

GlobalSign

Cumplimiento técnico y evidencia digital para la Ley 21.719

TRES CAPAS

Cifrado y canales

Identidad y acceso

Firma y evidencia

Contenido

01 El marco y el riesgo

02 Artículos traducidos a controles

03 Portafolio y sectores

04 Casos de uso por sector



SEGURIDADAMÉRICA.COM
Fortaleciendo Internet



GlobalSign®
by **GMO**

01

El marco y el riesgo

01 • EL MARCO Y EL RIESGO

Qué cambia el 1 de diciembre de 2026

La ley se publicó el 13 de diciembre de 2024 y entra en plena vigencia tras 24 meses de transición.

Nace la Agencia de Protección de Datos Personales, con facultades reales de fiscalización y sanción.

El Art. 14 quinquies convierte las medidas de seguridad en obligación exigible, no en buena práctica.

La carga de la prueba es del responsable: debe demostrar consentimiento, licitud y control.



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



GlobalSign®
by **GMO**

01 • EL MARCO Y EL RIESGO

Lo que cuesta no tener evidencia

INFRACCIÓN	TOPE DE MULTA	QUÉ CAE EN EL TRAMO
Leves	5.000 UTM	Incumplimientos formales y de información
Graves	10.000 UTM	Seguridad inadecuada, derechos no atendidos
Gravísimas	20.000 UTM	Datos sensibles sin base legal, brechas graves
Reincidencia	hasta 4%	De los ingresos anuales, o la multa triplicada

Un modelo de prevención certificado (Art. 49) opera como atenuante; las sanciones se publican por cinco años.



01 • EL MARCO Y EL RIESGO

Hasta dónde llega esta conversación

Lo que resuelve

Controles técnicos: cifrado, firma, integridad, autenticación, gestión de certificados y evidencia verificable.

Lo que no reemplaza

Asesoría legal, políticas, gestión de consentimiento, atención de derechos ni el modelo integral de cumplimiento.



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



GlobalSign®
by **GMO**

02

Artículos traducidos a controles

02 · ARTÍCULOS TRADUCIDOS A CONTROLES

Alguien tendrá que probarlo

La Agencia no pregunta por intenciones: pide registros, fechas y firmas.

El equipo que responde es el mismo que opera los sistemas todos los días.

Cada control que deja rastro exportable ahorra una discusión legal.



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



GlobalSign®
by **GMO**

02 · ARTÍCULOS TRADUCIDOS A CONTROLES

Cuatro exigencias, no cuatro capítulos

Seguridad y confidencialidad

ART. 3 · 14 BIS · 14 QUÁTER · 14 QUINQUES

Proteger los datos y los sistemas que los tratan, y mantener el deber de secreto.

Datos especialmente protegidos

ART. 16 · 16 BIS · 16 TER · 16 QUÁTER · 16 SEXIES

Datos sensibles, salud, biometría, menores y geolocalización, con exigencia reforzada.

Prueba y trazabilidad

ART. 11 · 12 · 15 · 15 BIS · 15 TER

Demostrar consentimiento, licitud, respuestas a titulares y acuerdos con terceros.

Terceros, Estado y fronteras

ART. 21 · 22 · 27 · 47 A 49

Encargados, órganos públicos, transferencia internacional y prevención de infracciones.



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



Seguridad y confidencialidad

ARTÍCULO	QUÉ EXIGE	CONTROL TÉCNICO
Art. 3 letra f Principio de seguridad	Proteger los datos contra tratamiento no autorizado, pérdida o filtración.	SSL/TLS: cifra portales, formularios, APIs y plataformas de recolección.
Art. 3 h · Art. 14 bis Confidencialidad y secreto	Deber de secreto exigible al responsable y a todo quien trate los datos.	Managed PKI y S/MIME: acceso por identidad digital y correo cifrado.
Art. 14 quinquies Medidas de seguridad	Confidencialidad, integridad, disponibilidad y resiliencia de los sistemas.	CLM y ACME: certificados siempre vigentes, sin caídas por vencimiento.
Art. 14 quinquies d Verificación periódica	Verificar y evaluar regularmente la eficacia de las medidas adoptadas.	Atlas Discovery y Managed SSL: inventario y evidencia de gestión continua.



Prueba y trazabilidad

ARTÍCULO	QUÉ EXIGE	CONTROL TÉCNICO
Art. 12 Consentimiento y licitud	Probar que hubo consentimiento y que el tratamiento fue lícito y transparente.	Digital Signing Service: consentimientos y contratos con autoría e integridad.
Art. 11 Derechos del titular	Atender solicitudes con identidad autenticada, fecha y contenido íntegro.	Timestamping y certificados de cliente: respuestas fechadas y verificables.
Art. 15 • Art. 15 bis Cesión y encargados	Formalizar cesiones y el tratamiento por encargado, con seguridad exigible.	Documentos firmados más TLS, S/MIME y PKI en la cadena con el proveedor.
Art. 15 ter Evaluación de impacto	Evaluar el impacto en protección de datos de los tratamientos de riesgo.	CLM y Atlas aportan el inventario técnico que alimenta la evaluación.



02 · DATOS ESPECIALMENTE PROTEGIDOS

Datos especialmente protegidos

ARTÍCULO	QUÉ EXIGE	CONTROL TÉCNICO
Art. 16 · Art. 16 bis Sensibles y salud	Tratamiento reforzado de datos sensibles, de salud y perfil biológico.	S/MIME, TLS y PKI para cifrar el traslado; firma para las autorizaciones.
Art. 16 ter Datos biométricos	Restringe el tratamiento de biometría a supuestos y resguardos específicos.	Certificados de autenticación: identidad fuerte sin almacenar biometría.
Art. 16 quáter Niños y adolescentes	Protección especial de los datos de niños, niñas y adolescentes.	TLS y S/MIME en portales de apoderados, matrícula y comunicaciones.
Art. 14 quáter · 16 sexies Diseño y geolocalización	Protección desde el diseño y por defecto, incluida la geolocalización.	IoT Identity Platform y Code Signing: identidad de dispositivo e integridad.



Terceros, Estado y fronteras

ARTÍCULO	QUÉ EXIGE	CONTROL TÉCNICO
Art. 21 Órganos públicos	Tratamiento por órganos públicos con resguardos de seguridad y control.	Managed PKI, CLM y TLS: identidad, canales y gestión centralizada.
Art. 22 Cesión entre servicios	Comunicación o cesión de datos entre órganos públicos de forma acreditable.	S/MIME y documentos firmados: remitente verificable y contenido íntegro.
Art. 27 Transferencia internacional	Garantías adecuadas y cláusulas contractuales para transferir datos.	Firma digital de las cláusulas; PKI, S/MIME y TLS como resguardos.
Art. 47 · 48 · 49 Modelo de prevención	Prevención de infracciones; el modelo certificado atenúa la sanción.	Firma, sello de tiempo y CLM producen el rastro que sostiene el modelo.





SEGURIDADAMÉRICA.COM
Fortaleciendo Internet



GlobalSign®
by **GMO**

03

Portafolio y sectores

03 · PORTAFOLIO Y SECTORES

Tres capas de confianza digital

Cifrado y canales

SSL/TLS · MANAGED SSL · ACME

Cifrado en tránsito y autenticación de servidor para portales, formularios, APIs y extranets, con emisión y renovación automatizadas.

Identidad y acceso

MANAGED PKI · CLIENT AUTH · IOT

Certificados para personas, servidores y dispositivos: acceso por identidad digital a aplicaciones internas, VPN, WiFi y flotas conectadas.

Firma y evidencia

DSS · TIMESTAMP · CODE SIGNING

Autoría, integridad y fecha cierta sobre consentimientos, contratos, correo y software: el material probatorio del cumplimiento.



SEGURIDADAMÉRICA.COM
Fortaleciendo Internet



03 · PORTAFOLIO Y SECTORES

Por dónde empieza cada sector



Banca y finanzas

ART. 12 · 14 QUINQUIES · 16

Consentimientos y contratos firmados, portales y APIs cifrados, correo con datos de clientes bajo S/MIME.



Gobierno

ART. 21 · 22 · 27

Identidad digital para funcionarios y sistemas, y cesión entre servicios con remitente verificable y contenido íntegro.



Educación

ART. 16 QUÁTER · 14 QUINQUIES

Datos de niños, niñas y adolescentes: portales de apoderados, matrícula en línea y comunicaciones cifradas.

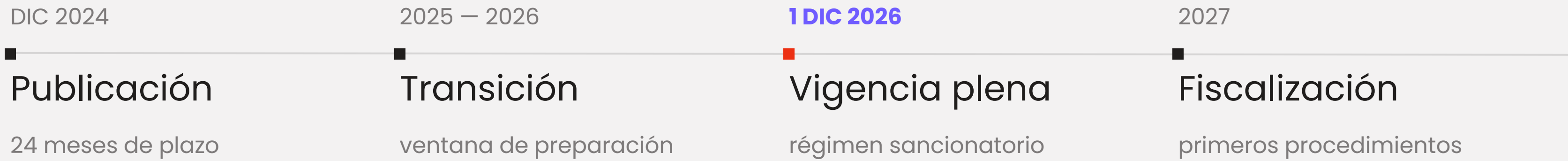


SEGURIDADAMÉRICA.com
Fortaleciendo Internet



03 · PORTAFOLIO Y SECTORES

El calendario que queda



La evidencia técnica no se improvisa el día de la fiscalización: certificados, firmas y sellos de tiempo valen por el rastro que dejaron antes.



SEGURIDADAMÉRICA.COM
Fortaleciendo Internet



GlobalSign®
by **GMO**

04

Casos de uso por sector

Coca-Cola



04 · CASOS DE USO POR SECTOR — BANCA Y FINANZAS

El consentimiento que nadie pudo mostrar

El escenario

Un ejecutivo comparte por correo el historial financiero de un cliente con una empresa externa de cobranza. Todo parecía en regla, hasta que la Agencia pidió el consentimiento firmado. No existía ningún documento que lo probara: solo un correo sin cifrar y un “sí” verbal en una llamada.

“Un consentimiento sin firma digital es un préstamo sin contrato: existe en la conversación, pero no existe para la ley.”

Cesión sin consentimiento acreditable = infracción grave. Hasta 10.000 UTM — Art. 15.

La salida GlobalSign

Digital Signing Service: consentimientos y cesiones firmados, con autoría e integridad (Art. 12, 15).

Timestamping: fecha cierta e inalterable de cada autorización.

S/MIME: cifra el correo con datos financieros antes de enviarlos.

+188%

de las filtraciones en Chile golpean sectores con brechas en autenticación y credenciales (Entel, Reporte Ciberseguridad 2026).



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



04 · CASOS DE USO POR SECTOR — GOBIERNO

Una contraseña, miles de datos expuestos

El escenario

Un funcionario perdió el control de sus credenciales. No hizo falta vulnerar ningún sistema: bastó ese usuario y contraseña para acceder a servicios públicos y filtrar nombres, direcciones e incluso fichas médicas. La ANCI confirmó el incidente; los expertos hablan de “arquitecturas de seguridad excesivamente optimistas”.

“Proteger sistemas de Estado solo con contraseñas es como cerrar la puerta principal del edificio... y dejar la llave maestra bajo el felpudo.”

Cesión de datos entre órganos sin resguardo acreditable = infracción bajo Art. 21 y 22.

La salida GlobalSign

Managed PKI / Client Auth: reemplaza contraseñas por identidad digital; no se roba con phishing, no se adivina.

TLS: cifra el canal entre sistemas y portales de trámites.

S/MIME + firma: cesión entre servicios con remitente verificable e íntegro (Art. 22).

8,8B

intentos de ciberataque registró Chile en 2025 (Fortinet Global Threat Landscape Report).

04 · CASOS DE USO POR SECTOR — EDUCACIÓN

La ficha médica que corrió por WhatsApp

El escenario

Un profesor comparte por WhatsApp el informe con el diagnóstico de salud de un estudiante para coordinarse con otro docente. Nadie pidió autorización específica a los padres. El colegio conserva esos datos años después de que el alumno egresó, sin que nadie sepa con certeza quién los ha visto.

“Enviar la ficha médica de un niño por WhatsApp es como dejar su carpeta confidencial abierta en el pasillo: no hay forma de saber quién la leyó, ni cuándo.”

Datos de niños y adolescentes: protección reforzada (Art. 16 quáter) — consentimiento parental específico y verificable.

La salida GlobalSign

TLS y S/MIME: portales de apoderados y comunicaciones docentes cifradas; se acabó el WhatsApp no oficial para datos sensibles.

Digital Signing Service: consentimiento específico y verificable por tramo de edad, firmado en la matrícula.

Certificados de autenticación: solo personal autorizado accede al informe.

100%

de los colegios analizados vulnera datos de sus estudiantes (Fundación Observatorio Ciudadano@ Digital).

04 · CASOS DE USO POR SECTOR — SALUD

250 GB de historiales que no debían salir

El escenario

En diciembre de 2025, un grupo de ransomware exfiltró cerca de 250 GB de datos de pacientes de una clínica chilena: fichas clínicas, cédulas de identidad y resultados de exámenes de alta sensibilidad, incluidos diagnósticos de VIH. SERNAC exigió una cronología oficial; la clínica aún no puede precisar cuántos pacientes fueron afectados.

“Guardar la ficha clínica de un paciente sin cifrado es como dejar su historial médico fotocopiado en la sala de espera : cualquiera que pase puede llevárselo .”

Datos de salud sin resguardo reforzado = infracción gravísima. Hasta 20.000 UTM — Art. 16 · 16 bis.

La salida GlobalSign

S/MIME y TLS: cifran el traslado de fichas entre clínica, laboratorio, aseguradora y telemedicina.

Managed PKI / Client Auth: solo personal autorizado accede a sistemas clínicos y expedientes.

IoT Identity Platform: identidad fuerte para dispositivos médicos conectados (IoMT).

250 GB

de información sensible expuesta en un solo incidente de ransomware a una clínica chilena (SERNAC, dic. 2025).



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



04 · CASOS DE USO POR SECTOR — RETAIL Y E-COMMERCE

Las llaves de la tienda sin contrato firmado

El escenario

Un e-commerce entrega a diario nombre, dirección y teléfono de sus clientes a la pasarela de pago, al courier y a la plataforma de email marketing. Nadie firmó un contrato de encargo (DPA) con ninguno de ellos. El día que uno de esos proveedores sufre una brecha, la tienda responde igual: la ley hace responsable a quien encarga el dato, no solo a quien lo filtró.

“Enviar los datos de tus clientes a un proveedor sin DPA firmado es como entregarle las llaves de tu tienda a un repartidor: confías en que la cerrará bien, pero no tienes cómo probarlo.”

Tratamiento por encargo sin contrato acreditable = brecha más frecuente del retail — Art. 15 · 15 bis · 15 ter.

La salida GlobalSign

Digital Signing Service: DPA firmados y con fecha cierta para cada proveedor de pago, courier y marketing.

TLS / Managed SSL: cifra checkout, APIs y formularios de cada canal de venta.

Managed PKI / Client Auth: autenticación fuerte entre tienda, pasarela y marketplace.



SEGURIDADAMÉRICA.com
Fortaleciendo Internet



04 · CASOS DE USO POR SECTOR — EMPRESAS Y RECURSOS HUMANOS

La puerta blindada... con la ventana abierta

El escenario

Una empresa invierte en ciberseguridad para proteger a sus clientes, pero las liquidaciones de sueldo, contratos y evaluaciones de desempeño de sus propios trabajadores circulan por correo sin cifrar entre RR.HH. y jefaturas. El 60% de las empresas en Chile ya sufrió una fuga de datos confidenciales en los últimos dos años, y los datos de empleados están entre los menos protegidos y los menos reportados.

“Blindar la puerta de calle para proteger a los clientes y dejar la ventana de la oficina abierta para los propios empleados : la fuga entra igual , solo que por el lado que nadie vigila .”

El deber de secreto aplica a todo dato personal, también el laboral —
Art. 3 h · 14 bis · 14 quinquies.

La salida GlobalSign

S/MIME: cifra liquidaciones, contratos y evaluaciones entre RR.HH. y jefaturas.

Digital Signing Service: contratos laborales y finiquitos firmados, con autoría e integridad.

Managed PKI / Client Auth: acceso por identidad digital a portales internos de RR.HH. y nómina.

60%

de las empresas chilenas sufrió fuga de datos confidenciales en los últimos dos años (Kaspersky).



Gracias...

CONTACTO

ventas@seguridadamerica.com