APRUEBA POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

DECRETO EX. Nº 1594

MELIPILLA, 02 JUN 2025

LA ALCALDÍA DECRETÓ HOY LO SIGUIENTE:

VISTOS:

a) La Política General de la Seguridad de la Información, emitida por el Departamento de Informática de la I. Municipalidad de Melipilla;
b) Las necesidades del Servicio.

TENIENDO PRESENTE:

a) Las facultades y atribuciones que me confiere la Ley N° 18.695, Orgánica Constitucional de Municipalidades y sus modificaciones posteriores.
b) Lo dispuesto en la Ley N° 18.883, Estatuto Administrativo para Funcionarios Municipales, y sus posteriores modificaciones.

CONSIDERANDO:

I. Que, propósito de esta política es definir el objetivo, dirección, principios, reglas y lineamientos generales, en materias de Seguridad de la Información, que deben ser observados por todos los funcionarios que se desempeñan en la Ilustre Municipalidad de Melipilla, a saber, personal de planta, personal a contrata y prestadores de servicios a honorarios.

II. Que, frente a lo advertido, los objetivos específicos de la misma corresponden a: a) Velar por la Seguridad de la Información, considerando la confidencialidad, integridad y disponibilidad de ésta; b) Verificar a través de indicadores la implementación del sistema de gestión de Seguridad de la Información, de acuerdo a la dirección, principios, reglas y lineamientos contemplados en esta Política; y c) Crear y promover una cultura de Seguridad de la Información en la Ilustre Municipalidad de Melipilla. Razón por la que;

D E C R E T O:

1.- APRUÉBASE la Política General de la Seguridad de la Información de la I. Municipalidad de Melipilla, cuyo texto íntegro es el siguiente:

POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I: DISPOSICIONES GENERALES

Artículo 1°. Objeto

1. Objetivo General

El propósito de esta Política es definir el objetivo, dirección, principios, reglas y lineamientos generales, en materias de Seguridad de la Información, que deben ser observados por todos los funcionarios que se desempeñan en la Ilustre Municipalidad de Melipilla, a saber, personal de planta, personal a contrata y prestadores de servicios a honorarios.

2. Objetivos Específicos

a) Velar por la Seguridad de la Información, considerando la confidencialidad, integridad y disponibilidad de ésta.

b) Verificar a través de indicadores la implementación del sistema de gestión de Seguridad de la Información, de acuerdo a la dirección, principios, reglas y lineamientos contemplados en esta Política.

c) Crear y promover una cultura de Seguridad de la Información en la Ilustre Municipalidad de Melipilla.

Artículo 2°. Ámbito de aplicación

Las disposiciones de la presente Política serán aplicables a todos los procesos que elaboren, obtengan, manipulen, transporten o almacenen activos de información de la Ilustre Municipalidad de Melipilla y comprende a toda la Organización, considera el involucramiento y compromiso de todos los integrantes de la Ilustre Municipalidad de Melipilla, independientemente de su rango, función o localización, y de sus proveedores cuando corresponda.

Artículo 3°. Glosario

1. **Activos de información:** Corresponde a toda aquella información desde su creación, procesamiento, almacenamiento o eliminación, tanto en formato digital como físico, que tenga valor para la Organización y que se haya determinado que deba ser protegida, considerando su confidencialidad, integridad y disponibilidad. Si se dañan los activos de información, la Organización se expone a la pérdida, corrupción, indisponibilidad, divulgación o acceso no autorizados a terceros, respecto de dicha información.

2. **Política:** Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado. El propósito de una Política, es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégicos establecidos por la Institución. Documento que fija reglas en un organismo respecto de qué se autoriza a ser realizado. Existe para proteger a las personas, los recursos, los activos, o para mantener el orden y la seguridad dentro del organismo.

3. **Falta grave:** Aquella conducta intencionada o dolosa que se comete con infracción a la presente Política por un integrante de la Ilustre Municipalidad de Melipilla, o por un tercero a quién esta política le resulte aplicable.

4. **Evento de seguridad de la información:** Cualquier ocurrencia relacionada con los activos o el entorno, que indique un posible compromiso de la política o la falla de los controles, o incluso una situación no prevista que pueda afectar a la Seguridad de la Información.

5. **Incidente de seguridad de la información:** Uno o más eventos de Seguridad de la Información que comprometen las diferentes operaciones de la Ilustre Municipalidad de Melipilla y la Seguridad de la Información.

6. **Gestión de incidentes de Seguridad de la Información:** Procesos seguidos para detectar, notificar, evaluar y/o analizar incidentes de Seguridad de la Información, y así dar respuesta, tratamiento y aprendizaje, de modo de mitigar el impacto y responder ante éste.

7. **Red de confianza:** Red que se conforma por usuarios que poseen llaves públicas, a través de las cuales es posible codificar mensajes como también verificar firmas.

8. **Redes Institucionales:** Todas aquellas redes y equipos de comunicaciones de propiedad del respectivo organismo, que sean utilizados para comunicar a dos o más usuarios entre sí y/o hacia Internet. Esta denominación incluye servidores, equipos de comunicaciones (routers, switches), equipos de seguridad perimetral (firewalls, IPSs, IDSs), infraestructura de

comunicaciones (cables de red, puntos de red), y en general cualquier otro equipo de comunicaciones en uso en instalaciones del organismo.

9. **VPN:** Siglas en ingles de Red Virtual Privada (Virtual Private Networt), permite la conexión segura entre dos puntos remotos.

Artículo 4°: Revisión, aprobación, cumplimiento y difusión.

1. De la revisión

La presente Política se revisará anualmente a contar de su última aprobación, salvo que el Encargado de Seguridad de la Información determine una periodicidad menor. Dicha revisión deberá ser efectuada por el Comité de Seguridad de la Información. El objetivo de la revisión será:

a) Verificar si la Política está de acuerdo con los cambios en la legislación vigente y con la normativa publicada desde la última revisión.

b) Verificar si la Política requiere de modificaciones debido a cambios que se hayan producido en el Estado de Chile, en el Ministerio de Defensa Nacional y/o por mandato presidencial.

2. De la aprobación

El Comité de Seguridad de la Información propondrá por escrito los cambios que considere necesarios al Encargado de Seguridad de la Información, quien presentará la propuesta de cambios al Jefe de Servicio.

El departamento de informática, será responsable de mantener informado a los funcionarios y prestadores de servicios, de los cambios en la Política de Seguridad de la Información y de dictar la respectiva resolución, con los cambios acordados.

3. Del cumplimiento

a) Las disposiciones contenidas en la presente Política son obligatorias para todas las personas que se desempeñen como funcionarios ya sea de planta o a contrata, prestadores de servicios a honorarios y personal externo que preste servicios en o para la Ilustre Municipalidad de Melipilla.

b) El incumplimiento de esta Política podrá dar origen a las responsabilidades administrativas, civiles o penales, según lo establece la legislación vigente.

c) Cualquier excepción a esta Política deberá ser aprobada mediante acto administrativo por el Jefe de Servicio.

4. De la difusión

a) La Política deberá ser difundida por el Departamento de Informática de la Ilustre Municipalidad de Melipilla, mediante el correo electrónico informatica@munimelipilla.cl a todos los funcionarios y prestadores de servicio a honorarios que desempeñan funciones en la Ilustre Municipalidad de Melipilla.

b) La Política deberá ser publicada en la intranet de la Ilustre Municipalidad de Melipilla.

a) El documento en que conste la Política se deberá entregar a cada funcionario y a los prestadores de servicios a honorarios, que ingresen o se integren a la Ilustre Municipalidad de Melipilla dentro del plazo de 20 días hábiles, lo cual deberá constar en formulario o declaración que se elaborará al efecto. En este último documento deberá constar su recepción, lectura y aceptación. Sin perjuicio de lo expuesto, la autoridad deberá velar y asegurar que la presente Política sea conocida por todos los integrantes de la Ilustre Municipalidad de Melipilla, como también por el personal externo.

CAPÍTULO II: MARCO INSTITUCIONAL

Artículo 5°: Lineamientos

1. La Institución deberá contar con un marco global e integrado de normativa interna, estructura organizacional, estructura física material y aplicaciones de *software* y/o *hardware* que permitan la Seguridad de la Información, y que, a su vez, protejan la información buscando preservar su confidencialidad, disponibilidad, integridad y privacidad.

2. La Institución deberá definir, implementar, mantener, actualizar y monitorear controles para asegurar que se cumplan los objetivos de seguridad específicos que en esta Política se mencionan, con el objeto de gestionar los riesgos asociados a la Seguridad de la Información en un nivel adecuado y aceptable. Para ello, el Encargado de Seguridad de la Información deberá dar cuenta de los riesgos asociados a la Seguridad de la Información y resolver respecto de las medidas de mitigación que deba adoptar el Jefe de Servicio.

3. Las excepciones a la normativa relativa a Seguridad de la Información, deberán ser presentadas al Comité de Seguridad de la Información, quien resolverá de acuerdo atendiendo al riesgo que pudiese enfrentar la Institución.

4. Aspectos organizativos de la Seguridad de la Información

    a) El departamento de Informática deberá definir, documentar y formalizar los roles y responsabilidades de los integrantes de la Ilustre Municipalidad de Melipilla, proveedores de servicios y terceros que corresponda, necesarios para brindar Seguridad de la Información de la Institución, con el objeto de minimizar los riesgos asociados a ella.

    b) El departamento de Informática en conjunto con el Comité de Seguridad de la Información, deberán establecer y mantener un programa de sensibilización y capacitación continua en temas de Seguridad de la Información con el objeto de que los funcionarios, prestadores de servicios, proveedores y terceros, conozcan sus responsabilidades en relación a la Seguridad de la Información.

5. Seguridad de la Información relacionada a los recursos humanos

        a) El departamento de Informática, deberá mantener controles de seguridad relativos a la contratación o desvinculación de sus funcionarios y personal a honorarios, con el objetivo de mitigar el riesgo de actos ilícitos o manejo inadecuado de recursos e información.

        b) A su vez, el Comité de Seguridad de la Información deberá establecer las obligaciones de los integrantes de la Ilustre Municipalidad de Melipilla respecto a la Seguridad de la Información.

6. Todo el personal que se desempeñe o que preste servicios en o para la Ilustre Municipalidad de Melipilla, ya sea interno o externo, será responsable del cumplimiento de esta Política y del marco normativo de Seguridad de la Información y tendrá la obligación de informar de su incumplimiento a su Jefe de División o al Encargado de la Seguridad de la Información. El Encargado deberá realizar el seguimiento y control de las medidas implantadas, proponiendo las sanciones que procedan según lo establecido en el Reglamento de Orden, Higiene y Seguridad.

Artículo 6°: Funcionario responsable

El Encargado de Seguridad de la Información (ESI) de la Ilustre Municipalidad de Melipilla.

Artículo 7°: Funciones y atribuciones del funcionario responsable

1. Deberá velar y verificar el cumplimiento de las normas descritas en la presente Política al interior de la Institución, controlar su implementación y velar por su correcta aplicación.

2. Deberá elaborar los planes de instrucción e inducción para asegurar que todos los integrantes de la Ilustre Municipalidad de Melipilla conozcan y comprendan las medidas dispuestas en la Política.

3. Dar respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos operacionales.

4. Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos.

5. Mantener la coordinación con otras unidades de la municipalidad para apoyar los objetivos de seguridad y establecer puntos de enlace con los 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.

6. Coordinar actividades en el Comité de Seguridad de la Información.

CAPÍTULO III: OBLIGACIONES DE SEGURIDAD

Artículo 8°: Gestión de Activos de Información

1. La información deberá ser clasificada. Para ello, se deberá mantener la normativa Interna que determine los criterios de clasificación en relación a su importancia para el Servicio, especialmente en concordancia a lo establecido en el artículo 8° de la Constitución Política de la República, los artículos 5°, 21° y 22° de la Ley 20.285 "Sobre Acceso a la Información Pública" y demás normas aplicables a esta materia".

2. Para garantizar la protección de la Información, se deberán establecer, implementar y monitorear controles según su criticidad.

3. Todo funcionario y prestador de servicios a honorarios debe disponer de los accesos, y de la información exclusivamente relacionada a las funciones que le son asignadas al cargo.

Artículo 9°: Clasificación de la información

1. **Público**: La información pública no necesita de un tratamiento especial. Un documento público puede ser enviado a personas que no pertenecen al organismo, y puede ser publicado en Internet, salvaguardando los datos personales según dispone el artículo 19° N° 14 de la Constitución Política de la República y la Ley N° 19.628, sobre "Protección de la Vida Privada".

2. **Reservado**: Un documento reservado debe ser creado, modificado y mantenido dentro de redes institucionales. En particular:
   - No deberá ser publicado en Internet.
   - Para ser publicado en la Intranet institucional debe contar con un sistema de autentificación de usuario.

3. **Secreto**: Un documento secreto debe ser creado, modificado y mantenido sólo dentro de la red institucional y, en particular:
   - No deberá ser publicado en sitios de Internet o de una Intranet.
   - No deberá ser enviado a través de correo electrónico.
   - Deberá ser transmitido sólo a través de los medios seguros que cada Institución y organismo dependiente o relacionado determine.
   - Deberá ser almacenado en contenedores físicos, en caja fuerte con llave, o bien en formato digital, mediante mecanismos de cifrado que se determine.

Artículo 10°: Seguridad en el control de accesos

1. El Departamento de Informática deberá mantener controles de acceso a los distintos medios de información, para ello a lo menos se deberán regular las cuentas de usuarios.

2. Deberá tener especial atención en la definición e implementación de los controles sobre las cuentas de altos privilegios y cuentas de sistemas.

3. Deberá mantener controles de acceso a los distintos medios físicos de información, para ello a lo menos se deberá registrar y regular quién puede acceder a ellos.

4. Deberá implementar y monitorear los controles acordes con la criticidad de la información.

Artículo 11°: Seguridad en el cifrado

El departamento de Informática deberá proponer e implementar mecanismos con técnicas criptográficas para la protección de la información, con el fin de asegurar una adecuada protección de la confidencialidad e integridad de la información, en base a la normativa interna que se dicte al efecto.

Artículo 12°: Seguridad en la relación con proveedores de servicios

El Departamento de Informática, deberá implementar y mantener controles de monitoreo sobre las actividades relacionadas con la seguridad de la información
El Departamento de Informática deberá implementar y mantener un adecuado control y monitoreo de la Seguridad de la Información sobre tales actividades y de la información manejada o a la cual acceden terceros. Se deberá tener especial resguardo respecto de los proveedores de servicios tecnológicos que estén a cargo de los servicios esenciales para la continuidad operativa de la Ilustre Municipalidad de Melipilla.

Artículo 13°: Seguridad en la operación

1. Cada División deberá implementar controles y mecanismos que permitan prevenir, detectar, controlar, eliminar y corregir los problemas de integridad, disponibilidad y confidencialidad de información debido a la explotación de vulnerabilidades propias de softwares o medios de procesamiento.

2. Se deberán implementar controles y mecanismos que permitan prevenir, detectar, controlar, eliminar y corregir los problemas de integridad, disponibilidad y confidencialidad de información, debido a la manipulación no autorizada sobre medios físicos.

Artículo 14°: Seguridad en el uso de tecnologías de comunicación.

El Departamento de Informática en conjunto con el Comité de Seguridad de la Información deberán proponer, desarrollar, aprobar e implementar los controles necesarios para regular los accesos y uso apropiado de Internet, correo electrónico u otros servicios de redes y comunicaciones relacionados, respecto de todos los integrantes de la Ilustre Municipalidad de Melipilla y de terceros que accedan a ellos.

Asimismo, se deberán definir los lineamientos para una correcta administración.

Artículo 15°: Trabajo colaborativo y remoto.

El Departamento de Informática en conjunto con el Comité de Seguridad de la Información, deberá definir, diseñar, aprobar e implementar los controles necesarios para regular el uso de VPN (Virtual Private Networt), teletrabajo, videoconferencia y colaborativo, con al menos los mismos niveles de seguridad que el trabajo presencial.

Artículo 16°: Seguridad en la adquisición, desarrollo y mantenimiento de sistemas

1. El departamento de Informática, deberá establecer la regulación y controles necesarios para garantizar que la Seguridad de la Información sea una parte integral de los sistemas y servicios de información.

2. La Seguridad de la Información deberá considerar controles de desde el inicio hasta el fin de todo proyecto. Éstos deben ser implementados y probados antes de la puesta en producción, se aplicarán para desarrollos internos, externos y/o adquiridos.

Artículo 17°: Gestión de incidentes de seguridad

El Comité de Seguridad de la Información deberá implementar y mantener mecanismos y herramientas que permitan detectar, manejar y controlar los incidentes relacionados con la Seguridad de la Información, en los activos tecnológicos y de información.

Artículo 18°: Cumplimiento normativo relativo a la Seguridad de la Información

El Comité de Seguridad de la Información deberá establecer los controles necesarios para cumplir con normativa interna, leyes aplicables y regulaciones vigentes, respecto a la reserva y privacidad de la información de los integrantes de la Ilustre Municipalidad de Melipilla y de terceros. Así como de los derechos de propiedad intelectual y licenciamiento de *software*.

Artículo 19°: Gestión de riesgos

El Comité de Seguridad de la Información deberá elaborar un plan de trabajo anual, el que debe ser aprobado por el Jefe de Servicio y será propuesto por el Encargado de Seguridad de la Información, debiendo incorporar todas las actividades del proceso de gestión de riesgos y en específico, la evaluación y el tratamiento de dichos riesgos.

Artículo 20°: Protección física de la Seguridad de la Información

El Departamento de Informática deberá establecer controles que aseguren el transporte, almacenamiento y destrucción de los activos de información físicos según sea el caso, salvaguardando la confidencialidad, integridad y disponibilidad.

2.-TÉNGASE PRESENTE que la política que por este acto se aprueba iniciará su vigencia una vez dictado el presente acto administrativo.

Anótese, comuníquese, publíquese y archívese

PAULA GARATE ROJAS
ALCALDESA
I. MUNICIPALIDAD DE MELIPILLA

CAROLINA LÓPEZ GALDAMES
SECRETARIA MUNICIPAL (S)

CLG/FLF/lca

DISTRIBUCIÓN:
-Administración Municipal
- Secretaria Municipal
- Dirección de Control
- Dirección de Asesoría Jurídica
- Departamento de Informática
- Transparencia Municipal
- Archivo Oficina de Partes/