MUNICIPALIDAD DE
REQUÍNOA

DECRETO ALCALDICIO Nº 2383/
APRUEBA POLITICA DE SEGURIDAD DE LA INFORMACION MUNICIPAL.

REQUINOA, 02 AGO 2024

Esta Alcaldía decretó hoy lo siguiente:

VISTOS :

Las Facultades que me confiere la Ley Nº 18.695 de 1988, Orgánica Constitucional de Municipalidades, Texto refundido coordinado y sistematizado, fijado por el D.F.L N°1 del Ministerio del Interior año 2006.

La Ley N° 18.575, Sobre Bases Generales de la Administración del Estado.

La Ley N° 19.880, Sobre Bases de los procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado.

CONSIDERANDO :

La necesidad del Municipio de contar con Procedimiento de Información en Equipos Computacionales Dados de Baja, que permita guiar los procesos de control del área informática.

El Pre informe de Auditoria N°128 de 2024, sobre Auditoria a las Tecnologías de la Información y Comunicaciones, en la Municipalidad de Requinoa.

El Memo N°523 de fecha 01.08.2024 de Dirección de Administración y Finanzas el cual remite "Política de Seguridad de la Información Municipal", el cual deberá aplicarse a todas las Direcciones de la Gestión Municipal.

La Providencia del Sr. Administrador Municipal, quien indica que el Reglamento citado se encuentra revisado, por lo que se deberá proceder a la dictación del decreto Alcaldicio correspondiente.

DECRETO :

APRUEBASE la Política de Seguridad de la Información de la Municipalidad de Requínoa, y déjese sin efecto cualquier acto administrativo anterior.

ANOTESE, COMUNIQUESE Y ARCHIVESE.-

ILUSTRE MUNICIPALIDAD DE REQUINOA
SECRETARIO MUNICIPAL

MARIO MENA NORIEGA
SECRETARIA MUNICIPAL(S)

ILUSTRE MUNICIPALIDAD DE REQUINOA
ALCALDE

WALDO VALDIVIA MONTECINOS
ALCALDE

WVM/CAB/MMN/FNM/knc.
DISTRIBUCION:
Secretaria Municipal
Dirección Administración y finanzas
Dideco
Dpto. de Tránsito y Transporte público
Control
Dirección de Obras Municipales
Juzgado de Policía Local
Secpla
Dirección de Seguridad Pública
Archivo

POLITICA DE SEGURIDAD DE LA INFORMACION

POLITICA DE SEGURIDAD DE LA INFORMACION MUNICIPAL

El desarrollo de una estrategia de seguridad digital tiene por misión la protección de los usuarios, privados y públicos, junto con la privacidad de los ciudadanos. En razón de lo anterior, se han propuesto para los órganos del estado la adopción de una Política Nacional de Ciberseguridad, la cual tiene por objetivo el diseño, implementación y puesta en marcha de medidas que permitan proteger la seguridad y la libertad de los usuarios del ciberespacio. Por otro lado, la Estrategia de Transformación Digital del Estado, posee como uno de sus principios estratégicos la Ciberseguridad, protección de datos y privacidad, la cual busca enfatizar la seguridad de las plataformas digitales, la protección y privacidad de los datos, de modo de dar confianza a las personas que interactúan con los servicios públicos.

Ambas estrategias descritas no consideran a las municipalidades, las que, en base a información empírica, no están preparadas estructuralmente para estos cambios, dado que tienen problemas de integración y homologación, falta de procesos estandarizados, no cuentan con profesionales especializados en ciberseguridad, no cuentan con redes y/o sistemas certificados y carecen de gestión de riesgos que les permita protegerse de actividades de espionaje, sabotaje, fraudes o ciberataques que puedan resguardar la información que cada día producen y utilizan.

Por ello, se busca apoyar mediante la entrega de un documento estándar para que las Municipalidades puedan adaptar e implementar una Política Municipal de Seguridad de la Información, que incorpore aspectos de ciberseguridad como el control de acceso, clasificación de la información, seguridad física y ambiental, derechos y deberes del usuario final, respaldos, transferencia de la información, protección contra malware, gestión de vulnerabilidades técnicas, seguridad en las comunicaciones, relaciones con proveedores y privacidad y protección de información personal.

Adicionalmente, se ha visto que Contraloría realiza periódicamente Auditorias en las cuales ha consultado si el municipio cuenta con Política de Seguridad de la Información. A continuación, se comparte alguna de las consultas más comunes:

- ¿Cuenta con Política de Seguridad de la Información? ¿Cada cuánto tiempo es revisada y actualizada? Enviar documentos de evidencia.
- La última evaluación de riesgos sobre seguridad de la información efectuada por el servicio, la que debe contener al menos activos, amenazas, vulnerabilidades, impacto y valoración. Además, en caso de existir, señalar el tratamiento para cada uno de los riesgos identificados.
- Nombramiento del comité de seguridad de la información y del encargado/a de seguridad de la información.
- Medidas de resguardo de la información crítica. Informar sobre la seguridad en el perímetro de sala de servidores, controles de acceso físico, extintores, equipos alternativos de energía, alarmas, sensores de temperatura, humedad y humo, registro de mantenciones efectuadas al equipamiento y contratos de mantención.
- Informar procedimientos de destrucción de información y que estos sean implementados por la entidad.

- Inventario de equipos computacionales, detallando ubicación, estado, serie, número de inventario o identificador, responsable y si están separados por ambientes de prueba.
- Documentación sobre capacitaciones efectuadas a los funcionarios sobre el riesgo asociado al uso del correo electrónico e instalación de software no autorizado, listado de usuarios y administradores de los sistemas operativos.
- Procedimientos técnicos de respaldo de información y recuperación.

Para finalizar, se mencionarán algunas aclaraciones a consultas comunes que han realizado municipios a SUDBERE, con motivo de responder a las Auditorías de Contraloría en materia de TIC y Seguridad:

- Su municipalidad es beneficiaria del Programa SIFIM de SUBDERE, el cual en su oportunidad les proveyó un conjunto de sistemas integrados para su operación (Contabilidad, Ordenes de Ingreso, Conciliación Bancaria, Activo Fijo, Adquisiciones, Personal, Remuneraciones y otros Sistemas Giradores como Patentes Comerciales, Licencias de Conducir y/o Permisos de Circulación), los cuales pertenecen a su activo intangible como licencias de uso indefinido de software. El código pertenece al proveedor CAS Chile y las medidas de seguridad son administrables por el municipio a través del perfilamiento de usuario. Cada usuario debe tener una clave que solo él conozca, la contraseña del administrador sólo debe ser usada por un único funcionario responsable de las plataformas y para modificar configuraciones mayores, en ningún caso para realizar trabajo.
- La Cloud SIFIM, es un servicio de Cloud Computing que provee SUBDERE para la operación y acceso de los sistemas de su municipalidad, servicio que incluye servidor virtual para la municipalidad, alojado en dependencias del Datacenter, el cual está certificado TIER III (significa que tiene una disponibilidad garantizada del 99,982%, lo que implica que anualmente solo se detendrá 1 hora y 57 minutos aproximadamente). Este beneficio, se provee a través de un contrato de servicios, asociado a la licitación pública ID N° 761-37-LR19, aprobado por Resolución Exenta N° 63/2020, totalmente tramitada el 02 de junio de 2020, en una modalidad CLOUD, a través de Servicios de Datacenter, adjudicados a la empresa GTD Intesis.

Tabla de 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 presentes, 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.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, es necesario que como documento forme parte de la cultura organizacional de la Municipalidad, y contar con el compromiso de todos los funcionarios municipales, para contribuir con la difusión, conocimiento e integración.

Documentos de Referencia

i) Norma Chilena NCh-ISO 27001:2013, Sistemas 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.

ii) 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.

iii) Ley 20.285, de 2008, del Ministerio Secretaria General de la Presidencia, Sobre Acceso a la Información Pública.

iv) Ley 19.223, de 1993, del Ministerio de Justicia, Tipifica Figuras Penales Relativas a la Informática.

v) 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.

vi) Ley 18.883, de 1989, del Ministerio del Interior, Aprueba Estatuto Administrativo para Funcionarios Municipales.

vii) 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.

Documentos secretos. Los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y su Reglamento.

Encargado de Seguridad y Ciberseguridad. Persona responsable por la implementación de medidas de control que garanticen la seguridad de la información, así coma 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 Específicos

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 Superintendencia de Educación y prevenir la ocurrencia de incidentes de seguridad de la información.
7. 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.
8. Establecer los mecanismos de difusión de la presente Política para el conocimiento de terceras partes, especialmente en lo referente a la confidencialidad de la información de la que tome conocimiento mientras dure el contrato y convenios, sus derechos y obligaciones en materia de seguridad de la información del Municipio y las consecuencias en caso de no cumplimiento, que se establecen en los respectivos contratos y convenios.
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, 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.

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.

Asignación de Responsabilidades

El Administrador Municipal de la Municipalidad designó, en materia de Seguridad de la Información a, nominado con el cargo de "Encargado de Seguridad de la Información", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Municipio, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.

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 independientes 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.

Política de uso de medios removibles y dispositivos móviles

El objetivo de la presente política es mantener un estándar de seguridad coherente con el fin de establecer las normas que regulen el uso de los dispositivos móviles y medios removibles, dentro y fuera de la institución, permitiendo minimizar los riesgos asociados a estos y con el fin de evitar incidentes de seguridad con los datos contenidos en estos.

Los dispositivos móviles y medio removibles permiten facilitar las actividades relacionadas con la institución, no obstante, el uso de dichos dispositivos también implica algunos riesgos, que deben ser analizados y gestionados. Principalmente tener el cuidado de asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada y/o procesada en ellos.

Esta política se aplica a todas las áreas de la Municipalidad y a todos los procesos de provisión de bienes y servicios. Norma la utilización de medios removibles (conectados por puerto USB, bluetooth u otro medio) y dispositivos móviles que son entregados por la Institución a los Usuarios (funcionarios, colaboradores, practicantes o personal externo que preste servicios permanentes o temporales, y/o aquellos utilizados dentro de las dependencias de la Municipalidad), específicamente:

- Pendrive.
- Discos duros portátiles. Dispositivos de banda ancha móvil. Teléfono móvil.
- Tablets.
- Cámara fotográfica.
- Grabadora de audio.
- Cámara de video.
- Grabador portátil CD/DVD/Blu-ray.

Directrices

- Los medios removibles no son alternativa de respaldo de información de la Municipalidad, siendo responsabilidad del usuario almacenar y mantener la información en la nube institucional o almacenamiento autorizado. Está restringido el uso de dispositivos de almacenamiento removibles conectados a puertos USB tales como discos externos, celulares, cámaras, etc. Exceptuando aquellos dispositivos necesarios para la operación como mouse, teclados, impresoras que únicamente poseen puerto USB como mecanismo de conexión a la red. Se incluyen en esta política equipos que, mediante una solicitud, se deriva al Encargado/a de Seguridad de la Información y Ciberseguridad para que autorice su acceso.
- Se debe contar con protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos. Protegiendo el acceso con claves, tokens, huella digital o el mecanismo que permita el dispositivo.
- Los usuarios deben dar un buen uso a los medios removibles y dispositivos móviles asignados para el cumplimiento de sus funciones, en caso de que éstos presenten cualquier deterioro o evento de seguridad, debe informarlo oportunamente al encargado de la Política de Seguridad.
- En caso de pérdida o robo del equipamiento asignado por la Municipalidad, el usuario afectado, debe informar a su Jefatura directa, posteriormente a Carabineros de Chile dejando en la constancia la información relativa al equipo (marca, característica, número de serie).

Marco de utilización de dispositivos móviles y medios removibles de almacenamiento.

a. Los dispositivos móviles y medios removibles son asignados a los funcionarios para apoyar la relación de su trabajo y deben ser utilizados solamente para estos fines.
b. Los usuarios que hagan uso de su móvil personal para apoyar su trabajo, deben tomar los resguardos que estén a su alcance, en relación a tener el cuidado de asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada en el móvil.
c. El uso de un medio removible debe ser autorizado y justificado por la Jefatura directa del usuario, quien debe solicitarlo por email al Encargado de la Seguridad de la Información, quién una vez que reciba este requerimiento, habilitará el acceso al medio removible.

d. La asignación de un medio removible debe ser autorizado, justificado y solicitado por la Jefatura directa del usuario por email al Encargado de la Seguridad de la Información quién evaluará que se cumpla con el estándar asignado para este tipo de medio, el que, en caso de contar con disponibilidad, será asignado al usuario, previa firma de recepción conforme, y registrado en el sistema de activos.
e. Es responsabilidad de cada usuario el buen uso y traslado de los dispositivos que tiene a su cargo.
f. Es responsabilidad de cada jefatura que solicita uso de medio removible y asignación de medio removible resguardar que el funcionario a su cargo realice un buen uso y cuidado en el traslado de los dispositivos a cargo.
g. Los dispositivos móviles y medios de almacenamiento removibles no se deben exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).
h. Cualquier falla o deterioro de los componentes o dispositivos móviles asignados, debe ser informada la Jefatura directa quién informará por mail al Encargado de la Seguridad de la Información.

Respecto al 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 Seguridad 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.

Respecto al uso de dispositivos de almacenamiento removibles

a. Los usuarios tendrán prohibición de utilizar dispositivos de almacenamiento personales y será de su responsabilidad mantener respaldar la información en la nube institucional asignada por la Municipalidad.
b. No está permitido almacenar información institucional en los dispositivos de almacenamiento personales, sólo debe usarse para facilitar el porte de información funcional (ej. presentaciones, documentos de trabajo, etc.).
c. En general, la Municipalidad no proveerá de pendrives o discos duros externos o cualquier medio de almacenamiento externo, por el riesgo que estos representan a la seguridad de la información.
d. Los discos duros externos ya existentes en las distintas Unidades deben ser gradualmente eliminados y su información traspasada a la red institucional provista para ello.
e. Para los dispositivos que ya estén en la institución y que han sido asignado a usuarios no se debe exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).
f. Todo medio de almacenamiento removible que sea utilizado fuera de la plataforma tecnológica de la institución debe ser revisado por posible presencia de virus, a través del escaneo de éste por el antivirus instalado.
g. El responsable del medio de almacenamiento removible deberá velar por el buen uso de la información almacenada en el mismo, manteniendo su adecuado control y distribución limitada. Deberá usar mecanismos de protección, como el uso de contraseñas y/ encriptación de archivos.
h. El responsable del medio de almacenamiento removible deberá adoptar las medidas que se encuentren a su alcance para asegurarse que los archivos contenidos en él se encuentren libres de virus, software y/o código malicioso, que puedan poner en riesgo la confidencialidad, integridad y disponibilidad de la información, como también exponer a los equipos informáticos de la Municipalidad a eventos de vulnerabilidad.
i. Los usuarios deberán eliminar los activos de información de carácter restringida, y contenida en un medio de almacenamiento removible.
j. El usuario debe cuidar el equipamiento y guardarlo en lugares seguros cuando no lo esté utilizando, preferentemente muebles con llave.

Uso de cámaras fotográficas, de video y grabadoras

a. Para los dispositivos que ya estén en la institución y que han sido asignado a usuarios, no se deben exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).
b. El usuario debe cuidar el equipamiento y guardarlo en lugares seguros cuando no lo esté utilizando, preferentemente muebles con llave.
c. El usuario debe seguir las indicaciones de los fabricantes tanto en la utilización como en el cuidado del equipo.

Política para el uso de internet, correo electrónico institucional, instalación y uso de Software.

Para el correcto funcionamiento de los sistemas tecnológicos y los servicios relacionados con Internet (mensajería electrónica, cuentas de correo electrónico, navegación web, etc.), la Municipalidad, establece normas y reglas de uso aceptable de los equipos y servicios, con el fin que estos recursos sean utilizados correctamente para que tanto el funcionario y la institución estén protegidos de amenazas que pongan en peligro los sistemas y la información contenida en estos.

El propósito de esta política es determinar y normar el uso aceptable de los sistemas servicios de navegación a internet y el uso de software en la Municipalidad.

Todo usuario de la Municipalidad deberá poseer una cuenta de usuario personal, que actuará como credencial que lo identifique unívocamente, y que le permita tener acceso a los recursos de la red informática institucional. Para todo sistema informático de la Municipalidad, el usuario debe señalar quien es (identificación) y luego debe comprobar que es quien dice ser (autenticación). La identificación se realizará normalmente por un "nombre de usuario" que permite acceso el sistema informático de la institución y la autentificación se realiza mediante algo que solo el usuario conoce (contraseña) y que es algo que solo él posee.

Es importante señalar que el uso inapropiado de software, expone a la Municipalidad contra riesgos legales y de seguridad informática, tales como la pérdida de información, filtración de datos, infracción de derechos de autor, exposición de los sistemas de uso interno a códigos maliciosos, interrupciones o degradación de servicios de red, suplantación de identidad, daños de sistemas, entre otros.

La presente política es aplicable a todos los funcionarios, personal a honorarios y contrata, ayudantes, que utilicen equipamiento computacional inventariado por la Municipalidad o que hayan sido adquiridos por medio de proyectos, programas, en las mismas condiciones de seguridad y control que un equipo computacional inventariado.

Sobre el uso de Internet

a) Los sistemas de comunicación y acceso a internet de la Municipalidad, deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las funciones de trabajo establecidas por la institución y no para actividades personales.

b) Los Usuarios de la Red Municipal deben utilizar, como primera opción para conectarse a Internet, los medios dispuestos por la institución. De existir problemas con la conexión principal, los Usuarios pueden acceder a través de otros canales de proveedores de servicios de Internet externos.
c) Cuando se use la opción alternativa, esta debe ser resguardada con medidas de seguridad tales como firewall entre la institución y la salida a Internet, equipos de escritorio actualizados en cuanto a antivirus, firewall del equipo, antimalware y parches de seguridad. Herramientas que serán provistas e instaladas por el Encargado/a de Seguridad de la Información.
d) Las operaciones realizadas a través de internet por los usuarios de la Municipalidad podrán ser intervenidas y auditadas, por el Encargado/a de Seguridad de la Información, en cuanto a los accesos realizados en la red, a internet y el contenido de lo accedido.
e) Las soluciones inalámbricas deben contar con portales cautivos para que los invitados o externos de la Municipalidad que necesiten conexión a Internet solo puedan usar de manera controlada este medio, además de asegurar que la red de trabajo de la institución se mantenga aislada de los mismos.
f) Toda información entrante y saliente a Internet, es monitoreada y registrada por el Encargado/a de Seguridad de la Información, con el propósito de garantizar el nivel de servicio de navegación a internet y priorizando las comunicaciones que la institución requiere mantener con otras entidades gubernamentales y privadas, necesarias para el funcionamiento de los Sistemas Informáticos.
g) Los usuarios de la Municipalidad no deben almacenar contraseñas en los navegadores web.
h) El Encargado/a de Seguridad de la Información debe asegurarse que el sitio web institucional cuente con su correspondiente certificado de seguridad.

Sobre Cuentas de Usuario y Contraseñas.

a) El Usuario es responsable del mantenimiento de la seguridad tanto de su propia información como de sus cuentas asignadas y contraseñas. El cambio y uso de contraseñas debe ser de acuerdo a la "Política Uso de Contraseñas" vigente.
b) Las cuentas y contraseñas son asignadas a Usuarios individuales y no pueden ser compartidas con otras personas o funcionarios de Municipalidad ni con externos a la institución. Los Usuarios son responsables también por el tráfico y el contenido de la información de las cuentas asignadas. La violación de una cuenta y contraseña puede conllevar la revocación de cualquier tipo de privilegio de uso.
c) El uso de la red se encuentra disponible para todos los funcionarios de la Municipalidad, pero los permisos para el uso de Internet, estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada funcionario o según lo soliciten los jefes de la institución, al Encargado/a de Seguridad de la Información.
d) La asignación de perfiles de Usuario es realizada por cada Director/a, de acuerdo al perfil de cargo de cada funcionario/a, este perfil de Usuario es informado al Encargado/a de

Seguridad de la Información, quien realizara la asignación de privilegios de acuerdo a lo indicado por cada jefatura.

Sobre Restricciones al Uso de Internet

a) Se prohíbe descargar desde Internet, material que infrinja el Ordenamiento Jurídico Nacional o en la normativa interna establecida en la Municipalidad.
b) No está permitido almacenar información institucional en sitios o nubes de almacenamiento virtual provisto por terceros (Dropbox, Google Drive, etc.), la institución provee de recursos específicos para ello.
c) No está permitido copiar y distribuir software que secretamente recoge o difunde información acerca de la institución.
d) No está permitido utilizar los equipos computacionales entregados por la Municipalidad para actividades no relacionadas con las asignadas a su función. El cumplimiento de estas restricciones, se regularán de acuerdo al perfil de cada Usuario, en particular se debe evitar:
    i. Descargar sistemas de audio/video vía Internet (radios online, Spotify, Netflix, entre otros). Se excluyen de esta condición a los medios de prensa de la institución.
    ii. Cargar y/o descargar archivos de música.
    iii. Cargar y/o descargar archivos de imágenes y videos.
    iv. Cargar y/o descargar juegos o jugar juegos online.
    v. Instalar sistemas de telecomunicaciones ajenos a los corporativos.
    vi. Construcción y/o hosting de sitios web personales o ajenos a la institución.
    vii. Transferencia de archivos a través de protocolo SFTP, FTP, u otros no autorizados bajo convenios de interoperabilidad.
    viii. Está prohibido ingresar a páginas con contenidos pornográficos, pedófilos y otros relacionados.
e) Cuando el Usuario requiera el acceso a un sitio que se encuentre bloqueado, debe ser autorizado y solicitado por la Jefatura directa vía email al Encargado/a de Seguridad de la Información, quién evaluara que el sitio no esté catalogado como malicioso, en lista negra o vulnere una política de seguridad, antes de dar acceso al usuario. Los casos que no entren en la anterior clasificación, serán, evaluados y revisados por el/la Encargado/a de Seguridad de la Información y Ciberseguridad.
f) En cuanto al uso de redes sociales, están autorizadas solo para los funcionarios que sus funciones se relacionen con comunicaciones de la Municipalidad o cuando su jefatura lo disponga.

Sobre Correo Electrónico Institucional

Uso de Correo Electrónico

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

Los correos electrónicos enviados y recibidos están almacenados en los equipos informáticos de la Municipalidad y serán retenidos por el tiempo necesario de acuerdo a criterios legales y administrativos.

Ocasionalmente los funcionarios/as utilizarán los sistemas de correo electrónico para propósitos personales siempre y cuando esto no interrumpa el normal desarrollo de sus funciones. Esto está permitido siempre que no afecte el trabajo para el cual fue contratado ni su contenido pueda afectar negativamente a los intereses y/o lineamientos generales de la institución. Es importante que se tenga en cuenta que este tipo de comunicación se genera bajo el nombre de la Municipalidad y esto puede afectar la imagen de la institución.

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.

Correos personales no deben estar archivados en el sistema por más tiempo del estrictamente necesario.

Toda casilla de correo electrónico institucional está directamente vinculada al funcionario/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 funcionario, no se deben divulgar, compartir ni anotarlas en lugares visibles y/o de fácil acceso.

Los funcionarios 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 funcionarios 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 10 megabytes. Para casos que se requieran enviar información que supere esta cantidad de megabytes, el funcionario 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 y Ciberseguridad. 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 entregara 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 funcionario 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.

Para la utilización del web mail solo podrá ser accedido mediante la herramienta institucional provista para acceder a los recursos informáticos desde cualquier lugar o equipo con conexión a internet con la cuenta de usuario que se utiliza para el acceso al sistema informático de la Municipalidad.

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 funcionario 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 funcionario/a que lo reemplazará.

Sobre Cuenta y estructura de la dirección de correo electrónico

a) Una dirección de correo electrónico consta de dos partes: el nombre de usuario (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.
b) La creación de cuentas genéricas, destinada a representar un servicio de envío de mensajería electrónica colectiva, se gestionarán a través de la jefatura del área solicitante, quien la solicitará vía correo electrónico al Encargado/a de Seguridad de la Información, con un mínimo de dos días hábiles de aviso para gestionarla. Las cuentas genéricas no reemplazan a ningún correo electrónico de funcionario/a, solo se utilizan como listas de distribución masivo.

Sobre Restricciones al uso y contenido del correo electrónico

El Usuario interno o externo que utilice el correo electrónico institucional podrá enviar mensajes con un tamaño de hasta 10 MB, y recibirlos con un tamaño de hasta 20 MB, sin prejuicio 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 o accidente.

El funcionario 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 y Ciberseguridad.

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 sea desvinculado.
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.

Sobre el uso e instalación de software.

a) Todo software debe ser instalado por el personal autorizado de la municipalidad, lo cual debe ser revisado en forma periódica.
b) Los funcionarios no pueden descargar software desde internet, o traer el software de su casa sin autorización.
c) Cuando un funcionario 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 funcionario 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 funcionario.
f) Será por vía de Comité Técnico Administrativo participar en la decisión sobre la adquisición de un nuevo software. Una vez que se ha tomado la decisión, el Encargado/a de Seguridad de la Información procederá a incluir el software en su inventario e instalará el software.
g) Las actualizaciones de software solo podrán ser efectuadas a través del Encargado/a de Seguridad de la Información
h) En el caso de actualizaciones de sistema operativo y antivirus, estos serán son ejecutados de manera centralizada por el Encargado/a de Seguridad de la Información.
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 valida, deberán ser canalizados formalmente a través de la jefatura directa al que está adscrito el funcionario, 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.

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 de contraseñas:

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.
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 y Ciberseguridad.
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 cibercafé o 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 (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:
    i. Símbolos de Teclados i@-%&.,0 i?1,
    ii. 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.

MUNICIPALIDAD DE
REQUÍNOA

Evaluación de Riesgo de la seguridad de la información para la Ilustre Municipalidad de Requínoa

1: Identificación de Activos

1. Servidor de bases de datos municipal local.
2. Segundo servidor de respaldo, donde además se implementa la intranet municipal.
3. Servidor principal alojado en las dependencias de la empresa Gtd Intesis, Santiago de Chile.
4. Equipos computacionales.
5. Red interna de la municipalidad.
6. Documentos electrónicos (actas, registros).
7. Fichas de funcionarios.
8. Registros de patentes comerciales de comuna.

2: Identificación de Amenazas y Vulnerabilidades

Amenazas

1. Ataques cibernéticos (malware, ransomware, hacking).
2. Acceso no autorizado (interno y externo).
3. Desastres naturales (inundaciones, terremotos).
4. Pérdida o robo de equipos computacionales.
5. Errores humanos (borrado accidental de datos, mal manejo de información).
6. Fallos técnicos (fallos de hardware o software).

Vulnerabilidades:

1. Contraseñas débiles.
2. Falta de autenticación de dos factores.
3. Sistemas desactualizados sin parches de seguridad.
4. Ausencia de procedimientos de respaldo y recuperación de datos.
5. Falta de capacitación en seguridad de la información para el personal.
6. Equipos sin medidas de seguridad física adecuadas.

3: Análisis de Riesgos

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo
Servidor de bases de datos municipal local	Ataque cibernético	Contraseñas débiles	Alto	Medio	Alto
Segundo servidor de respaldo e intranet municipal	Acceso no autorizado	Falta de autenticación de dos factores	Alto	Alto	Alto

Activo	Amenaza	Vulnerabilidad	Impacto	Probabilidad	Nivel de Riesgo
Servidor principal alojado en Gtd Intesis	Desastres naturales	Ubicación externa, dependencia de proveedores	Alto	Bajo	Medio
Equipos computacionales	Robo de equipos	Falta de seguridad física	Medio	Medio	Medio
Red interna de la municipalidad	Acceso no autorizado	Falta de autenticación de dos factores	Alto	Alto	Alto
Documentos electrónicos	Pérdida de datos	Ausencia de procedimientos de respaldo	Alto	Medio	Alto
Fichas de funcionarios	Acceso no autorizado	Falta de capacitación en seguridad	Alto	Medio	Alto
Registros de patentes comerciales de comuna	Fallos técnicos	Sistemas desactualizados	Medio	Medio	Medio

4: Evaluación y Priorización de Riesgos

1. **Riesgo Alto**: Ataque cibernético al servidor de bases de datos municipal local.
2. **Riesgo Alto**: Acceso no autorizado al segundo servidor de respaldo e intranet municipal.
3. **Riesgo Alto**: Acceso no autorizado a la red interna de la municipalidad.
4. **Riesgo Alto**: Pérdida de documentos electrónicos.
5. **Riesgo Alto**: Acceso no autorizado a las fichas de funcionarios.
6. **Riesgo Medio**: Robo de equipos computacionales.
7. **Riesgo Medio**: Fallos técnicos en los registros de patentes comerciales de comuna.

5: Plan de Tratamiento de Riesgos

1. **Riesgo: Ataque cibernético al servidor de bases de datos municipal local**
    - **Medidas de Control**:
        - Implementar políticas de contraseñas fuertes.
        - Configurar autenticación de dos factores para el acceso al servidor.
        - Mantener el sistema y las aplicaciones actualizadas con los últimos parches de seguridad.
        - Realizar auditorías de seguridad periódicas.

2. **Riesgo: Acceso no autorizado al segundo servidor de respaldo e intranet municipal**
    - **Medidas de Control**:
        - Configurar autenticación de dos factores para el acceso al servidor de respaldo.
        - Establecer políticas de acceso basadas en roles.
        - Monitorear y registrar el acceso al servidor.
        - Realizar capacitaciones en seguridad de la información para el personal.
3. **Riesgo: Acceso no autorizado a la red interna de la municipalidad**
    - **Medidas de Control**:
        - Configurar firewalls y sistemas de detección de intrusiones.
        - Implementar autenticación de dos factores para el acceso a la red.
        - Monitorear y registrar el acceso a la red.
        - Capacitar al personal en prácticas de seguridad de la información.
4. **Riesgo: Pérdida de documentos electrónicos**
    - **Medidas de Control**:
        - Establecer procedimientos de respaldo regular y recuperación de datos.
        - Almacenar copias de seguridad en ubicaciones físicas y en la nube.
        - Implementar controles de acceso a los documentos electrónicos.
5. **Riesgo: Acceso no autorizado a las fichas de funcionarios**
    - **Medidas de Control**:
        - Establecer políticas de acceso basadas en roles.
        - Implementar autenticación de dos factores para el acceso a sistemas que contengan fichas de funcionarios.
        - Realizar capacitaciones en seguridad de la información para el personal.
6. **Riesgo: Robo de equipos computacionales**
    - **Medidas de Control**:
        - Implementar medidas de seguridad física (cerraduras, cámaras de seguridad).
        - Configurar cifrado de disco en los equipos portátiles.
        - Mantener un inventario actualizado de los equipos y sus ubicaciones.
7. **Riesgo: Fallos técnicos en los registros de patentes comerciales de comuna**
    - **Medidas de Control**:
        - Realizar mantenimiento preventivo regular de hardware y software.

- Mantener sistemas y aplicaciones actualizados.
- Establecer un plan de contingencia para fallos técnicos.

8. **Riesgo: Desastres naturales que afecten el servidor principal alojado en Gtd Intesis**
    - **Medidas de Control**:
        - Establecer acuerdos de nivel de servicio (SLA) con el proveedor para asegurar la continuidad del servicio.
        - Realizar respaldos periódicos de los datos almacenados en el servidor externo.
        - Establecer un plan de recuperación ante desastres.

6: Monitoreo y Revisión

Acciones:

- Realizar auditorías de seguridad trimestrales para evaluar la efectividad de las medidas implementadas.
- Revisar y actualizar las políticas de seguridad anualmente o cuando se produzcan cambios significativos en el entorno de TI.
- Monitorear continuamente los sistemas para detectar y responder a incidentes de seguridad en tiempo real.
- Capacitar al personal de manera continua en prácticas de seguridad de la información y actualizar los procedimientos de acuerdo con las nuevas amenazas y vulnerabilidades.