CORPORACION MUNICIPAL
Gabriel González Videla
La Serena

PROTOCOLO DE RESGUARDO Y TRATAMIENTO DE INFORMACIÓN SENSIBLE DEPARTAMENTO DE CONTROL INTERNO

2025

PROTOCOLO DE RESGUARDO Y TRATAMIENTO DE INFORMACIÓN SENSIBLE

DEPARTAMENTO CONTROL INTERNO
CORPORACIÓN MUNICIPAL GABRIEL GONZÁLEZ VIDELA

Este protocolo ha sido aprobado por el Secretario General de la Corporación Municipal Gabriel González Videla:

NOMBRE	CARGO	FIRMA	FECHA
NILO LUCERO ARANCIBIA	SECRETARIO GENERAL		02.SEP.2025

CORP. MUNICIPAL GABRIEL GONZÁLEZ VIDELA SECRETARIO GENERAL LA SERENA

EQUIPO DE TRABAJO

NOMBRE	CARGO	ROL
GUSTAVO PRADENAS CRUCES	AUDITOR GENERAL	ELABORACIÓN
GONZALO PINOCHET ABARCA	DIRECTOR DE CUMPLIMIENTO Y PREVENCIÓN DEL DELITO	REVISIÓN
JENNY CONCHA CASANOVA	DIRECTORA DEPARTAMENTO CONTROL INYERNO	REVISIÓN

CONTENIDO

I. INTRODUCCIÓN

La adecuada protección, tratamiento y resguardo de la información sensible es un pilar fundamental para el cumplimiento de los principios de legalidad, transparencia, confidencialidad y seguridad dentro de la Corporación Municipal Gabriel González Videla. En un contexto institucional que maneja datos personales, antecedentes financieros, jurídicos y documentos directivos, se hace imprescindible la existencia de un marco normativo interno que regule el ciclo de vida de la información sensible desde su recolección hasta su eliminación segura.

Este protocolo busca establecer los principios, criterios y procedimientos que orienten el actuar del personal del Departamento de Control Interno en el manejo seguro y responsable de los datos, en cumplimiento de la legislación chilena vigente, especialmente la Ley N° 19.628 sobre protección de la vida privada y su modificación mediante la Ley N° 21.719, así como los lineamientos del Consejo para la Transparencia y otras disposiciones aplicables.

1. OBJETIVO

Establecer un marco procedimental y normativo para el resguardo, tratamiento y protección de la información sensible en posesión o bajo tratamiento del Departamento de Control Interno de la Corporación Municipal Gabriel González Videla, con énfasis en:

- Proteger los datos personales y sensibles de funcionarios, usuarios y terceros vinculados.
- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Prevenir filtraciones, accesos indebidos o pérdidas de información.
- Definir roles y responsabilidades en el ciclo de vida de la información.
- Cumplir con la normativa legal y técnica vigente.

2. ALCANCE

Este protocolo aplica a todos los funcionarios, profesionales, administrativos, prestadores externos y cualquier persona que tenga acceso a información clasificada como sensible en el contexto de las funciones del Departamento de Control Interno.

La información sensible considerada incluye:

- Datos personales y sensibles (RUT, domicilio, salud, filiación, antecedentes laborales, etc.).
- Informes de auditoría, denuncias, investigaciones internas.
- Documentación financiera, de compras públicas, sumarios y sanciones.
- Registros internos en soporte físico y digital.

II. BASE LEGAL Y NORMATIVA

- Ley N° 19.628 sobre protección de la vida privada.
- Ley N° 21.719 (modificación de la ley anterior, 2024).
- Ley N° 20.285 sobre acceso a la información pública.
- Recomendaciones del Consejo para la Transparencia.
- Ley N° 18.575 sobre Bases Generales de la Administración del Estado.
- Reglamento interno y políticas institucionales.

III. DEFINICIONES

1. Información sensible

Toda información que, al ser divulgada o utilizada indebidamente, pueda afectar la intimidad, seguridad, honra o derechos fundamentales de las personas. Incluye, entre otras, información relativa a salud, orientación sexual, convicciones religiosas, políticas, datos biométricos o antecedentes penales.

2. Datos personales

Cualquier información relativa a una persona natural, identificada o identificable, directa o indirectamente, mediante datos como nombre, RUT, domicilio, correo electrónico, etc.

3. Datos personales sensibles

Aquellos que se refieren a las características más íntimas de la persona y que requieren de un mayor grado de protección legal, tales como origen étnico, estado de salud, orientación sexual, creencias religiosas, opiniones políticas, y afiliación sindical.

4. Tratamiento de datos

Cualquier operación o conjunto de operaciones que se realicen sobre datos personales, ya sea por medios automatizados o manuales, incluyendo la recolección, almacenamiento, modificación, acceso, transmisión, eliminación o cualquier otra forma de utilización.

5. Responsable del tratamiento

Unidad, persona natural o jurídica que decide sobre la finalidad, medios y alcance del tratamiento de datos personales. En este protocolo, el responsable es el Departamento de Control Interno.

6. Encargado del tratamiento

Persona natural o jurídica que realiza el tratamiento de datos por cuenta del responsable, siguiendo sus instrucciones.

7. Titular de los datos

Persona natural a quien se refieren los datos personales o sensibles.

8. Delegado de Protección de Datos (DPD)

Funcionario del Departamento de Control Interno encargado de velar por el cumplimiento de la normativa vigente sobre protección de datos dentro de la organización. Debe supervisar las políticas internas, recibir solicitudes y denuncias, y actuar como enlace con las autoridades competentes.

9. Incidente de seguridad

Evento que compromete la confidencialidad, integridad o disponibilidad de los datos personales o sensibles, como accesos no autorizados, filtraciones, pérdidas o alteraciones indebidas.

10. Consentimiento informado

Manifestación libre, específica, inequívoca e informada del titular de los datos, mediante la cual acepta el tratamiento de sus datos personales para una finalidad determinada.

11. Medidas de seguridad

Conjunto de políticas, procedimientos, herramientas tecnológicas y controles físicos destinados a proteger los datos personales y sensibles frente a accesos no autorizados, alteración, pérdida, robo o destrucción.

12. Ciclo de vida de la información

Todas las fases que atraviesa la información desde su creación o recolección, uso, almacenamiento, transferencia (compartición), hasta su eliminación o destrucción segura.

IV. PRINCIPIOS RECTORES

La aplicación de principios rectores constituye la base para un tratamiento responsable, coherente y legítimo de la información sensible. Estos principios orientan el actuar de la Corporación en todas las etapas del ciclo de vida de los datos, asegurando el respeto a los derechos de los titulares y el cumplimiento de la normativa vigente. Establecerlos de

forma explícita permite definir un marco ético y normativo para prevenir vulneraciones y fortalecer la cultura organizacional en torno a la protección de datos.

1. **Licitud**

Todo tratamiento de datos debe basarse en una causa legalmente permitida o en el consentimiento informado del titular. La obtención, uso y conservación de datos sin una base legal válida constituye una infracción grave a los derechos fundamentales de las personas.

2. Finalidad

Los datos personales y sensibles sólo podrán ser utilizados para los fines específicos, explícitos y legítimos para los cuales fueron recolectados. Queda prohibida su utilización posterior para fines incompatibles sin el consentimiento del titular.

3. Proporcionalidad

Se deben recopilar únicamente los datos estrictamente necesarios para cumplir con la finalidad establecida. La recolección excesiva o irrelevante constituye un riesgo para los derechos de los titulares.

4. Seguridad

La Corporación debe adoptar todas las medidas técnicas, administrativas y organizativas razonables para proteger los datos frente a accesos no autorizados, pérdidas accidentales, destrucción o alteración indebida. Estas medidas deben revisarse periódicamente.

5. Confidencialidad

Todos los funcionarios, proveedores o terceros que accedan a datos personales o sensibles están obligados legal y contractualmente a mantener reserva sobre ellos,

incluso después del término de su relación con la institución. El incumplimiento podrá acarrear sanciones administrativas y legales.

La confidencialidad implica también la obligación de clasificar correctamente la información según su nivel de acceso:

- **Información Pública:** de libre acceso conforme a la Ley N.º 20.285 y disposiciones institucionales.
- **Información Reservada:** restringida a funcionarios autorizados, cuya divulgación podría afectar procesos administrativos, auditorías o investigaciones.
- **Información Secreta o Crítica:** limitada a personal expresamente autorizado, cuya divulgación indebida podría comprometer derechos fundamentales, generar responsabilidades legales o poner en riesgo la seguridad institucional.

El respeto a esta clasificación es obligatorio y se formaliza mediante la firma del "Compromiso de Confidencialidad" (Anexo Nº 1).

6. Responsabilidad proactiva

El Departamento de Control Interno debe no solo cumplir con la normativa, sino también demostrar dicho cumplimiento a través de políticas documentadas, controles internos, registros de actividades y respuesta ante incidentes. Esto implica una gestión preventiva y no solo reactiva de los riesgos asociados al tratamiento de datos.

Para comprender de manera integral la gestión de datos y su adecuada protección, se ha definido el "Ciclo de Vida de la Información", que establece las etapas que atraviesa todo dato sensible o personal en la Corporación. Dicho ciclo permite visualizar las responsabilidades en cada fase y constituye la base para las medidas de resguardo y controles descritos en este protocolo.

V. Ciclo de Vida de la Información

La gestión de la información en la Corporación se sustenta en un enfoque integral que considera todas las etapas que atraviesan los datos personales y sensibles desde su origen hasta su eliminación definitiva. Este ciclo constituye una herramienta fundamental para garantizar la trazabilidad, seguridad y transparencia del tratamiento de los datos, alineado con los principios rectores ya expuestos.

El Ciclo de Vida de la Información permite identificar los momentos críticos donde deben aplicarse controles y medidas de resguardo, asegurando así que cada fase cuente con estándares adecuados de protección y uso responsable. Sus etapas son:

1. Recolección o creación

Corresponde a la obtención inicial de los datos, ya sea de funcionarios, usuarios o terceros. Se debe verificar la base legal y clasificar la información como pública, reservada o secreta (Anexo N° 2).

2. Almacenamiento

Una vez creada, la información debe resguardarse en repositorios físicos o digitales que garanticen su integridad, disponibilidad y confidencialidad. El almacenamiento debe realizarse en plataformas institucionales autorizadas y, en el caso de medios digitales, considerar medidas de respaldo y cifrado (véase Política de Respaldo y Cifrado, Anexo N° 3).

3. Compartición

La transferencia de información entre funcionarios, unidades o terceros debe realizarse bajo protocolos definidos, garantizando que sólo tengan acceso quienes cuenten con autorización expresa. El registro de accesos y transferencias constituye un mecanismo esencial para mantener la trazabilidad.

4. Uso

La utilización de la información debe ajustarse estrictamente a los fines para los cuales fue recolectada y autorizada. Se prohíbe expresamente el uso indebido, la manipulación con fines ajenos a la institución o cualquier acción que vulnere los derechos de los titulares de datos.

5. Eliminación

La información, una vez cumplida su finalidad o transcurridos los plazos legales de conservación, debe ser eliminada de forma segura. En el caso de información digital, esto implica la destrucción lógica mediante procesos certificados; en el caso de soportes físicos, la eliminación debe realizarse mediante procedimientos de destrucción segura (triturado, incineración o técnicas equivalentes).

Figura N° 1 “Ciclo de Vida de la Información”
Fuente: Elaboración propia.

VI. RESPONSABILIDADES

La adecuada gestión de la información sensible requiere una clara asignación de responsabilidades a fin de garantizar que cada actor institucional conozca sus funciones y límites de actuación. Las responsabilidades se estructuran de la siguiente manera:

1. Auditor General

Tiene la responsabilidad general de asegurar la implementación, supervisión y actualización del presente protocolo. Debe velar por que todos los procesos de tratamiento de datos se ajusten a la normativa vigente y a las políticas institucionales. Además, debe disponer y/o gestionar los recursos humanos, técnicos y financieros necesarios para el cumplimiento de las medidas de resguardo.

2. Delegado de Protección de Datos (DPD)

Responsable de coordinar la ejecución de este protocolo, supervisar el cumplimiento de las medidas técnicas y organizativas, canalizar las solicitudes de ejercicio de derechos de los titulares, gestionar incidentes de seguridad y actuar como enlace con la autoridad de control en materia de protección de datos. Además, es responsable de mantener actualizado el “Registro de Incidentes de Seguridad” (Anexo N° 5), asegurando que todos los casos reportados se documenten con fecha, descripción, medidas adoptadas y resultados. Este registro deberá estar disponible para auditorías internas y externas, garantizando la trazabilidad y la mejora continua.

3. Funcionarios Autorizados

Obligados a cumplir estrictamente con las políticas y procedimientos establecidos, así como a firmar el “Compromiso de Confidencialidad” (Anexo N° 1), el cual constituye un requisito previo e indispensable para el acceso y tratamiento de información sensible. Deben reportar de inmediato cualquier incidente, anomalía o sospecha de vulneración de la seguridad de la información.

4. Unidad de Informática y Seguridad de la Información

En coordinación con el Departamento de Control Interno, debe implementar y mantener las herramientas tecnológicas y medidas técnicas necesarias para proteger la información sensible. También es responsable de la detección y mitigación de amenazas cibernéticas y de la ejecución de la "Política de Respaldo y Cifrado" (Anexo N° 3), incluyendo:

- Generación y almacenamiento seguro de respaldos periódicos.
- Aplicación de mecanismos de cifrado de datos en reposo y en tránsito.
- Control de accesos y trazabilidad de usuarios.
- Destrucción segura de información cuando corresponda.

5. Proveedores y Terceros

Aquellos que accedan a información sensible deben suscribir acuerdos de confidencialidad y cumplir con las medidas de seguridad especificadas en los contratos o convenios, estando sujetos a auditorías o revisiones para verificar su cumplimiento.

Cuadro Sinóptico de Roles y Responsabilidades

Rol	Responsabilidades Principales	Documentos/ Anexos vinculados
Auditor General	– Supervisar la implementación y actualización del protocolo. – Velar por el cumplimiento de la normativa y políticas institucionales. – Gestionar recursos humanos, técnicos y financieros necesarios.	___
Delegado de Protección de Datos (DPD)	– Coordinar la ejecución del protocolo. – Supervisar medidas técnicas y organizativas. – Canalizar solicitudes de titulares de datos. – Gestionar incidentes de seguridad. – Mantener el Registro de Incidentes de Seguridad.	Anexo N° 5

Funcionarios autorizados	– Cumplir políticas y procedimientos. – Firmar el Compromiso de Confidencialidad. – Reportar incidentes o sospechas de vulneración de seguridad.	Anexo N° 1
Unidad de Informática y Seguridad de la Información	– Implementar y mantener medidas técnicas de seguridad. – Detectar y mitigar amenazas cibernéticas. – Colaborar en la elaboración y actualización del Registro de Incidentes de Seguridad. – Administrar la Política de Respaldo y Cifrado.	Anexo N° 3 Anexo N° 5
Proveedores y Terceros	– Suscribir acuerdos de confidencialidad. – Cumplir medidas de seguridad definidas en contratos/convenios. – Someterse a auditorías o revisiones.	Contratos y convenios

VII. MEDIDAS DE RESGUARDO

Las medidas de resguardo son el conjunto de acciones y controles implementados para garantizar que la información sensible se mantenga protegida frente a accesos no autorizados, alteraciones indebidas, pérdidas accidentales o destrucción. Estas medidas comprenden:

1. Controles de acceso

Implementación de credenciales personales, contraseñas robustas, autenticación multifactor y permisos diferenciados según funciones. La gestión de estos accesos será supervisada por el DPD y registrada en las auditorías internas.

2. Seguridad física

Uso de cerraduras, gabinetes con llave, control de ingreso a oficinas y bodegas de archivo, así como sistemas de vigilancia y registro de visitas, para reducir riesgos de acceso indebido.

3. Seguridad lógica

Cifrado de datos en reposo y en tránsito, actualización constante de software y parches de seguridad, protección antivirus y firewalls. Estas acciones deben cumplir con los estándares definidos en la “Política de Respaldo y Cifrado” (Anexo N° 3).

4. Copias de respaldo

Realización periódica de respaldos completos y diferenciales, almacenados en ubicaciones seguras y con cifrado. Se deben verificar periódicamente la integridad de los respaldos, conforme a lo establecido en la “Política de Respaldo y Cifrado” (Anexo N° 3).

5. Política de dispositivos externos

Control y restricción del uso de pendrives, discos duros y otros dispositivos portátiles, permitiendo únicamente aquellos autorizados y escaneados previamente escaneados por la Unidad de Informática y Seguridad de la Información.

6. Destrucción segura de información

Uso de trituradoras de corte cruzado para documentos en papel y herramientas de borrado seguro para archivos digitales, evitando cualquier posibilidad de recuperación indebida.

7. Concientización y capacitación

Programas regulares de formación para el personal sobre buenas prácticas en el manejo de información y prevención de incidentes, bajo supervisión del DPD y el Departamento de Control Interno.

8. Monitoreo y auditorías

Revisión periódica de accesos, registros de actividad y sistemas para detectar usos indebidos o vulnerabilidades. Todos los incidentes detectados deberán registrarse en el

"Registro de Incidentes de Seguridad" (Anexo N° 5), administrado por el DPD con apoyo técnico de la Unidad de Informática.

Estas medidas se complementan con el trabajo coordinado entre el Departamento de Control Interno y la Unidad de Informática y Seguridad de la Información, asegurando que la protección de datos sea integral y que las amenazas sean abordadas de manera preventiva y efectiva, fortaleciendo la rendición de cuentas en cada etapa del ciclo de vida de la información.

VIII. DERECHOS DEL TITULAR DE DATOS

El titular de los datos personales o sensibles tiene derechos garantizados por la legislación chilena, particularmente por la Ley N° 19.628 y la Ley N° 21.719. Estos derechos deben ser respetados y garantizados en todo momento por el Departamento de Control Interno y las demás unidades que traten dichos datos. Entre ellos se encuentran:

1. Derecho de acceso

El titular puede solicitar información sobre si sus datos están siendo tratados, el origen de los mismos, la finalidad del tratamiento y los destinatarios de la información.

2. Derecho de rectificación

Permite corregir datos inexactos o incompletos, garantizando que la información tratada sea siempre veraz, actualizada y pertinente para la finalidad con la que fue recolectada.

3. Derecho de cancelación o eliminación

Posibilita la supresión de los datos cuando hayan dejado de ser necesarios para el fin con el que fueron recogidos o cuando el tratamiento no se ajuste a la normativa.

4. Derecho de oposición

Permite al titular negarse al tratamiento de sus datos en circunstancias específicas, como cuando se afecten sus derechos fundamentales.

5. Derecho a la portabilidad

Recibir sus datos en un formato estructurado y transferirlos a otro responsable cuando corresponda.

El Departamento de Control Interno debe establecer un canal formal y accesible para que los titulares ejerzan estos derechos, con procedimientos claros, plazos establecidos y registro de las solicitudes.

Mecanismo formal para el ejercicio de derechos

Con el fin de garantizar la aplicación efectiva de los derechos reconocidos por la Ley N° 19.628 y la Ley N° 21.719, la Corporación dispondrá de un instrumento formal que facilite a los titulares ejercerlos de manera clara, accesible y trazable. Dicho instrumento será el “Formulario de Consentimiento Informado” (Anexo N° 6), el cual cumple las siguientes funciones:

- Permitir al titular manifestar de manera expresa e inequívoca su consentimiento para el tratamiento de datos personales y sensibles.
- Constituir un canal oficial para solicitar el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad.
- Dejar constancia escrita de que el titular ha recibido información completa, suficiente y comprensible sobre el uso, finalidad y resguardo de sus datos.
- Asegurar la trazabilidad documental de cada solicitud y su debido registro para fines de control interno y auditorías posteriores.

La recepción, tramitación y resguardo de estos formularios será responsabilidad directa del Departamento de Control Interno, el cual deberá establecer un procedimiento

estandarizado para su registro y seguimiento, garantizando respuesta dentro de los plazos legales vigentes.

IX. GESTIÓN DE INCIDENTES

La gestión de incidentes de seguridad es un proceso esencial para minimizar el impacto de cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de la información sensible. Una gestión adecuada permite contener el daño, cumplir con las obligaciones legales y normativas, y fortalecer la capacidad de respuesta institucional.

Ante un incidente, se deben seguir las siguientes directrices:

1. Detección y reporte inmediato

Cualquier funcionario que detecte o sospeche de un incidente debe informarlo de inmediato al Delegado de Protección de Datos (DPD) y a la Jefatura del Departamento de Control Interno. La rapidez en la comunicación es clave para minimizar el impacto.

- Toda filtración, acceso indebido, pérdida o manipulación indebida debe ser reportada al DPD en un plazo máximo de 24 horas.
- El DPD evaluará el impacto y determinará si se debe informar al Secretario General y paralelamente al Auditor General.
- Se deben generar informes de mejora para evitar recurrencia. Estos informes deben ir copiados al Director de Cumplimiento y Prevención del Delito.

2. Evaluación inicial

El DPD, en conjunto si es que corresponde con la Unidad de Informática y Seguridad de la Información, evaluará la naturaleza, el alcance y la gravedad del incidente. Esto incluye identificar el tipo de datos afectados y las posibles consecuencias para los titulares.

3. Contención y mitigación

Implementar medidas inmediatas para detener la amenaza y reducir el daño, como aislar sistemas comprometidos, cambiar credenciales de acceso o bloquear usuarios no autorizados.

4. Notificación

En caso de incidentes graves, se informará con conocimiento del Auditor General al Secretario General, cumpliendo con los plazos legales vigentes. En los informes que se generen, si corresponde, se copiará al Director de Cumplimiento y Prevención del Delito.

5. Documentación y registro

Todo incidente deberá quedar consignado en el “Registro de Incidentes de Seguridad” (Anexo N° 5), indicando datos básicos como fecha, descripción, responsables, acciones adoptadas y estado de resolución. El Delegado de Protección de Datos (DPD) administrará este registro y lo utilizará para auditorías internas, control interno y cumplimiento normativo.

6. Lecciones aprendidas

Tras la resolución del incidente, se realizará un análisis para identificar las causas, evaluar la efectividad de la respuesta y proponer mejoras que eviten la recurrencia.

Referencia gráfica

El procedimiento descrito se complementa con el “Flujo Gráfico de Información ante Incidentes” (Figura N° 2), que permite visualizar de manera esquemática la secuencia de responsabilidades y acciones.

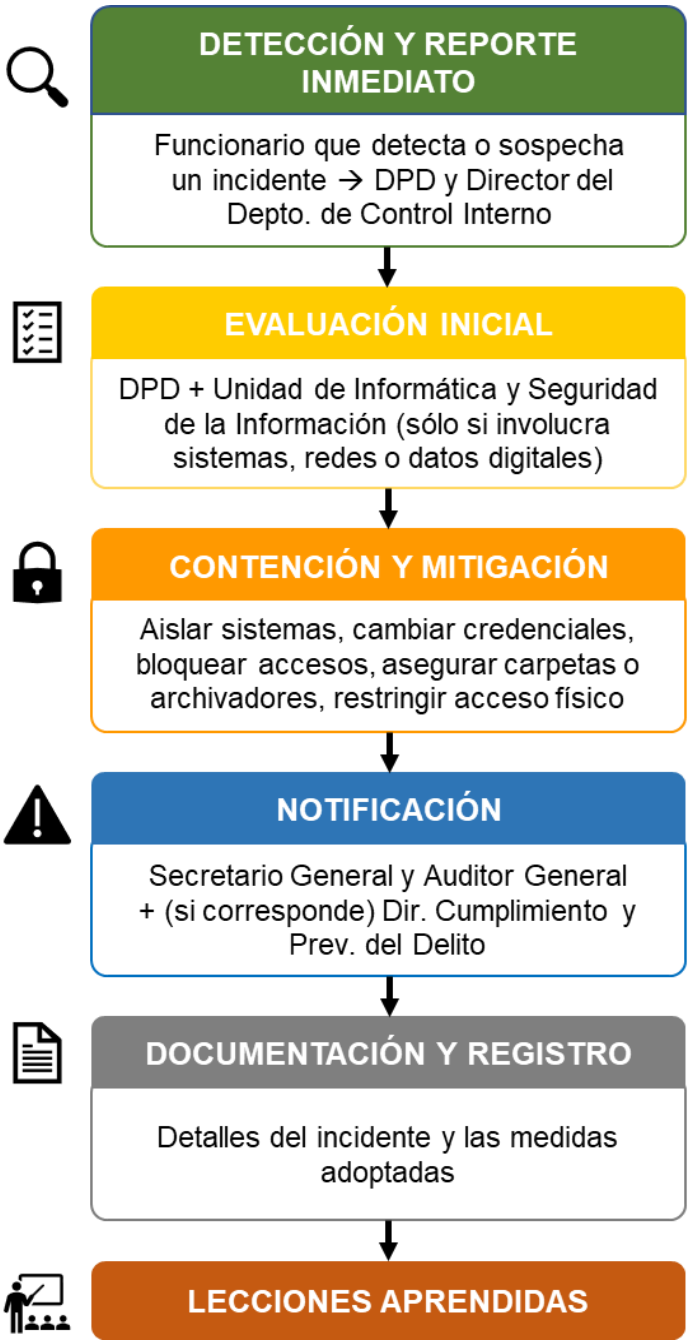

Figura N° 2 “Flujo Gráfico de Información ante Incidentes”
Fuente: Elaboración propia.

X. COORDINACIÓN CON LA UNIDAD DE INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN

La protección efectiva de la información sensible requiere una coordinación activa entre el Departamento de Control Interno y la Unidad de Informática y Seguridad de la Información. Esta articulación es clave para garantizar la implementación de medidas técnicas adecuadas, conforme a la normativa chilena y a los estándares de seguridad de la información.

1. Responsabilidades compartidas

Este apartado se refiere a las funciones y tareas que deben ejecutarse de manera coordinada entre el Departamento de Control Interno y la Unidad de Informática y Seguridad de la Información, con el fin de garantizar que la protección de datos sensibles, ya sean físicos o digitales, se realice de forma integral. Implica combinar la supervisión normativa con la aplicación de medidas técnicas, asegurando que la gestión de la información cumpla con la legislación chilena y con buenas prácticas de seguridad.

- Evaluar e implementar controles de acceso físico y lógico a los sistemas y archivos institucionales.
- Definir conjuntamente los protocolos de respaldo, cifrado, trazabilidad y destrucción segura de la información digital.
- Supervisar el uso de sistemas institucionales de mensajería, almacenamiento y gestión documental que cumplan con estándares de confidencialidad y trazabilidad.
- Garantizar que la respuesta ante incidentes abarque tanto el cumplimiento normativo como la aplicación de medidas técnicas eficaces, reduciendo riesgos y previniendo recurrencias.

2. Medidas adicionales recomendadas

Este apartado se refiere a aquellas acciones preventivas y correctivas que, si bien no siempre son exigidas por la normativa, fortalecen significativamente la seguridad de la información y reducen la probabilidad e impacto de incidentes. Su implementación conjunta por el Departamento de Control Interno y la Unidad de Informática y Seguridad de la Información permite ir más allá del cumplimiento mínimo, alineándose con buenas prácticas y estándares internacionales como la **ISO/IEC 27001**.

- **Capacitación y concientización:** Realizar entrenamientos periódicos para todo el personal en buenas prácticas de manejo de información sensible, incluyendo ciberseguridad, confidencialidad y resguardo físico.
- **Monitoreo y detección temprana:** Implementar sistemas de monitoreo continuo e IDS/IPS que alerten sobre accesos no autorizados, actividad anómala o intentos de intrusión.
- **Controles de acceso y contraseñas:** Establecer una política institucional de contraseñas que contemple claves robustas, autenticación de dos factores, vencimiento periódico y prohibición de reutilización de contraseñas.
- **Seguridad de red y dispositivos:** Aplicar segmentación de redes internas para aislar sistemas críticos y restringir el uso de dispositivos de almacenamiento externo (pendrives, discos duros, etc.).
- **Actualizaciones y protección antivirus:** Mantener actualizados los antivirus corporativos y aplicar parches de seguridad de forma periódica, reduciendo vulnerabilidades conocidas.
- **Almacenamiento seguro en la nube:** Utilizar plataformas institucionales que cumplan con estándares internacionales de seguridad, garantizando cifrado, trazabilidad y control de acceso.
- **Respaldo y recuperación:** Definir y cumplir protocolos de respaldo periódico y pruebas de restauración de datos, asegurando su disponibilidad ante contingencias.

- **Auditorías internas:** Ejecutar evaluaciones periódicas de cumplimiento y eficacia de las medidas técnicas y administrativas implementadas.
- **Cultura de seguridad:** Fomentar buenas prácticas mediante campañas internas, material informativo y simulacros de respuesta a incidentes.

3. Relación con la normativa vigente

Estas acciones están en concordancia con lo dispuesto por la Ley Nº 21.180 sobre Transformación Digital del Estado, la Ley Nº 19.628 y sus reformas, así como las recomendaciones del CSIRT de Gobierno y del Consejo para la Transparencia.

Esta colaboración interdepartamental fortalece la capacidad de respuesta ante incidentes, mitiga riesgos y permite una gestión integral de la información sensible institucional.

XI. VIGENCIA Y ACTUALIZACIÓN

Este protocolo entra en vigencia a contar de la fecha de su aprobación formal por el Secretario General, manteniéndose aplicable hasta que sea reemplazado o modificado por una versión posterior. Su objetivo es garantizar que los lineamientos y procedimientos aquí establecidos permanezcan actualizados, alineados con la normativa vigente, las mejores prácticas internacionales y la evolución de los riesgos asociados al manejo de información.

La vigencia de este protocolo será indefinida, sujeta a un proceso de revisión periódica al menos una vez cada 12 meses, o antes si se presentan cualquiera de las siguientes circunstancias:

- Cambios relevantes en la legislación nacional o internacional sobre protección de datos e información sensible.

- Incorporación de nuevas tecnologías, herramientas o metodologías que modifiquen la gestión de la información institucional.
- Resultados de auditorías internas o externas que recomienden ajustes.
- Lecciones aprendidas tras la gestión de incidentes significativos.
- Cambios en la estructura organizacional que afecten las responsabilidades asignadas.

Figura N° 3 “Ciclo de Revisión y Actualización del Protocolo”
Fuente: Elaboración propia.

La Unidad de Informática y Seguridad de la Información, en coordinación con el Departamento de Control Interno y bajo la supervisión del Delegado de Protección de Datos, será responsable de:

- Monitorear la vigencia de las disposiciones contenidas en este documento.
- Proponer modificaciones y actualizaciones, las que deberán ser evaluadas por el Auditor General y aprobadas por el Secretario General.
- Comunicar de manera formal y oportuna cualquier cambio a todo el personal, asegurando que la versión actualizada esté siempre disponible en los canales oficiales.

Cada actualización deberá registrarse en el “Historial de Cambios” (Anexo N° 4), indicando la fecha, el motivo de la modificación y las secciones afectadas. Este registro permitirá dar trazabilidad al proceso de mejora continua y garantizará transparencia en la gestión documental.

ANEXOS

- Anexo N° 1: Compromiso de Confidencialidad.
- Anexo N° 2: Matriz de Clasificación de la Información
- Anexo N° 3: Política de Respaldo y Cifrado.
- Anexo N° 4: Historial de Cambios.
- Anexo N° 5: Registro de Incidentes de Seguridad.
- Anexo N° 6: Formulario de Consentimiento Informado.
- Anexo N° 7: Ciclo de Vida de la Información.
- Anexo N° 8: Glosario de Términos

ANEXO N° 1: Compromiso de Confidencialidad

Yo, _____, RUT: _____, funcionario(a) del Departamento de Control Interno de la Corporación Municipal Gabriel González Videla, me comprometo formalmente a mantener estricta confidencialidad respecto de toda la información sensible, documentos reservados o datos personales a los que tenga acceso durante el ejercicio de mis funciones.

Asimismo, declaro conocer y aceptar las responsabilidades legales y administrativas derivadas del incumplimiento de este compromiso, en conformidad con las leyes vigentes.

Firma:_____

Nombre:_____

Cargo:_____

Fecha:_____

ANEXO N° 2: Matriz de Clasificación de la Información

La presente matriz establece los niveles de clasificación de la información. Su objetivo es uniformar criterios para la protección de datos y documentos, de acuerdo con su grado de confidencialidad y las medidas de resguardo asociadas.

Nivel de Confidencialidad	Definición	Ejemplos	Medidas de Resguardo
Información Pública	Documentos o datos de libre acceso por disposición legal o institucional. Su divulgación no genera riesgos para la institución ni para las personas.	Normativa interna publicada, memoria anual, organigrama, información obligatoria por Ley de Transparencia.	Disponibilidad en portales institucionales, acceso sin restricciones, actualización periódica.
Información Reservada	Información cuyo acceso se restringe a funcionarios y autoridades autorizadas. Su divulgación podría afectar procesos administrativos o auditorías.	Informes de auditoría en curso, estados financieros intermedios, investigaciones internas no concluidas.	Acceso restringido mediante credenciales, almacenamiento en repositorios institucionales seguros, trazabilidad de accesos.
Información Secreta o Crítica	Información cuyo acceso se limita estrictamente a personal autorizado. Su divulgación indebida puede afectar derechos fundamentales, generar responsabilidades legales o comprometer la seguridad institucional.	Datos personales sensibles (salud, sanciones, antecedentes laborales), estrategias jurídicas, respaldos cifrados, claves de acceso.	Cifrado obligatorio, acceso limitado y registrado, firma de Compromiso de Confidencialidad, destrucción segura al finalizar su uso.

ANEXO N° 3: Política de Respaldo y Cifrado

- Todos los documentos electrónicos que contengan información sensible deberán respaldarse semanalmente en servidores seguros de la Corporación.
- Los respaldos deberán estar cifrados con protocolos seguros (AES-256 o equivalente).
- El acceso a las copias de respaldo estará restringido solo a funcionarios designados por la jefatura.
- Los sistemas de respaldo deben ser evaluados periódicamente.
- Se mantendrá un registro de auditoría digital de cada respaldo generado (fecha, contenido, responsable).

ANEXO N° 4: Historial de Cambios

Fecha	Versión	Motivo de la Modificación	Secciones Afectadas
DD/MM/AAAA	x.x	Ej.: Actualización por cambio normativo, incorporación de nuevas medidas de seguridad, etc.	Indicar capítulo, punto o anexo modificado

Nota: Este historial forma parte integral del Protocolo y deberá revisarse y completarse en cada proceso de actualización, en conjunto con la sección Vigencia y Actualización.

Cada modificación o actualización del presente Protocolo deberá quedar registrada en el siguiente cuadro de control, con el fin de otorgar trazabilidad al proceso de mejora continua y garantizar la transparencia en la gestión documental. El registro debe incluir, como mínimo, la fecha de la modificación, el motivo del cambio y las secciones afectadas.

ANEXO N° 5: Registro de Incidentes de Seguridad

Fecha del incidente: _____ Hora: _____

Tipo Incidente: _____

Descripción del incidente:

_____

_____

_____

Tipo de información comprometida: _____

Unidad afectada: _____

Medidas adoptadas:

_____

_____

Firma: _____

Funcionario que reporta: _____

Cargo: _____

Fecha: _____

ANEXO N° 6: Formulario de Consentimiento Informado

Yo, _____, RUT: _____, en calidad de [funcionario/usuario/proveedor] de la Corporación Municipal Gabriel González Videla, declaro haber sido informado(a) de forma clara y completa acerca del tratamiento de mis datos personales y sensibles, de acuerdo con la Ley N.º 19.628 y su modificación mediante la Ley N.º 21.719.

Autorizo expresamente el uso de mis datos para los fines institucionales establecidos por la Corporación, comprometiéndose esta última a resguardar su confidencialidad y protegerlos conforme a la normativa vigente.

Firma:_____
Nombre:_____
Fecha:_____

Anexo N° 7: Ciclo de Vida de la Información

Fase	Descripción	Acciones Claves
Creación	Generación de datos e información en cualquier formato, físico o digital.	– Identificar la naturaleza de los datos (sensibles, personales, públicos). – Clasificar según nivel de confidencialidad.
Almacenamiento	Conservación de la información en sistemas o archivos físicos seguros, con respaldo y cifrado.	– Aplicar controles de acceso físico y lógico. – Uso de repositorios institucionales seguros (Servidores, base de datos, archivadores, etc.) – Aplicación de la Política de Respaldo y Cifrado (Anexo N° 3). – Respaldo periódico (véase Historial de Cambios: Anexo N° 4).
Compartición	Transferencia o intercambio de información entre áreas internas o con terceros autorizados.	– Uso de canales institucionales seguros (correo oficial, plataformas cifradas). – Prohibición de dispositivos externos no autorizados.
Uso	Etapa en que la información es utilizada para fines institucionales.	– Acceso limitado a funcionarios autorizados. – Firma de Compromiso de Confidencialidad (Anexo N° 1). – Registro de accesos.
Eliminación	Etapa final en que la información deja de ser necesaria.	– Destrucción segura (triturado de papel, borrado seguro de archivos digitales). – Registro de la eliminación.

ANEXO N° 8: Glosario de Términos

Término	Definición
Dato sensible	Información personal que se refiere al origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, estado de salud físico o psíquico, vida sexual u orientación sexual, datos biométricos, o cualquier otro que pueda afectar derechos fundamentales.
Dato personal	Cualquier información concerniente a personas naturales, identificadas o identificables.
Incidente de seguridad	Evento que compromete la confidencialidad, integridad o disponibilidad de la información, ya sea por acceso no autorizado, pérdida, alteración o destrucción de datos.
Confidencialidad	Garantía de que la información solo es accesible a personas autorizadas.
Integridad	Propiedad que asegura que la información no ha sido alterada de forma indebida o accidental.
Disponibilidad	Condición en la que la información está accesible y utilizable cuando se requiere por usuarios autorizados.
Cifrado	Proceso de conversión de información en un formato codificado para proteger su confidencialidad durante el almacenamiento o transmisión.
Backup (copia de respaldo)	Duplicado de la información almacenada de forma segura, destinado a su recuperación en caso de pérdida, daño o incidente.
Portabilidad de datos	Derecho del titular a recibir sus datos en un formato estructurado y transferirlos a otro responsable de tratamiento.
Autenticación multifactor (MFA)	Mecanismo de seguridad que exige más de un método de verificación para validar la identidad de un usuario.
Ciclo de vida de la información	Conjunto de fases que atraviesa un dato desde su creación hasta su eliminación segura, incluyendo almacenamiento, uso, compartición y respaldo.
Destrucción segura	Conjunto de técnicas para eliminar información de manera irreversible, ya sea en soporte físico o digital.