12.3 Responsables de negocio y operaciones

Defina la tarea esencial como una acción que el usuario pueda completar. Para un hospital, puede incluir gestionar horas urgentes. Para un servicio público, una vía alternativa a una solicitud necesaria. Para una instalación operacional, use criterios aprobados de aceptación de ingeniería.

12.4 Fraude, tesorería y operaciones de clientes

Tesorería debe verificar cambios de instrucciones de pago por una vía conocida. Quien aprueba no debe autenticar un cambio únicamente con el mensaje que lo pidió. Registre la verificación y decisión bajo el procedimiento de pagos de la organización.

12.5 Asesoría jurídica, privacidad y comunicaciones

Mantenga una cronología compartida de hechos establecidos y registre por separado cada decisión de notificación y comunicación. Respuesta técnica, notificación a una autoridad, denuncia penal y mensaje a personas afectadas pueden tener condiciones y responsables distintos.

Siga los cambios legales hasta el instrumento oficial final. La consulta MFA de ANCI y el avance parlamentario de la postergación de datos tienen condiciones jurídicas distintas. Conserve fuente y fecha de respaldo de cualquier cambio al calendario de cumplimiento aplicable. [S15][S31][S32]

12.6 Un tablero de directorio basado en evidencia

El directorio necesita un conjunto pequeño de resultados, sin depender de una puntuación nacional de amenazas. Las siguientes preguntas permiten revisar el programa sin afirmar una meta numérica no respaldada por el informe.

Área de decisión	Pregunta de dirección	Evidencia que solicitar
Identidad	¿Puede el equipo distinguir un evento de cuenta activa del material histórico?	Caso validado con decisiones de cuenta y sesiones
Continuidad del servicio	¿Pueden los usuarios completar la tarea esencial durante la degradación?	Prueba presenciada de alternativa y aceptación de negocio
Dependencia de proveedores	¿Puede un proveedor crítico notificar y apoyar una respuesta oportuna?	Ejercicio conjunto con hechos acotados y horas
Protección al cliente	¿Puede una persona verificar independientemente una solicitud plausible?	Vía probada de contacto y respuesta de atención capacitada
Notificación	¿Puede la organización llegar a una decisión autorizada dentro del plazo aplicable?	Cronología de conocimiento y envío de práctica
Recuperación	¿Puede restaurar el servicio y conciliar el trabajo interrumpido?	Resultado de restauración, pruebas de integridad y revisión de pendientes
Estado jurídico	¿Se basan las obligaciones en instrumentos promulgados vigentes?	Verificación fechada de fuente y evaluación jurídica con responsable

12.7 Use el informe como registro entre evidencia y decisión

Las observaciones de Brandefense Blackhole y las entradas de Ransompedia aportan poblaciones de evidencia distintas en este informe. El valor defensivo está en revisar una señal pertinente con sus límites, asignar responsable y registrar una conclusión proporcional. Los recuentos siguen separados de los incidentes organizacionales confirmados.

Para una demostración de Brandefense, visite Solicitar una demostración. Use la conversación para conectar prioridades de evidencia, responsables y pruebas de cumplimiento de la organización.

CONCLUSIONES CLAVE

01

Establezca responsables de alertas, validación de cuentas, alternativas de servicio y preparación de notificaciones al día 30.

02

Pruebe proveedores, autenticación, verificación de clientes y alternativas pertinentes al día 60.

03

Demuestre recuperación y decisiones conjuntas; informe las excepciones con responsables a la dirección al día 90.

ANEXOS

Anexos

A–D

ESTE CAPÍTULO RESPONDE

¿Qué poblaciones, fechas y limitaciones rigen los hallazgos del informe?

Separe

publicaciones, entradas, organizaciones, personas y transacciones

Anexo A. Alcance y límites de evidencia 97

Anexo B. Registro de evidencia 100

Anexo C. Fuentes 102

Anexo D. Glosario 106

Anexo A. Alcance y límites de evidencia

Los países de comparación se seleccionaron como ejemplos únicamente para aportar contexto; su elección no implica una clasificación ni una valoración política.

A.1 Periodo y fechas

El periodo principal cubre publicaciones fechadas del 1 de enero–22 de noviembre de 2026. La vista reciente abarca el 8–22 de noviembre. Las versiones públicas de incidentes conservan las fechas de evento, descubrimiento, divulgación y actualización respaldadas por sus fuentes.

El informe describe la evidencia disponible al corte. No es un censo completo de todos los incidentes chilenos ni de cada evento del día de corte. Investigaciones posteriores pueden cambiar alcance, mecanismo o atribución de un evento reportado.

A.2 Poblaciones de fuentes

El informe usa publicaciones clandestinas conservadas, entradas públicas de ransomware, observaciones de dominios seleccionados y noticias públicas. Cada población tiene su unidad y cobertura. Una publicación asociada al país, una entrada delictiva, un dominio y un aviso organizacional no son registros intercambiables de incidentes. [S1][S2][S3][S5]

La serie mensual suma 27,891 observaciones; una observación de julio no figura entre las 27,890 publicaciones conservadas usadas para porcentajes. [S1]

A.3 Dominios seleccionados y observaciones pasivas

La cartera tiene 250 registros seleccionados de dominios principales en diez sectores fusionados. La selección refleja relevancia institucional y de servicio. No es una clasificación por ingresos, un censo ni una estimación estadísticamente representativa de organizaciones chilenas. [S5]

Los resultados pasivos describen la configuración evaluada en una fecha indicada. Cada resultado conserva su denominador disponible. Las observaciones no concluyentes siguen siendo desconocidas. Un resultado ausente no equivale a un control ausente; un control visible no establece eficacia en cada servicio. [S3]

Atlas aporta la cifra principal nacional de 58/100 (B) para la cartera seleccionada. Solo se publica esa calificación nacional. Dispositivos, dispositivos de trabajadores, registros de credenciales, anuncios y documentos describen poblaciones separadas que pueden superponerse. Los resultados pasivos conservan sus propios denominadores evaluados. [S210][S3]

A.4 Entradas de ransomware

Ransompedia registra 41 filas chilenas en el periodo solicitado, con 39 cadenas distintas de nombres de organizaciones y 13 etiquetas de quienes hacen las afirmaciones. Las cadenas no son entidades jurídicas validadas independientemente. Una entrada sigue siendo una afirmación delictiva sobre la organización mencionada. [S2]

Los cuatro países regionales comparados usan el mismo periodo actual solicitado. Sus totales brutos no controlan escala económica, poblaciones de organizaciones ni prácticas de divulgación. La comparación chilena de 2025 abarca el año anterior completo y no es crecimiento entre periodos equivalentes.

A.5 Alcance de tarjetas de pago

Estas cifras describen una población observada limitada de material de tarjetas de pago. No establecen la prevalencia nacional, la posibilidad de uso actual, transacciones realizadas ni pérdidas por fraude. [S4]

A.6 Límites de casos y relaciones

El conjunto detallado contiene seis expedientes de afirmaciones clandestinas y las versiones públicas acotadas del capítulo 5. Un expediente puede tratar varias publicaciones o actualizaciones relacionadas. No equivale automáticamente a una intrusión confirmada de manera independiente.

El Caso A y el contexto de proveedor del cliente minero comparten una referencia de proveedor. Eso no establece el mismo evento o archivos. El contexto no se cuenta como otra intrusión independiente. Un cliente nombrado en un anuncio no es una víctima confirmada por separado.

Las relaciones entre fuentes y proposiciones son distintas de los hallazgos de operador común. Compartir sector, cantidad, idioma o técnica no establece una campaña. El modelo de cadena de fraude es expresamente analítico, sin verificar un recorrido del mismo operador por cada etapa.

A.7 Confianza y alternativas

La confianza corresponde a una proposición. Puede ser alta sobre la existencia de un mensaje conservado y baja sobre el acceso afirmado. Una declaración oficial puede establecer la posición de su fuente sin resolver independientemente cada pregunta técnica.

A.8 Nombres, fuentes y neutralidad

Los roles de víctimas permanecen amplios cuando no se cumplen las condiciones para nombrarlas. Las direcciones públicas que identificarían un sujeto reservado se acortan a la raíz del medio y se marcan como reservadas. El estado de la fuente de respaldo se conserva por separado de la dirección pública de cita.

El informe no toma posición sobre las elecciones presidenciales y parlamentarias de 2025, el gobierno posterior, partidos políticos ni decisiones gubernamentales. Tampoco toma posición sobre asuntos mapuches o de La Araucanía ni sobre relaciones con Bolivia y Perú.

El encuadre político de un actor no establece motivo, nacionalidad ni dirección estatal. Las asociaciones estatales atribuidas a una fuente siguen siendo su evaluación. La afirmación de datos electorales no establece intrusión actual de sistemas ni efectos sobre una elección.

Anexo B. Registro de evidencia

Las doce fichas de publicaciones presentan extractos acotados y sus límites. Respaldan existencia y redacción de afirmaciones, sin validar autenticidad o integridad del material anunciado. Los identificadores de fichas son iguales en todas las ediciones.

Ficha	Publicación	Medio	Alias	Mostrada en
B01	2026-04-04	Foro	Reservado	Caso A
B02	2026-04-15	Foro	Reservado	Caso A
B03	2026-03-06	Foro	Reservado	Caso C
B04	2026-04-05	Foro	Reservado	Caso B
B05	2026-10-29	Foro	Reservado	Caso F
B06	2026-10-05	Foro	Reservado	Caso D
B07	2026-10-04	Foro	Reservado	Caso D
B08	2026-11-12	Foro	Reservado	Caso E
B09	2026-11-20	Foro	Reservado	Sección 4.5
B10	2026-11-22	Foro	Reservado	Sección 4.5
B11	2026-02-02	Foro	Reservado	Sección 4.5
B12	2026-01-14	Foro	Reservado	Sección 4.5

El índice distingue expedientes de recuentos de incidentes confirmados. La letra N no se utiliza.

Caso	Rol del sujeto	Evidencia principal
A	Proveedor de software empresarial y alojamiento	Anuncios relacionados; el contexto de fuentes del proveedor mantiene sus límites
B	Consultoría de software empresarial	Oferta de código y base de datos y lenguaje de rescate
C	Portal administrativo relacionado con banca	Anuncio de acceso y disputa de credibilidad
D	Administración educativa	Afirmaciones relacionadas de divulgación de datos
E	Red escolar	Oferta de venta con alcance histórico
F	Prestadores de salud	Afirmación de divulgación de múltiples objetivos

Caso	Rol del sujeto	Evidencia principal
G	Servicios públicos y comunicaciones	Avisos inicial y actualizado de ANCI sobre acceso a cuentas
H	Alerta de datos históricos	Evaluación de ANCI sobre filtración anterior
I	Información de imagenología hospitalaria	Noticias sobre una denuncia penal
J	Servicios de apoyo hospitalario	Declaración organizacional reportada y versión de continuidad
K	Instalación energética	Registros operacionales fechados y noticias posteriores
L	Organismo de servicio público	Versiones técnicas contrapuestas durante investigación
M	Comercio minorista	Divulgación oficial y actualización operacional posterior
O	Telecomunicaciones	Investigación reportada con actividad histórica
P	Organismo de servicio público	Mensajes no autorizados e interrupción reportados
Q	Servicio de salud	Declaración matizada de posible extracción de información
R	Grupo manufacturero	Incidente multinacional reportado con consecuencia chilena
S	Organismo público regional	Noticias regionales de un evento de cuenta administrativa
T	Firma jurídica	Denuncia de ransomware y versión de recuperación reportadas
U	Servicio público de publicación	Una declaración sobre cuentas reportada por dos medios

El Caso A y el contexto de fuente del proveedor del cliente minero no se tratan como intrusiones independientes. El Caso H corrige una alerta; varios otros expedientes conservan incertidumbre de investigación o alcance de datos. El índice ayuda a leer, sin contar víctimas nacionales.

Anexo C. Fuentes

Cada entrada registra la fecha de revisión de la fuente de respaldo. Algunas direcciones se acortan para proteger sujetos reservados. La dirección pública de cita es distinta del pasaje sustantivo de la fuente que respalda el hallazgo.

S1: Odin by Brandefense. Observaciones conservadas de publicaciones clandestinas asociadas a Chile. Investigación propia conservada; sin URL pública. Verificado el 2026-11-22.

S2: Ransompedia. Agregados de entradas de ransomware de Chile y países regionales comparados. Investigación propia conservada; sin URL pública. Verificado el 2026-11-22.

S3: Odin by Brandefense. Observaciones pasivas de DNS y TLS para dominios chilenos seleccionados. Investigación propia conservada; sin URL pública. Verificado el 2026-11-22.

S4: Brandefense Blackhole. Agregados acotados de tarjetas de pago del material de publicaciones recopilado. Investigación propia conservada; sin URL pública. Verificado el 2026-11-22.

S5: Odin by Brandefense. Cartera seleccionada de dominios de organizaciones chilenas y denominadores sectoriales. Investigación propia conservada; sin URL pública. Verificado el 2026-11-22.

S6: ANCI. Respuesta inicial de ANCI a publicaciones de datos reportadas. https://anci.gob.cl/noticias/anci-informa-sobre-reportes-de-las-ultimas-horas/ Verificado el 2026-11-22.

S7: ANCI. Actualización de ANCI: acceso no autorizado con credenciales válidas. https://anci.gob.cl/noticias/actualizacion-anci-filtraciones-por-robo-de-credenciales/ Verificado el 2026-11-22.

S8: ANCI. ANCI identifica material histórico en nueva alerta de filtración. https://anci.gob.cl/noticias/sobre-reciente-informacion-de-supuestas-filtraciones/ Verificado el 2026-11-22.

S9: ANCI. Panorama Actual de Amenazas: primer semestre de 2026. https://anci.gob.cl/documents/5140/Panorama_Actual_de_Amenazas_2026_Octubre.pdf Verificado el 2026-11-22.

S10: ANCI. Lanzamiento del Mes de la Ciberseguridad y total de reportes de ANCI. https://anci.gob.cl/noticias/anci-mes-de-la-ciberseguridad-2026/ Verificado el 2026-11-22.

S11: ANCI. ANCI cierra el primer proceso de calificación de OIV. https://anci.gob.cl/noticias/anci-finaliza-el-primer-proceso-de-calificacion-de-operadores-de-importancia-vital/ Verificado el 2026-11-22.

S12: ANCI. Medidas de mitigación OIV bajo la Instrucción General 4. https://anci.gob.cl/noticias/obligaciones-instruccion-general-n4/ Verificado el 2026-11-22.

S13: Diario Oficial. Publicación oficial de la Ley 21.663. https://www.diariooficial.interior.gob.cl/publicaciones/2024/04/08/43820/01/2475674.pdf Verificado el 2026-11-22.

S14: Diario Oficial. Publicación original de la Instrucción General 4. https://www.diariooficial.interior.gob.cl/publicaciones/2025/12/26/44333-B/01/2747332.pdf Verificado el 2026-11-23.

S15: ANCI. Apertura de consulta pública sobre estándar MFA. https://anci.gob.cl/noticias/consulta-publica-normativa-mfa/ Verificado el 2026-11-22.

S16: ANCI. Proyecto MFA en consulta pública. https://anci.gob.cl/documents/5200/Estandar_1_20261105.pdf Verificado el 2026-11-22.

S17: ANCI. Recomendaciones de ANCI sobre ataques asistidos por IA. https://anci.gob.cl/noticias/recomendaciones-anci-ante-el-uso-de-herramientas-de-ia-en-ciberataques/ Verificado el 2026-11-22.

S18: ANCI. Advertencia ciudadana sobre ClickFix. https://anci.gob.cl/ciberconsejos/ciberconsejos-clickfix/ Verificado el 2026-11-22.

S19: ANCI. Orientación de respuesta después de un clic. https://anci.gob.cl/ciberconsejos/ciberconsejos-y-si-ya-hice-clic/ Verificado el 2026-11-22.

S20: ANCI. Advertencia sobre ofertas laborales falsas. https://anci.gob.cl/ciberconsejos/ciberconsejos-estafas-en-falsas-ofertas-laborales/ Verificado el 2026-11-22.

S21: ANCI. Advertencia de ingeniería social con bloqueo de cuenta bancaria. https://anci.gob.cl/ciberconsejos/ciberconsejos-el-fraude-de-la-cuenta-bancaria-bloqueada/ Verificado el 2026-11-22.

S22: ANCI. Advertencia sobre phishing de reservas hoteleras. https://anci.gob.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S23: ANCI. Advertencia de suplantación en temporada tributaria. https://anci.gob.cl/ciberconsejos/ciberconsejos-operacion-renta-2026/ Verificado el 2026-11-22.

S24: ANCI. Advertencia de correos que suplantan una empresa estatal. https://anci.gob.cl/ciberconsejos/ciberconsejos-claves-para-identificar-un-email-falso/ Verificado el 2026-11-22.

S25: CMF. CMF advierte sobre extorsión en aplicaciones de crédito y posible usura. https://www.cmfchile.cl/portal/prensa/625/w4-article-115042.html Verificado el 2026-11-22.

S26: CMF. CMF advierte sobre fraude de préstamos con pagos anticipados. https://www.cmfchile.cl/portal/prensa/625/w4-article-115043.html Verificado el 2026-11-22.

S27: CMF. Entrada en plena vigencia de la autenticación reforzada de CMF. https://www.cmfchile.cl/portal/prensa/625/w4-article-112253.html Verificado el 2026-11-22.

S28: CMF. Advertencia de CMF sobre trece aplicaciones de crédito. https://www.cmfchile.cl/portal/prensa/625/w4-article-111149.html Verificado el 2026-11-22.

S29: Fiscalía de Chile. Mesa nacional de coordinación contra fraude financiero. https://www.fiscaliadechile.cl/actualidad/noticias/organismos-publicos-y-del-sector-privado-financiero-crean-mesa-nacional-contra Verificado el 2026-11-22.

S30: Biblioteca del Congreso Nacional. Historia legislativa de la ley de datos personales. https://www.bcn.cl/balance-legislativo/detalle/ficha_LEY_21719_2024-12-13 Verificado el 2026-11-23.

S31: Cámara de Diputadas y Diputados. La Cámara informa envío a promulgación del proyecto de postergación. https://www.camara.cl/cms/2026/11/20/datos-personales-combustibles-y-sala-cuna-en-los-temas-despachados-por-la-camara/ Verificado el 2026-11-22.

S32: Cámara de Diputadas y Diputados. Informe de comisión sobre postergación de la ley de datos. https://www.camara.cl/verDoc.aspx?prmID=79766&prmTipo=DOCUMENTO_COMISIONINFORME Verificado el 2026-11-22.

S33: T13. Incidente de datos de imagenología hospitalaria reportado a partir de denuncia penal. https://www.t13.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S34: BioBioChile. Interrupción hospitalaria de noviembre y atención clínica mantenida. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S35: 24 Horas. Interrupción energética tras ciberataque reportado por el operador. https://www.24horas.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S36: El Mostrador. Incidente de servicio público: diferencias entre alegaciones y respuestas oficiales. https://www.elmostrador.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S37: NIVEL4 Labs. Entrada Qilin sobre asegurador de salud sin verificar. https://blog.nivel4.com/ (URL del artículo reservada) Verificado el 2026-11-23.

S38: ANCI. Orientación de ANCI para el sector salud. https://anci.gob.cl/noticias/anci-y-cens-lanzan-recomendaciones-de-ciberseguridad-para-sistemas-de-informacion-en-salud/ Verificado el 2026-11-22.

S40: CMF. Advertencia de CMF sobre plataformas de inversión en enero. https://www.cmfchile.cl/portal/prensa/625/w4-article-102694.html Verificado el 2026-11-22.

S41: CMF. Advertencia de CMF sobre plataformas de inversión en febrero. https://www.cmfchile.cl/portal/prensa/625/w4-article-103951.html Verificado el 2026-11-22.

S42: CMF. Advertencia de CMF sobre préstamos con anticipo en marzo. https://www.cmfchile.cl/portal/prensa/625/w4-article-108614.html Verificado el 2026-11-22.

S43: CMF. Advertencia de CMF sobre préstamos con anticipo en abril. https://www.cmfchile.cl/portal/prensa/625/w4-article-109384.html Verificado el 2026-11-22.

S44: BioBioChile. Respuesta de un cliente minero a incidente de proveedor. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S45: BioBioChile. Noticias sobre investigación de actividad en redes de telecomunicaciones. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S46: BioBioChile. Mensajes no autorizados y breve interrupción de un servicio público. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S47: BioBioChile. Actuación de persecución penal de septiembre por comercio de datos. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S48: BioBioChile. Respuesta preventiva de ANCI ante preocupación por cadena de suministro de integración con IA. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S49: trendTIC. Caso de ransomware manufacturero con año del evento sin resolver. https://www.trendtic.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S50: Cámara de Diputadas y Diputados. Seguimiento legislativo de postergación de la ley de datos. https://www.camara.cl/legislacion/proyectosdeley/tramitacion.aspx?prmBOLETIN=18623-07&prmID=19307 Verificado el 2026-11-23.

S51: Operador minorista. Hecho esencial oficial del incidente minorista. Dirección del emisor reservada para proteger al sujeto. Verificado el 2026-11-22.

S52: Operador minorista. Actualización oficial de octubre del incidente minorista. Dirección del emisor reservada para proteger al sujeto. Verificado el 2026-11-22.

S53: Coordinador Eléctrico Nacional. Registro operacional del coordinador eléctrico del 27 de agosto. https://www.coordinador.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S54: Coordinador Eléctrico Nacional. Registro operacional del coordinador eléctrico del 9 de noviembre. https://www.coordinador.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S55: Institución financiera. Declaración bancaria oficial de continuidad de servicio. Dirección del emisor reservada para proteger al sujeto. Verificado el 2026-11-22.

S56: T13. Declaración hospitalaria reportada el 16 de noviembre. https://www.t13.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S57: Cámara de Diputadas y Diputados. Consulta parlamentaria sobre continuidad hospitalaria. https://camara.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S60: Cámara de Diputadas y Diputados. Solicitud parlamentaria sobre incidentes eléctricos. https://www.camara.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S63: BioBioChile. Declaración de servicio de salud sobre posible extracción de información. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S64: BioBioChile. Noticias de ransomware en grupo manufacturero con efecto en Chile. https://www.biobiochile.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S65: Araucanía Noticias. Noticias de acceso a cuenta de organismo público regional. https://araucanianoticias.cl/ (URL del artículo reservada) Verificado el 2026-11-23.

S68: BeyondTrust. Aviso original BeyondTrust BT26-02. https://www.beyondtrust.com/trust-center/security-advisories/bt26-02 Verificado el 2026-11-22.

S69: NVD. Página NVD de CVE-2026-1731. https://nvd.nist.gov/vuln/detail/CVE-2026-1731 Verificado el 2026-11-23.

S70: 24Horas. Firma jurídica confirma denuncia de ransomware y recuperación. https://www.24horas.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S71: BioBioChile. Reportes de incidentes significativos de respuesta de transparencia de ANCI hasta el 15 de octubre. https://www.biobiochile.cl/especial/bbcl-investiga/noticias/de-pasillo/2026/11/07/ciberataques-a-servicios-esenciales-organismos-han-reportado-566-incidentes-significativos-en-2026.shtml Verificado el 2026-11-22.

S72: BlackDoor. Entrada de extorsión de septiembre sobre financiera sigue sin confirmar. https://www.blackdoor.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S73: DeXpose. Retransmisión de afirmación pública Qilin sobre empresa marítima. https://www.dexpose.io/ (URL del artículo reservada) Verificado el 2026-11-22.

S74: Diario Financiero. Declaración de distribuidora energética sobre acceso no autorizado a almacenamiento interno. https://www.df.cl/ (URL del artículo reservada) Verificado el 2026-11-23.

S75: El Mostrador. Respuesta pública de distribuidora energética y afirmación de extorsión contrapuesta. https://www.elmostrador.cl/ (URL del artículo reservada) Verificado el 2026-11-23.

S76: Instructure. Actualización del proveedor sobre incidente Canvas. https://www.instructure.com/incident_update Verificado el 2026-11-23.

S77: T13. Respuesta fechada de organización del sector salud ante alerta de mayo. https://www.t13.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S78: T13. Investigación de presunta venta interna de información por empleado judicial. https://www.t13.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S82: ADN Radio. Retransmisión original de julio de afirmación sobre un servicio público. https://www.adnradio.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S83: Emol/ATON. Declaración institucional acota exposición de cuentas de publicación. https://www.emol.com/ (URL del artículo reservada) Verificado el 2026-11-22.

S84: ADN Radio. Corroboración del alcance de cuentas de publicación de una institución. https://www.adnradio.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S85: DataReportal/Simon Kemp. Digital 2027 Chile: contexto de adopción de internet de octubre de 2026. https://datareportal.com/reports/digital-2027-chile Verificado el 2026-11-22.

S86: Coordinador Eléctrico Nacional. El informe diario del operador eléctrico amplía la observación de indisponibilidad solar y de baterías. https://www.coordinador.cl/ (URL del artículo reservada) Verificado el 2026-11-22.

S87: CMF. CMF consulta sobre archivos de reportes bancarios, incluido el archivo de ciberincidentes I12. https://www.cmfchile.cl/portal/prensa/625/w4-article-115004.html Verificado el 2026-11-22.

S200: NIST. Definición de autenticación multifactor. https://csrc.nist.gov/glossary/term/multi_factor_authentication Verificado el 2026-11-22.

S201: NIST. Definición de denegación de servicio distribuida. https://csrc.nist.gov/glossary/term/distributed_denial_of_service Verificado el 2026-11-22.

S202: Servicio de Impuestos Internos. Definición de unidad tributaria mensual. https://www.sii.cl/ayudas/ayudas_por_servicios/4669-u.html Verificado el 2026-11-22.

S203: RFC Editor. Especificación de DMARC. https://www.rfc-editor.org/rfc/rfc9989 Verificado el 2026-11-22.

S204: RFC Editor. Especificación de SPF. https://www.rfc-editor.org/rfc/rfc7208 Verificado el 2026-11-22.

S205: RFC Editor. Especificación de DKIM. https://www.rfc-editor.org/rfc/rfc6376 Verificado el 2026-11-22.

S206: RFC Editor. Especificación de DNSSEC. https://www.rfc-editor.org/rfc/rfc4033 Verificado el 2026-11-22.

S207: RFC Editor. Especificación de TLS. https://www.rfc-editor.org/rfc/rfc9846 Verificado el 2026-11-22.

S208: RFC Editor. Especificación de HSTS. https://www.rfc-editor.org/rfc/rfc6797 Verificado el 2026-11-22.

S209: Biblioteca del Congreso Nacional. Ley 21.663: texto legal vigente y regímenes especiales del artículo 53. https://www.bcn.cl/leychile/navegar?i=1202434 Verificado el 2026-11-23.

S210: Calificaciones de exposición de Brandefense Atlas y observaciones de Blackhole sobre dispositivos, dispositivos de trabajadores, registros de credenciales, documentos y anuncios vigentes para 250 dominios seleccionados; agregados de exposición y tarjetas de bancos emisores. Leídas el 22 de noviembre de 2026. Verificado el 2026-11-22.

Anexo D. Glosario

Término	Significado sencillo
ANCI	Agencia Nacional de Ciberseguridad de Chile [S11]
Clave API	Credencial que usa un programa para acceder a un servicio
Momento de conocimiento	Hora registrada en que una organización conoce los hechos pertinentes para evaluar un incidente
Etiqueta de quien afirma	Nombre usado en una publicación delictiva, sin demostrar operación común
ClickFix	Engaño mediante un aviso falso de error o verificación que induce una acción insegura [S18]
Credencial	Información usada para autenticar, como contraseña o token de acceso
DDoS	Ataque de denegación de servicio que usa muchos equipos [S201]
DKIM	Método para firmar correos que permite a los receptores comprobar su asociación con un dominio [S205]
DMARC	Política de un dominio para gestionar autenticación de correo y alineación del remitente [S203]
DNSSEC	Extensiones que respaldan validar la autenticidad de los datos DNS [S206]
HSTS	Política web que indica a navegadores compatibles usar HTTPS para un servicio [S208]
MFA	Autenticación que requiere más de un tipo distinto de evidencia [S200]
OIV	Operador calificado como de importancia vital bajo el marco chileno de ciberseguridad, con deberes reforzados [S11]
Sesión privilegiada	Acceso autenticado con permisos capaces de afectar funciones sensibles
Ransompedia	Fuente de entradas de ransomware de Brandefense; sus publicaciones siguen siendo afirmaciones delictivas
SPF	Declaración de un dominio sobre los servicios que pueden enviar correos en su nombre [S204]
Dependencia de proveedor	Servicio, repositorio de información o vía de acceso controlados por otra organización

Término	Significado sencillo
TLS	Protocolo usado para proteger comunicaciones de red [S207]
UTM	Unidad tributaria mensual chilena, expresada en pesos y actualizada según cambios de precios al consumidor [S202]

Acerca de este informe

Elaborado por Odin by Brandefense para dirección de seguridad, equipos de respuesta, infraestructura y operaciones, especialistas de fraude, atención al cliente y responsables jurídicos y de privacidad. La versión 1.0 abarca el periodo solicitado del 1 de enero–22 de noviembre de 2026, con vista reciente separada del 8–22 de noviembre.

La edición en español se traduce del documento maestro en inglés y lleva un aviso visible de traducción con IA. La edición en inglés prevalece ante discrepancias. El informe no afirma que evidencia no disponible, investigación sin resolver o servicio restablecido respondan todas las preguntas de seguridad pendientes.

© 2026 Brandefense. Todos los derechos reservados.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO