Providencia
Vida Buena
Secretaría Municipal

PROVIDENCIA, 28 ENE 2026

EX.N° 98 **/ VISTOS:** Lo dispuesto por los artículos 5 letra d), 12 y 63 letra i) de La Ley N°18.695, Orgánica Constitucional de Municipalidades; y

CONSIDERANDO: 1.- Que, mediante Decreto Alcaldicio EX.N°1.815 de 18 de diciembre de 2025, se aprobó la creación del "Comité de Gobernanza de Datos de la Municipalidad de Providencia", se aprobó la conformación del "Comité de Seguridad de la Información y Ciberseguridad de la Municipalidad de Providencia" y se aprobó la creación del "Comité de Transformación Digital de la Municipalidad de Providencia".-

2.- La "Política Seguridad y Confidencialidad de la Información y Ciberseguridad".-

3.- El Memorándum N°1.547 de 26 de enero de 2026 de la Administración Municipal.-

DECRETO:

Apruébase la **"POLÍTICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD",** cuyo texto se adjunta al presente Decreto y será considerado parte integrante del mismo.-

Anótese, comuníquese y archívese.-

MUNICIPALIDAD DE PROVIDENCIA
SECRETARIO ABOGADO MUNICIPAL

MARIA RAQUEL DE LA MAZA QUIJADA
Secretario Abogado Municipal

JAIME BELLOLIO AVARIA
Alcalde

RBC/MRMQ/fhm.-
Distribución:
Todas las Direcciones
Archivo
Decreto en Trámite 329 **/**

DIRECCIÓN DE TECNOLOGÍA Y GESTIÓN DIGITAL

"Política Seguridad y Confidencialidad de la Información y Ciberseguridad"

Decreto EX N°

Fecha:

1 Introducción

La masificación de tecnologías de información en todas las industrias y ámbitos del quehacer, junto con un crecimiento exponencial de los volúmenes de datos que se almacenan y transmiten, hacen imprescindible a todas las instituciones tomar los resguardos necesarios para asegurar la información y su adecuado uso. Así, la seguridad de la información y la protección de los datos personales constituyen uno de los mayores desafíos actuales. En tal grado es su importancia, que el año 2018 se consagró su cautela a nivel Constitucional, insertándolo en el artículo 19° numeral 4.

Esto adquiere especial relevancia cuando es un órgano público el que debe resguardar la información que recibe, almacena y produce, puesto que toda su actividad se despliega en beneficio de las personas y en aras del bien común.

En esencia, se establecen lineamientos y principios; se definen roles y responsabilidades; se crea un Comité de Seguridad Permanente y se determina un Plan de Contingencia, entre otros.

Así, se instaura un instrumento fundamental con pautas claras, que permitirá a la Municipalidad tutelar de mejor forma los derechos de las personas, y continuar ciñéndose al marco normativo vigente.

La transformación digital y la creciente interconexión de los sistemas de información han incrementado significativamente los riesgos asociados a la gestión de datos, razón por la cual, la ciberseguridad se ha convertido en un eje estratégico para proteger los activos de información institucionales frente a amenazas internas y externas.

En este contexto, la seguridad de la información y la ciberseguridad constituyen pilares fundamentales para garantizar la confidencialidad, integridad y disponibilidad de los datos gestionados por la Municipalidad de Providencia. Esta política actualiza el marco institucional conforme a la legislación vigente en Chile, incluyendo la Ley N°21.663, Ley Marco de Ciberseguridad, y la Ley N°21.719 sobre Protección de Datos Personales, junto con el Decreto Supremo N°7 del año 2023, que establece los lineamientos para la gestión de la seguridad de la información en los órganos de la Administración del Estado.

2 Objetivo

Como ya se ha establecido previamente, el objetivo de esta política es propender a gestionar la seguridad de la información como un imperativo. Por ende, se deberá velar por su cumplimiento, como también por el cumplimiento de las políticas complementarias, normativas, reglamentos, procedimientos, manuales, instructivos, guías y otros documentos que emanen de ella, además de toda Ley relacionada a la materia de Seguridad y Confidencialidad de la Información, las buenas prácticas y normativas aplicables para este efecto.

En el entendido de que siempre existirán riesgos identificables, los cuales pueden ser eliminados o mitigados, la institución se compromete a gestionar la seguridad de la información, como un proceso continuo en el tiempo, tendiente a homogeneizar los criterios de seguridad y preservar sus activos de información, en cuanto a:

1. **Integridad**: La información estará correcta y sin grado de corrupción alguno.
2. **Confidencialidad**: La información reservada o secreta estará debidamente protegida, permitiendo el acceso solamente a las personas autorizadas.
3. **Disponibilidad**: La información estará disponible y accesible en forma oportuna cuando sea requerida por aquellas personas debidamente autorizadas.

4. **Resiliencia**: la organización debe ser capaz de resistir, responder y recuperarse frente a incidentes de seguridad.
5. Cumplimiento de la Ley N°21.719, de protección de datos personales.

Con el fin de establecer los niveles de seguridad y medidas adecuadas, se aplicarán continuamente las metodologías y técnicas estándares desarrolladas para estas materias, introduciendo un ciclo de mejora continua sostenible en el tiempo. En consecuencia, la PSI se actualizará permanente de acuerdo a los lineamientos de la Organización y su evolución, con al menos una actualización cada dos años desde el momento de su publicación.

3 Alcance

La política es aplicable a todos los activos de información de la Municipalidad que incluyen: procesos, sistemas, aplicaciones, software, equipamiento computacional y no computacional, instalaciones físicas, y adicionalmente aplicará a los funcionarios municipales, independiente de su condición contractual (planta, contrata, honorario, practicante u otro) y trabajadores de otras empresas que presenten servicios a las Municipalidad, siendo las jefaturas del Municipio responsables de propender el cumplimiento.

Esta política, incluirá los alcances de cumplimiento, tomando en consideración las recomendaciones normativas del DS Nº 83 de 2004, Decreto Supremo que establece la norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos; Decreto Supremo N°7 del año 2023, que establece los lineamientos para la gestión de la seguridad de la información en los órganos de la Administración del Estado. y además los señalados en el artículo 3º, inciso segundo de la Ley Nº 19.880, sobre Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado.

4 Definición de Términos

Para efectos del presente documento, se entenderá por:

- **Activo de Información**: todo recurso y/o elemento relevante en la generación, distribución, visualización, almacenamiento y recuperación de información que tiene un valor sustancial para la Municipalidad de Providencia y, por lo tanto, debe protegerse. Se distinguen cuatro niveles:
  - La información propiamente tal, que puede ser estructurada, no estructurada y en múltiples formatos: impresa, escrita, digital, audio, video u otros.
  - Las instalaciones y equipos, computacionales o no, que la soportan.
  - Los procesos internos que generan y manipulan información.
  - Las personas que hacen uso o generan la información.
- **Riesgo**: la probabilidad de ocurrencia de un evento que produce algún nivel de daño. Se mide combinando la probabilidad de ocurrencia y su impacto.
- **Amenaza**: Acción de personas o programas que constituyen una posible causa de riesgo o perjuicio para los sistemas de información, sean físicos o digitales.
- **Vulnerabilidad**: debilidad de un activo o grupo de ellos, que podría permitir materializar una o más amenazas.
- **Seguridad de la Información**: conjunto de medidas que adopta una Organización para resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de datos. No debe confundirse con seguridad informática, cuyo alcance se limita a los sistemas tecnológicos.
- **Contramedida**: representa todas las acciones que se implementan para prevenir la amenaza.
- **TI**: Tecnologías de la Información

5 Descripción

5.1 Declaración de la Organización

La Municipalidad de Providencia (en adelante "la Municipalidad"), mantendrá una Política de Seguridad de la Información (en adelante, "PSI") que aúne todos los esfuerzos institucionales en tal sentido, con el fin de disminuir riesgos y evitar incidentes que pudieran traducirse en pérdidas de información, económicas y de imagen para la Municipalidad, así como infracciones regulatorias o vulneraciones de derechos y perjuicios a los ciudadanos. Esta política sustentará los siguientes principios:

- Asegurar prácticas tendientes a cautelar la integridad, confiabilidad y disponibilidad de la información administrada en todos los ámbitos de gestión municipal, propendiendo así a mantener la continuidad de los servicios que entrega la Institución.
- Mantener políticas, normativas y procedimientos de seguridad de información actualizados.
- Comprometer e involucrar a todo el personal municipal de la Municipalidad y sus proveedores, a la correcta difusión, implementación y cumplimiento de esta política.
- Promover una cultura organizacional orientada a la seguridad de la información.

5.2 Seguridad de activos de información

Los activos de información deben tener un dueño (Ver punto 6.4, letra (a)) responsable de identificar, registrar, clasificar y valorizar el activo, según su impacto en los objetivos municipales. Esta información será vital para la implementación del Plan de continuidad Operacional. Asimismo, debe definir los roles que pueden acceder al activo y sus niveles de autorización sobre el mismo.

Para aquellos activos considerados de alta criticidad, se debe mantener un análisis periódico de las amenazas y/o vulnerabilidades que puedan aparecer, así como la evaluación del riesgo y gestionar la mitigación o eliminación de los mismos.

Las gestiones que se deben realizar sobre los activos de información son:

1. **Inventario de los Activos**. Debe existir un registro general de todos los activos asociados a la información institucional, los que deben ser revisados y actualizados en forma periódica por quien corresponda, de acuerdo a la reglamentación vigente en la Municipalidad.
2. **Clasificación de la Información**. La información debe ser clasificada y etiquetada de acuerdo a su valor, requisitos legales y grado crítico para la Municipalidad.
3. **Generar y administrar los Protocolos**, como acciones conducentes a optimizar y actualizar las tareas cotidianas.

5.2.1 Riesgos y vulnerabilidades

Algunos de los riesgos y vulnerabilidades más comunes, y que deben ser gestionados por los responsables respectivos, son los siguientes:

- **Asociados a Sistemas tecnológicos**:
  - Cambios no controlados en el sistema
  - Adulteración de los registros del sistema, modificación no autorizada
  - Adulteración de los registros de actividades del operador y del administrador del sistema
  - Sistema de información y/o infraestructura TI vulnerable
  - Desarrollo inseguro de sistemas

- Incorrecta actualización o versionamiento de los sistemas
- Uso desprotegido de datos sensibles en pruebas.
- Acceso no autorizado.
- Ataque a través de ransomware provocando imposibilidad de lectura de la información.

- **Asociados a información digital o en soporte de papel**:
  - Manipulación indebida de información
  - Acceso no autorizado a la información
  - Pérdida, daño o deterioro del medio de Información
- **Asociados a personas**:
  - Fuga de información confidencial, por error o desconocimiento
  - Incorrecta asignación de funciones, lo que podría causar un mal uso de la información a su cargo
  - Conocimiento insuficiente de las responsabilidades y correcto uso de los activos de información a cargo
  - Capacitación insuficiente en seguridad de la información
  - Transgresión a las políticas de seguridad de la información por parte del funcionario
  - Acceso no autorizado a activos de información de personas desvinculadas de la institución. Robo de equipos, medios y/o documentos.
  - No devolución de dispositivos y/o activos de información a la institución una vez terminada la relación laboral
  - Uso de contraseñas inseguras y fáciles de deducir
- **Asociados a Equipos tecnológicos**
  - Daño por amenazas ambientales. Acceso no autorizado
  - Robo, daño o pérdida del equipo fuera de las dependencias de la institución
  - Eliminación insegura de la información contenida en el equipo
  - Contaminación con malwares
  - Instalación no autorizada de Software

5.2.2 Cuidado de la información personal, privada y/o confidencial

Respecto de los cuidados generales de protección de datos y de la información, y que aplican tanto a la información existente en formato digital como también en soporte de papel, las definiciones serán las siguientes:

1. La información de la Municipalidad debe ser protegida con controles acordes a la categoría de clasificación asignada de acuerdo a su nivel de confidencialidad, independientemente del medio en que se almacene o transporte. Esto se aplicará a todas las acciones y medios de almacenamiento y transporte de información confidencial.
2. Los documentos confidenciales deben ser protegidos de cualquier tipo de lectura casual, por ende, si son documentos físicos deben quedar almacenados en muebles con llave; los funcionarios que porten estos documentos confidenciales fuera de la oficina deben maximizar el cuidado para no extraviarlos o exponer su contenido.
3. La información confidencial enviada por correo interno o externo, debe ir en sobre sellado y con la frase "Sólo para ser abierto por el Destinatario".
4. El servicio de correo utilizado debe permitir el rastreo de la carta o paquete.
5. El método de distribución de información confidencial, o de uso interno, debe permitir que exista un acuse de recibo formal, por parte del destinatario.
6. Previo a enviar a un tercero un documento confidencial, o de uso interno, el emisor y el receptor deben firmar un Acuerdo de No-Divulgación de Información.
7. La Municipalidad protege la información confidencial que ha sido confiada por terceros. Los funcionarios tienen la obligación de no divulgar dicha información, a menos que el originador entregue una autorización por escrito, o exista un requerimiento legal.
8. Se debe evitar la discusión de información confidencial o privada por vía telefónica pública. Si se hace, se debe procurar tratar los temas en forma general y sin mencionar datos confidenciales.

9. No se debe discutir información confidencial o privada usando el altavoz del aparato telefónico o usando teléfonos inalámbricos o celulares.
10. Si los funcionarios de la Municipalidad viajan en transporte público colectivo, no deben llevar consigo información confidencial municipal. En caso de que esto sea estrictamente necesario, la Municipalidad proveerá un medio de transporte seguro.
11. La información confidencial no debe ser expuesta, leída o discutida en aviones, restaurantes, transporte colectivo u otros sitios públicos.
12. Todos los funcionarios que porten información confidencial en dispositivos portátiles, deben almacenarla cifrada, proteger el acceso lógico a la información o proteger el acceso físico al dispositivo.
13. Si se viaja en bus o avión, el dispositivo portátil debe ir como equipaje de mano, siempre bajo la supervisión del usuario, y no en el compartimiento de equipaje.
14. Cuando una empresa externa, un consultor o contratista se desvincula de la Municipalidad, no puede llevar consigo la información confidencial, o de uso interno a la cual ha tenido acceso.
15. Cuando un funcionario se desvincula de la Municipalidad, no debe llevar consigo información confidencial o de uso interno de la institución.
16. La divulgación voluntaria o involuntaria de información confidencial de la Municipalidad, o que atente contra la Ley de Protección de Datos Personales podría llevar a acciones disciplinarias y/o la respectiva denuncia a la autoridad competente.
17. Se debe considerar una "Política de Protección de Datos Personales".

5.2.3 Seguridad en el acceso a la información digital

Los detalles operativos tocantes al acceso a información en formato digital, se encuentran en la "Política de Control de Acceso, Identificación y Autenticación (N02)", la cual se sujeta específicamente al DS N°83 del año 2004 del Ministerio Secretaría General de la Presidencia, en su artículo N°28.

No obstante, en forma adicional a lo indicado en dicho documento, deberán implementarse mecanismos de bloqueo automático en las estaciones de trabajo que están desatendidas por un plazo prudente que evite o minimice la acción de un tercero. Asimismo, los usuarios serán responsables de mantener sus zonas de trabajo limpias, evitando que terceros puedan acceder a información confidencial.

Para las personas que utilicen teléfonos celulares entregados por la Municipalidad o configuren sus propios equipos con cuentas de la Municipalidad, deberán adherir a las políticas de seguridad acá establecidas y la "Política de uso de equipos y medios portátiles (N05)".

5.3 Seguridad de la Infraestructura informática

Para servicios de terceros que manejan activos de información será obligatorio contar con acuerdos de confidencialidad, niveles de servicio y disponibilidad comprometidos, asimismo su monitoreo y revisión permanente por parte de la Municipalidad. Además de lo anterior, todo proveedor de tecnología y/o transporte de equipamiento, debe conocer y cumplir con estas políticas de seguridad de la información en su totalidad, debiendo justificar sólidamente cualquier excepción necesaria a través de medios formales al encargado de seguridad tecnológica de la Municipalidad.

Para garantizar un óptimo cumplimiento de las políticas de seguridad, se definirán los siguientes instructivos y políticas complementarias, que permitirán clarificar a los usuarios lo que se entiende como conductas adecuadas o inadecuadas, así como sus niveles de responsabilidad personal en el incumplimiento u omisión.

1. N01 - Uso de Infraestructura informática.
2. N02 - Control de acceso, identificación y autenticación.
3. N03 - Utilización de correo electrónico.
4. N04 - Utilización del servicio de internet.
5. N05 - Política de uso aceptable de equipos y/o medios portátiles asignados por la Municipalidad.
6. N06 - Utilización de Accesos Remotos para teletrabajo (VPN).
7. N07 - Uso de Recursos Compartidos.

8. N08 - Privacidad y Protección de Datos Personales.
9. N09 – Desarrollo de Software.
10. N10 – Versionamiento y Control de Calidad de Código de Software

El cumplimiento de estas políticas de seguridad requiere que se sigan protocolos formales de operación. Estos protocolos deben ser estructurados y descritos en detalle en procedimientos operativos.

Los procedimientos operativos deben estar documentados, actualizados y ser conocidos por los involucrados. Las responsabilidades deben estar individualizadas y con una adecuada segregación de funciones que impida cambios no autorizados o hacer mal uso de los activos de información.

Los procedimientos operativos serán los siguientes:

1. P01 - Creación de usuarios.
2. P02 - Eliminación o inactivación de usuarios.
3. P03 - Solicitud de instalación de software adicional al estándar.
4. P04 - Atención de usuarios.
5. P05 - Acceso al o los sistemas de información y/o gestión documental.
6. P06 - Traslado de información de usuarios.
7. P07 - Respaldo de información de usuarios.
8. P08 - Creación de accesos VPN para teletrabajo.

Además, deberán existir adecuados controles para hacer cambios en los sistemas y plataformas tecnológicas que impidan modificaciones no autorizadas o erróneas, que afecten la integridad de la información. Para ello deben existir los siguientes procedimientos:

9. P09 - Paso a producción y/o Control de Cambios.
10. P10 - Mantención de sistemas aplicativos y/o infraestructura. (Incluído en P09)
11. P11 - Creación de reglas en Firewall, Switches, Servidores Web y otros.

Y para los activos tecnológicos y sus movimientos:

12. P12 - Incorporación, desvinculación, traslado y baja de Activos Tecnológicos.
13. P13 – Protocolo de Gestión de Incidentes de Seguridad.

Para cumplir con la Ley N°21.719, debe existir un protocolo que proteja los datos personales cuando se involucra compartir sistemas municipales a través de convenios de cooperación con otras instituciones.

14. P14 – Protocolo de "Entrega segura de Sistemas Informáticos en Convenios Municipales".

En la constante implementación de mejoras, el Comité de Seguridad puede aprobar nuevas políticas complementarias y/o procedimientos operativos, los cuales serán debidamente difundidas y publicadas para su cumplimiento.

5.3.1 Adquisición, desarrollo y mantenimiento de sistemas TI

1. Todo nuevo sistema de información deberá contar con controles de seguridad que eviten acceso no autorizado, pérdida o corrupción de información según la "Política de Control de Acceso, Identificación y Autenticación (N02)". Además, debe cumplir con lo dispuesto en la "Política de Desarrollo de Software (N09)" y la "Política de Versionamiento y Control de Calidad de Código de Software (N10)".
2. La información sensible debe disponer de controles criptográficos, y autenticación de doble factor, siempre que tecnológica y operativamente sea posible. Las excepciones deben ser debidamente informadas al Comité de Seguridad a través del Encargado de Seguridad de la Información.

3. Los datos de prueba deben ser cuidadosamente tratados y en lo posible enmascarados para evitar acceso de terceros a datos reales que se encuentran en producción.
4. Los programas fuentes que dan origen a los sistemas deben contar con mecanismos robustos de protección y resguardo que impidan su pérdida, daño o copia no autorizada.
5. Los sistemas y plataformas periódicamente deben ser sometidos a pruebas de vulnerabilidades que permitan revelarlas y ejecutar planes de acción para mitigarlas. Cualquier prueba de explotación de vulnerabilidades debe ser supervisada y autorizada por el encargado de seguridad de la información e informada al Comité de Seguridad de la Municipalidad especificando los riesgos y el alcance posible de éstos. La realización de pruebas de explotación de vulnerabilidades o escaneo de las redes sin autorización podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N°18.883, sobre estatuto administrativo municipal. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

5.4 Gestión de incidentes de seguridad

Nuestra organización, en su calidad de entidad que presta servicios esenciales y que no ha sido clasificada como Operador de Importancia Vital (OIV), adopta las medidas necesarias para dar cumplimiento a las obligaciones generales establecidas en la Ley N° 21.663, Marco de Ciberseguridad de la República de Chile.

Los eventos e incidentes de seguridad detectados, deberán ser registrados y comunicados a los responsables para su atención y resolución en el menor plazo posible, siguiendo los lineamientos de la Ley N°21.663 Marco de Ciberseguridad. Asimismo, las debilidades y vulnerabilidades conocidas en los sistemas y plataformas, deberán ser informadas al Encargado de Seguridad y al dueño de la información que pudiera ser afectado.

Deberán existir procedimientos conocidos para la detección, atención y resolución de los eventos e incidentes de seguridad junto con un mecanismo que permita recopilar información relacionada para los análisis y mejoras respectivas.

5.4.1 Planes de contingencia.

Las medidas del plan de contingencia están sujetas al estatuto administrativo de la Municipalidad de Providencia y, por ende, las medidas o sanciones en caso de incidente, serán decididas según el Estatuto vigente.

En este contexto, la organización se compromete a mantener un sistema de gestión de ciberseguridad que contemple los siguientes principios y acciones:

a) Gestión integral de la ciberseguridad

La organización dispondrá de un marco de gestión orientado a la prevención, detección, respuesta y recuperación ante incidentes de ciberseguridad. Este marco se fundamentará en el principio de mejora continua y se alineará con estándares reconocidos internacionalmente (como ISO 27001, NIST CSF o equivalentes).

b) Evaluación de riesgos y medidas de protección

Se realizará periódicamente una identificación y evaluación de riesgos asociados al uso de tecnologías de información y comunicaciones, considerando el impacto potencial sobre la confidencialidad, integridad y disponibilidad de los activos críticos.

En base a esa evaluación, se implementarán medidas técnicas, organizativas y físicas proporcionales para mitigar dichos riesgos, priorizando la seguridad desde el diseño ("security by design") y por defecto ("security by default").

c) Políticas y controles de seguridad de la información

Se establecerán y mantendrán políticas internas y controles que aseguren la gestión adecuada de accesos, la protección de redes, sistemas y datos, la continuidad operativa, el respaldo seguro de información y la actualización oportuna de software y parches de seguridad.

Estas políticas serán revisadas al menos una vez al año o cuando se produzcan cambios significativos en la infraestructura tecnológica o en el marco normativo.

d) Capacitación y cultura organizacional

La organización promoverá una cultura de ciberseguridad entre sus colaboradores, mediante actividades de formación y sensibilización periódicas. Cada integrante tendrá la responsabilidad de resguardar la información institucional y reportar oportunamente cualquier situación sospechosa o incidente.

e) Gestión y reporte de incidentes de ciberseguridad

Se mantendrán procedimientos formales para la detección, registro, análisis y respuesta a incidentes que puedan afectar los sistemas o la información institucional.

Cuando un incidente tenga un impacto significativo o pueda comprometer servicios esenciales, se reportará al CSIRT Nacional o a la autoridad competente, de conformidad con los plazos y canales establecidos por la Agencia Nacional de Ciberseguridad (ANCI). Es decir, cuando:

- Afecten la continuidad o disponibilidad del servicio esencial.
- Produzcan una interrupción relevante o prolongada.
- Impliquen acceso no autorizado, pérdida o alteración de información sensible o crítica.
- Tengan efecto en cadena sobre otros prestadores, servicios públicos o usuarios.

f) Colaboración y cooperación con las autoridades

La organización colaborará activamente con la ANCI y con el CSIRT Nacional, atendiendo los requerimientos de información y participando en los ejercicios o evaluaciones que contribuyan al fortalecimiento de la ciberresiliencia nacional.

g) Gobernanza y mejora continua

Se designará un Responsable Institucional de Seguridad de la Información y Ciberseguridad. El "Encargado de Seguridad de la Información" deberá coordinar la implementación, control y mejora de las medidas descritas. (Punto 6)

El sistema de gestión será objeto de revisiones internas y auditorías periódicas que permitan asegurar su eficacia y conformidad con la Ley N.º 21.663 y las directrices regulatorias vigentes.

El gestión de contingencia se llevará a cabo según los siguientes pasos:

1. **Reporte de eventos de seguridad**: Cualquiera sea el incidente de seguridad ocurrido que infrinja la política, debe ser reportado inmediatamente al Encargado de Seguridad de la Información (ESI/CISO) a través de la mesa de ayuda y el correo institucional dedicado a recolectar estos reportes (encargado.seguridadti@providencia.cl). El ESI debe reportar el incidente a la Agencia Nacional de Ciberseguridad (ANCI) durante las 3 primeras horas desde la detección. Posteriormente, el caso será discutido con la Comisión para tomar las medidas pertinentes. El encargado de Seguridad deberá reportar los antecedentes recopilados a la Dirección responsable para la gestión correctiva necesaria.
2. **Recopilación de evidencia**: En el caso de que el incidente ocurra en un sistema informático, la Dirección de Tecnología y Gestión Digital debe poner en marcha los procedimientos necesarios para poder revisar las acciones realizadas en el sistema vulnerado, con el fin de recopilar información necesaria para ser usada como evidencia del incidente.
3. **Documentar Eventos de Seguridad**. De acuerdo a la información entregada por quien denuncie y la evidencia recopilada, se procede a tomar una decisión por parte del comité respecto al procedimiento que se debe seguir, la cual será determinada por simple mayoría. Luego de lo anterior, se debe registrar formalmente lo ocurrido, incluyendo todos los antecedentes reunidos y la decisión final, a través del formulario correspondiente.
4. **Pruebas de Vulnerabilidades**. En caso de que el incidente involucre sistemas informáticos, se deberá realizar por parte de la Dirección de Tecnología y Gestión Digital, los procedimientos necesarios para evaluar la vulnerabilidad y desarrollar un protocolo en caso de ser necesario.
5. **Generar y administrar los Protocolos**: En relación al incidente ocurrido, se deben revisar los protocolos existentes y actualizarlos para evitar una recurrencia de este tipo de incidentes o crear un procedimiento, en caso de que no exista actualmente.
6. **Caso de pérdida de información**: En caso que el incidente genere pérdidas de cualquier tipo de información, se debe comunicar inmediatamente a los directores de la Municipalidad de Providencia, al (a la) alcalde(sa) en ejercicio, y a cualquier persona a la cual dicha falla pueda afectar directamente.

15. La gestión debe regirse de manera rigurosa usando el protocolo "P13 – Protocolo de Gestión de Incidentes de Seguridad".

5.5 Gestión de la continuidad de negocio

Una vez al año se deberán mantener y evaluar los planes de continuidad de negocio y de recuperación de desastres que permitan restaurar la continuidad y disponibilidad de los activos de información considerados críticos. Junto con lo anterior, evaluar anualmente sus riesgos. Esto es exigible a proveedores de plataformas y sistemas de misión crítica para la Municipalidad.

5.6 Gestión del cumplimiento normativo

La PSI, adhiere al marco normativo que regulan las leyes chilenas en esta materia y todas las disposiciones legales relativas al manejo y resguardo de datos personales, persistencia en el tiempo de ciertos datos que indique la normativa, documentos electrónicos, firma digital y propiedad intelectual.

La Municipalidad deberá realizar auditorías periódicas y selectivas, a cualquiera de sus activos de información y cooperar activamente con los organismos estatales pertinentes

en cuanto a auditorías externas se oficialicen. Sin perjuicio de lo anterior, la Municipalidad tomará los resguardos necesarios para evitar que la información pueda ser expuesta a un mal uso o se genere interrupción en los sistemas y procesos de negocio.

En el caso de los funcionarios que trabajen con información sensible o tengan acceso a ella, es necesario crear cláusulas de confidencialidad en los contratos, ya que podrían hacer mal uso de la información, de manera voluntaria o involuntaria.

6 Responsabilidades

6.1 Encargado de Seguridad de la Información

Se define al Encargado u Oficial de Ciberseguridad y Seguridad de la Información (ESI/CISO), como el funcionario municipal responsable de mantener actualizada la PSI, monitorear su aplicación, promover su difusión y proponer mejoras.

6.2 Comité de Seguridad de la Información

Se define un Comité de Seguridad de la Información y Ciberseguridad (desde ahora, "Comité"), que será una instancia permanente conformada por un titular y su respectivo suplente:

a) Alcalde/sa
b) Administrador/a Municipal
c) Director/a o Coordinador/a de Tecnología y Gestión digital
d) Director/a de SECPLA
e) Director/a de Comunicaciones
f) Director/a de Control
g) Director/a Jurídico/a
h) Encargado u Oficial de Ciberseguridad y Seguridad de la Información (CISO)
i) Delegado/a de Protección de Datos Control (DPO)
j) Encargado/a de Datos DTGD
k) Coordinador/a de Transformación Digital

En caso de ausencia de un miembro del Comité, éste podrá ser reemplazado por su suplente. El cual asumirá plena responsabilidad, funciones y facultades equivalentes a las del miembro titular durante su participación en las reuniones y decisiones del Comité, quedando consignado en el acta respectiva.

Las responsabilidades del Comité serán:

a) Orientar las acciones estratégicas destinadas a fortalecer la ciberseguridad y la protección de la información institucional del Municipio.
b) Definir lineamientos generales y promover la implementación de políticas, normas y procedimientos en materia de seguridad de la información.
c) Supervisar la gestión de riesgos asociados a las tecnologías de la información y proponer medidas preventivas y correctivas.
d) Pronunciarse y aprobar todas las resoluciones en aspectos de seguridad que sean de alcance estratégico y transversal a la Municipalidad.
e) Fomentar la capacitación y concientización de los funcionarios municipales en prácticas seguras de uso de sistemas y datos.
f) Promover la adopción de estándares y buenas prácticas nacionales e internacionales en materia de ciberseguridad, asegurando la mejora continua del sistema municipal.

El Comité se reunirá regularmente en forma trimestral para revisar el funcionamiento general de la PSI, analizar posibles incidentes del período y revisar otras materias relativas a la Seguridad de la Información, según necesidad.

Deberá existir un suplente para cada uno de los miembros integrantes del Comité, que lo reemplazará en sus funciones con derecho a voz y voto para aquellos casos en que el titular se encuentre impedido de participar en alguna reunión. Los suplentes podrán asistir a las reuniones, conjuntamente con su respectivo titular, pero en este caso, sólo tendrán derecho a voz. Esta designación deberá constar en acta de sesión.

En caso que ocurra algún incidente en relación a la información, el Encargado de Seguridad debe gestionar las medidas de mitigación necesarias y luego informar de lo acontecido a los miembros de Comité, pudiendo para ello, de ser necesario, citar a sesión extraordinaria, de tal forma que se pueda tomar decisiones tendientes a evitar eventos futuros de la misma naturaleza.

6.3 Responsabilidades del Encargado de Seguridad de la Información y Ciberseguridad

Sin perjuicio de lo ya indicado en secciones anteriores, las responsabilidades del Encargado de Seguridad de la Información y Ciberseguridad serán las siguientes:

a) Definir los controles necesarios para revisar el cumplimiento de la PSI.
b) Revisar y mantener actualizada la PSI, según los requerimientos de la municipalidad.
c) Velar por la implementación de los procesos y procedimientos de seguridad.
d) Monitorear el cumplimiento de los procedimientos establecidos.
e) Generar capacitaciones para los funcionarios municipales en temas relativos a Seguridad de Información.
f) Asesorar al alcalde/sa de la Municipalidad en las materias relativas a seguridad de los documentos electrónicos.
g) Coordinar la respuesta ante incidentes de seguridad de la información, manteniendo un registro actualizado de éstos.
h) Actuar como punto de contacto institucional ante la Agencia Nacional de Ciberseguridad (ANCI) y el CSIRT Nacional, gestionando la comunicación oficial sobre incidentes de ciberseguridad y requerimientos de información que dichas entidades emitan.
i) Evaluar la criticidad e impacto de los incidentes de seguridad de la información, determinando si estos alcanzan el umbral de "impacto significativo" conforme a la normativa vigente, y en caso afirmativo, reportarlos a la ANCI o al CSIRT Nacional dentro del plazo legal establecido (máximo 72 horas desde su detección).
j) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
k) Supervisar que las medidas técnicas y organizativas de seguridad se mantengan alineadas con la Ley 21.663 y sus normas complementarias, así como con otras disposiciones regulatorias aplicables a la gestión de servicios esenciales y protección de datos.
l) Coordinar la elaboración, mantenimiento y prueba periódica de los Planes de Continuidad Operativa y Recuperación ante Incidentes Cibernéticos, asegurando que contemplen los escenarios de mayor riesgo para la prestación de servicios esenciales.
m) Proponer mejoras al Comité, organizar periódicamente sus sesiones y dar seguimiento a los planes de acción que se deriven. Consolidar y reportar periódicamente al Comité de Seguridad los indicadores de desempeño, eventos relevantes, resultados de auditorías y lecciones aprendidas, fomentando la mejora continua del sistema de ciberseguridad institucional.
n) Actuar como secretario en las sesiones de Comité y tomar nota de acuerdos y temas relevantes, generando las actas respectivas y posteriormente enviarlas a cada integrante para su aprobación.

6.4 Responsabilidades generales de funcionarios y proveedores

Se definen los siguientes roles respecto de los activos de información:

a) **Dueño de la información**: persona responsable de un activo de información (o grupo), que incluye su valorización, clasificación y definiciones en torno a la protección, autorización y uso de la información.
b) **Administrador de la información**: persona encargada de resguardar la información y administrar las definiciones establecidas por el dueño de la información.
c) **Usuario de la información**: persona que tiene acceso a la información según los niveles de autorización definidos por el dueño de la información.

Todos los funcionarios de la Municipalidad deberán cooperar, contribuir y cumplir permanentemente con la PSI, así como denunciar las infracciones bajo los canales municipales establecidos. También es deber de cada funcionario municipal, preocuparse de conocer y comprender el contenido de todas las disposiciones que en materia de Seguridad de la Información se oficialicen por parte de la Municipalidad.

Respecto del personal externo que presta servicios a la Municipalidad, se le dará a conocer y se hará exigible el cumplimiento de la PSI, en lo que sea atingente a sus labores, incluyendo en todos los contratos cláusulas para asegurar el cumplimiento.

Todos los funcionarios municipales que manipulen o accedan a activos de información de la Municipalidad deben firmar acuerdo de confidencialidad y responsabilidad en el uso de la información. Así mismo se debe mantener un programa de difusión y capacitación permanente a los funcionarios en los temas de Seguridad de la Información.

El incumplimiento de las Políticas de Seguridad de la Información por parte de los funcionarios, dará lugar a la aplicación de medidas administrativas, disciplinarias, civiles o penales a las que haya lugar.

Los funcionarios que cambien de funciones o asuman nuevos roles o cargos, deberán ser actualizados en cuanto al acceso y autorización a los activos de información según sus nuevas funciones. En caso de ausencias prolongadas de los funcionarios, deberán ser suspendidos en sus accesos a los activos de información. Por último, los funcionarios que cesen sus contratos con la Municipalidad deberán ser revocados en todos sus accesos a los activos de información según los procedimientos implementados para dichos propósitos.

6.5 Roles y responsabilidades específicos

Por último, se detallan las siguientes responsabilidades específicas, con el propósito de cumplir los objetivos de la PSI:

6.5.1 Dirección de Tecnología y Gestión Digital

a) Velar por el cumplimiento de esta política y los 3 principios mencionados en el inicio: integridad, Confidencialidad y Disponibilidad. (Ver punto V, inciso 1)
b) Responder a los avisos de incorporación o desvinculación de funcionarios de la Municipalidad de Providencia, para mantener actualizados accesos y permisos a los sistemas.
c) Proporcionar y recibir información respecto a los activos de información, con el fin de mantener el inventario de activos actualizado.
d) Mantener actualizado el registro de permisos de accesos a cada sistema de información.

6.5.2 Directivos

a) Velar por el cumplimiento de los puntos indicados en la presente política según sus atribuciones y facultades.
b) Promover un ambiente de buenas prácticas con respecto a sistemas de la información en sus áreas.
c) Concientizar a los trabajadores respeto de sus responsabilidades, en materias de seguridad de la información.
d) Orientar a los funcionarios al cumplimiento de la PSI.
e) Informar al encargado de seguridad de la información sobre las Bases de Datos de sus respectivas direcciones y jefaturas, avisando si estas incluyen o no información sensible.
f) Mantener actualizada la información de sus bases de datos.
g) Administrar el uso de los Sistemas de Información relacionados con su negocio.
h) Autorizar o Denegar los permisos a las Bases de Datos de sus respectivas unidades, informando a la Dirección de Tecnología y Gestión Digital cuando sea necesario.

6.5.3 Dirección de Personas y DIDECO

Además de lo contemplado en el punto 6.5.2 del presente documento, es responsabilidad de las Direcciones de Personas y de Desarrollo Comunitario (DIDECO) notificar de forma consolidada y oportuna a la Dirección de Tecnología y Gestión Digital, sobre las vinculaciones y desvinculaciones del personal de cada área de la Municipalidad integrando esta actividad como parte importante de sus procedimientos de operación.

6.5.4 Usuarios de sistemas de información

Todos los funcionarios usuarios de Sistemas de Información Municipales, ya sean de planta, contrata u honorarios, estarán afectos a lo establecido en esta política debiendo asegurar su estricto cumplimiento. Además, los usuarios deben velar por el cumplimiento de los tres principios mencionados al inicio de la política: Integridad, Confidencialidad y Disponibilidad, alertando de manera oportuna y adecuada, cualquier incidente que atente contra la seguridad de la información.

7 Normativa Legal y Reglamentaria

El marco normativo sobre el cual descansa la presente política está compuesto por las siguientes leyes, decretos e instrucciones:

- Ley Nº 21.719 regula la protección y el tratamiento de los datos personales y crea la agencia de protección de datos personales.
- Ley Nº19.553 que concede asignación de modernización y otros beneficios que indica.
- Ley N° 21.663 ley Marco de Ciberseguridad.
- Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley Nº 20.285 sobre acceso a la información pública.
- Ley Nº 21.459 establece normas sobre delitos informáticos, deroga la ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.
- Ley N° 21.180 transformación digital del estado.
- Ley Nº 19.880 establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.
- Ley Nº 21.096, consagra el derecho a protección de los datos personales.

- Decreto Supremo Nº 83 de 2005, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo Nº 93 de 2006, norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios.
- Decreto Supremo Nº181 Aprueba reglamento de Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
- Decreto Supremo Nº 14 de 2014 modifica decreto Nº 181, de 2002, que aprueba reglamento de la ley 19. 799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.
- Decreto Supremo Nº158 de 2007. Modifica D.S. Nº 81 sobre norma técnica para la interoperabilidad de los documentos electrónicos.
- Instrucción General Nº2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia.
- Instrucción General Nº3, mayo de 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados.

8 Difusión y Revisión

La difusión de esta política, se realizará mediante correo electrónico a todo el personal de la Municipalidad y terceros relacionados directamente, además quedará a disposición en la Intranet de la Municipalidad para facilitar el acceso y su conocimiento. Junto a lo anterior, se realizarán capacitaciones a las personas que sean contratadas por la municipalidad.

La revisión se realizará durante las reuniones del Comité de Seguridad de la Información y ciberseguridad, sin embargo, en el caso de circunstancias excepcionales, la política podrá ser revisada y modificada con la aprobación del Comité.

9 Historial de Cambios

Versión	Fecha	Cambio	Responsable / Dirección
0	25-Oct-2018	- Creación del Documento	Felipe Frez / Administración Municipal.
1.0	25-May-2019	- Modificaciones menores.	Felipe Frez / Administración Municipal
2.0	24-Feb-2021	- Incorpora mayor detalle en políticas de seguridad, roles y responsabilidades. - Reestructuración general del documento	Juan Carlos Lillo M. / Dirección de Tecnología y Gestión Digital.
2.1	24-Feb-2022	- Cambio de estructura que se solicita en el Decreto EX N°1 sin fecha del año 2021 de la Dirección de Control	Juan Carlos Lillo M. / Dirección de Tecnología y Gestión Digital.
2.2	07-Nov-2024	- Agrega N08 Política de Privacidad y Protección de Datos Personales. Ley N°21.719	Juan Carlos Lillo M. / Dirección de Tecnología y Gestión Digital.
2.5	15-Dic-2025	- Mejora Introducción y Objetivos - Agrega responsabilidades, acciones y gestión referentes a la Ley N° 21.663 Marco de Ciberseguridad - Agrega referencias a la Ley N° 21.719 regula la protección y el tratamiento de los datos personales Punto 5.2.2. - Agrega: N09 – Desarrollo de Software. - Agrega N10 – Versionamiento y Control de Calidad de Código de Software - Redefine conformación del Comité de Seguridad de la Información y Ciberseguridad - Agrega P13 – Protocolo de "Gestión de Incidentes de Seguridad". - Agrega P14 – Protocolo de "Entrega segura de Sistemas Informáticos en Convenios Municipales".	Juan Carlos Lillo M. / Dirección de Tecnología y Gestión Digital.