REPÚBLICA DE CHILE
PROVINCIA DE LINARES
ILUSTRE MUNICIPALIDAD
R E T I R O
Depto. Adm. y Finanzas

I. MUNICIPALIDAD DE RETIRO
RECEPCIONADO
10 JUL 2024
OFICINA DE PARTES

DECRETO EXENTO Nº1.425

RETIRO, 28 de Mayo del 2024.-

VISTOS:

1.- Decreto N°83, Articulo 11 de 2004 del MINSEGPRES.

2- Norma ISO 27.002 de 2009, buenas prácticas para la gestión de la información.

3.- Ley N°20.285 Sobre acceso a la información pública.

4.- La Ley N°18.575 "Orgánica constitucional de bases Generales de la Administración del Estado";

5.- Las facultades que me confiere la Ley Nº18.695 De 1988 "Orgánica constitucional de Municipalidades";

CONSIDERANDO:

1.- La observación de Contraloría General de la Republica en informe Final N°947/2023 y la necesidad de contar con una política de seguridad de la información;

2.- Teniendo presente que, la información es un recurso importante, que tiene valor para los procesos que realiza diariamente la Ilustre Municipalidad de Retiro y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, la operación de los equipos computacionales, a su vez, minimizando los riesgos de daño y hurto de información, además de contribuir y facilitar la gestión administrativa de la Municipalidad.

3.-. Para que estos principios escritos en esta Política de Seguridad de la Información sean efectivos, es necesario que este documento forme parte de la cultura organizacional de la Municipalidad, lo que implica que se debe contar con el compromiso de todos los funcionarios municipales para contribuir con la difusión, conocimiento e integración.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

4.- Como consecuencia a lo expuesto previamente, la Ilustre Municipalidad de Retiro, llevo a cabo, la creación e implementación de Políticas de Seguridad de la Información, basándose en las características de varias fuentes de documentación al respecto, además, esta política se apoya de un Manual de Procedimientos en la cual se describen los pasos a seguir para ejecutar los lineamientos de esta política.

D E C R E T O:

1° Apruébese la Política de seguridad de la información de la Municipalidad de Retiro, como sigue a continuación:

Índice

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

CAPITULO 1: DEFINICIONES

Descripción los términos y definiciones utilizados en ese documento, para facilitar la debida comprensión del mismo.

.1. Seguridad de la Información

La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad:** que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **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.

Adicionalmente se deberían considerar parte de esta preservación, los siguientes conceptos:

- **Autenticidad:** asegura la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Duplicidad:** consiste en asegurar que un traspaso de información se realice sólo una vez, a menos que se especifique lo contrario. Impide las múltiples copias que permiten que se duplique innecesariamente la información.
- **Legalidad:** referido a que la información se ajuste al marco de leyes, normas, reglamentaciones o disposiciones a las que está sujeto el municipio.
- **Confiabilidad:** que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

.2. Información

Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, entre otras fuentes.

.3. Sistema de Información

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

.4. Tecnologías de la Información y Comunicación (TIC)

- Se refiere al hardware y software operados por los funcionarios públicos de esta organización, para llevar a cabo una función propia de la Municipalidad. -

5.- Conceptos Técnicos

- **Ataques de Diccionario:** Similar al de fuerza bruta, pero utilizando palabras existentes o combinaciones comunes en lugar de todas las combinaciones posibles.
- **Ataques de Fuerza Bruta:** Técnica de hacking que consiste en intentar adivinar una contraseña probando todas las combinaciones posibles hasta encontrar la correcta.
- **Autentificación de Dos Factores (2FA):** Método de seguridad que requiere dos formas de prueba de identidad antes de conceder acceso, típicamente algo que sabes (contraseña) y algo que tienes (un dispositivo).
- ***Autofill* (Autocompletar):** Funcionalidad de los gestores de contraseñas que permite rellenar automáticamente los campos de contraseña en los sitios web, basándose en la información almacenada.
- **Criptografía:** Ciencia que se ocupa de la codificación de la información para protegerla de accesos no autorizados. Es fundamental para la seguridad de las contraseñas y la información confidencial.
- **Contraseña Maestra:** En el contexto de un gestor de contraseñas, es la única contraseña que el usuario necesita recordar, la cual permite acceder al resto de sus contraseñas almacenadas de forma segura.
- **Funciones de *Hash*:** Funciones criptográficas que convierten una entrada de datos (como una contraseña) en un conjunto de caracteres de longitud fija, que es único para cada entrada única.
- ***Password Managers* (Gestores de Contraseñas):** Herramientas que ayudan a los usuarios a gestionar sus contraseñas, almacenándolas de forma segura y facilitando un acceso más seguro y eficiente a múltiples cuentas.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

- ***Phishing***: Técnica de engaño utilizada para obtener información sensible de una persona, como contraseñas o detalles bancarios, mediante la suplantación de una entidad de confianza en comunicaciones electrónicas.
- ***Rainbow Tables:*** Técnicas utilizadas en criptografía para acelerar el proceso de romper una contraseña *hash*, utilizando una tabla pre computada de hashes de contraseñas.
- **Social Engineering (Ingeniería Social):** Método de ataque que se basa en la manipulación psicológica de personas para que realicen acciones o revelen información confidencial.
- ***Spear Phishing*:** Forma de phishing altamente dirigida, donde el atacante tiene un conocimiento detallado de su víctima, lo que permite personalizar el ataque para incrementar sus chances de éxito.
- **Verificación de Identidad:** Proceso recomendado para confirmar la identidad de una persona antes de proporcionar acceso a información sensible o realizar acciones críticas, como medida preventiva contra la ingeniería social.
- **Autoridad Falsa:** Táctica de ingeniería social donde el atacante se hace pasar por una figura de autoridad para obtener acceso no autorizado a información o recursos.
- **Dominio de Correo:** Parte de una dirección de correo electrónico que sigue al '@', utilizado para identificar y verificar la legitimidad de la comunicación, especialmente en la prevención de phishing.
- **Enlaces Maliciosos:** Hipervínculos que dirigen a los usuarios a sitios web fraudulentos con el objetivo de extraer información personal o instalar malware en el dispositivo del usuario.
- **Ingeniería de Pretextos:** Método de ingeniería social que implica crear una situación ficticia convincente para obtener información confidencial o persuadir a alguien para que realice ciertas acciones.
- **Manipulación Emocional:** Uso de emociones como el miedo o la compasión por parte de atacantes para manipular a las víctimas y obtener información o acceso.
- ***Phishing*:** Táctica de engaño que busca obtener información confidencial (como credenciales de acceso y datos financieros) de usuarios a través de comunicaciones fraudulentas que aparentan ser fuentes confiables.
- **Social Engineering (Ingeniería Social):** Método de ataque que se basa en la

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

manipulación psicológica de personas para que realicen acciones o revelen información confidencial.

- ***Spear Phishing*:** Forma de phishing altamente dirigida, donde el atacante tiene un conocimiento detallado de su víctima, lo que permite personalizar el ataque para incrementar sus chances de éxito.
- **Verificación de Identidad:** Proceso recomendado para confirmar la identidad de una persona antes de proporcionar acceso a información sensible o realizar acciones críticas, como medida preventiva contra la ingeniería social.
  - **Análisis de Reputación de Archivos**: Evaluación de la confiabilidad de un archivo basada en su origen y comportamiento histórico, contribuyendo a la detección de amenazas potenciales.
  - **Antivirus**: Software diseñado para detectar, prevenir y eliminar malware, utilizando diversas técnicas de detección para proteger los sistemas informáticos.
  - **Buffer Overflow**: Defecto de software donde un programa escribe más datos en un búfer de lo que este puede contener, lo cual puede ser explotado para ejecutar código malicioso.
  - **Detección basada en firmas**: Método utilizado por los antivirus para identificar malware comparando archivos sospechosos con una base de datos de firmas de malware conocido.
  - **Detección de comportamiento**: Técnica de los antivirus para identificar actividades sospechosas o anómalas en tiempo real, útil para detectar malware nuevo o modificado.
  - **Gusano (*Worm*)**: Tipo de malware que se replica y propaga automáticamente, utilizando vulnerabilidades del sistema o de la red, sin necesidad de infectar archivos existentes.
  - ***Ransomware***: Malware que cifra los archivos del usuario y exige un pago para desbloquearlos, efectivamente secuestrando la información hasta que se pague el rescate.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

- **Remote code execution (RCE)**: Vulnerabilidad que permite a un atacante ejecutar código arbitrario en un sistema remoto, a menudo con privilegios elevados.
- ***SQL Injection***: Vulnerabilidad que permite a un atacante manipular las consultas SQL, potencialmente accediendo y modificando bases de datos sin autorización.
- ***Spyware***: Software que se instala sin el conocimiento del usuario y monitorea sus actividades, recolectando información personal y confidencial.
- **Virtualización y análisis en entornos aislados**: Técnica de antivirus que ejecuta archivos sospechosos en un entorno seguro y controlado para observar su comportamiento sin riesgo para el sistema principal.
- **Virus de Computadora**: Software malicioso que se replica y propaga entre computadoras, diseñado para infectar y alterar el funcionamiento de los sistemas sin el consentimiento del usuario.
- ***Zero-Day Vulnerability***: Vulnerabilidad en software o hardware que es explotada por los atacantes antes de que el desarrollador conozca y pueda parchear la falla.
- **Análisis de Reputación de Archivos**: Evaluación de la confiabilidad de un archivo basada en su origen y comportamiento histórico, contribuyendo a la detección de amenazas potenciales.
- **Antivirus**: Software diseñado para detectar, prevenir y eliminar malware, utilizando diversas técnicas de detección para proteger los sistemas informáticos.
- **Buffer Overflow**: Defecto de software donde un programa escribe más datos en un búfer de lo que este puede contener, lo cual puede ser explotado para ejecutar código malicioso.
- **Detección basada en firmas**: Método utilizado por los antivirus para identificar malware comparando archivos sospechosos con una base de datos de firmas de malware conocido.
- **Detección de comportamiento**: Técnica de los antivirus para identificar actividades sospechosas o anómalas en tiempo real, útil para detectar malware nuevo o modificado.

MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

- ***Ransomware***: Malware que cifra los archivos del usuario y exige un pago para desbloquearlos, efectivamente secuestrando la información hasta que se pague el rescate.
- **Remote code execution (RCE)**: Vulnerabilidad que permite a un atacante ejecutar código arbitrario en un sistema remoto, a menudo con privilegios elevados.
- ***SQL Injection***: Vulnerabilidad que permite a un atacante manipular las consultas SQL, potencialmente accediendo y modificando bases de datos sin autorización.
- ***Spyware***: Software que se instala sin el conocimiento del usuario y monitorea sus actividades, recolectando información personal y confidencial.
- **Virtualización y análisis en entornos aislados**: Técnica de antivirus que ejecuta archivos sospechosos en un entorno seguro y controlado para observar su comportamiento sin riesgo para el sistema principal.
- **Virus de Computadora**: Software malicioso que se replica y propaga entre computadoras, diseñado para infectar y alterar el funcionamiento de los sistemas sin el consentimiento del usuario.
- ***Zero-Day Vulnerability***: Vulnerabilidad en software o hardware que es explotada por los atacantes antes de que el desarrollador conozca y pueda parchear la falla.
- **Wi-Fi**: Wireless Fidelity, "Fidelidad Inalámbrica", es un mecanismo a la cual dispositivos tecnológicos pueden conectarse a internet sin necesidad de algún cable, a eso se le llama internet inalámbrico.
- **Time Out**: Periodos de tiempo en que la red se encuentra caída y no establece conexión a internet.
- **Hosting:** es un sistema que almacena información, imágenes, vídeo, o cualquier contenido a través de internet y permite mostrar todo ese contenido vía páginas web (asociando este hosting a un "dominio").
- **Dominio web**: La parte principal de una dirección en la Web que indica la organización o compañía que administra dicha página o sitio web, básicamente es el identificador para acceder a dicha página web.
- **Sniffing:** Proceso mediante el cual los datos que se trasmiten dentro de una red, son capturados o monitoreados por terceras personas.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

- **Spoofing:** en términos de seguridad de redes hace referencia al uso de técnicas a través de las cuales un atacante, generalmente con usos maliciosos o de investigación, se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.
- **Spyware:** Software malicioso cuya función es monitorear las acciones del usuario de un computador y reportar estas acciones a un tercero, sin el consentimiento del propietario del computador o del usuario legítimo.
- **Adware:** Cualquier paquete de software que automáticamente reproduce, muestra o descarga material publicitario en un computador después de que se instala un programa que contiene el material previamente mencionado.
- **Plug-in:** Programa computacional que interactúa con una aplicación principal, a modo de ejemplo, un cliente de email o un browser, para proveer una función cuando sea demandada.
- **Rack:** es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas para que sean compatibles con equipamiento de distintos fabricantes. También son llamados bastidores, cabinas, gabinetes o armarios.

CAPITULO II.- Políticas de Seguridad de la Información

.1. Objetivos generales

A. 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.

B. 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.

C. Mantener la Política de Seguridad del Municipio actualizado, para asegurar su vigencia y nivel de eficacia ante nuevas amenazas.

.2. Sanciones por incumplimiento de la política

El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información, conlleva a la correspondiente investigación administrativa, para establecer las responsabilidades

.3.- Organización de la Seguridad

Son sus objetivos:

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

A. Administrar la seguridad de la información dentro del Municipio y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
B. Fomentar la consulta y cooperación con otros Municipios especializados para la obtención de asesoría en materia de seguridad de la información.
C. Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros o de personal externo a la información de la Municipalidad.

4. Infraestructura de la Seguridad de la Información

4.1 Asignación de Responsabilidades

El Administrador Municipal de la Ilustre Municipalidad de Retiro, asignó, en materia de Seguridad de la Información, al funcionario Sr. Camilo Aravena Salvo, como "Encargado de Seguridad de la Información", según Decreto Exento N°1.318 de fecha 15 de Mayo del 2024, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Municipio, coordinará las respuestas a incidentes computacionales, Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad. También, propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan de los procesos de seguridad que se detallan a continuación:

a) Seguridad del Personal.
b) Seguridad Física y Ambiental.
c) Seguridad en las Comunicaciones y las Operaciones.
d) Control de Accesos.
e) Seguridad en el Desarrollo y Mantenimiento de Sistemas.
f) Planificación de la Continuidad Operativa.

Así mismo, el Encargado de Seguridad de la Información propondrá a la autoridad, para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que correspondan, a su vez quienes serán los responsables de los departamentos a cargo del manejo de la misma.

4.2 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.

4.3 Revisión de la Política de Seguridad de la Información

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

El Encargado y Comité 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.

4.4 Seguridad Frente al Acceso por Parte de Terceros

4.4.1 Identificación de Riesgos del Acceso de Personal Externo y Terceros

Cuando exista la necesidad de otorgar acceso a personal externo y a terceros, sobre la información del Municipio, el Encargado de Seguridad de la Información y el Propietario de la Información de que se trate, llevarán a cabo, una evaluación de riesgos, para identificar los requerimientos de controles específicos, teniendo en cuenta, los siguientes aspectos:

- El tipo de acceso requerido (físico/lógico y a qué recurso).
- Los motivos para los cuales se solicita el acceso.
- El valor de la información (nivel de criticidad o importancia de la información).
- Los controles empleados por la tercera parte.
- La incidencia de este acceso en la seguridad de la información del Municipio.

El acceso a la sala de servidores, será restringido, y solo ingresaran las personas debidamente autorizadas y bajo los controles apropiados, en caso, que deba ser un tercero, debe existir una previa evaluación de informática.

5.- Clasificación y Control de Activos

Son sus objetivos:

A. Garantizar que los activos de información reciban un apropiado nivel de protección.
B. Clasificar la información para señalar su sensibilidad y criticidad.
C. Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Esta Política se aplica a toda la información administrada en la Municipalidad, cualquiera sea el soporte en que se encuentre (ya sea física o información virtual).
El Encargado de Seguridad de la Información es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información, contemplen los requerimientos de seguridad establecidos, según la criticidad de la información que procesan, es decir, según el grado de importancia de los recursos de información, con la que, obtendrán mayor prioridad, según la clasificación de riesgos.
Cada usuario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplido de acuerdo a lo establecido en la presente Política.

a. Inventario de activos

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Se identificarán los activos físicos que procesan datos e información, con sus respectivos usuarios y su ubicación, para luego elaborar un inventario con dicha información.
El departamento encargado de elaborar el inventario y mantenerlo actualizado ante cualquier modificación de la información, es la Dirección de Administración y Finanzas de la Municipalidad.

b. Clasificación de activos

Los Activos de información, se caracterizan por;

- Confidencialidad.
- Integridad.
- Disponibilidad.
- Sensibilidad
- Evolución constante

b.1 Tipos de activos de información

- Información confidencial
- Sistemas informáticos
- Aplicaciones
- Infraestructura
- Instalaciones de red
- Instalaciones físicas
- Activos tangibles

c. Rotulado de la Información

Los recursos de información, tanto, en formatos físicos, como electrónicos, deberán ser rotulados, bajo este esquema:

- Nombre del recurso.
- Tipo.
- Almacenamiento.
- Criticidad. (Medible bajo un análisis de criticidad descrito en el punto).
- Descripción Breve.

6. Desasistencia de Equipos Informáticos

Todo equipo computacional que deje de contener las características técnicas necesarias, y evaluado así por unidad de informática, será dado de baja, una vez realizado el respaldo correspondiente de datos.

Los equipos, dados de baja, serán trasladados a Bodega Municipal, para su almacenaje.
Dando el aviso a la Dirección de Administración y Finanzas, para que realice la modificación en el Activo Fijo Municipal.

a. Cambio o Actualización de Equipo Computacional

El proceso de cambio de un equipo computacional, se realizará previo informe de informático, donde

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

establece que el equipo cumplió su vida útil o no cumple con lo requerido, para el normal funcionamiento.

Sobre el respaldo de la información del equipo a dar de baja o cambiar su destino, se puede dar que:

- Informática realiza el respaldo.
- El funcionario realiza el respaldo (dejado documento, que indica que la información respaldada, se encuentra bajo su responsabilidad).

El Directivo o Jefe de unidad, requirente, solicita la compra del equipo, bajo especificaciones, entregadas por el informático, de acuerdo a la necesidad y/o la labor, que realiza el funcionario.

Si se da que un equipo informático, cambia su destino, ya sea, por reutilización o usuario hace entrega de él, se debe dar el correspondiente aviso por escrito a la unidad de Adquisiciones para que realice el cambio de usuario.

El Decreto exento, que da de alta o cambio de destino, en inventario General de bienes, de un equipo computacional, debe contener:

- Especificaciones mínimas del equipo computacional a entregar, tales como marca, modelo y número de serie, valor y nombre del funcionario, que se hará cargo del equipo.

7. Seguridad del Personal

Objetivos:

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

- Describir las responsabilidades en materia de seguridad en la etapa de entrega de equipos computacionales al funcionario.

- Garantizar que los funcionarios, mantengan información de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Municipalidad en el transcurso de sus tareas normales.

- Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal del Municipio, Planta y Contrata y prestadores de servicio, que efectúe labores, dentro del ámbito de la Municipalidad.

El Encargado de Seguridad de la Información, tiene a cargo el seguimiento y análisis de los incidentes de seguridad reportados, así como su comunicación al personal municipal sobre las tendencias en cuanto a amenazas y riesgos que puedan afectar a los equipos informáticos del municipio.

Todo el personal del Municipio en general, es responsable del reporte en forma oportuna de debilidades e incidentes de seguridad, que se detecten, informando sobre dudas o sospechas de

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

amenazas, al Encargado de Seguridad de la Información.

7.1 Definición de Puestos de Trabajo y la Asignación de Recursos

✓ **Inducción de Seguridad de la información en los Puestos de Trabajo**

Al entregar un equipo computacional, a un funcionario, se debe dar a conocer las responsabilidades generales, relacionadas con la implementación y el mantenimiento de las Políticas de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

7.2. Capacitación del funcionario

Todos los funcionarios y prestadores de servicios, que desempeñen funciones dentro del Municipio, recibirán capacitación y actualización periódica, en referente a la política de seguridad, en sus diversos ámbitos.

7.3 Respuesta a incidentes y Anomalías en Materia de Seguridad

i. Comunicación de incidentes Relativos a la Seguridad

Los acontecimientos, relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Se establecerá un procedimiento de comunicación y de respuesta a incidentes, indicando la acción que deberán emprender al recibir un informe sobre acontecimientos. Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad; el Encargado de Seguridad de la Información, debe ser informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución de incidentes, encargándose de su monitoreo.

ii. Comunicación de Debilidades en Materia de Seguridad

Los funcionarios, que manejan equipos informáticos municipales, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar estas al Encargado de Seguridad de la Información.

iii. Comunicación de Anomalías del Software

La comunicación de anomalías de software y otros riesgos informáticos deben de ser de este modo para una respuesta más rápida frente a estos riesgos, la pauta es la siguiente:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Alertar inmediatamente al Encargado de Seguridad de la Información referente al activo comprometido al cual se presenta la anomalía.
- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.

iv. Aprendiendo de los incidentes

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Dentro del procedimiento de identificación de anomalías y evaluación de riesgos está un apartado en donde se registra el incidente ocurrido, esta información se utilizará para responder rápidamente ante incidentes recurrentes y a su vez establecer un registro estadístico de cómo actuar, identificar más rápidamente las causas de la anomalía y tener identificada la información, los costos asociados a ello y los métodos de recuperación, así como sus soluciones.

7.4.- Seguridad Física y Ambiental

Objetivos:

- ✓ Prevenir e impedir accesos no autorizados, daños e interferencia, y robo de información de la Municipalidad.
- ✓ Proteger los equipos computacionales, que contienen información crítica, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
- ✓ Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Municipio.
- ✓ Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
- ✓ Brindar protección, en proporción a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Municipalidad: instalaciones, equipamiento, cableado, medios de almacenamiento, etc.

El Encargado de Seguridad de la Información, junto al Comité de Seguridad, deberán definir las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlar el mantenimiento, del equipamiento informático de acuerdo a las indicaciones de proveedores, tanto dentro como fuera de las instalaciones de la Municipalidad.

Todos los funcionarios municipales son responsables del cumplimiento de las buenas prácticas correspondientes a pantallas y escritorios limpios, para la protección y el orden de la información relativa al trabajo diario en las oficinas.

En la Ilustre Municipalidad de Retiro, la única área protegida total, que se describe en esta política de seguridad de la información es la Sala de Servidores, cableado, routers o switch, ubicada en patio Los Naranjos.

7.4.1.- Seguridad Física y ambiental

La dirección de cada unidad, debe determinar, de acuerdo, a las herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que manejen, las medidas de protección necesarias, para el debido control físico de los bienes.

El Municipio utilizará perímetros de seguridad de acceso, determinando como zona restringida,

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

la sala de servidor municipal, y proveerle a esta de suministro:

- Electricidad.
- Aire Acondicionado.
- Luces de Emergencia.
- Extintores CO2 y PQS.
- Sensores que controlen el humo, humedad.
- Cámaras de seguridad
- Puerta de acceso metálica y características cortafuegos

A. Controles de Acceso Físico

El área protegida se resguardará, mediante, el empleo de controles de acceso físico. El ingreso a la sala de servidores, se encuentra ubicado en edificio patio los naranjos; debe utilizar la señalética en su puerta que indica **"Sólo personal autorizado"**, como serán el Encargado de Computación o quien este designe y Encargado de Seguridad de la Información. Aquellos funcionarios distintos a los mencionados anteriormente, deberán contar con la autorización formal del Alcalde, Administrador Municipal, encargado de informática o Encargado de seguridad de la información, dejando el debido registro en bitácora de acceso de personal, ya sea, interno o externo, a la dependencia, registrando las actividades realizadas y numero de Rol de la persona que ingresa.

En relación a los Racks, estarán protegidos con llave, que sólo, el Encargado de Informática mantendrá.

B. Ubicación de los Medios de Almacenamiento de Respaldos

Los respaldos se realizarán en discos duros externos portátiles, designados para tal propósito, también, el almacenamiento de respaldo de bases de datos históricas del servidor municipal. Debe ser debidamente resguardada en caja fuerte principal, ubicada en Oficina de Administración y Finanzas.

C. Seguridad del Cableado

El cuanto al cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información, deberá estar protegido contra intercepción o daño, y se ubicará en la parte posterior del equipo computacional, para evitar la intercepción del funcionario.

D. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su integridad y operatividad permanente, teniendo en cuenta a tal efecto:

- ✓ La realización de tareas de mantenimiento físico al equipamiento, de acuerdo con los intervalos del servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsable del Área Informática.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

- ✓ Sólo el Área de informática, puede brindar mantenimiento y llevar a cabo reparaciones en los equipos computacionales.
- ✓ El registro de todas las fallas "supuestas y/o reales" y de todo el mantenimiento preventivo y correctivo realizado.
- ✓ La eliminación de toda información confidencial, que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

También se realizará un mantenimiento preventivo, en el cual, se revisarán aspectos previamente definidos por el Encargado de Seguridad de la Información; la periodicidad de las revisiones de mantenimiento preventivo es completamente aleatoria.

E. Seguridad de los Equipos Fuera de las Instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Municipalidad será autorizado por el Alcalde o Administrador Municipal. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Municipalidad, para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

8.- Gestión de Operaciones en Aplicaciones y Cambios

Son sus objetivos:

- ✓ Garantizar el funcionamiento correcto y seguro de la sala de servidores municipal, así como los equipos computacionales de los funcionarios municipales.
- ✓ Establecer responsabilidades y procedimientos para la gestión operativa y la marcha de los sistemas municipales, incluyendo comportamientos técnicos, procedimiento para la respuesta a incidentes y separación de funciones ante esos incidentes.
- ✓ Respaldar toda la información sensible (documentos, medios digitales, bases de datos, entre otros.), ante eventuales ataques e imprevistos.
- ✓ Proteger a los equipos computacionales y a la información que procesan, entre ellos realizar mantención a la información, control de red y el procesamiento de medios extraíbles.

Además, se consideran la protección de redes y programas, la gestión operativa de los equipos computacionales, el intercambio de la información, el mantenimiento de la información digital, entre otros.

8.1- Control de Cambios y Separación de Funciones

8.1.1. Control de Cambios en las Operaciones

Se definirá un procedimiento para el control de los cambios en el ambiente operativo, programas licenciados y sistemas municipales. Todo cambio a los sistemas debe de ser registrado según:

- Tipo del cambio (menor, mayor).
- Que recursos afecta.
- Versión.
- Compatibilidad con otros programas, entre otros aspectos específicos.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

El Encargado de Seguridad de la Información, controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos, ni de la información que soportan. El Encargado de Computación evaluará, el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

8.1.2 Procedimientos de Manejo de incidencias

Se establecerán funciones y procedimientos de manejo de incidencias, garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a resguardar la información, además se documentarán las incidencias, que sean pertinentes, para su rápida respuesta y coordinación posterior, además de llevar un registro estadístico indicando cuáles son las fallas más comunes, los costos asociados a tiempo, y el conocimiento previo de esa situación.

8.1.3 Separación de Funciones

Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

En los casos en los que este método de control no se pueda cumplir, se implementarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

8.2 Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Encargado de Computación, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Para ello tomará en cuenta, además, los nuevos requerimientos de los sistemas, así como las tendencias actuales y proyectadas en el procesamiento de la información de la Municipalidad para el período estipulado de vida útil de cada componente.

Asimismo, informará las necesidades detectadas a la Alcaldía para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2 Aprobación del Sistema

El Encargado de Informática o la persona a quien este designe y el Encargado de Seguridad de la Información sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

8.2.3 Registro de Actividades del Personal Operativo

El Encargado de Computación asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

- ✓ Errores del sistema y medidas correctivas tomadas.
- ✓ Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas.
- ✓ Ejecución de operaciones críticas.
- ✓ Cambios a información crítica.

También se realizarán controles aleatorios de equipos municipales, a fin de detectar anomalías e infracciones que puedan incurrir, los funcionarios sobre el uso de sus equipos, estos Check-list se deben hacer de forma aleatoria y bimestralmente.

8.2.4 Registro de Fallas

El Encargado de Computación, establecerá un modelo para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas, así como su registro.

9.- Políticas de instalación y usos de software y prevención contra código malicioso.

- ✓ Está prohibida la instalación y/o uso de software no autorizado por el área de informática.

- ✓ El área informática es responsable de administrar la lista de aplicaciones permitidas.

- ✓ El área de informática, es responsable de administrar los accesos y restricciones de navegación sobre sitios web, para lo cual deberá considerar herramientas informáticas de gestión de listas blancas y negras.

- ✓ Cuando se desee instalar cualquier software, sea o no de administración informática, la jefatura respectiva, debe hacer la solicitud a la unidad de informática, quien estará encargado de hacer la instalación. El uso de software no licenciado está estrictamente prohibido. Todo software que se pretenda instalar debe guardar relación con materias de competencias institucionales.

- ✓ Los funcionarios(as), son responsables de dar aviso la Unidad informática, a través del medio establecido por la Municipalidad, de cualquier anomalía detectada en relación al funcionamiento de un software.

- ✓ La Unidad de informática, es responsable de la eliminación de softwares no

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

autorizados de equipos computacionales, que contengan posibles amenazas para la seguridad de los datos.

- ✓ Está prohibido abrir software, archivos ejecutables o macros desde algún correo de fuente desconocida, sospechosa o que no sea de confianza. Si los funcionarios(as), reciben un correo con contenido sospechoso debe dar aviso al encargado de seguridad de la información, para que tome las medidas pertinentes.

- ✓ Con el fin de mitigar las vulnerabilidades, los equipamientos computacionales de la Municipalidad, deben contar con conexiones que provean de forma segura actualizaciones automáticas de seguridad para los sistemas operativos y aplicaciones que corresponda.

- ✓ El equipamiento computacional de la Municipalidad, conectado al dominio organizacional debe contar con la instalación de un software de detección, análisis y reparación de malware.

- ✓ En el caso, de algún equipo computacional no sea propiedad de la institución, este deberá contar con antivirus actualizado y actualizaciones de seguridad al día. Esta validación la realizara por informática, antes que del equipo sea conectado a la red Institucional.

- ✓ La actualización de software, así como las actualizaciones y parches de seguridad, en el ambiente operacional, debe ser realizado por la Unidad de informática.

- ✓ La Unidad de informática, debe estar en condiciones de hacer un restablecimiento a un estado anterior en el ambiente operacional en caso de fallas por instalaciones nuevas (proceso de Rollback).

- ✓ El encargado de seguridad de la información, debe implementar un control de versión del software.

10.- Seguridad de Redes

- ✓ Deberán establecer el uso de firewall licenciado para proteger la Red Municipal, para optimizar el tráfico y seguridad.
- ✓ La transmisión de Redes Wí-Fi y su uso es exclusivo para Computadores que cumplan los requisitos de Seguridad para estar dentro de la Red Municipal. Todo equipo externo a la red municipal como invitados se conectará a través de una red dmz.

11. Procedimiento de Respaldo de la Información

Los respaldos de la Información es uno de los puntos más importantes que permitirán a la

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

municipalidad el funcionamiento después de un desastre.
El objetivo de esta política es otorgar un medio, por el cual se pueda recuperar información importante para no paralizar el funcionamiento normal del municipio.
Todos los documentos deberán ser almacenados obligatoriamente en la Carpeta Mis Documentos del usuario. Además, estará totalmente prohibido trabajar directamente sobre dispositivos externos.

1. Respaldo Documentos Desktop y Notebook

Este proceso será ejecutado automáticamente en las fechas programadas y/o cuando el usuario lo estime conveniente.

2. Respaldo Documentos, base de datos en Servidor

Este proceso programado y automatizado por la Unidad de Informática en los Servidores a través de trabajos del agente sql server y definido en tiempo periódicos diarios al cierre de la jornada laboral.

3. Seguridad de los Respaldos

Los respaldos, tanto Servidores, Desktops y Notebooks serán realizados con clave de encriptación, independiente para cada tipo de respaldo.

4. Periodicidad de los Respaldos

Los respaldos Desktop y Notebook o laptop críticos serán realizados al menos 1 vez al mes. Cuando se trate de un respaldo completo y/o diario cuando sea Incremental.
Los servidores tendrán un respaldo diario incremental y un respaldo completo semanal.

5. Ubicación de los Respaldos

Desktop y Notebook, serán Respaldos en Discos NAS en ubicaciones opuestos de la Municipalidad.
El respaldo principal de los servidores será realizado en Disco Externo el cual quedará almacenado en la Caja Fuerte Principal de la municipalidad. Se deberá dejar un registro firmado por la persona que realizó el proceso de respaldo, indicando fecha, hora, archivos respaldados de Servidores, además del Nombre y Firma del funcionario.

12. Seguridad del Correo Electrónico Institucional

12.1. Riesgos de Seguridad

Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

- La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
- La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
- Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
- La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
- El impacto de un cambio en el medio de comunicación en los procesos del Municipio.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

- Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
- El uso inadecuado por parte del personal.

12.2. Política de Correo Electrónico

El Encargado de Seguridad de la Información define una política de correos electrónicos institucionales que trata respecto al uso del correo electrónico, esta política está separada de esta política general de seguridad de la información, e incluye los siguientes aspectos:

- ✓ Definición de los alcances del uso del correo electrónico por parte del personal de la Municipalidad.
- ✓ Cuentas de usuarios y contraseñas.
- ✓ Uso del Correo electrónico institucional
- ✓ Señalar medidas en caso de términos de contratos
- ✓ Seguridad y uso de contraseñas
- ✓ Comunicación efectiva de la política

13. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

Además, se integran los sistemas que son del Gobierno, estos sistemas y su uso están en exclusiva responsabilidad del funcionario en cuestión, y también el soporte que se le brinda a ese sistema, si un funcionario tiene una falla con un sistema del gobierno, el área de computación no se hace responsable por estas fallas.

13.1. Control de Accesos

Son sus objetivos:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de funcionarios por medio de técnicas de autenticación y autorización a los perfiles correspondientes al funcionario de acuerdo a su función designada.
- Controlar la seguridad en la conexión entre la red del Municipio y otras redes públicas o privadas.
- Registrar y revisar eventos y actividades críticas llevadas a cabo por los funcionarios en los sistemas.
- Concientizar a los funcionarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
- Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

13.2. Administración de Accesos de Funcionarios

Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

13.2.1. Registro de nuevos Funcionarios

El Encargado de Seguridad de la Información definirá un procedimiento formal de registro de nuevos funcionarios para definir la concesión del acceso a todos los sistemas, bases de datos y servicios de información, dependiendo de las necesidades establecidas en la contratación, además de tener claro cuales sistemas ocupaba un usuario que ya no tiene calidad de funcionario, para la revocación del acceso y su posterior eliminación.

13.2.2. Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente, el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal de parte de la Alcaldía.

13.2.3. Administración de Contraseñas de Funcionarios

La asignación de contraseñas se realizará bajo ciertos patrones secretos definidos por el Área de Informática, también, el funcionario puede asignar sus propias contraseñas, debidamente escritas, por comunicación interna, dependiendo del sistema que utilice, también debe notificar al área de Computación cuando un funcionario desea cambiar la clave.

13.2.4. Administración de Contraseñas Críticas

Existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y deben de estar protegidas por contraseñas con un mayor nivel de complejidad que el habitual, estas cuentas son superusuario, es decir, pueden cambiar a voluntad todos los parámetros de un sistema en concreto. -

13.2.5. Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Encargado de Informática, llevará a cabo un proceso formal, a intervalos regulares de no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

13.3. Responsabilidades del Usuario

13.3.1. Uso de Contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas, existen dos buenas prácticas para el uso de las contraseñas que son las siguientes:

- La contraseña no debe ser menor a 6 caracteres
- Debe contener mayúsculas y minúsculas

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

13.4.-Recomendaciones para la elección de contraseñas seguras

a) Sustituir las contraseñas que le han sido asignadas por defecto por contraseñas difíciles de adivinar, de acuerdo con los criterios de robustez recomendados por la Unidad de Informática;

b) Mantener estricta reserva de sus contraseñas y no hacer uso de cuentas ajenas, ni siquiera, con el permiso expreso del titular. Las cuentas de Usuario y sus contraseñas son personales e intransferibles,

e) Las contraseñas, deberán contener al menos ocho caracteres, y en una mezcla de cuatro diferentes tipos de caracteres: letras mayúsculas, letras minúsculas, números y caracteres especiales como: ¡Mn1! OR$%AS8*;" Sí sólo hay una letra o carácter especial, no debe ser el primero ni el último en la contraseña.

d) La contraseña no deberá ser un nombre propio o una parte del nombre de la persona o su dirección de correo electrónico.

e) La contraseña deberá ser robusta para los sitios en donde se almacena información cuya privacidad sea importante. Se deberán utilizar contraseñas diferentes para todos los sitios.

13.5. Control de Acceso a la Red

13.5.1. Política de Utilización de los Servicios de Red

Se controlará el acceso a los servicios de red tanto internos como externos. El Encargado de Informática, tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente, de acuerdo a solicitud formal del titular de un Departamento que lo solicite para personal de su incumbencia.

13.5.2. Autenticación de Usuarios para Conexiones Externas

El Encargado de Seguridad de la Información, conjuntamente con el Propietario de la

MUNICIPALIDAD DE RETIRO SECRETARIO MUNICIPAL

Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

13.5.3. Autenticación de Nodos

Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación de la Municipalidad. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas y verificadas.

13.5.4. Subdivisión de Redes

Se definirán y documentarán los perímetros de seguridad que sean convenientes, que se implementarán mediante la instalación de "Gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

13.5.5. Uso responsable de internet

Internet es un servicio que la Municipalidad pondrá a disposición de su personal para uso estrictamente profesional. Considerando que este recurso en el ámbito laboral aumenta las amenazas a la seguridad de la red pudiendo afectar la productividad de sus usuarios éstos deberán cumplir con las siguientes obligaciones:

a) Los Usuarios serán los únicos responsables de las sesiones iniciadas en Internet desde sus terminales de trabajo y se comprometen a acatar las reglas y normas de funcionamiento establecidas en la presente normativa.

b) El acceso a Internet por personal externo requerirá la autorización previa y por escrito del encargado de la dirección o jefe de departamento respectivo.

c) En ningún caso, un Usuario podrá modificar las configuraciones de los navegadores (opciones de Internet), de los equipos ni la activación de servidores o puertos sin la autorización correspondiente.

d) Prohíbase expresamente el acceso, la descarga y/o el almacenamiento en cualquier dispositivo de páginas con contenidos ilegales, dañinos, inadecuados o que atenten contra la moral y las buenas costumbres y, en general, de todo tipo de contenido que incumpla las normas éticas y de cortesía del municipio.

e) Prohíbase, asimismo, el almacenamiento en los equipos de archivos y contenidos que violen la legislación vigente relativa a Propiedad Intelectual. Los Usuarios deberán respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y

MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

derechos de propiedad intelectual de cualquier información visualizada u obtenida mediante Internet haciendo uso de los recursos informáticos y de la red municipal.

f) Bajo ningún concepto los usuarios podrán utilizar programas de descarga de archivos P2P o similares.

g) Prohíbase el uso de Internet mediante los recursos informáticos o de red de la municipalidad con fines recreativos, así como para obtener o distribuir material violento, pornográfico, que atente contra la dignidad de las personas o incompatible con los valores de la municipalidad.

h) El uso de chat o programa de conversación en tiempo real estará permitido solo a través de las plataformas que disponga la Unidad de informática. Si un director, jefe de departamento o sección necesita autorizar a su personal para el uso de una plataforma distinta a las autorizadas, deberá justificar y solicitar de manera escrita la aprobación del uso de esta plataforma a la Unidad de Informática,

i) No se deberá buscar, hacer uso o apoderarse de información personal, ni se deberán obtener copias del software, archivos, datos ni contraseñas pertenecientes a usuarios de internet. No se deberá llevar a cabo, en ningún caso, la suplantación de forma voluntaria o consciente de otro usuario.

j) Cualquier Incidente de Seguridad relacionado con la navegación por Internet, deberá ser comunicado sin demora al jefe inmediato y a la Unidad de Informática.

k) Prohíbase la descarga de software ejecutables desde Internet sin autorización, especialmente la utilización de imágenes (como los formatos GIF, JPG, BMP o TIFF entre otros), sonido (formatos WAV y MP3 principalmente) y video (MPG, DivX, AVI, RAW o similares) para fines ajenos a la actividad laboral.

13.5.6. Control de Ruteo de Red

Se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino.

13.6. Control de Acceso al Sistema Operativo

13.6.1. Identificación Automática de Equipos

El Encargado de Seguridad de la Información junto con el Encargado de Computación realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo, esta evaluación de riesgos se define por lo siguiente:

13.6.2. Sistema de Administración de Contraseñas

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

El sistema de administración de contraseñas debe:

A. Imponer el uso de contraseñas individuales para determinar responsabilidades.
B. Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
C. Imponer una selección de contraseñas de calidad según lo señalado en el punto "Uso de Contraseñas".
D. Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto "Uso de Contraseñas".
E. Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
F. Mantener un registro de las últimas contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.
G. Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
H. Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
I. Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado robusto.
J. Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, hubs, routers, etc.).
K. Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

13.6.3. Uso de Utilitarios de Sistema

Existen programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado.

13.7. Control de Acceso a las Aplicaciones

13.7.1. Restricción del Acceso a la Información

Los usuarios de sistemas municipales, tendrán acceso a la información sensible de la Municipalidad como, por ejemplo, activos fijos, patentes municipales, tesorería, entre otros sistemas según corresponda la función del personal municipal y además esté conforme con las responsabilidades descritas en la Política de Control de Acceso.

Cualquier otro acceso a los sistemas municipales que no esté definido y previamente autorizado se considerará como intrusión a los sistemas municipales.

13.8. Monitoreo del Acceso y Uso de los Sistemas

13.8.1. Registro de Eventos

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

13.8.2. Monitoreo del Uso de los Sistemas

13.8.2.1. Procedimientos y Áreas de Riesgo

Se usarán programas y aplicaciones para monitorear el uso de los sistemas y equipos computacionales, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

13.8.2.2. Factores de Riesgo

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

14. Desarrollo y Mantenimiento de Sistemas

Son sus objetivos:

A. Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
B. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
C. Definir los métodos de protección de la información crítica o sensible.
D. Definir instructivos en la cual se pueda coordinar respuestas rápidas frente a incidentes.

Esta Política se aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los Sistemas Operativos y/o Software de Base que integren cualquiera de los ambientes administrados por la Municipalidad en donde residan los desarrollos mencionados.

El Encargado de Seguridad de la Información junto con el Propietario de la Información, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos.

El Encargado de Seguridad de la Información, junto con el Propietario de la Información, definirán en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Encargado de Seguridad de la Información definirá junto con el Responsable del Área de Sistemas, los métodos de encriptación a ser utilizados.

14.1. Requerimientos de Seguridad de los Sistemas

14.1.1. Análisis y Especificaciones de los Requerimientos de Seguridad

Esta Política se implementa para incorporar seguridad a los sistemas de información (propios

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

o de terceros) y a las mejoras o actualizaciones que se les incorporen. Los requerimientos para nuevos sistemas o mejoras a los existentes especificarán la necesidad de controles. Estas especificaciones deben considerar los controles automáticos a incorporar al sistema, como así también controles manuales de apoyo.

14.2. Controles Criptográficos

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

14.2.1. Política de Utilización de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

1. Para la protección de claves de acceso a sistemas, datos y servicios.
2. Para la transmisión de información clasificada, fuera del ámbito del Municipio.
3. Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el Propietario de la Información y el Encargado de Seguridad de la Información.

14.2.2. Cifrado

Mediante la evaluación de riesgos que llevará a cabo el Propietario de la Información y el Encargado de Seguridad de la Información, se identificará el nivel requerido de protección, tomando en cuenta el tipo y la calidad del algoritmo de cifrado utilizado y la longitud de las claves criptográficas a utilizar.

14.2.3. Firma Digital

Se tomarán recaudos para proteger la confidencialidad de las claves privadas. Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.

14.2.4. Servicios de No Repudio

Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

14.3. Seguridad de los Procesos de Soporte

14.3.1. Revisión Técnica de los Cambios en el Sistema Operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

14.3.2. Restricción del Cambio de Paquetes de Software

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

La modificación de paquetes de software suministrados por proveedores, previa autorización del Encargado de Computación, deberá:

A. Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
B. Evaluar el impacto que se produce si el Municipio se hace cargo del mantenimiento.
C. Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

14.3.3. Canales Ocultos y Código Malicioso

Se evaluarán los siguientes aspectos para asegurar que ningún software posea algún código malicioso que pueda atacar a los distintos sistemas.

A. Adquirir programas a proveedores acreditados o productos ya evaluados.
B. Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
C. Controlar el acceso y las modificaciones al código instalado.
D. Utilizar herramientas para la protección contra la infección del software con código malicioso.

14.3.4. Desarrollo Externo de Software

Para el caso que se considere la subcontratación del desarrollo de software, se exigirán los siguientes puntos:

A. Acuerdos de licencias, propiedad de código y derechos conferidos.
B. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
C. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.
D. Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto 4.3.1. Requerimientos de Seguridad referentes a la Subcontratación.
E. Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

15. Administración de la Continuidad de las Actividades del Municipio

Son sus objetivos:

A. Minimizar los efectos de las posibles interrupciones de las actividades normales de la Municipalidad (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
B. Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

C. Maximizar la efectividad de las operaciones de contingencia del Municipio con el establecimiento de planes que incluyan al menos las siguientes etapas:
   a. Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
   b. Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
   c. Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

D. Asegurar la coordinación con el personal del Municipio y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

E. El Encargado de Seguridad de la Información participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Encargado de Seguridad de la Información cumplirán las siguientes funciones:
   - Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Municipio.
   - Evaluar los riesgos para determinar el impacto de dichas interrupciones.
   - Identificar los controles preventivos.
   - Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Municipio.
   - Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Municipio.

15.1. Continuidad de las Actividades y Análisis de los Impactos

Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la Municipalidad que contemple los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
- Identificar los controles preventivos.

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Encargado de Seguridad de la Información, considerando todos los procesos de las actividades de la Municipalidad y no limitándose a los equipos computacionales municipales.

15.2. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Municipio

Los propietarios de procesos y recursos de información, con la asistencia del Encargado de Seguridad de la Información, elaborarán los planes de contingencia necesarios para

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

garantizar la continuidad de las actividades de la Municipalidad.

15.3. Marco para la Planificación de la Continuidad de las Actividades del Municipio

Se mantendrá un solo marco para los planes de continuidad de las actividades del Municipio, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

16. Cumplimiento

Son sus objetivos:

A. Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Municipalidad y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
B. Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Municipalidad.
C. Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
D. Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
E. Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
F. Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Municipalidad.

16.1. Cumplimiento de Requisitos Legales

16.1.1. Identificación de la Legislación Aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

16.1.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

16.1.2.1 Derecho de Propiedad Intelectual del Software

- El Encargado de Seguridad de la Información, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:
- Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
- Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
- Mantener un adecuado registro de activos.
- Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
- Verificar que sólo se instalen productos con licencia y software autorizado.
- Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
- Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
- Utilizar herramientas de auditoría adecuadas.
- Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

16.1.3. Protección de los Registros de la Municipalidad

Los registros críticos del Municipio se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la Municipalidad. La destrucción de archivos digitales se llevará a cabo cuando un equipo computacional del inventario haya sido de baja mediante el correspondiente informe y certificado por la unidad requirente, para la destrucción de datos se llevará a cabo un formateo en baja densidad y eliminación de particiones para asegurar su total borrado.

16.1.4. Protección de Datos y Privacidad de la Información Personal

Todos los funcionarios deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

16.1.5.Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Municipio se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido. Todos los funcionarios deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

16.1.6. Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha Firma y su reglamento, el Decreto Supremo Nº181/2002, que establecen las condiciones bajo las cuales una firma digital es legalmente válida.

16.1.7. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

16.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

16.2.1. Cumplimiento de las Políticas de Seguridad

Cada directivo de departamento, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

El Encargado de Seguridad de la Información, realizará revisiones periódicas de todas las áreas del Municipio a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

A. Sistemas de información.
B. Proveedores de sistemas.
C. Propietarios de la Información.
D. Funcionarios Municipales.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

16.2.2. Verificación de la Compatibilidad Técnica

El Encargado de Seguridad de la Información verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

16.3. Consideraciones de Auditorías de Sistemas

16.3.1. Controles de Auditoría de Sistemas

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

16.3.2. Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido. Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas por la Contraloría General de la República.

17. Puesto de trabajo seguro y escritorio limpio

Será responsabilidad de los funcionarios de la Municipalidad de Retiro, cumplir con los requisitos y procedimientos de seguridad definidos para proteger el equipamiento desatendido y evitar así los accesos no autorizados a la información propiedad de la municipalidad. Para tales efectos se establecen como normas de obligado cumplimiento las siguientes:

a) Los documentos que contengan información sensible o confidencial permanecerán guardados bajo llave cuando no estén siendo utilizados, especialmente si el usuario no se encuentra en su puesto de trabajo.

b) Todas las estaciones de trabajo dispondrán de control de acceso mediante Usuario y contraseña, y mecanismos de bloqueo automático tras un período de inactividad del sistema.

c) Cuando el Usuario se ausente de su puesto de trabajo, deberá bloquear su terminal mediante Windows + L, o bien apagarlo directamente.

d) Los buzones de correo convencional, y fotocopiadoras nunca deben quedar desatendidos sino poseen algún tipo de protección.

e) La información impresa deberá ser recogida inmediatamente de las impresoras, una vez haya sido enviada a las mismas.

f) Al terminar la jornada laboral, el usuario deberá recopilar y asegurar el material confidencial, cerrar con llave cajones y oficinas, y desconectar todos los dispositivos y terminales que no vayan a ser utilizados, el equipo computacional deberá quedar siempre apagado al finalizar la jornada laboral.

9) No deberán quedar a la vista: nombres de Usuario, contraseñas, direcciones IP, directorios, contratos, números de cuenta, datos de funcionarios, impresiones y, en general, todo aquello que contenga información municipal.

MUNICIPALIDAD DE RETIRO SECRETARIO MUNICIPAL

h) Deberá promoverse la práctica de escritorio limpio. (D.S. 83 Art. 18),

18. Difusión.

Esta Política será difundida, de acuerdo a protocolos de información a cada Departamento y el Encargado de Seguridad de la Información gestionará su publicación y actualización en la página web institucional.

19. Denuncias y notificaciones.

Los funcionarios de la Municipalidad de Retiro, sus proveedores o terceros deben notificar toda debilidad, incidente o evento asociado a actividades no permitidas o malas prácticas de acceso que pudieran derivar en un posible incumplimiento, uso indebido u otra situación asociada, inmediatamente, al correo seguridad.informacion@retiro.cl.

20.-Control de cambios.

Versión	Fecha	Principales Puntos	Resumen de las Modificaciones
0			

ANÓTESE, REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE.

I. MUNICIPALIDAD DE RETIRO
DIRECTOR ADM. Y FINANZAS

I. MUNICIPALIDAD DE RETIRO
ALCALDE

RODRIGO RAMIREZ PARRA
Alcalde

JIMENA IBAÑEZ IBAÑEZ
Director(s) Depto. Adm. y Finanzas

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL

GERARDO BAYER TORRES
Secretario Municipal

DISTRIBUCIÓN
Alcaldía /Secretaria Municipal/ Unidad de Control/ Administración/ Secretaria de Planificación/ Desarrollo Comunitario/ Departamento de Obras/ Departamento de Transito/Informática/ Archivo Depto. Adm. y Finanzas. /
RRP/JII/GBT/jii

I. MUNICIPALIDAD DE RETIRO
SECRETARIO MUNICIPAL