Ciberseguridad: El Pariente Pobre de la Gestión Interna Municipal

Desafíos y Estrategias para Gobiernos Locales

Pilares de la Seguridad en la Gestión Municipal

Ciberespacio

Entorno digital donde interactúan personas, organizaciones y máquinas.

Seguridad de la Información

Protección de activos críticos y ciberseguridad municipal.

Servicios Esenciales

Identificación y resguardo de la infraestructura crítica local.

Protección de Datos

Gestión ética y legal de la información de los ciudadanos.

Transformación Digital

Influencia de la digitalización en la seguridad institucional.

Marco Normativo

Cumplimiento de normas generales y sectoriales vigentes.

Marco normativo

Ley N° 21.663 (Ley Marco de Ciberseguridad)

Ley N° 21.459 (Ley de Delitos Informáticos)

Política Nacional de Ciberseguridad 2023-2028

Ley N° 19.628 vigente, Ley N° 21.719, Nueva Ley de Protección de Datos

Ley N° 19.799 (Firma Electrónica)

Ley N° 20.285 (Ley de Transparencia)

CMF: Capítulo 20-10 RAN Gestión de Seguridad de la Información y Ciberseguridad 20-7 RAN Externalización de Servicios

SUBTEL: Resolución Exenta N° 1.318 norma técnica sobre ciberseguridad para el diseño, instalación y operación de redes de telecomunicaciones.

Sector Energía: Estándar de Ciberseguridad para el Sector Eléctrico.

Sector Salud : Instructivo ITS-NC-007 Seguridad de la Información y Ciberseguridad para el Sector Salud

Decreto Supremo N° 83 de 2005: seguridad y confidencialidad de los documentos electrónicos en el sector público,

Introducción a la Protección de Datos Personales

Conceptos Fundamentales

Definición de datos personales, tipos y principios rectores.

Ley 19.628

Marco legal actual sobre la protección de la vida privada.

Nueva Ley 21.719

Actualización normativa y nuevos estándares de protección.

Desafíos en la Gestión

Retos actuales para la implementación en municipalidades.

Evolución Normativa en Chile

1999: Ley 19.628

Primera ley sobre protección de datos personales en Chile, centrada en la protección de la vida privada.

Principales limitaciones: Sin órgano fiscalizador, sanciones insuficientes, consentimiento tácito.

2018: Reforma Constitucional

Modificación del artículo 19 N°4 de la Constitución, incorporando explícitamente la protección de datos personales como derecho fundamental.

2022: Ley 21.459

Establece normas sobre delitos informáticos, incluyendo acceso ilícito a datos personales.

2024: Ley 21.719

Nueva ley integral de protección de datos personales, alineada con estándares internacionales como el RGPD europeo.

Entrada en vigencia: 01-DIC-2026

Fuente: Biblioteca del Congreso Nacional de Chile.

El Derecho Fundamental a la Protección de Datos

Definición Legal

"Cualquier información vinculada o referida a una persona natural identificada o identificable." (Ley 21.719)

Marco Constitucional

Artículo 19 N°4: "El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales."

Principios Rectores

- **Licitud**
- **Proporcionalidad**
- **Responsabilidad**
- **Transparencia**
- **Finalidad**
- **Calidad**
- **Seguridad**

Categorías Especiales de Protección

Según la **Ley 21.719**, los datos sensibles son aquellos que requieren un nivel superior de resguardo debido a su potencial impacto en la privacidad y dignidad de las personas.

- **Datos biométricos**
- **Salud y perfil biológico**
- **Origen étnico o racial**
- **Afiliación política o sindical**
- **Situación socioeconómica**
- **Creencias religiosas o filosóficas**
- **Vida y orientación sexual**
- **Identidad de género**

Principales Cambios con la Ley 21.719

Agencia de Protección de Datos

Creación de un órgano autónomo con facultades fiscalizadoras y sancionatorias para velar por el cumplimiento de la ley.

Sanciones Efectivas

Multas de hasta **10.000 UTM** para infracciones graves (aproximadamente 600 millones de pesos).

Consentimiento Explícito

Manifestación de voluntad libre, específica, inequívoca e informada del titular para el tratamiento de sus datos.

Obligaciones Municipales

Designación de **Delegado de Protección de Datos (DPO)**, registro de actividades y evaluaciones de impacto.

Brechas Críticas en la Gestión de Datos

Recursos Limitados

No hay políticas o no están actualizadas, no hay un encargado o personal del área capacitado o simplemente no hay, además de la falta de infraestructura

Sistemas Heredados

Sistemas e Infraestructura obsoleta que dificulta implementar medidas de seguridad modernas.

Capacitación Insuficiente

No se capacita a los funcionarios, no se dispone de un manual de protección de dato, no se alfabetiza a los usuarios y vecinos

Estrategias para enfrentar esta nueva realidad

Actualización de Políticas

Revisar y adaptar las políticas de protección de datos a la nueva Ley 21.719.

Capacitación Continua

Formar a los funcionarios municipales en el manejo ético y legal de la información.

Evaluaciones de Impacto

Realizar análisis de riesgos periódicos sobre el tratamiento de datos personales.

Designación de Delegado

Nombrar un Delegado de Protección de Datos (DPD) según lo exige la normativa.

Inventario de Datos

Mapear todos los datos personales que maneja la municipalidad y sus flujos.

Plan de Acción

Desarrollar una hoja de ruta para la implementación gradual.

Custodia de Datos de Salud: Ley 21.668

Interoperabilidad

Obligación de los prestadores de salud de permitir el acceso y transferencia de datos clínicos entre instituciones para asegurar la continuidad del cuidado.

Ficha Clínica Digital

Exigencia de mantener registros electrónicos seguros, garantizando la integridad, autenticidad y confidencialidad de la información médica.

Plazo de Custodia Obligatoria: Mínimo de 15 años desde la última atención registrada en la ficha clínica del paciente.

Ley Marco de Ciberseguridad (Ley 21.663)

Objetivos Principales

Establecer la institucionalidad necesaria para robustecer la ciberseguridad nacional.

- Fijar requisitos mínimos de prevención, contención y respuesta ante incidentes.
- Regular las atribuciones y deberes de los órganos del Estado y servicios esenciales.

Alcance Municipal: Obligatoriedad de implementar medidas de seguridad y reportar incidentes significativos a la ANCI.

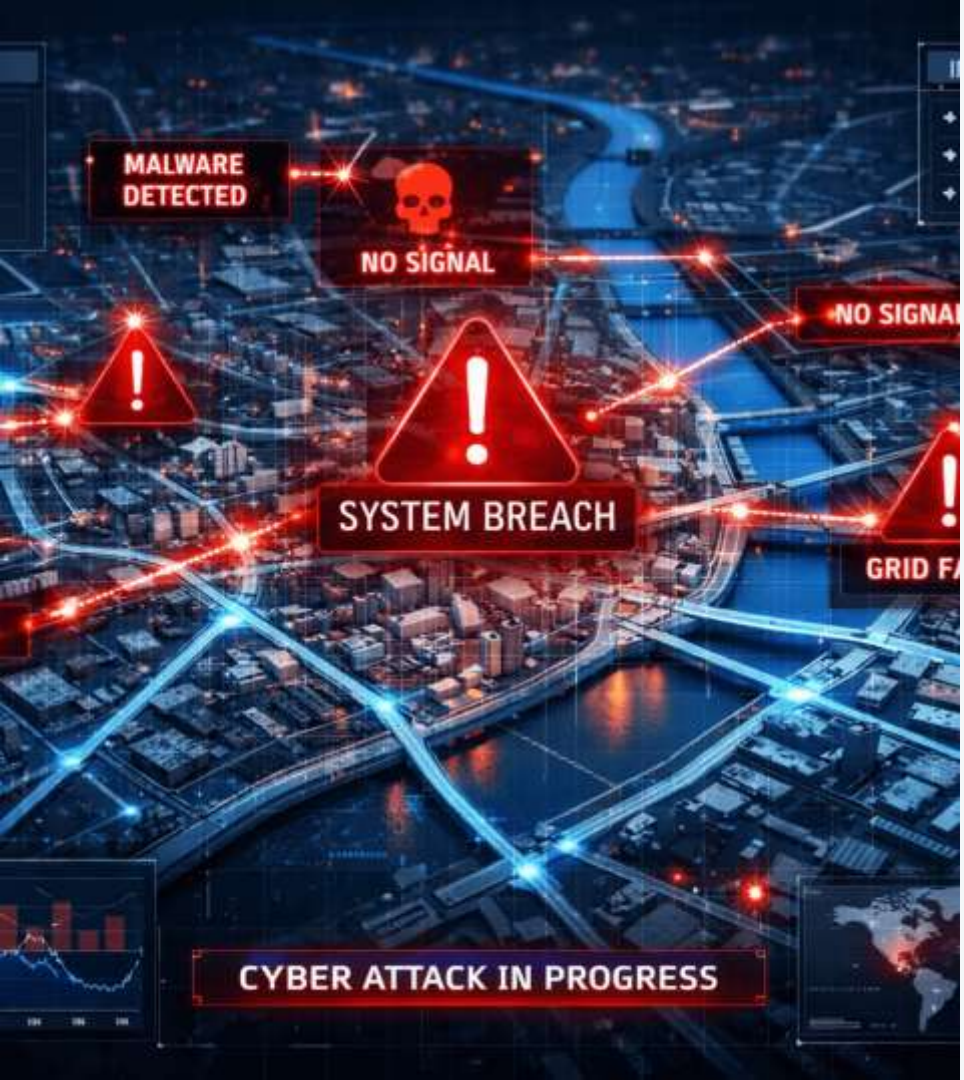
Nueva Institucionalidad

ANCI: Agencia Nacional de Ciberseguridad, órgano rector con facultades normativas y sancionatorias.

- **CSIRT Nacional:** Centro de Respuesta ante Incidentes de Seguridad Informática.
- **Consejo Consultivo:** Instancia de colaboración público-privada y académica.

Multas Ley Marco de Ciberseguridad (Ley 21.663) - Chile

Gravedad	Servicios Esenciales (SE)	Operadores de Importanica Vital (OIV)
Leves	Hasta 5.000 UTM	Hasta 10.000 UTM
Graves	Hasta 10.000 UTM	Hasta 20.000 UTM
Gravisimas	Hasta 20.000 UTM	Hasta 40.000 UTM



Ciberataques en el Sector Público (Chile 2024)

+200%

Incremento en Intentos de Ataque

- **Ransomware:** Principal amenaza para la continuidad de servicios municipales y secuestro de bases de datos.
- **Phishing Dirigido:** Suplantación de autoridades para obtener credenciales de acceso a sistemas internos.
- **Exfiltración de Datos:** Robo de información sensible de ciudadanos para su venta en mercados ilícitos.

Fuente: Reporte de Ciberseguridad CSIRT de Gobierno (2024).

Ecosistema Legal de Ciberseguridad

Ley 21.663

Ley Marco de Ciberseguridad e Infraestructura Crítica de la Información.

Ley 21.719

Nueva ley de protección de datos personales y creación de la Agencia.

Ley 20.285

Sobre acceso a la información pública. Regula el principio de transparencia y el derecho de acceso a la información del Estado.

Ley 21.459

Normas sobre delitos informáticos y persecución penal en el ciberespacio.

Ley 21.180

Sobre transformación digital del Estado. Obliga a las municipalidades a digitalizar sus procesos y servicios.

Ley 19.799

Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.

Interconexión Legal

Estas leyes forman un bloque normativo integral para la seguridad digital.

Tipificación de Delitos (Ley 21.459)

Acceso Ilícito

Acceder a un sistema informático sin autorización o excediendo la que se posee, superando medidas de seguridad.

Interceptación Ilícita

Captar o interceptar transmisiones de datos informáticos no públicos hacia, desde o dentro de un sistema informático.

Ataque a la Integridad

Dañar, borrar, deteriorar, alterar o suprimir datos informáticos, o impedir el funcionamiento de un sistema.

Falsificación Informática

Introducir, alterar, borrar o suprimir datos para generar información no auténtica con el fin de que sea utilizada como legal.

Ley 21.459: Establece normas sobre delitos informáticos y deroga la Ley 19.223.

Casos en Municipalidades

Municipalidad de Chiguayante (2023)

Ataque ransomware que cifró bases de datos de contribuyentes y paralizó servicios

Municipalidad de Concepción (2025)

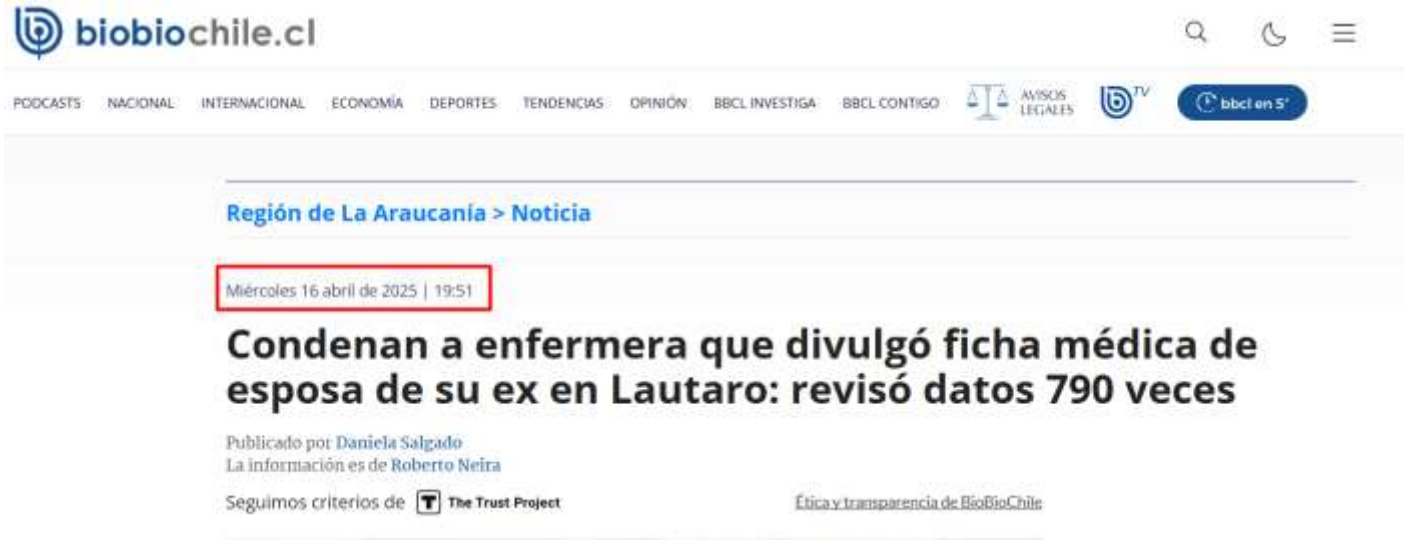
Hackeo de clave única: Se gira factura por $39 millones.

Municipalidad de Temuco (y otras) (2023)

Ataque a la cadena de suministro (GTD) provocó interrupción de servicios,

Impacto Común: Interrupción de servicios esenciales, daño reputacional y exposición legal.

Fuente: Notas de prensa: https://www.biobiochile.cl/noticias/nacional/region-del-bio-bio/2023/12/27/ciberataque-paraliza-servicios-digitales-de-la-municipalidad-de-chiguayante.shtml
https://www.biobiochile.cl/noticias/nacional/region-del-bio-bio/2025/05/08/municipio-de-concepcion-se-querella-por-hackeo-de-clave-unica-detectan-factura-por-39-millones.shtml
https://www.biobiochile.cl/noticias/nacional/region-de-la-araucania/2023/10/25/sistemas-informaticos-de-la-municipalidad-de-temuco-fueron-afectados-por-ataque-de-hackers.shtml



…el fiscal Enrique Vásquez explicó que la enfermera accedía a las fichas clínicas a través del sistema computacional del Servicio de Salud Araucanía. Por lo anterior, fue declarada culpable de revelar información confidencial obtenida gracias a su acceso al sistema de salud.

La condena en su contra implica la suspensión de cargos públicos por un año y una multa de más de 400 mil pesos (6 UTM).

Fuente: https://www.biobiochile.cl/noticias/nacional/region-de-la-araucania/2025/04/16/condenan-a-enfermera-que-divulgo-ficha-medica-de-esposa-de-su-ex-en-lautaro-reviso-datos-790-veces.shtml

Deberes Críticos del Municipio

Reporte de Incidentes

Obligación de informar incidentes significativos a la ANCI y al CSIRT Nacional de manera oportuna.

Capacitación Continua

Formar a los funcionarios en buenas prácticas de ciberseguridad y manejo de información sensible.

Actualización de Sistemas

Mantener la infraestructura tecnológica al día con los últimos parches de seguridad y normativas.

Gestión de Riesgos

Realizar evaluaciones periódicas para identificar y mitigar vulnerabilidades en la gestión municipal.

Referencias Clave para la Gestión

Asociatividad

Asociación Chilena de Municipalidades, Asociación de informáticos municipales y Asociación de Encargados de ciberseguridad municipal

CSIRT de Gobierno

Equipo de Respuesta ante Incidentes del Ministerio del Interior. **www.csirt.gob.cl**

ANCI / Agencia de protección de Datos

Organismos rectores creados por las leyes 21.663 y 21.719 para supervisión nacional.

SGD - Transformación Digital

Normativa y guías técnicas para digitalización del Estado. **www.segpres.gob.cl**

Equipos robustos y con separación de funciones

Encargados por cada área y personales especializado en cada disciplina

Medidas Técnicas y Organizativas Esenciales

Control de Acceso

Implementación de **Autenticación de Doble Factor (MFA)** y gestión de privilegios mínimos para reducir la superficie de ataque interna.

Seguridad Perimetral

Uso de Firewalls de nueva generación, sistemas de detección de intrusos (IDS/IPS) y segmentación de redes críticas municipales.

Respaldos (Backups)

Estrategia **3-2-1**: tres copias de seguridad, en dos medios distintos y una copia fuera de línea (offline) para protección contra ransomware.

Cifrado de Datos

Encriptación de información sensible tanto en reposo (servidores y dispositivos) como en tránsito (comunicaciones seguras HTTPS/TLS).

Hoja de Ruta para la Gestión Cibersegura

01 Diagnóstico Inicial

Evaluar el estado actual de la infraestructura, políticas y capacitación. Identificar **activos críticos** y brechas normativas.

02 Planificación Estratégica

Diseñar un plan de adecuación a las leyes 21.663 y 21.719. Definir presupuestos, roles y el cronograma de implementación.

03 Implementación de Controles

Ejecutar medidas técnicas (MFA, cifrado, respaldos) y organizativas (manuales, DPO). Establecer **protocolos de respuesta**.

04 Monitoreo y Mejora

Realizar auditorías periódicas y simulacros. Actualizar políticas según nuevas amenazas y lecciones aprendidas de incidentes.

¡Muchas Gracias por su Atención!

Mauricio Hernández Moraga

Ingeniero de Ejecución en Informática

Municipalidad de Mulchén

Diplomado en ciberseguridad y ciberdefensa Universidad Autónoma

Artics - Sociedad Chilena de Seguridad de la información - Fundación Whilolab

+56971385298 // mhernandez@munimulchen.cl