REPÚBLICA DE CHILE

PROVINCIA DE CURICÓ

MUNICIPALIDAD DE ROMERAL

ALCALDÍA.

DECRETO ALCALDICIO N° 0000917 /

REF.: APRUEBA POLITICA GENERAL DE SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LA ILUSTRE MUNICIPALIDAD DE ROMERAL.

Romeral, 05 ABR 2024

VISTOS

1. La ley N° 19.880 que Establece las Bases de los Procedimientos Administrativos que rigen los actos de los Órganos de la Administración del Estado.
2. La Ley N° 18.883, sobre Estatuto Administrativo para Funcionarios Municipales.
3. El Decreto Exento N° 1652, que Aprueba el Reglamento de la Organización Interna Municipal de fecha 02 de Diciembre de 2019.
4. El Decreto Supremo No 83, que Aprueba la Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos, MINSEGPRES, promulgado con fecha 03 de Junio de 2004.
5. Las facultades que me confiere la ley N° 18.695 Orgánica Constitucional de Municipalidades, y sus modificaciones.

CONSIDERANDO:

1. La necesidad de la I. lustre Municipalidad de Romeral de contar con una Política General del Sistema de Gestión de la Seguridad de la Información.

2. Que, el Decreto Supremo N° 83, que Aprueba la Norma Técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los documentos electrónicos, establece en su Artículo 9° que: *"Durante la primera etapa de aplicación de esta norma, los órganos de la Administración del Estado desarrollarán las políticas, procedimientos, acciones y medidas tendientes a obtención del Nivel Básico de Seguridad de los documentos electrónicos que se establecen en este Título".*

DECRETO:

PRIMERO: APRUÉBESE, la Política General del Sistema de Gestión de la Seguridad de la Información para la Ilustre Municipalidad de Romeral, que es del siguiente tenor:

POLITICA GENERAL DEL SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION

Contenido

INTRODUCCIÓN

La información es un recurso estratégico, que tiene valor para los procesos que realiza diariamente la Municipalidad y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, la operación de los equipos computacionales, minimizando los riesgos de daño y hurto de información, además de contribuir y facilitar la gestión administrativa de la Municipalidad.

En el entendido de que los riesgos que se logren identificar estarán siempre presente, ya que no se pueden eliminar, la Municipalidad se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, a través de un programa de mantención del "Sistema de Gestión de Seguridad de la Información (SGSI)", basado en la norma chilena NCh-ISO 27001:2013 y en los lineamientos de ciberseguridad entregado por Presidencia, tendiente a homogeneizar los criterios de seguridad y ciberseguridad, con el objetivo de preservar los activos de información institucional.

DOCUMENTO DE REFERENCIA

- Noma Chilena NCh-ISO 27001:2013, Sistema de gestión de la seguridad de la información-Requisitos; y en la norma chilena NCh-ISO 27002:2013 código de prácticas para los controles de seguridad de la información.

- Decreto Supremo 83, de 2005, del Ministerio Secretaria General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
- Ley 20.285, de 2008, del Ministerio Secretaria General de la Presidencia Sobre Acceso da la Información pública.
- Ley 19.223, de 1993, del Ministerio de Justicia, Tipifica Figuras Penales Relativas a la Informática.
- Ley 19.927, de 2004, del Ministerio de Justicia, Modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de Delitos de Pornografía Infantil.
- Ley 18.883, de 1989, del Ministerio del Interior, Aprueba Estatuto Administrativo para Funcionarios Municipales.
- Decreto con Fuerza de Ley 1/19.653, de 2001, del Ministerio Secretaria General de la Presidencia, Fija texto refundido, coordinado y sistematizado de la ley 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado.

DEFINICIONES

Activo de Información. Aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información, de valor para la Institución. Se distinguen 3 niveles básicos de activos de información:

1. La Información propiamente tal, en sus múltiples formatos, a modo de ejemplo, papel, digital, texto, imagen, audio, video.
2. Los Equipos, Sistemas de Información e Infraestructura que soportan esta información.
3. Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Autenticación: Proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.

Comité de Seguridad de la Información Institucional. Agrupación de personas que tienen como misión validar y aprobar las políticas de seguridad de la información, y los controles tendientes a regular el uso y manejo de la información. Arbitrar conflictos que se generen en materias de seguridad de la información, apoyar planes de difusión y formación de la cultura de la seguridad de la información.

Confidencialidad: Aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.

Contenido del documento electrónico. Información, ideas y conceptos que un documento expresa.

Continuidad del negocio. Continuidad de las operaciones de la institución.

Disponibilidad. Aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.

Documento electrónico. Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

Documentos públicos. Aquellos documentos que no son ni reservados ni secretos, cuyo conocimiento no está circunscrito.

Documentos reservados. Aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en Conformidad a ella, que les confiere tal carácter.

Encargado de Seguridad y Ciberseguridad. Persona responsable por la implementación de medidas de control que garanticen la seguridad de la información, así como también aplicar las medidas de ciberseguridad que promueve el Estado.

Ejecutivo. Autoridad dentro de la institución.

Identificador formal de autenticación. Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.

Incidentes de seguridad. Situación adversa que amenaza o pone en riesgo un sistema informático.

Integridad. Salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas *por* entes debidamente autorizados.

Negocio. Función o servicio prestado por la organización.

Política de seguridad. Conjunto de normas o buenas prácticas, declaradas y aplicadas *por* una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

Repositorio. Estructura electrónica donde se almacenan documentos electrónicos.

Riesgo. La posibilidad de sufrir daños o perdidas, la amenaza es un componente del riesgo y se puede considerar coma: un agente de amenazas ya sea humano o no humano.

Seguridad de la Información. Es el nivel de certeza y confianza que la organización desea tener de su capacidad para preservar la confidencialidad, factibilidad de autenticación, integridad y disponibilidad de la información. De esta forma, proteger el recurso o activo de información de una amplia gama de amenazas, asegurando la continuidad de las operaciones de la Subsecretaría, minimizando el daño y cumpliendo su misión y objetivos estratégicos.

Sistema de Gestión de Seguridad de la Información. Parte del sistema de gestión, basada en un enfoque hacia los riesgos de una institución, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión considera la estructura organizacional, políticas, actividades de planificación, responsabilidad, prácticas, procedimientos, procesos y recursos.

Sistema informático. Conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz

de obtener, almacenar, tratar, administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información.

Usuario. Entidad o individuo que utiliza un sistema informático.

ROLES Y RESPONSABILIDADES

Rol: Comité de Seguridad de la Información Institucional.

Responsabilidad: Es responsable del ciclo de vida de las políticas de seguridad de la información. Velar por la implementación de los controles de seguridad en la plataforma tecnológica. Fomentar planes de difusión, capacitación y formación de la cultura de la seguridad de la información. Arbitrar conflictos que se generen en materias de seguridad de la información. Revisar, al menos una vez al año, el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI).

Rol: Encargado/a de la Seguridad de la Información.

Responsabilidad: Proponer, desarrollar y actualizar las políticas de seguridad de la información al interior de la institución, coordinar su implementación y evaluación, velando por Su correcta aplicación. Monitorear el correcto funcionamiento de los procedimientos vinculados al Sistema de Gestión de la Seguridad de la Información (SGSI). Mantener coordinación con otros departamentos y unidades de la Municipalidad para apoyar el cumplimiento de los objetivos de seguridad. Establecer enlaces con encargados de seguridad de la información de otros organismos públicos, con las instancias gubernamentales encargadas de la Seguridad de la Información y con especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad de la información y ciberseguridad pertinentes. Mantener actualizado el inventario de activos de información de la municipalidad, de acuerdo con los procedimientos definidos. Mantener informado periódicamente al Comité de Seguridad de la Información acerca del estado del Sistema de Gestión de Seguridad de la información en la Institución. Promover acciones tendientes a la difusión y sensibilización respecto a la Seguridad de la Información y Ciberseguridad a los funcionarios, colaboradores y practicantes vinculados a la institución. Ejecutar, aplicar e implementar las medidas de Ciberseguridad que sean instruidas por la Presidencia.

Rol: Usuarios(as)

Responsabilidad: Son las personas, funcionarios, colaboradores, practicantes o personal externo que preste servicios permanentes o temporales, que usan los activos de información y los sistemas computacionales de la institución. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente, así coma las políticas específicas, manuales y procedimientos asociados al SGSI y a la ciberseguridad y, además, tienen la obligación de reportar cualquier incidente o evento de seguridad del que tengan conocimiento.

Rol: Jefaturas de la Municipalidad

Responsabilidad: Las jefaturas de las Direcciones, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política, así como de las políticas específicas, manuales y procedimientos asociados al SGSI.

OBJETIVO

El propósito de esta Política es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información para la Municipalidad. La Autoridad Comunal reconoce la importancia y el valor de los activos de información como un elemento crítico al proceso de toma de decisiones para el cumplimiento de su Misión Institucional y, por tanto, establece la Política del Sistema de Gestión de la Seguridad de la Información. En el marco de este Objetivo, se establecen las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos, como también, estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico, y facilitar la relación electrónica al interior de la municipalidad con otros órganos de la Administración del Estado, la ciudadanía y el sector privado.

OBJETIVOS ESPECIFICOS

1. Proteger los recursos de información de la Municipalidad y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los conceptos de confidencialidad, integridad y disponibilidad, partes claves de la seguridad de la información *y* la protección de datos.
2. Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
3. Mantener la Política de Seguridad del Municipio actualizado, para asegurar su vigencia y nivel de eficacia ante nuevas amenazas.
4. Proteger eficientemente los activos de información institucionales, asegurando su confidencialidad, integridad y disponibilidad.
5. Establecer procedimientos, instrucciones u otros documentos para la clasificación y catastro de los activos de información de la Municipalidad.
6. Establecer procedimientos para efectuar una evaluación anual de riesgos destinada a proteger eficazmente los activos de información de la
7. Superintendencia de Educación y prevenir la ocurrencia de incidentes de seguridad de la información.
8. Establecer los mecanismos de difusión de la presente Política para el conocimiento de todos los funcionarios de planta y a contrata y personal a honorarios del Servicio, especialmente en lo referente a capacitaciones periódicas en materias de seguridad de la información.
9. Ejecutar, aplicar e implementar las medidas de ciberseguridad instruidas mediante el Instructivo Presidencial N° 8, del 23 de octubre de 2018, del presidente de la República, que Imparte instrucciones urgentes en materia de ciberseguridad, para la protección de redes, plataformas y sistemas informáticos de los órganos de la Administración del Estado.

SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información se entiende como la preservación de los activos de información institucional con respecto a:

- La Confidencialidad: que la información se accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- La Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- La Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

EVALUACIÓN Y DIFUSIÓN

La presente política será evaluada en el municipio al menos una vez al año, o bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar su continua idoneidad, eficiencia *y* efectividad.

Una vez que el documento entre en vigencia el/la Encargado/a de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

ACEPTACIÓN

Todos los usuarios de la Municipalidad sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar esta política y procedimientos relacionados. Para el caso de terceros y solo por el hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política, manuales y procedimientos vigentes de seguridad de la información, publicados en el sitio web de la municipalidad y sus correspondientes modificaciones, la cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

SANCIONES POR INCUMPLIMIENTO DE LA POLÍTICA.

El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información, procedimientos u otros documentos que se deriven de estos, debidamente acreditado, conlleva a la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a las funcionarios/as de la Municipalidad o al termino anticipado del contrato por incumplimiento de obligaciones, sea cuando se trate de personas que no tengan responsabilidad administrativa y en el caso de 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.

EXCEPCIONES

La presente Política, y las políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad *y* debidamente autorizados por la autoridad.

ASESORAMIENTO EN MATERIA DE SEGURIDAD DE LA INFORMACIÓN

El Encargado de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles al Municipio, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Municipios o asistir a capacitaciones para incrementar el conocimiento sobre esta materia.

REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Encargado de Seguridad de la Información realizarán revisiones periódicas sobre la vigencia e implementación de las Políticas de Seguridad de la Información, esta política se revisará cada semestre (6 meses) a contar de su aprobación. Estas revisiones aseguran que los puntos expuestos en la presente política cumplan con la vigencia correspondiente y establece planes de acción para realizar mejoras e integrar nuevas ideas.

ACERCA DE FUNCIONARIOS

Para efectos de este documento se considera "usuario" al funcionario, prestador de servicios o trabajador que ejerza funciones en la Municipalidad de Romeral.

POLITICAS CORREOS ELECTRÓNICOS INSTITUCIONALES

Activación de una cuenta de correo electrónico municipal

Para la creación de una cuenta se debe seguir los siguientes pasos.

a) El director responsable del usuario será la única persona que puede solicitar formalmente la creación de una cuenta de correo electrónico.
b) En esta solicitud el director deberá informar de esta petición de activación

de cuenta de un usuario mediante correo electrónico o mediante una notificación interna municipal a los siguientes cargos o sus subrogantes:

a. Administrador Municipal.
b. Encargados de la Dirección Departamento o Unidad solicitante.
c. Encargado de la seguridad de la información.
d. Departamento de Informática.

c) Esta petición se realizará formalmente a la siguiente dirección de correo

electrónico informatica@muniromeral.cl en donde se debe hacer envió de la siguiente información:

a. Rut usuario:
b. Nombre usuario:
c. Modalidad de nombramiento o contratación:
d. Cargo usuario:
e. Fecha de activación de la cuenta:
f. Nombre Encargado del usuario:
g. Dirección donde se ubicará:
h. Departamento:
i. Lugar físico del usuario:
j. Numero de contacto del usuario:
k. Email personal del usuario:

d) Una vez recibida la solicitud formal por parte del director, el encargado de cuentas de correo electrónica de la municipalidad deberá verificar la disponibilidad que exista, y este procederá a la activación de la cuenta de correo electrónico.

e) Cuando se realice la activación de la cuenta el encargado de las cuentas de correo electrónica del departamento de informática de la municipalidad será la persona que informara mediante correo electrónico a los directores mencionados y se deberá poner en contacto telefónico o mediante correo electrónico personal del solicitante de que su cuenta esta activa, entregándole los pasos a seguir de como deberá ingresar a su cuenta.

USO DE CUENTAS DE CORREO ELECTRÓNICO MUNICIPAL

Los correos electrónicos proveen de una comunicación rápida. Está prohibido el uso de correos personales para fines laborales *y* el uso de correos laborales para fines personales, solo se debe utilizar las herramientas provistas por la Municipalidad para la comunicación electrónica.

El uso de correos electrónicos es un recurso compartido, por lo tanto, los mensajes y archivos personales deben manejarse en el rango mínimo de almacenamiento de espacio. Toda casilla de correo electrónico institucional está directamente vinculada al usuario/a y es responsable del contenido y de los archivos adjuntos a cada mensaje. El resguardo de las claves de acceso al correo electrónico es de exclusiva responsabilidad del usuario, no se deben divulgar, compartir ni anotarlas en lugares visibles *y/o* de fácil acceso. Los usuarios administradores de correo electrónico del departamento informático y los usuarios institucionales tienen prohibido intentar acceder en forma no autorizada a la cuenta de correo de otro usuario y tratar de tomar su identidad, salvo su expresa autorización escrita.

Los usuarios de la Municipalidad deberán usar un lenguaje respetuoso en sus mensajes con usuarios internos o externos y estos mensajes de ninguna forma podrán ser de contenido difamatorio, insultante, injurioso, amenazados, ofensivo, obsceno, racista o sexista.

El usuario deberá enviar por correo electrónico documentos que, individualmente o en conjunto, no contengan más de 25 megabytes. Para casos que se requieran enviar información que supere esta cantidad de megabytes, el usuario puede solicitar al Encargado/a de Seguridad de la Información la asesoría para determinar la mejor alternativa de compartir estos documentos.

Como regla general, toda información de la Municipalidad no debe ser compartida con terceros sin la debida autorización de la respectiva Jefatura y Encargado/a de Seguridad de la Información. Siempre se debe tener en cuenta que existe un alto riesgo de intercepción de la información, por esta razón se recomienda no enunciar el contenido de información confidencial o sensible en el título de un correo electrónico.

Cualquier información que contenga datos personales o información sensible, debe ser encriptada con una contraseña para su envío, la que se entregará por parte del remitente vía telefónica, sin dejar registro escrito de ella en el correo electrónico.

Si los Usuarios tienen dudas respecto a la información que enviará, debe consultar con su Jefatura o con el/la Encargado/a de Seguridad de la Información.

El usuario debe identificar en el correo sus datos (nombre, apellido, unidad) para que el receptor del mensaje identifique con certeza la identidad del remitente y la unidad de su procedencia.

Se prohíbe personificar o intentar personificar a otra persona a través de la utilización de encabezados falsificados u otra información personal, es decir, tomar el nombre de usuario de otra persona y hacerse pasar por ella, para enviar un correo electrónico.

Si un usuario se ausenta de sus labores por un tiempo considerable (uso de feriado legal, licencias médicas, Comisión de servicio, etc.), debe dejar su correo electrónico con respuesta automática, donde comunique que estará ausente por un periodo de tiempo, especificando las fechas e indicando el nombre y correo electrónico del usuario/a que lo reemplazará.

SOBRE CUENTA Y ESTRUCTURA DE CORREO ELECTRÓNICO

Una dirección de correo electrónico consta de dos partes: el nombre de usuario o departamento/oficina (a la izquierda) o también identificado como alias y el dominio (a la derecha): ambos unidos por el símbolo @. El nombre de usuario o alias es el identificativo de la persona que usará y gestionará dicho correo electrónico. Por su parte el dominio este compuesto por el dominio que corresponde al nombre del servidor de la organización.

SORE RESTRICCIONES AL USO Y CONTENIDO DEL CORREO ELECTRONICO

El Usuario interno o externo que utilice el correo electrónico institucional podrá enviar mensajes con un tamaño de hasta 25 MB, *y* recibirlos con un tamaño de hasta 25 MB, sin perjuicio que esta definición pueda cambiar de acuerdo con las necesidades, roles y funciones de cada uno de los Usuarios, la cual será debidamente autorizada por su respectiva Jefatura. Los usuarios deben respetar la naturaleza confidencial de los datos que puedan ser de su conocimiento ya sea como parte de su trabajo.

El usuario tiene prohibido el uso de seudónimos u otros sistemas para ocultar su identidad, en todos los mensajes debe estar claramente identificado el origen y propietario del mensaje. Se prohíbe el envío de publicidad o cualquier información de tipo comercial por correo institucional. Los mensajes contenidos en el correo institucional no podrán ser contrarios a las disposiciones del orden público y al respeto de los derechos fundamentales de las personas.

No se debe enviar por correo institucional, contenidos que no tengan relación con el trabajo o que excedan al tamaño asignado tales como videos, imágenes, archivos de audio (mp3), etc., a fin de no sobrecargar la red institucional.

Se prohíbe utilizar la cuenta de correo electrónico institucional para emitir opiniones en foros de discusión externas a la institución, listas temáticas u otras instancias de naturaleza polémica, que pueda crear conflictos al interior de la institución.

El Usuario de correo electrónico institucional debe evitar la instalación y ejecución de archivos adjuntos que sean desconocidos, cualquier duda que tenga respecto de la seguridad de algún adjunto, debe consultarla al Encargado/a de Seguridad de la información.

El Usuario de correo electrónico debe tener cuidado con archivos adjuntos que descargue a su equipo, escanear con antivirus en caso de dudas u origen desconocido (formato imagen: jpg o gif, archivos en formato Word: doc o docx o archivos en formato PDF).

El uso del listado de contactos difundidos por los sistemas de la institución es solo para consultas y de uso exclusivo dentro de la Municipalidad. Este prohibido difundir cualquier listado (ejemplo: correos, teléfonos u otro tipo

de información publicada) por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

SOBRE PRIVACIDAD DE LOS MENSAJES ELECTRÓNICOS

El resguardo de información clasificada como confidencial secreta o reservada, de acuerdo con lo establecido en el Artículo N°21 de la Ley 20.285 requiere medidas apropiadas. Si las necesidades de la institución obligan al envío de información mediante el sistema de correo, los Usuarios deben enviarlo únicamente a las personas que lo requieren. Es importante considerar que un mensaje de correo electrónico puede ser impreso o reenviado a personas no autorizadas. En la confección y envío de mensajes confidenciales por e-mail, los Usuarios deben tomar las mismas precauciones a las empleadas a los documentos confidenciales impresos. Se reitera que el manejo de la información confidencial debe ser encriptada.

SOBRE USO DEL CORREO ELECTRÓNICO EN EL CASO DE DESVINCULACIONES, RENUNCIAS Y OTROS:

a) La Unidad encargada del Personal de la Municipalidad, informará mediante correo electrónico institucional al Encargado/a de Seguridad de la Información, cuando un funcionario/a deje de prestar servicios a la municipalidad.

b) Se procederá a respaldar y deshabilitar la cuenta de correo electrónico institucional e informará a través de respuesta automática que el Usuario ya no pertenece a la institución, acompañado de los datos de contacto de la persona que lo reemplace.

c) La deshabilitación de la cuenta de correo electrónico, será por un periodo de 6 meses, al término de este periodo, la cuenta será cerrada.

d) Se respaldará el correo igual que cualquier otro que este en uso. El contenido del correo institucional será resguardado como información institucional.

POLÍTICA SOBRE EL USO E INSTALACIÓN DE SOFTWARE

a) Todo software debe ser instalado por el departamento de informática de la municipalidad, lo cual debe ser revisado en forma periódica.

b) Los usuarios no pueden descargar software desde internet, o traer el software de su casa sin autorización del encargado de la información.

c) Cuando un usuario detecta la necesidad de utilizar un software en particular, debe solicitarlo a su jefatura directa, quién mediante e-mail, envía solicitud de evaluación al Encargado/a de Seguridad de la Información. La solicitud tiene que almacenarse como un registro.

d) Los privilegios para la instalación de software por parte de los usuarios deben ser limitados a un mínimo, estos privilegios deben ser revisados cada cierto tiempo, ya que un usuario puede cambiar de área, departamento.

e) El Encargado/a de Seguridad de la Información tiene que determinar si la Municipalidad tiene licencia del programa solicitado. Si no existe licencia, notifica al usuario.

f) El Departamento de Informática deberá ser informado acerca de las inversiones sobre la adquisición de un nuevo software. Una vez que se ha tomado la decisión, el Departamento de Informática procederá a incluir el software en su inventario e instalará el software.

g) Las actualizaciones de software solo podrán ser efectuadas a través del Departamento de informática.

h) En el caso de actualizaciones de sistema operativo y antivirus, estos serán ejecutados de manera centralizada por el Departamento de Informática.

i) No se podrá instalar software protegido por derechos de autor, sin la respectiva licencia en los equipos computacionales que estén inventariados por la Municipalidad, con la excepción de licencias que permitan su uso y distribución libre.

j) Los requerimientos de instalación de software que no cuenten con una licencia válida, deberán ser canalizados formalmente a través de la jefatura directa al que está adscrito el usuario, quien deberá escalar y evaluar el requerimiento junto al Encargado/a de Seguridad de la Información para analizar si existen alternativas de software libre, si es posible asignar una licencia disponible, o se gestiona la compra.

k) Todos los equipos contarán con una instalación de software básico correspondiente a funciones administrativas como: sistema operativo, software de oficina, Antivirus y utilidades de uso libre.

POLITICA DE USO DEL TELÉFONO MÓVIL

a. Los usuarios deben evitar la difusión de información confidencial o privada por vía telefónica cuando se está en lugares públicos o fuera de las dependencias de la Municipalidad. Si se hace, se debe procurar tratar los temas en forma general y sin mencionar información sensible o confidencial.

b. Los usuarios deben procurar no almacenar información confidencial en los teléfonos móviles institucionales. Asimismo, y entendiendo que, dado el uso del teléfono móvil institucional, existe la posibilidad de que terceros accedan a la información contenida en él, se sugiere la utilización de claves de acceso al equipo con un número limitado de intentos, de manera de minimizar el riesgo de acceso no autorizado.

c. Los usuarios no deben participar de juegos, concursos, cadenas u otros similares, utilizando el teléfono móvil otorgado por la Municipalidad.

d. Es responsabilidad del usuario dar buen uso y cuidado al teléfono móvil asignado.

e. Los usuarios no deben exponer el teléfono móvil a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).

f. El Encargado de la Séguridad de la Información deberá resguardar que los equipos proporcionados por la Municipalidad tengan, por defecto, bloqueados los servicios de mensajería de texto y roaming internacional.

g. Cuando un equipo móvil es utilizado en lugares públicos o privados, y es conectado a una red no administrada por la Municipalidad, el usuario de dicho equipo es responsable de la seguridad física y lógica del mismo y de la información que comparta con terceros a través de dicha red.

h. Terceras personas no están autorizadas a utilizar el dispositivo móvil que la Municipalidad asigne a un usuario

i. El usuario debe seguir las indicaciones de los fabricantes tanto en la utilización y actualización, como en el cuidado del equipo móvil asignado para el cumplimiento de sus funciones.

j. El usuario no debe realizar descarga de sitios inseguros, será su responsabilidad la instalación de aplicaciones no seguras en el dispositivo móvil.

POLÍTICA PARA EL USO DE CONTRASEÑAS

Esta política se aplica a todas las áreas de la Municipalidad a los procesos de provisión de bienes y servicios definidos. Es aplicable a todos los usuarios ya sean funcionarios/as de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios y que necesiten tener acceso a los recursos de la red institucional.

Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27001:2013

A.09.03.01 Uso de información & de autenticación secreta.

SOBRE RECOMENDACIONES DE USO Y DE AUTENTICACION SECRETA

a) El nombre de usuario y su contraseña deben ser individuales, es decir, debe ser privada, única e intransferible, no debe ser compartida, el usuario será el único responsable de las acciones efectuadas bajo el uso de su cuenta personal.

b) Se debe mantener la información de autenticación secreta como confidencial, está prohibida su divulgación, sin excepciones.

c) Se debe evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta.

d) Cada vez que un usuario se ausente de su estación de trabajo, bloquear su computador para proteger el acceso a las aplicaciones, servicios e información de la institución de personal no autorizado, exceptuando situaciones que lo amerite.

e) Se debe tener presente que en ningún momento se solicitará contraseñas por correo electrónico o mensaje de texto de modo que debería ignorar cualquier petición recibida por estas vías de comunicación. En caso de que se presente un evento de este tipo se puede reportar al Encargada/o de Seguridad de la Información.

f) Está prohibido compartir la información de autenticación secreta de usuario, ya sea propia o de un tercero.

g) Se debe evitar escribir la contraseña en computadores públicos, compartidos o aquellos en que se desconozca su nivel de seguridad o se estime que pueda estar monitorizados de forma remota, por ejemplo, desde un terminal de acceso a internet de un aeropuerto.

h) No emplear la cuenta de identificación y contraseña para registrarse en ningún servicio de redes sociales y/o servicios de almacenamientos online distinto a los dispuestos por la Municipalidad (X (entes Twitter), por ejemplo). Si se expone su cuenta a servicios externos, pueden existir incidentes de seguridad que pueden poner en riesgo su identificación en los sistemas informáticos y los sistemas de la Municipalidad.

i) Nunca debemos usar las contraseñas por defecto o que haya sido proporcionada una tercera persona o por la misma institución, dado que debemos conocerla únicamente nosotros.

SOBRE IDENTIFICACIÓN Y CONTRASEÑAS REQUERIDAS

Antes de tener acceso a cualquier recurso de la red de la Municipalidad todos los usuarios deben ser identificados exitosamente mediante su nombre de usuario y su contraseña.

Se debe cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso de seguridad.

Aparte de cambiar la clave en forma semestral, es recomendable cambiarla de forma periódica la contraseña (cada 3 meses), dado que esto ayudara a prevenir accesos no autorizados a la cuenta de usuario asignada por la institución. En caso de que existan problemas con el cambio de contraseña se puede solicitar apoyo al Encargada/o de Seguridad de la Información.

Los usuarios no deben emplear la misma contraseña que usan para la cuenta de la Municipalidad en otros servicios o aplicaciones (Por ejemplo: cuenta de correos electrónicos personales, redes sociales, aplicaciones móviles, entre otros).

Evitar el autoguardado de contraseñas en los exploradores de internet o en cualquier aplicación que lo solicite. Se sugiere seleccionar contraseñas con una longitud mínima suficiente (que tenga como mínimo 8 caracteres) y posean las siguientes características:

a) Fáciles de recordar.

b) Pueda contener al menos un símbolo y una letra mayúscula. Como, por ejemplo:

- Símbolos de Teclados @-%&.,0 i?1,
- Letras Mayúsculas A, B, C, D, E, F, G...

c) Que no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con la persona, es decir, nombres, números de teléfono y fechas de nacimiento, etc.

d) Que no sean vulnerables a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios).

e) Que estén libre de caracteres idénticos consecutivos, que sean todos numéricos o alfabéticos.

SOBRE ELIMINACIÓN SEGURA DE LA INFORMACIÓN

Roles y Responsabilidades

Jefatura de Unidad, Departamento: Debe definir que información debe conservarse y por cuánto tiempo.

Soporte y Seguridad de Información: Debe definir, actualizar y ejecutar los procedimientos de destrucción de medios de almacenamiento (cintas, discos duros, etc.) que contengan información sensible para la institución.

Alcance

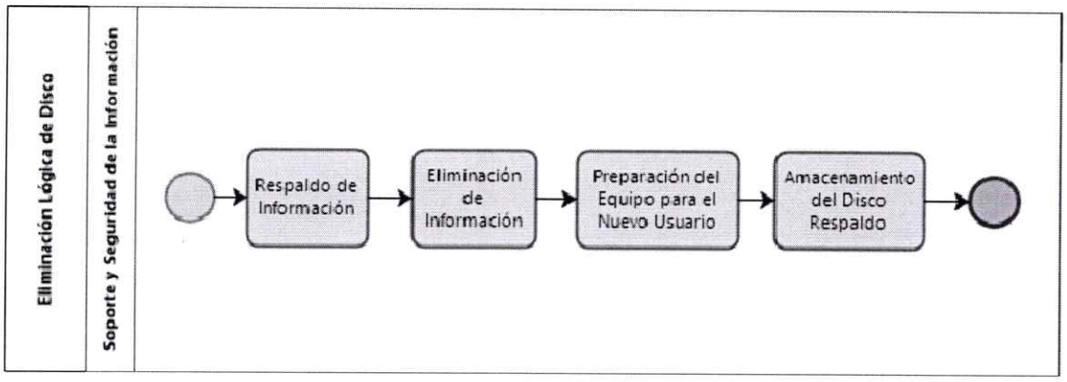
El presente procedimiento se rige por los controles A.08.03.02 y A.11.02.07 de la normachilena NCh-ISO 27001 y abarca a todos los medios de información y almacenaje de estos que maneja el servicio.

Procedimiento

A continuación, se presentan los diferentes procedimientos que debe seguir el personalresponsable de la institución para asegurar la eliminación segura de información manteniendo la disponibilidad, integridad y confidencialidad.

Eliminación Lógica de Discos Duros

Flujograma "Procedimiento de Eliminación Lógica de Discos



Simbología

Simbología	Descripción
	Inicio
	Fin
	Proceso

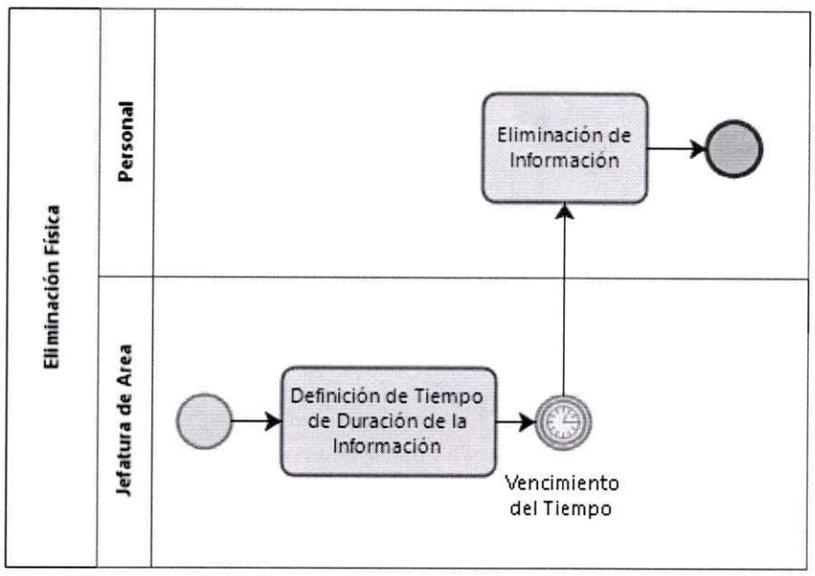
Descripción del Procedimiento

Al recibir un computador los miembros de la unidad Soporte deben respaldar en un disco duro externo la información contenida en este y luego eliminar toda información que el computador contenga para, posteriormente actualizar los programas y sistema operativo y. finalmente, almacenarlo o entregarlo a el miembro correspondiente según se necesite.

Se debe llenar la plantilla del anexo en la cual se señale la fecha del respaldo, el ejecutor, el computador respaldado (a través del código de inventario de este), el nombre del disco donde fue almacenado el respaldo y el nombre de la carpeta ubicada en el disco.

Eliminación Física de Medios

Flujograma Procedimiento de Eliminación Física de Medios



Descripción del Procedimiento

Una vez se cumple el tiempo en que la información debe encontrarse disponible se debe proceder a eliminar esta según el medio físico en el que se encuentre, las cuales pueden ser:

a) Disco Duro, Cintas, Pen Drive. Para cualquiera de estos casos, que son reescribidles, se debe primero eliminar la información de forma lógica para luego proceder a la eliminación física, la cual consiste en dejar el dispositivo inutilizable antes de ser desechado, mediante perforaciones.
b) CD, DVD, Minidisc o similares. Para estos casos, normalmente no reescribidles, el procedimiento consiste en doblar el disco de tal manera que no pueda ser introducido nuevamente en el lector de discos de un computador.
c) Papel, Fotocopias, Calco, etc. Estos medios deben ser rotos ya sea de forma manual o por medio de una trituradora de tal forma que no se puedan volver a enlazar las piezas.

Registro de Operación

Se considera como registro de operación la plantilla de respaldo de disco presentada en el Anexo a continuación. El procedimiento debe ser revisado y actualizado una vez al año.

Anexo

0000917
05 ABR 2024

Planilla Respaldo de Disco

Ilustre Municipalidad de Romeral
Departamento de Informática

PLANILLA DE RESPALDO DE DISCO

Fecha:

Responsable:

Código Activo Fijo de Computador	
Usuario Origen	
Disco Respaldo	
Carpeta de Respaldo	

_____

Firma Responsable

SEGUNDO: COMUNÍQUESE el presente Decreto a las Direcciones, Departamentos y Oficinas Municipales, y publíquese en la pagina web de transparencia activa de la Ilustre Municipalidad de Romeral.

ANÓTESE, COMUNIQUESE, Y ARCHIVESE

GUILLERMO MONTERO RAMÍREZ
SECRETARIO MUNICIPAL

CARLOS VERGARA ZEREGA
ALCALDE

CVZ/GMR/JGR/fom
DISTRIBUCIÓN:

- Informática
- Oficina de Partes
- Departamento RRHH