APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACION PARA LA MUNICIPALIDAD DE MELIPILLA.

DECRETO EXENTO N° 1690

MELIPILLA, 13 de mayo de 2016.-

LA ALCALDIA DECRETO HOY LO SIGUIENTE:

VISTOS: Lo dispuesto en el D.S N°83, de 2005, de MINSEGPRES, que aprueba norma técnica para los órganos de la administración del Estado sobre la seguridad y confidencialidad de los documentos electrónicos, la norma chilena NCh-ISO 27001:2013, sobre Sistema de Gestión de Seguridad de la Información; la Resolución N° 1600 de 2008, deja, Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón; Las facultades que me confiere la Ley N° 18.695, Orgánica Constitucional de Municipalidades y sus posteriores modificaciones;

CONSIDERANDO: a) Que se han dictado una serie de normas, entre las que se encuentra el Decreto Supremo N° 83, del 2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos y las Normas-Chilenas NCh-ISO 27001:2013 y NCh-ISO 27002:2013 que proporcionan un marco de gestión de Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada; b) La necesidad evaluada, como resultado de la revisión efectuada por parte de la Encargada de Seguridad de la Información, de crear la Política General de Seguridad de la Información para la Municipalidad de Melipilla:

DECRETO:

1.- APRUÉBESE, LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD DE MELIPILLA, la que se detalla a continuación:

CONTROL DE VERSIONES

VERSION	FECHA APROB.	MOTIVO DE LA REVISION	AUTOR (ES)
1	Mayo 2016	Creación de la Política General de Seguridad de la Información de la Municipalidad de Melipilla.	Limbi Ortiz Neira/ Encargada de Seguridad de la Información de la Municipalidad de Melipilla.

A. DECLARACIÓN INSTITUCIONAL: La Municipalidad de Melipilla ha decidido establecer, implementar, mantener y mejorar continuamente los Sistemas de Seguridad de la información - *en adelante el SSI* -, siendo éste un compromiso en el fomento y desarrollo de una cultura de seguridad, basada en preservar los principios de confidencialidad, integridad y disponibilidad de la información y asegurar la continuidad operacional, en beneficio de los usuarios, ciudadanos y partes interesadas para alcanzar los objetivos institucionales, contribuyendo al desarrollo de la comuna. De este modo, la información es un activo esencial para que la Municipalidad alcance sus objetivos con el propósito de cumplir con su misión. Por tal motivo, entendemos por activo de información todos aquellos elementos que hacen posible o sustentan los procesos operativos o del negocio, tal como las personas que utilizan los sistemas e infraestructura que soporta la *información; y la información propiamente tal, los equipos, en cualquiera de sus múltiples formatos,* incluyendo en papel y digital. Para el desarrollo del SSI la presente política general, las políticas específicas, procedimientos y otros documentos relacionados, se ajustarán a los requerimientos normativos vigentes en seguridad de la información, además de considerar los aspectos pertinentes del marco normativo de la Municipalidad.

B. OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN. La gestión de seguridad de la información en la Municipalidad tiene como principales objetivos:

- Resguardar los activos de información mediante controles de seguridad aplicables a partir del análisis, evaluación y tratamiento de los riesgos que afecten su confidencialidad, integridad y disponibilidad.
- Asegurar la continuidad operacional a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.

Para lo anterior, en el marco del SSI, se desplegará un conjunto de lineamientos y prácticas de seguridad de la información —en consistencia con las disposiciones indicadas en esta política en los puntos 5 y 6 — debiendo ser formalizadas a través de políticas específicas, procedimientos y otros documentos para su cumplimiento y aplicación por parte de las personas, especialmente en procesos definidos en el alcance.

C. ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y DEL SSI

La presente política es aplicable a funcionarios de planta, contrata y honorarios que formen parte de la Municipalidad de Melipilla, así como también a asesores, consultores, practicantes y personas naturales o jurídicas que presten servicios para la Municipalidad.

Para el desarrollo del SSI, se consideran los requisitos de la norma NCh-ISO 27001 2013, desplegando las buenas prácticas según orientaciones indicadas en la NCh-ISO 27002:2013.

D.- ROLES Y RESPONSABILIDADES

Los roles y responsabilidades: para el SSI serán definidos en cuanto a su composición y funciones, mediante la formalización de un acto administrativo que considere al menos:

- Un/a Encargado/a de Seguridad de la Información, en cuyo rol el jefe de Servicio delega las decisiones relativas a la seguridad de la información institucional y su coordinación, asegurando la alineación de SSI y sus objetivos al cumplimiento de los objetivos estratégicos, coordinando las acciones necesarias para satisfacer los requisitos aplicables; favoreciendo la mejora continua de este sistema de gestión y la satisfacción de las partes Interesadas.
- Un Comité de Seguridad de la Información —o Comité de similar denominación—, formado por un equipo multidisciplinario que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, a partir de los dominios que regulan los diferentes aspectos.

E. DISPOSICIONES PARA RESGUARDAR LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

A continuación se describe cómo el Municipio abordará estos principios básicos de Seguridad de la información.

E.1 DE LA CONFIDENCIALIDAD DE LA INFORMACIÓN

La Municipalidad se comprometerá a resguardar la confidencialidad de la información institucional, estableciendo lineamientos prácticas de seguridad y mecanismos para clasificar y reconocer la información de carácter confidencial en la gestión interna, que deba ser protegida ante filtración o divulgación no autorizada.

Por lo anterior, y dada la condición publica de la información elaborada con presupuesto público y que obre en poder de los órganos de la administración del Estado, es importante señalar que-, su resguardo no implica desconocimiento ni obstaculización del derecho de toda persona a solicitar y recibir información, en la forma y condiciones qué establece la Ley 20.285.

Además, el resguardo de la información involucra la obligación de las personas que trabajan en el tratamiento de datos personales -o tengan acceso a éstos de otra forma de guardar secreto sobre los mismos, según Ley 19.628 de Protección de Datos de Carácter Personal

De este modo, la Municipalidad se comprometerá a implementar los controles necesarios para garantizar que tanto la Información física como digital sea accesible sólo por aquellos usuarios autorizados y de acuerdo a la legislación vigente revisando periódicamente estos lineamientos.

E.2 DE LA INTEGRIDAD DE LA INFORMACIÓN

La Municipalidad se comprometerá a preservar la integridad de la información Institucional asegurando la máxima factibilidad que esta sea mantenida con exactitud tal cual fue generada, trasportada o trasmitida, sin ser manipulada o alterada por personas o procesos no autorizados. Para ello, se establecerán lineamientos, prácticas de seguridad y mecanismos que aseguren la integridad de la información contenida en cualquier espacio, equipo, sistema o infraestructura, en todos los formatos posibles, salvaguardando además la mayor completitud, coherencia consistencia y actualización de sistemas y procesos.

E.3 DE LA DISPONIBILIDAD DE LA INFORMACIÓN

La Municipalidad asegurará la disponibilidad de la Información Institucional, Incluyendo la disponibilidad de equipos, sistemas e infraestructura que la contengan o la provean en los niveles y tiempos requeridos tanto a escala Interna como externa estableciendo lineamientos, prácticas de seguridad y mecanismos que prevengan cualquier acción que elimine o exponga a pérdida la Información relevante y que mantengan la continuidad del flujo de información.

F. DISPOSICIONES PARA ASEGURAR LA CONTINUIDAD DE LAS OPERACIONES

Las actividades en procesos, y los activos de información que contienen, se encuentran expuestos a incidentes que pueden derivar en contingencias en las operaciones del Municipio. El SSI propicia disminuir la probabilidad de ocurrencia y las consecuencias negativas de estos sucesos, mediante lineamientos y la aplicación de prácticas de seguridad tendientes a su gestión y efectiva solución.

F.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Municipalidad, a través del Comité de Seguridad de la información, definirá lineamientos a través de una política específica y describirá las prácticas de gestión de Incidentes de seguridad de la Información, mediante procedimientos que aborden los tipos de Incidentes que corresponda.

La gestión de Incidentes de seguridad de la Información contemplará actividades claves, tales como: la detección, registro y reporte a áreas pertinentes de un Incidente de seguridad de la información, su análisis (considerando su priorización, su declaración como incidente y descarte); su pronta solución, su escalamiento a autoridades internas como externas, su respuesta y seguimiento, además de la recopilación y preservación de evidencias.

F.2 GESTIÓN DE LA CONTINUIDAD ANTE CONTINGENCIAS

La Municipalidad establecerá lineamientos a través de una política específica y determinará las prácticas de gestión de continuidad de las operaciones, mediante uno o más de planes de contingencia o continuidad en los niveles que corresponda.

La gestión de continuidad de las operaciones considerará aspectos claves, tales como: la definición de una estructura organizacional adecuada para resolver acciones en cada plan; la determinación de escenarios posibles; un análisis de riesgos y consecuencias asociadas a dichos escenarios; las estrategias de continuidad de los procesos; el desarrollo de procedimientos alternativos de operación, si corresponde; los componentes informáticos y no Informáticos de apoyo y las acciones de recuperación ante contingencias.

G. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

G.1 GENERACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Para el desarrollo de las políticas de seguridad se adoptará un formato especificado para él SSI, ciñéndose a pautas convenidas con los actores que tengan injerencia en el despliegue de este sistema de gestión.

Asimismo, para la implementación operativa de algunas políticas específicas de seguridad se elaborarán procedimientos u otros documentos qué se alineen con parámetros establecidos de documentación.

G.2 APROBACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Las políticas específicas de seguridad serán aprobadas por el Alcalde y los procedimientos serán aprobados por el Comité de Seguridad de la Información.

G.3 PUBLICACIÓN Y COMUNICACIÓN DE UNA POLÍTICA Y OTROS DOCUMENTOS

Las versiones vigentes de la presente política serán difundidas en el sitio web de la Municipalidad. La comunicación de la presente política, las políticas específicas de seguridad, los procedimientos y otros documentos se efectuará de manera que el contenido de la documentación sea accesible y comprensible para todos los usuarios, pudiendo utilizarse los canales de difusión establecidos.

G.4 REVISIÓN DE LA POLÍTICA

La presente política será revisada anualmente, o cuando la Municipalidad lo requiera, para asegurar su continuidad e idoneidad, considerando los cambios que puedan producirse, tales como enfoques a la gestión de seguridad, circunstancias de la Institución, cambios legales, cambios al ambiente técnico, recomendaciones realizadas por autoridades pertinentes, tendencias relacionadas con amenazas y las vulnerabilidades entre otras.

DECRETO EXENTO N° 1690

MELIPILLA, 13 de mayo de 2016.-

Asimismo, la Municipalidad evaluará el cumplimiento de la presente política general, a lo menos cada tres años, mediante auditorías internas, externas y/o revisiones independientes.

H.- SANCIONES APLICABLES

El incumplimiento o violación a esta política debidamente acreditada conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo 18.883, o a aquellas que determine el Sr. Alcalde respecto a los funcionarios de la Municipalidad o al término anticipado del contrato por Incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

2.- La presente política de seguridad de la información de la Municipalidad de Melipilla, entrará en vigencia a partir de la publicación del presente decreto en la página web institucional www.melipilla.cl.

Anótese, comuníquese y archívese.

MARIO GEBAUER BRINGAS
ALCALDE
I. MUNICIPALIDAD DE MELIPILLA

CARLO GUTIERREZ ARAVENA
SECRETARIO MUNICIPAL
SUBROGANTE

CGA/MFM/LON/ygs.-
DISTRIBUCION:
- Administración Municipal
- Secretaría Municipal
- Direcciones Municipales
- Departamentos Municipales
- Secciones Municipales
- Relaciones Públicas
- Juzgado de Policía Local
- Transparencia
- ARCHIVO OFICINA DE PARTES/