Ilustre
Municipalidad
de Punta Arenas

ILUSTRE MUNICIPALIDAD DE PUNTA ARENAS
AVDA INDEPENDENCIA Nº820 – 2 do. PISO
TELÉFONO N° 61 2200368 – SERVICIOS GENERALES

PUNTA ARENAS, 22 SEP 2023

NUM. 2788 **.- (SECCIÓN "B") VISTOS:**

1. Lo dispuesto en el D.S N°83, de 2005, de MINSEGPRES, que aprueba norma técnica para los órganos de la administración del Estado sobre la seguridad y confidencialidad de los documentos electrónicos, la norma chilena NCh-ISO 27001:2013, sobre Sistema de Gestión de Seguridad de la Información, la resolución N° 1600 de 2008, deja, Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón;
2. Las facultades que confiere la Ley N° 18.695, Orgánica Constitucional de Municipalidades y sus posteriores modificaciones;
3. Decreto Alcaldicio (Sección "D") N°1779 de 21 de septiembre y Decreto Alcaldicio (Sección "D") N°1652 de 31 de agosto de 2023;

CONSIDERANDO:

1. Que toda municipalidad que maneja sistemas de información debe resguardar y proteger su información de las personas y entidades con que se relaciona, que se deriva en la necesidad de establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información electrónica.

2. Que el D.S. N°83, de 2005, de MINSEGPRES, en sus artículos 7, 9 y 11 dispone la obligatoriedad de elaborar políticas de seguridad, y establece las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los órganos de la Administración del Estado, con la finalidad de garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico; facilitar la relación electrónica entre los órganos de la Administración del Estado y entre éstos y la ciudadanía y el sector privado en general como salvaguardar el uso del documento electrónico de manera segura, confiable y en pleno respeto a la normativa vigente sobre confidencialidad de la información intercambiada.

3. Los documentos electrónicos constituyen un activo para la entidad que los obtiene, ya que la información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.

4. La necesidad liderada por parte de un Encargado de Seguridad de la Información y un Comité de Seguridad de la Información que permita, crear y revisar frecuentemente la Política General de Seguridad de la Información para la Ilustre Municipalidad de Punta Arenas.

DECRETO:

APRUÉBESE, LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DE LA I. MUNICIPALIDAD DE PUNTA ARENAS, la que se detalla a continuación:

I. MUNICIPALIDAD DE PUNTA ARENAS
SECRETARIA MUNICIPAL

POLITICAS DE SEGURIDAD DE LA INFORMACION

INDICE

1. INTRODUCCION 5

2. POLITICAS DE SEGURIDAD DE LA INFORMACION 7

3. ORGANIZACION DE LA SEGURIDAD 11

3.1 INFRAESTRUCTURA DE LA SEGURIDAD DE LA INFORMACIÓN 12
3.1.1 Comité de Seguridad de la Información 12
3.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información 12
3.1.3 Proceso de Autorización para Instalaciones de Procesamiento de Información 12
3.1.4 Asesoramiento Especializado en Materia de Seguridad de la Información 12
3.1.5 Revisión Independiente de la Seguridad de la Información 13
3.2 SEGURIDAD FRENTE AL ACCESO POR PARTE DE TERCEROS 13
3.2.1 Identificación de Riesgos del Acceso de Terceras Partes 13
3.2.2 Requerimientos de Seguridad en Contratos o Acuerdos con Terceros 13
3.3 TERCERIZACIÓN / EXTERNALIZACIÓN / OUTSOURCING 13
3.3.1 Requerimientos de Seguridad en Contratos de Tercerización 13

4. CLASIFICACION Y CONTROL DE ACTIVOS 14

4.1 POLÍTICA DE INVENTARIO DE ACTIVOS 14
4.1.1 Inventario de activos 14
4.1.2 Clasificación de la información 15
4.1.2.1 Confidencialidad 15
4.1.2.2 Integridad 15
4.1.2.3 Disponibilidad 15
4.2 ROTULADO DE LA INFORMACIÓN 16
4.3 DESATENCIÓN DE EQUIPOS INFORMÁTICOS 16
4.4 CAMBIO O ACTUALIZACIÓN DE EQUIPO COMPUTACIONAL 17

5. SEGURIDAD DEL PERSONAL 18

5.1 POLÍTICA SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y EL PERSONAL 19
5.1.1 Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos 19
5.1.1.1 Incorporación de la Seguridad en los Puestos de Trabajo 19
5.1.1.2 Control y Política del Personal 19
5.1.1.3 Compromiso de Confidencialidad 19
5.1.1.4 Términos y Condiciones de Empleo 19
5.1.2 Capacitación del Funcionario 20
5.1.2.1 Formación y Capacitación en Materia de Seguridad de la Información 20
5.1.3 Respuesta a Incidentes y Anomalías en Materia de Seguridad 20
5.1.3.1 Comunicación de Incidentes Relativos a la Seguridad 20
5.1.3.2 Comunicación de Debilidades en Materia de Seguridad 21
5.1.3.3 Comunicación de Anomalías del Software 21
5.1.3.4 Aprendiendo de los Incidentes 21

6. SEGURIDAD FISICA Y AMBIENTAL 22

6.1 POLÍTICA SOBRE SEGURIDAD FÍSICA 23
6.1.1 Perímetro de Seguridad Física 23
6.1.2 Controles de Acceso Físico 23
6.1.3 Protección de Oficinas, Recintos e Instalaciones 23
6.1.4 Ubicación y Protección del Equipamiento y Copias de Seguridad 24
6.1.5 Mantenimiento de Equipos 24
6.1.6 Políticas de Escritorios y Pantallas Limpias 25
6.1.7 Retiro de los Bienes 25

7. GESTION DE COMUNICACIONES Y OPERACIONES 26

7.1 MANEJO DE SOFTWARE Y CONFIGURACIONES PREDETERMINADAS 27
7.1.1 Instalación Estándar de los Equipos Computacionales 27
7.1.2 Instalación de Software que no es estándar 27
7.1.3 Sanciones por Incumplimiento de Procedimiento 28

7.1.4 Protección Contra Software Malicioso 28
7.1.5 Mantenimiento 28
7.1.5.1 Resguardo de la Información 28
7.1.6 Administración de la Red 30
7.1.6.1 Controles de Redes 30
7.1.7 Administración de Medios Informáticos Removibles 30
7.1.7.1 Eliminación de Medios de Información 31
7.1.8 Respaldo de la Información 31
7.1.8.1 Selección de Respaldos 31
7.1.8.2 Periodicidad de Respaldos 32
7.1.8.3 Seguridad del Correo Electrónico 32
7.2 ADMINISTRACIÓN DE LA RED 33
7.2.1 Controles de Redes 33
7.3 CONTROL DE CAMBIOS Y SEPARACIÓN DE FUNCIONES 33
7.3.1 Control de cambios en las operaciones 33
7.3.2 Procedimientos de Manejo de Incidentes 34
7.3.3 Separación de Funciones 34
8. CONTROL DE ACCESOS 35
8.1 ADMINISTRACIÓN DE ACCESOS DE FUNCIONARIOS 37
8.1.1 Registro de nuevos Funcionarios 37
8.1.2 Administración de Privilegios 37
8.1.3 Administración de Contraseñas de Funcionarios 37
8.1.4 Administración de Contraseñas Críticas 37
8.1.5 Revisión de Derechos de Acceso de Funcionarios 38
8.2 RESPONSABILIDADES DEL FUNCIONARIO 38
8.2.1 Uso de Contraseñas 38
8.3 CONTROL DE ACCESO A LA RED 38
8.3.1 Política de Utilización de los Servicios de Red 38
8.3.2 Autenticación de Funcionarios para Conexiones Externas 38
8.3.3 Autenticación de Nodos 38
8.3.4 Subdivisión de Redes 38
8.3.5 Acceso a Internet 39
8.3.6 Control de Ruteo de Red 39
8.4 CONTROL DE ACCESO AL SISTEMA OPERATIVO 39
8.4.1 Identificación Automática de Equipos 39
8.4.2 Sistema de Administración de Contraseñas 39
8.4.3 Uso de Utilitarios de Sistema 39
8.4.4 Alarmas Silenciosas para la Protección de los Funcionarios 40
8.4.5 Suspensión de equipos por Tiempo Muerto 40
8.4.6 Subdivisión de Redes 40
8.4.7 Acceso a Internet 40
8.4.8 Control de Conexión a la Red 41
8.4.9 Control de Ruteo de Red 41
8.4.10 Seguridad de los Servicios de Red 41
8.5 CONTROL DE ACCESO A LAS APLICACIONES 41
8.5.1 Restricción del Acceso a la Información 41
8.5.2 Aislamiento de los Sistemas Sensibles 42
8.6 MONITOREO DEL ACCESO Y USO DE LOS SISTEMAS 42
8.6.1 Registro de Eventos 42
8.6.2 Monitoreo del Uso de los Sistemas 42
8.6.2.1 Procedimientos y Áreas de Riesgo 42
8.6.2.2 Factores de Riesgo 42
8.7 POLÍTICA SOBRE EL CUMPLIMIENTO DE REQUISITOS LEGALES 42
8.7.1 Cumplimiento de requisitos legales. 42
9. DESARROLLO Y MANTENIMIENTO DE SISTEMAS 44
9.1 REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS 45
9.1.1 Análisis y Especificaciones de los Requerimientos de Seguridad 45
9.2 CONTROLES CRIPTOGRÁFICOS 45

9.2.1 Política de Utilización de Controles Criptográficos 45
9.2.2 Cifrado 45
9.2.3 Firma Digital 45
9.2.4 Servicios de No Repudio 45
9.3 SEGURIDAD DE LOS PROCESOS DE SOPORTE 45
9.3.1 Revisión Técnica de los Cambios en el Sistema Operativo 45
9.3.2 Restricción del Cambio de Paquetes de Software 46
9.3.3 Canales Ocultos y Código Malicioso 46
9.3.4 Desarrollo Externo de Software 46

10. GESTION DE LA CONTINUIDAD DE LA MUNICIPALIDAD 47

10.1 CONTINUIDAD DE LAS ACTIVIDADES Y ANÁLISIS DE LOS IMPACTOS 48
10.2 ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES DE CONTINUIDAD DE LAS ACTIVIDADES DEL MUNICIPIO 48
10.3 MARCO PARA LA PLANIFICACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL MUNICIPIO 49

11. CUMPLIMIENTOS 50

11.1 CUMPLIMIENTO DE REQUISITOS LEGALES 51
11.1.1 Identificación de la Legislación Aplicable 51
11.1.2 Derechos de Propiedad Intelectual 51
11.1.2.1 Derecho de Propiedad Intelectual del Software 51
11.1.3 Protección de los Registros de la Municipalidad 51
11.1.4 Protección de Datos y Privacidad de la Información Personal 51
11.1.5 Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información 51
11.1.6 Regulación de Controles para el Uso de Criptografía 52
11.1.7 Recolección de Evidencia 52
11.2 REVISIONES DE LA POLÍTICA DE SEGURIDAD Y LA COMPATIBILIDAD TÉCNICA 52
11.2.1 Cumplimiento de las Políticas de Seguridad 52
11.2.2 Verificación de la Compatibilidad Técnica 52
11.3 CONSIDERACIONES DE AUDITORÍAS DE SISTEMAS 52
11.3.1 Controles de Auditoría de Sistemas 52
11.3.2 Protección de los Elementos Utilizados por la Auditoría de Sistemas 52
11.4 SANCIONES PREVISTAS POR INCUMPLIMIENTO 53

12. POLÍTICA DE TRABAJO A DISTANCIA Y TELETRABAJO 54

12.1 TRABAJO A DISTANCIA Y TELETRABAJO 55

13. POLÍTICA DE DESTRUCCIÓN DE LA INFORMACIÓN 62

13.1 CRITERIOS APLICABLES 63
13.2 ORGANIZACIÓN DE DOCUMENTOS 64
13.3 PARA LA CONSERVACIÓN DE DOCUMENTOS EN SOPORTE PAPEL 64
13.4 DIGITALIZACIÓN DOCUMENTAL O MICROFORMA DE LOS DOCUMENTOS OFICIALES. 65
13.5 DE LA DIGITALIZACIÓN DE DOCUMENTOS NO OFICIALES 66
13.6 CONSERVACIÓN Y USO DE LAS MICROFORMAS 67
13.7 DESTRUCCIÓN DE DOCUMENTOS OFICIALES 68
13.8 DESTRUCCIÓN DE DOCUMENTOS NO OFICIALES 68
13.9 PROCEDIMIENTO PARA LA DESTRUCCIÓN DE DOCUMENTOS 68
13.10 SITUACIONES ESPECIALES EN QUE NO SE DEBE DESTRUIR DOCUMENTACIÓN 69

14. PROCEDIMIENTOS 72

15. ANEXOS 73

1. INTRODUCCION

En atención al proceso de mejoramiento de los servicios de este municipio, tendiente a avanzar hacia la eficiencia al servicio de la comunidad, el Departamento de Informática y Sistemas de Comunicaciones debe enfocarse hacia la gestión de sus procesos orientándose hacia la visión de la Municipalidad.

Dado lo anterior y producto de los cambios, tanto en infraestructura tecnológica, como en la forma en que se entregan los servicios relacionados con tecnología al interior del Municipio, ha sido necesario adecuar las normas que regulan el uso de los recursos del servicio de manera de establecer de forma clara las condiciones y políticas de su uso.

Las tecnologías de la información y las comunicaciones (TIC) contribuyen a optimizar y elevar los niveles de productividad y eficiencia, correspondiéndole a el Departamento de informática velar porque dichas tecnologías se integren a los procesos y actividades del servicio de manera tal de brindar al usuario el máximo apoyo en cuanto a su gestión y que este tenga a disposición todas las herramientas y facilidades que otorgan las plataformas, haciendo necesario que todos los usuarios conozcan de forma clara y precisa, por un lado las normas que regulan su uso y por otro los procedimientos y mecanismos establecidos para asistencia.

La información es un recurso importante, que tiene valor para los procesos que realiza diariamente 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 de Punta Arenas.

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 debe contarse con el compromiso de todos los funcionarios municipales para contribuir con la difusión, conocimiento e integración.

Como consecuencia a lo expuesto previamente, la Ilustre Municipalidad de Punta Arenas integrara mediante este manual, como una de sus tareas esenciales, la creación e implementación de Políticas de Seguridad de la Información, basándose en las características de varias fuentes de documentación al respecto.

En la actualidad la información es uno de los activos más importantes y preciados, es por esta razón que se invierte a nivel mundial gran cantidad de otros recursos (profesionales, tecnológicos, económicos, etc.) para protegerla, pero ¿es solo la protección de ella la que debe preocuparnos? La respuesta es no, existen otros factores igual de importantes que considerar, como, por ejemplo: la oportunidad, integridad, validez o contabilidad, de lo anterior surge la necesidad entonces de "Asegurar" el conjunto elementos que dan su valor.

La información puede existir de muchas formas, puede ser impresa, escrita, o almacenada o transmitida electrónicamente. Cualquier forma que tome o los dispositivos por los cuales es compartida o almacenada, siempre deberán estar sujetos al mismo cuidado.

La seguridad de la información se caracteriza aquí como la preservación de:

b) Confidencialidad: asegurar que la información sea accesible sólo por aquellos usuarios autorizados para tener acceso;

c) Integridad: salvaguardar que la información y los métodos de procesamiento sean exactos y completos;

d) Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información y bienes asociados cuando lo requieran.

La seguridad de la información se logra mediante la implementación de un adecuado conjunto de controles, los que podrían ser políticas, prácticas, procedimientos, estructuras Organizacionales y funciones. Es por lo anteriormente expuesto que en el siguiente documento se establecen los procedimientos y mecanismos básicos de resguardo de la información de la I. Municipalidad de Punta Arenas.

Leyes, bases y normas técnicas en que se basa este Manual.

- Norma chilena NCh-ISO 27002-2009.
- Ley 17.336 sobre Propiedad Intelectual.
- Ley 19.628 sobre documentos Protección de la Vida Privada.
- Ley 19.799 sobre documentos electrónicos, firma electrónica y los servicios de certificación de dicha firma.
- Ley 19.880 sobre procedimientos administrativos que rigen los actos de los órganos de la administración del estado.
- Ley 19223 Delitos Informáticos.
- Ley 20.285 sobre acceso a la información pública.
- Instructivo Presidencial N° 008 – 2006 sobre Transparencia Activa y Publicidad de la Información de la Administración del Estado.
- Instructivo Presidencial N° 005 de Gobierno Electrónico.
- Decreto Supremo 100/2006 - Ministerio Secretaría General de la Presidencia sobre el desarrollo de sitios web de los órganos de la administración del estado.
- Decreto Supremo 93/2006 - Ministerio Secretaría General de la Presidencia sobre la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios.
- Decreto Supremo 83/2004 - Ministerio Secretaría General de la Presidencia sobre la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo 81/2004 - Ministerio Secretaria General de la Presidencia sobre interoperabilidad de documentos electrónicos.
- Decreto Supremo 77/2004 - Ministerio Secretaría General de la Presidencia sobre eficiencia de las comunicaciones electrónicas entre órganos de la administración del estado y entre estos y los ciudadanos
- Decreto Supremo 14/2014 - Ministerio Secretaria General de la Presidencia sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.
- Reglamento de la Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma
- Manual sobre Procedimiento Administrativo Ley 19.880

2. POLITICAS DE SEGURIDAD DE LA INFORMACION

a) Alcance

Debe ser conocida y cumplida por todos los funcionarios de la Municipalidad de Punta Arenas, cualquiera sea su relación contractual, y sea cual fuere su nivel jerárquico.

Esta política se aplica en todo el ámbito de la Municipalidad, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

b) Términos y Definiciones

A los efectos de este documento se aplican las siguientes definiciones:

i. Seguridad de la Información

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

Confidencialidad; se garantiza 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 funcionarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad; busca asegurar 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.

Auditabilidad; define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió

Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: 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.

Tecnología de la Información: Se refiere al hardware y software operados por la Municipalidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Municipalidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

ii. Evaluación de Riesgos.

Se entiende por evaluación de riesgos a la evaluación de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, la probabilidad de que ocurran y su potencial impacto en la operatoria de la Municipalidad.

iii. Administración de Riesgos.

Se entiende por administración de riesgos al proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a la información. Dicho proceso es cíclico y debe llevarse a cabo en forma periódica.

iv. Comité de Seguridad de la Información.

El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Municipio, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

v. Responsable de Seguridad Informática.

Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes de la Municipalidad que así lo requieran.

vi. Incidente de Seguridad.

Un incidente de seguridad es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

c) Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Municipio y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos.

Es importante que los principios de la Política de Seguridad sean parte de la cultura municipal, para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades y de los titulares de Unidades Municipales para la difusión, consolidación y cumplimiento de la presente Política.

d) Objetivo

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 la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

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. Mantener la Política de Seguridad de la Municipalidad actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

e) Responsabilidad

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Municipalidad, cualquiera sea su situación de contrato, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

El Alcalde, es la autoridad que aprueba esta Política (y sus respectivas modificaciones), asesorado por el comité de Seguridad de la Información.

El Comité de Seguridad de la Información de la Municipalidad, procederá a revisar y proponer a la máxima autoridad de la Municipalidad de Punta Arenas para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información, monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes, tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad, aprobar las principales iniciativas para incrementar la seguridad de la información , de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información, garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, promover la difusión y apoyo a la seguridad de la información dentro de la Municipalidad y coordinar el proceso de administración de la continuidad de las actividades de la Municipalidad.

Los contenidos de esta política de seguridad serán reevaluados a lo menos cada dos (2) años, incorporando las modificaciones que correspondan.

El comité se deberá reunirse a lo menos una vez al año para efectuar revisiones respecto al estado y aplicación de la política de seguridad.

El Coordinador del Comité de Seguridad de la Información, será el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento de la presente Política.

El Responsable de Seguridad Informática y el Coordinador del Comité de Seguridad de la Información cumplirán funciones relativas a la seguridad de los sistemas de información de la Municipalidad de Punta Arenas, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política. Los Propietarios de la Información son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué funcionarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El responsable de la Dirección de Gestión de Personas o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa al Municipio a cumplir obligaciones, comunicándole respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continúan en materia de seguridad.

Adicionalmente, la Dirección de Gestión de Personas, deberá informar al jefe del Departamento de Informática y Sistemas de Comunicaciones o quien lo subrogue del personal que ingresa al Municipio de Punta Arenas, con el objetivo de proceder con la preparación del equipamiento a utilizar si lo requiriese.

El jefe del Departamento de Informática y Sistemas de Comunicaciones cumplirá la función de generar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de sistemas y recursos de tecnología de la Municipalidad de Punta Arenas. Por otra parte, tendrá la función de coordinar las tareas de desarrollo y mantenimiento de sistemas, siguiendo una metodología de ciclo de vida de sistemas apropiada, y que contemple la inclusión de medidas de seguridad en los sistemas informáticos.

El Director de Asesoría Jurídica o a quien asigne verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos u otra documentación de la Municipalidad de Punta Arenas con sus funcionarios y con terceros. Asimismo, asesorará en materia legal al Organismo, en lo que se refiere a la seguridad de la información.

Los funcionarios que hacen uso de la información y de los sistemas utilizados para su procesamiento, son responsables de conocer, dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente. La Dirección de Control, o en su defecto quien sea propuesto por el Comité de Seguridad de la Información es responsable de practicar auditorias periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta Política y por las normas, procedimientos y prácticas que de ella surjan.

3. ORGANIZACION DE LA SEGURIDAD

a) Generalidades

La presente Política de Seguridad establece la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la Municipalidad.

Por ello, se definirá formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades. Asimismo, se contemplará la necesidad de disponer de fuentes con conocimiento y experimentadas para el asesoramiento, cooperación y colaboración en materia de seguridad de la información. Por otro lado, debe tenerse en cuenta que ciertas actividades de la Municipalidad pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información.

En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

b) Objetivo

Administrar la seguridad de la información dentro de la Municipalidad de Punta Arenas y establecer un marco para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la Municipalidad de Punta Arenas.

c) Alcance

Esta Política se aplica a todos los recursos de la Municipalidad de Punta Arenas y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

d) Responsabilidad

El Coordinador del Comité de Seguridad de la Información será el responsable de impulsar la implementación de la presente Política.

El Comité de Seguridad de la Información tendrá a cargo el mantenimiento y la presentación para la aprobación de la presente Política, ante el alcalde de la Municipalidad de Punta Arenas, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

El responsable de seguridad Informática asistirá al personal de la Municipalidad en materia de seguridad de la información y coordinará la interacción con organismos especializados.

Asimismo, junto con los propietarios de la información, analizará el riesgo de los accesos de terceros a la información de la Municipalidad de Punta Arenas y verificará la aplicación de las medidas de seguridad necesarias para la protección de la misma.

Los directores de las direcciones Municipales cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

La Dirección de Control Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información será responsable de realizar revisiones independientes sobre la vigencia y el cumplimiento de la presente Política.

3.1 Infraestructura de la Seguridad de la Información

3.1.1 Comité de Seguridad de la Información

La seguridad de la información es una responsabilidad de la Municipalidad de Punta Arenas, compartida por todas las Autoridades políticas, Directores y jefaturas, sin distinción del estado contractual que posean, por lo cual se creará el Comité de Seguridad de la Información destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad. El mismo contará con un Coordinador, quien cumplirá la función de impulsar la implementación de la presente Política.

3.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información

El Sr. Alcalde asigna las funciones de la Seguridad Informática al jefe del Departamento de Informática y Sistemas de Comunicaciones, quien encomendará a un funcionario del mismo departamento como el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la Municipalidad de Punta Arenas, lo cual incluye la supervisión de todos sus aspectos inherentes tratados en la presente Política.

El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación la definición y asignación de las responsabilidades que surjan del presente Modelo.

3.1.3 Proceso de Autorización para Instalaciones de Procesamiento de Información

Los nuevos recursos de procesamiento de información serán autorizados por los responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas de la Municipalidad de Punta Arenas.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso está Prohibido.

3.1.4 Asesoramiento Especializado en Materia de Seguridad de la Información

El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles en el Organismo a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos, privados o públicos, pudiendo en casos justificados adquirir asesoría vía contratación, de la capacidad a empresas o personas debidamente acreditadas.

Encargado de Seguridad de la Información 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 que corresponda 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.

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.

El Responsable de Seguridad Informática 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.

3.1.5 Revisión Independiente de la Seguridad de la Información

La Dirección de Control o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas de la Municipalidad de Punta Arenas, reflejan adecuadamente sus disposiciones.

3.2 Seguridad Frente al Acceso por Parte de Terceros

3.2.1 Identificación de Riesgos del Acceso de Terceras Partes

Cuando exista la necesidad de otorgar acceso a terceras partes a información de la Municipalidad de Punta Arenas, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos.

3.2.2 Requerimientos de Seguridad en Contratos o Acuerdos con Terceros

Se revisarán los contratos o acuerdos existentes.

3.3 Tercerización / Externalización / Outsourcing

3.3.1 Requerimientos de Seguridad en Contratos de Tercerización

Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC de la Municipalidad de Punta Arenas, contemplarán además de los puntos especificados en "Requerimientos de Seguridad en Contratos o Acuerdos con Terceros".

4. CLASIFICACION Y CONTROL DE ACTIVOS

a) Generalidades

El Municipio debe tener un acabado conocimiento sobre los activos que posee como parte importante de la administración de riesgos, entre algunos están;

Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de funcionario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc.

Recursos de software: software de aplicaciones, sistemas operativos, herramientas de desarrollo, utilitarios, etc.

Activos físicos: equipamiento informático (monitores, computadoras portátiles), equipos de comunicaciones (routers, PABXs) y otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado), mobiliario, lugares de emplazamiento, etc.

Servicios: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo con la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

b) Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección.
Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

c) Alcance

Esta Política se aplica a toda la información administrada en el Municipio de Punta Arenas, cualquiera sea el soporte en que se encuentre.

d) Responsabilidad

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática 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.

Cada Propietario 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.

4.1 Política de Inventario de Activos

4.1.1 Inventario de activos

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 12 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es la sección de Inventario de la Municipalidad de Punta Arenas por medio del sistema de activo Fijo a partir del control de los activos propuesto por el Departamento de informática y Sistemas de Comunicaciones.

4.1.2 Clasificación de la información

Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad.

A continuación se establece el criterio de clasificación de la información en función a cada una de las mencionadas características:

4.1.2.1 Confidencialidad

0 PUBLICO:
Información que puede ser conocida y utilizada sin autorización por cualquier persona, sea empleado de la Organización o no.

1 RESERVADA - USO INTERNO:
Información que puede ser conocida y utilizada por todos los empleados de la Organización y algunas entidades externas debidamente autorizadas, y cuya divulgación o uso no autorizados podría ocasionar riesgos o pérdidas leves para el Organismo, o terceros.

2 RESERVADA- CONFIDENCIAL:
Información que sólo puede ser conocida y utilizada por un grupo de empleados, que la necesiten para realizar su trabajo, y cuya divulgación o uso no autorizados podría ocasionar pérdidas significativas al Organismo o a terceros.

3 RESERVADA SECRETA:
Información que sólo puede ser conocida y utilizada por un grupo muy reducido de empleados, generalmente de la alta dirección de la Organización, y cuya divulgación o uso no autorizados podría ocasionar pérdidas graves al mismo, al Sector Público o a terceros.

4.1.2.2 Integridad

0 Información cuya modificación no autorizada puede repararse fácilmente, o no afecta la operatoria de la Organización.
1 Información cuya modificación no autorizada puede repararse aunque podría ocasionar pérdidas leves para el Organismo o terceros.
2 Información cuya modificación no autorizada es de difícil reparación y podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.
3 Información cuya modificación no autorizada no podría repararse, ocasionando pérdidas graves al Organismo, al Sector Público Nacional o a terceros.

4.1.2.3 Disponibilidad

0 información cuya inaccesibilidad no afecta la operatoria de la Organización.
1 información cuya inaccesibilidad permanente durante una semana podría ocasionar pérdidas significativas para el Organismo, el Sector Público Nacional o terceros.

2 información cuya inaccesibilidad permanente durante un día podría ocasionar pérdidas significativas al Organismo o a terceros.
3 información cuya inaccesibilidad permanente durante una hora podría ocasionar pérdidas significativas al Organismo o a terceros.

Al referirse a pérdidas, se contemplan aquellas medibles (materiales) y no medibles (imagen, valor estratégico de la información, obligaciones contractuales o públicas, disposiciones legales, etc.).

Se asignará a la información un valor por cada uno de estos criterios. Luego, se clasificará la información en una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 1.
CRITICIDAD MEDIA: alguno de los valores asignados es 2
CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el Propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos:

- Asignarle una fecha de efectividad.
- Comunicárselo al depositario del recurso.
- Realizar los cambios necesarios para que los Usuarios conozcan la nueva clasificación.

Luego de clasificada la información, el propietario de la misma identificará los recursos asociados (sistemas, equipamiento, servicios, etc.) *y* los perfiles funcionales que deberán tener acceso a la misma.

En adelante se mencionará como "información clasificada" (o "datos clasificados") a aquella que se encuadre en los niveles 1, 2 o 3 de Confidencialidad.

4.2 Rotulado de la Información

Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

- Copia
- Almacenamiento;
- Transmisión por correo, correo electrónico;
- Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.)

Este rotulado de la información se puede realizar bajo este esquema:

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

4.3 Desatención de Equipos Informáticos

Todo equipo computacional que no reúna las condiciones mínimas de uso y características técnicas será dado de baja y desatendido, previo a eso se realizará un respaldo para asegurar los datos.

Todos los equipos desatendidos deben de ser transferidos a la Bodega Municipal, para su almacenaje, así como también, se debe de dar el aviso a la Dirección de Administración y Finanzas, para que realice el cambio en el Activo Fijo Municipal.

4.4 Cambio o Actualización de Equipo Computacional

Se explica el proceso de cambio de equipo computacional, basándose bajo un análisis previo (que puede ser a simple vista del Departamento de Informática y Sistemas de Comunicaciones o por ordenanza escrita, con la consecuencia de que el cambio sea forzado), incluyendo los respaldos de datos de los funcionarios y la posibilidad de dar de baja un equipo la cual está ya desactualizado y no puede seguir las tendencias actuales.

Los respaldos de la información del funcionario tienen dos casos:

- El Departamento de Informática y Sistemas de Comunicaciones realiza el respaldo.
- El funcionario realiza el respaldo (debe de declarar por escrito que la información que respalde está bajo su responsabilidad).

Una vez retirado el equipo computacional, el Director(a) de Servicios Generales puede asesorar al Departamento de Informática y Sistemas de Comunicaciones sobre qué equipo puede entregar al nuevo funcionario, este asesoramiento es opcional, siempre y cuando el nuevo equipo computacional sea bajo la instrucción del Director(a) de Servicios Generales.

Si otra Dirección así lo requiriera, debe canalizar su requerimiento a través del Director(a) de Servicios Generales.

Dentro de este mismo círculo del proceso, se puede verificar que el activo puede ser dado de baja o no, gatillando un nuevo procedimiento. El certificado de entrega de equipos computacionales, pueden ser 2 opciones:

- A través de un Acta de Entrega, indicando especificaciones mínimas del equipo computacional a entregar, tales como marca, modelo y número de inventario.
- A través de un certificado emitido por adquisiciones, indicando los mismos datos.

Una vez instalado el equipo computacional, se da aviso al funcionario, indicando las responsabilidades del equipo computacional entregado.

5. SEGURIDAD DEL PERSONAL

a) Generalidades

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos tomando acciones preventivas. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

b) Objetivo

- Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información. Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como funcionario.
- Garantizar que los funcionarios estén al corriente 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 de Punta Arenas en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con todo el personal y funcionarios externos de las instalaciones de procesamiento de información.
- 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

c) Alcance

Esta Política se aplica a todo el personal de la Municipalidad, cualquiera sea su situación de contrato, y al personal externo que efectúe tareas dentro del ámbito de la Municipalidad.

d) Responsabilidad

El Director(a) de Gestión de personas incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los funcionarios, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de funcionarios respecto de la presente Política con el Departamento de Informática y Sistemas de Comunicaciones.

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los funcionarios y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal de la Municipalidad es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

5.1 Política sobre la seguridad de la información y el personal

5.1.1 Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

5.1.1.1 Incorporación de la Seguridad en los Puestos de Trabajo

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política 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.

5.1.1.2 Control y Política del Personal

Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que, a tal efecto, alcanzan al Municipio de Punta Arenas.

5.1.1.3 Compromiso de Confidencialidad

Como parte de sus términos y condiciones iniciales, los funcionarios, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la Municipalidad de Punta Arenas. La copia firmada del Compromiso deberá ser retenida en forma segura por la dirección de Gestión de personas. Asimismo, mediante el Compromiso de Confidencialidad del funcionario declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del funcionario.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre:

a) Suscripción inicial del Compromiso por parte de la totalidad del personal.
b) Revisión del contenido del Compromiso cada año.
c) Método de aprobación en caso de modificación del texto del Compromiso.

5.1.1.4 Términos y Condiciones de Empleo

Los términos y condiciones de empleo establecerán la responsabilidad del funcionario en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la Municipalidad de Punta Arenas y del horario normal de trabajo.

Los derechos y obligaciones del funcionario relativos a la seguridad de la información, por ejemplo, en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo

5.1.2 Capacitación del Funcionario

5.1.2.1 Formación y Capacitación en Materia de Seguridad de la Información

Todos los funcionarios de la Organización y, cuando sea pertinente, los funcionarios externos y los terceros que desempeñen funciones en el Municipio de Punta Arenas, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Organización. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable de la Dirección de Gestión de Personas será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Cada año se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

Las siguientes áreas serán encargadas de producir el material de capacitación

Áreas Responsables del Material de Capacitación;

- Dirección de Gestión de Personas

El personal que ingrese al Municipio recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

5.1.3 Respuesta a Incidentes y Anomalías en Materia de Seguridad

5.1.3.1 Comunicación de Incidentes Relativos a la Seguridad

Los incidentes relativos a la seguridad serán comunicados al jefe del Departamento de Informática y Sistemas de Comunicaciones tan pronto como sea posible.

Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes.

Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Todos los funcionarios y contratistas deben conocer el procedimiento de comunicación de incidentes de seguridad, y deben informar de los mismos tan pronto hayan tomado conocimiento de su ocurrencia.

5.1.3.2 Comunicación de Debilidades en Materia de Seguridad

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

5.1.3.3 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:

A. Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
B. Alertar inmediatamente al Encargado de Seguridad de la Información referente al activo comprometido al cual se presenta la anomalía.
C. Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
D. El encargado de la seguridad responderá por e-mail al o los usuarios el incidente.

5.1.3.4 Aprendiendo de los Incidentes

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.

6. SEGURIDAD FISICA Y AMBIENTAL

a) Generalidades

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones de la Municipalidad de Punta Arenas. Asimismo, se pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

Se distinguen tres conceptos a tener en cuenta: *la protección física de accesos, la protección ambiental y el transporte, protección y mantenimiento de equipamiento y documentación.*

El establecimiento de perímetros de seguridad y áreas protegidas (protección física de accesos) facilita la implementación de controles tendientes a proteger las instalaciones de procesamiento de información crítica o sensible de la Municipalidad de Punta Arenas, de accesos físicos no autorizados.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio. Deben contemplarse tanto los riesgos de las instalaciones de la Municipalidad de Punta Arenas, como en instalaciones próximas a la sede del mismo que pueda interferir con las actividades.

La información almacenada en los sistemas de procesamiento y la documentación contenida en diferentes medios de almacenamiento, son susceptibles de ser recuperadas mientras no están siendo utilizados. Es por ello que el transporte y la disposición final presentan riesgos que deben ser evaluados.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

b) Objetivo

- Prevenir e impedir accesos no autorizados a instalaciones con información de la Municipalidad.
- Proteger el equipamiento de procesamiento de información crítica de la Municipalidad de Punta Arenas ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad, 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 equipamiento informático que alberga la información de la Municipalidad de Punta Arenas.
- Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
- Proporcionar protección proporcional a los riesgos identificados.

c) Alcance

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la Municipalidad de Punta Arenas tales como instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

d) Responsabilidad

El Responsable de Seguridad Informática definirá junto con el jefe del Departamento de Informática y Sistemas de Comunicaciones, y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos,

controlando su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El jefe del Departamento de Informática y Sistemas de Comunicaciones, asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la Municipalidad de Punta Arenas.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal de la Municipalidad a las áreas restringidas bajo su responsabilidad.

La Dirección de control o en su defecto quien sea propuesto por el Comité de Seguridad de la Información podrá revisar los registros de acceso a las áreas protegidas de todo el personal de la Municipalidad para verificar el cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

6.1 Política sobre seguridad Física

6.1.1 Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de la Municipalidad de Punta Arenas y de las instalaciones de procesamiento de información.

El Organismo utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo, una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

El emplazamiento y la fortaleza de cada barrera estarán definidas por el jefe del Departamento de Informática y Sistemas de Comunicaciones con el asesoramiento del Responsable de Segundad Informática, de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:
a) Definir y documentar claramente el perímetro de seguridad.
b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida.
c) Verificar la existencia de un área de recepción atendida por personal.
d) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real).
e) Identificar claramente todas las puertas de incendio de un perímetro de seguridad

6.1.2 Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el jefe del Departamento de Informática y Sistemas de Comunicaciones, a fin de permitir el acceso sólo al personal autorizado.

6.1.3 Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados

por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y segundad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas.

6.1.4 Ubicación y Protección del Equipamiento y Copias de Seguridad

El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado, teniendo en cuenta los siguientes puntos:

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por:

Amenazas Potenciales

- Robo o hurto
- Incendio
- Explosivos
- Humo
- Inundaciones o filtraciones de agua (o falta de suministro)
- Polvo
- Vibraciones
- Efectos químicos
- Interferencia en el suministro de energía eléctrica (cortes de suministro, variación de tensión)

e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información. Esta revisión se realizará cada: 12 meses.
f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede de la Municipalidad de Punta Arenas.

6.1.5 Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del jefe de Departamento de Informática y Sistemas de Comunicaciones. El Departamento de Informática y Sistemas de Comunicaciones mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

d) Registrar el retiro de equipamiento de la sede de la Municipalidad de Punta Arenas para su mantenimiento.
e) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

6.1.6 Políticas de Escritorios y Pantallas Limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo. Se aplicarán los siguientes lineamientos:

a) Almacenar bajo llave, cuando corresponda, los documentos en papel y los medios informáticos, en gabinetes y/u otro tipo de mobiliario seguro cuando no están siendo utilizados, especialmente fuera del horario de trabajo.
b) Guardar bajo llave la información sensible o crítica de la Municipalidad de Punta Arenas (preferentemente en una caja fuerte o gabinete a prueba de incendios) cuando no está en uso, especialmente cuando no hay personal en la oficina.
c) Desconectar de la red / sistema / servicio las computadoras personales, terminales e impresoras asignadas a funciones críticas, cuando están desatendidas. Las mismas deben ser protegidas mediante cerraduras de seguridad, contraseñas u otros controles cuando no están en uso (como por ejemplo la utilización de protectores de pantalla con contraseña). Los responsables de cada área mantendrán un registro de las contraseñas o copia de las llaves de seguridad utilizadas en el sector a su cargo. Tales elementos se encontrarán protegidos en sobre cerrado o caja de seguridad para impedir accesos no autorizados, debiendo dejarse constancia de todo acceso a las mismas, y de los motivos que llevaron a tal acción.

6.1.7 Retiro de los Bienes

El equipamiento, la información y el software no serán retirados de la sede de la Municipalidad de Punta Arenas sin autorización formal del jefe del Departamento de informática y Sistemas de Comunicaciones o quien el designe para este efecto.

7. GESTION DE COMUNICACIONES Y OPERACIONES

a) Generalidades

La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas. Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas de la Municipalidad de Punta Arenas, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen en el ámbito operativo, a fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa. Los sistemas de información están comunicados entre sí, tanto dentro de la Municipalidad de Punta Arenas como con terceros fuera de él. Por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

Las comunicaciones establecidas permiten el intercambio de información, que deberá estar regulado para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

b) Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

c) Alcance.

Todas las instalaciones de procesamiento y transmisión de información de la Municipalidad de Punta Arenas.

d) Responsabilidad.

El Responsable de Seguridad Informática tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.
- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva. Verificar que dichos procedimientos de aprobación de software incluyan aspectos de segundad para las aplicaciones de Gobierno Electrónico.
- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.
- Definir y documentar una norma clara con respecto al uso del correo electrónico.
- Controlar los mecanismos de distribución y difusión de información dentro del Organismo.
- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la Municipalidad de Punta Arenas.
- Desarrollar procedimientos adecuados de concientización de funcionarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

El jefe del Departamento de Informática y Sistemas de Comunicaciones tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de comunicaciones y operaciones.
- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.
- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.
- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del funcionario.
- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.
- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.
- Desarrollar y verificar el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.
- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.
- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.
- Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el jefe del Departamento de Informática y Sistemas de Comunicaciones, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

7.1 Manejo de Software y Configuraciones Predeterminadas

7.1.1 Instalación Estándar de los Equipos Computacionales

Cada vez que se formatea un equipo computacional, se deben de tomar en cuenta las siguientes consideraciones:

- Sistema Operativo Windows
- Lector de PDF
- Antivirus
- Programa de descompresión de archivos
- Navegadores de Internet
- Microsoft Office
- Sistemas municipales dependiendo de la labor del usuario

7.1.2 Instalación de Software que no es estándar

Para instalar un software que sea específico y que sea relevante para la labor funcionaria, se debe realizar una solicitud por escrito, al Departamento de Informática y Sistemas de Comunicaciones, con la Autorización de su jefatura Directa, y una vez que se ha aprobado y adquirido el licenciamiento por la Municipalidad de Punta Arenas, se procede a verificar que el equipo cumpla con los requisitos, para proceder con su instalación.

7.1.3 Sanciones por Incumplimiento de Procedimiento

Si el funcionario es sorprendido con software instalado sin autorización y/o sin licenciamiento, la responsabilidad recae en el funcionario al cual se le fue asignado dicho equipo y cuando se realice un control de equipos, se desinstalará de su computador sin previo aviso y se informará al Responsable de Seguridad Informática y al jefe del Departamento de Informática y Sistemas de Comunicaciones para su investigación.

Además, si persiste la instalación de software no autorizado, el/los funcionarios se exponen a que se revoquen los accesos a los sistemas informáticos, informando a su superior el uso de este.

7.1.4 Protección Contra Software Malicioso

El responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El jefe del Departamento de Informática y Sistemas de Comunicaciones, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática informara a los funcionarios en materia de seguridad respecto a controles de acceso al sistema y administración de cambios. Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por el Organismo (Ver 11.1.2.1. Derecho de Propiedad Intelectual del Software).
b) Informar el/los procedimientos para evitar los riesgos relacionados con la obtención de archivos y software desde o a través de redes externas, o por cualquier otro medio, señalando las medidas de protección a tomar.
c) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, como medida precautoria y rutinaria.
d) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles (revisar dichas actualizaciones en un entorno de prueba previamente si es que constituyen cambios críticos a los sistemas).
e) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de la Municipalidad, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas.
f) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.
g) Informar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.
h) Concientizar al personal acerca del problema de los falsos virus y de cómo proceder frente a los mismos.

7.1.5 Mantenimiento

7.1.5.1 Resguardo de la Información

El jefe del departamento de Informática y Sistemas de Comunicaciones, junto al Responsable de Seguridad Informática y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

El jefe del Departamento de Informática y Sistemas de Comunicaciones dispondrá y controlará la realización de dichas copias, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software crítico del Organismo. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que

cumplen con los requerimientos de los planes de continuidad de las actividades de la Municipalidad de Punta Arenas.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a) Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas *y* administrarlas debidamente.
b) Establecer un esquema de reemplazo de los medios de almacenamiento de las copias de resguardo, una vez concluida la posibilidad de ser reutilizados, de acuerdo a lo indicado por el proveedor, *y* asegurando la destrucción de los medios desechados. (Ver 7.1.7.1 Eliminación de Medios de Información).
c) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos *y* completos de las mismas *y* los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal. Se deberán retener al menos tres generaciones o ciclos de información de resguardo para la información *y* el software esenciales para el Organismo. Para la definición de información mínima a ser resguardada en el sitio remoto, se deberá tener en cuenta el nivel de clasificación otorgado a la misma, en términos de disponibilidad *y* requisitos legales a los que se encuentre sujeta.
d) Asignar a la información de resguardo un nivel de protección física *y* ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.
e) Probar periódicamente los medios de resguardo.
f) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos. Los procedimientos de realización de copias de resguardo y su almacenamiento deberán respetar las disposiciones del punto 4. Clasificación y Control de Activos y 11.1.3. Protección de los Registros de la Municipalidad de la presente Política.

7.1.6 Administración de la Red

7.1.6.1 Controles de Redes

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos *y* los servicios conectados en las redes de la Municipalidad de Punta Arenas, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "Asignación de Responsabilidades en Materia de Seguridad de la Información".
b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información. El jefe del Departamento de Informática y Sistemas de Comunicaciones implementará dichos controles.

7.1.7 Administración de Medios Informáticos Removibles

El jefe del Departamento de Informática y Sistemas de Comunicaciones, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como discos, dispositivos USB, informes impresos. El cumplimiento de los procedimientos se hará de acuerdo al capítulo 8 - "Control de Accesos". Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.
b) Requerir autorización para retirar cualquier medio de la Municipalidad de Punta Arenas y realizar un control de todos los retiros a fin de mantener un registro de auditoría.
c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores. Se documentarán todos los procedimientos y niveles de autorización, en concordancia con el capítulo 4. Clasificación y Control de Activos.

7.1.7.1 Eliminación de Medios de Información

El jefe del Departamento de Informática y Sistemas de Comunicaciones, junto con el Responsable de Seguridad Informática definirán procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

Los procedimientos deberán considerar que los siguientes elementos requerirán almacenamiento y eliminación segura:

a) Documentos en papel.
b) Voces u otras grabaciones.
c) Papel carbónico.
d) Informes de salida.
e) Cintas de impresora de un solo uso.
f) Cintas magnéticas.
g) Discos o cáseles removibles.
h) Medios de almacenamiento óptico (todos los formatos incluyendo todos los medios de distribución de software del fabricante o proveedor).
i) Listados de programas.
j) Datos de prueba.
k) Documentación del sistema.

Asimismo, se debe considerar que podría ser más eficiente disponer que todos los medios sean recolectados y eliminados de manera segura, antes que intentar separar los ítems sensibles.

7.1.8 Respaldo de la Información

7.1.8.1 Selección de Respaldos

Se establecerá un procedimiento especial para las bases de datos de los servidores, asimismo se realizarán respaldos a los archivos que solicite el Propietario de la Información, también se llevará un registro de los respaldos históricos de base de datos.

Se ha definido que los respaldos de la información se harán en estos casos:

1. Respaldos a la Base de Datos Municipal.
2. Respaldos al funcionario en caso de que se realice un cambio de equipo por reparación o mantenimiento.
3. Respaldos en caso de que un funcionario lo solicite. Bajo este estamento, se respaldarán en un disco duro externo definido por el Área de Computación, también se indica que no se respaldan archivos de música (*.mp3 y similares) y archivos de video que no estén relacionados con las funciones municipales.

7.1.8.2 Periodicidad de Respaldos

Se hará un respaldo diario en un disco duro externo, la cual se realizará a las 18:30 hrs. De cada jornada laboral, y este disco duro externo se almacenará fuera de las dependencias del municipio cuando no se esté cursando la jornada laboral.

También se genera un respaldo en el servidor, de acuerdo al plan de mantenimiento programado por el servidor SQL, este respaldo estará almacenando varios días dependiendo de las capacidades del HDD del servidor, en promedio este HDD puede almacenar 6 días de respaldos.

El Respaldo de las bases de datos históricas del servidor se hará de forma mensual y ese medio de almacenamiento a la cual recaerá esa información se encontrará protegido en una caja fuerte y en Servidor NAS de respaldos.

El respaldo al funcionario es cuando solicite que se le respalde la información en casos que le estime conveniente.

7.1.8.3 Seguridad del Correo Electrónico

7.1.8.3.1 Riesgos de Seguridad

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

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
d) 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.
e) El impacto de un cambio en el medio de comunicación en los procesos de la Municipalidad de Punta Arenas.
f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
g) Las implicancias de la publicación externa de listados de personal, accesibles al público.
h) El acceso de funcionarios remotos a las cuentas de correo electrónico.
i) El uso inadecuado por parte del personal

7.1.8.3.2 Política de Correo Electrónico

El Responsable de Seguridad Informática junto con el jefe del Departamento de Informática y Sistemas de Comunicaciones definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo, virus, intercepción, etc.
b) Protección de archivos adjuntos de correo electrónico.
c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 9.2. Controles Criptográficos).
d) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.

f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del funcionario, etc.).
g) Definición de los alcances del uso del correo electrónico por parte del personal del Organismo.
h) Potestad de la Municipalidad de Punta Arenas para auditar los mensajes recibidos o emitidos por los servidores de la misma, lo cual se incluirá en el "Compromiso de Confidencialidad" (5.1.1.3. Compromiso de Confidencialidad)

Estos dos últimos puntos deben ser leídos a la luz de las normas vigentes que no sólo prohíben a los funcionarios a hacer uso indebido o con fines particulares del patrimonio estatal, sino que también imponen la obligación de usar los bienes y recursos del estado con los fines autorizados y de manera racional, evitando su abuso, derroche o desaprovechamiento (11.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información).

Se debe entender al correo electrónico como una herramienta más de trabajo provista al funcionario a fin de ser utilizada conforme el uso al cual está destinada.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismo debe informar claramente a sus funcionarios:

a) Cuál es el uso que el organismo espera que los funcionarios hagan del correo electrónico provisto por el organismo.
b) En qué condiciones los mensajes pueden ser objeto de control y monitoreo.

7.2 Administración de la Red

7.2.1 Controles de Redes

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la Municipalidad de Punta Arenas, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto "Asignación de Responsabilidades en Materia de Seguridad de la Información".
b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información. El Responsable del Área Informática implementará dichos controles.

7.3 Control de cambios y separación de funciones

7.3.1 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.

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 jefe del Departamento de Informática y Sistemas de Comunicaciones evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

7.3.2 Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a resguardar la información, además se documentarán todos los incidentes 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.

7.3.3 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

8. CONTROL DE ACCESOS

a) Generalidades

El acceso por medio de un sistema de restricciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento. Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los funcionarios de todos los niveles, desde el registro inicial de nuevos funcionarios hasta la privación final de derechos de los funcionarios que ya no requieren el acceso.

La cooperación de los funcionarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

b) Objetivo

- 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.
- Controlar la seguridad en la conexión entre la red de la Municipalidad de Punta Arenas 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.

c) Alcance

La Política definida en este documento se aplicará a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información de la Municipalidad de Punta Arenas, cualquiera sea la función que desempeñe.

Asimismo, se aplicará al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

d) Responsabilidad

El Responsable de Seguridad Informática estará a cargo de:

- Definir normas y procedimientos para: la gestión de accesos a todos los sistemas, bases de datos y servicios de información multifuncionario; el monitoreo del uso de las instalaciones de procesamiento de la información; la solicitud y aprobación de accesos a Internet; el uso de computación móvil, trabajo remoto y reportes de incidentes relacionados; la respuesta a la activación de alarmas silenciosas; la revisión de registros de actividades; y el ajuste de relojes de acuerdo a un estándar preestablecido.
- Definir pautas de utilización de Internet para todos los funcionarios.
- Participar en la definición de normas y procedimientos de seguridad a implementar en el ambiente informático (ej.: sistemas operativos, servicios de red, enrutadores o gateways, etc.) y validarlos periódicamente.

- Controlar la asignación de privilegios a funcionarios.
- Analizar y sugerir medidas a ser implementadas para efectivizar el control de acceso a Internet de los funcionarios.
- Verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos, registración de funcionarios, administración de privilegios, administración de contraseñas, utilización de servicios de red, autenticación de funcionarios y nodos, uso controlado de utilitarios del sistema, alarmas silenciosas, desconexión de terminales por tiempo muerto, limitación del horario de conexión, registro de eventos, protección de puertos, subdivisión de redes, control de conexiones a la red, control de ruteo de red, etc.
- Concientizar a los funcionarios sobre el uso apropiado de contraseñas y de equipos de trabajo. Verificar el cumplimiento de los procedimientos de revisión de registros de auditoría.
- Asistir a los funcionarios que corresponda en el análisis de riesgos a los que se expone la información y los componentes del ambiente informático que sirven de soporte a la misma.

Los Propietarios de la Información estarán encargados de:

- Evaluar los riesgos a los cuales se expone la información con el objeto de:
  - Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
  - Definir los eventos y actividades de funcionarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.
  - Aprobar y solicitar la asignación de privilegios a funcionarios.
  - Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información.
  - Definir un cronograma de depuración de registros de auditoría en línea.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Los Responsable de las unidades municipales, junto con el Responsable de Seguridad Informática, autorizarán el trabajo remoto del personal a su cargo, en los casos en que se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con las normas vigentes. Asimismo, autorizarán el acceso de los funcionarios a su cargo a los servicios y recursos de red y a Internet.

El jefe del Departamento de Informática y Sistemas de Comunicaciones cumplirá las siguientes funciones:
- Implementar procedimientos para la activación y desactivación de derechos de acceso a las redes.
- Analizar e implementar los métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.
- Evaluar el costo y el impacto de la implementación de "enrutadores" o "gateways" adecuados para subdividir la red y recomendar el esquema apropiado.
- Implementar el control de puertos, de conexión a la red y de ruteo de red.
- Implementar el registro de eventos o actividades de funcionarios de acuerdo a lo definido por los propietarios de la información, así como la depuración de los mismos.
- Definir e implementar los registros de eventos y actividades correspondientes a sistemas operativos y otras plataformas de procesamiento.
- Evaluar los riesgos sobre la utilización de las instalaciones de procesamiento de información, con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de funcionarios (Ej.: biometría, verificación de firma, uso de autenticadores de hardware).
- Definir e implementar la configuración que debe efectuarse para cada servicio de red, de manera de garantizar la seguridad en su operatoria.

- Analizar las medidas a ser implementadas para efectivizar el control de acceso a Internet de los funcionarios.
- Otorgar acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal correspondiente.
- Efectuar un control de los registros de auditoría generados por los sistemas operativos y de comunicaciones.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad.

El Comité de Seguridad de la Información aprobará el análisis de riesgos de la información efectuado. Asimismo, aprobará el período definido para el mantenimiento de los registros de auditoría generados.

8.1 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.

8.1.1 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 el contrato, además de tener claro cuales sistemas ocupaba un funcionario que es dado de baja, para la revocación del acceso y su posterior eliminación.

8.1.2 Administración de Privilegios

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado del privilegio del sistema resulta frecuentemente en 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.

8.1.3 Administración de Contraseñas de Funcionarios

La asignación de contraseñas se realizará bajo ciertos patrones secretos definidos por el Departamento de Informática y Sistemas Computacionales, también el funcionario puede asignar sus propias contraseñas, debidamente escritas por comunicación interna, dependiendo del sistema que se le presente, también debe notificar al Departamento de Informática y Sistemas Computacionales cuando un funcionario desea cambiar la clave.

8.1.4 Administración de Contraseñas Críticas

Existen cuentas de funcionarios 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 superfuncionario, es decir, pueden cambiar a voluntad todos los parámetros de un sistema en concreto

8.1.5 Revisión de Derechos de Acceso de Funcionarios

A fin de mantener un control eficaz del acceso a los datos y servicios de información, el jefe del Departamento de Informática y Sistemas Computacionales 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 funcionarios.

8.2 Responsabilidades del Funcionario

8.2.1 Uso de Contraseñas

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

- La contraseña no debe ser menor a 8 caracteres.
- Fáciles de Recordar.
- Debe contener mayúsculas, minúsculas, dígitos y caracteres de puntuación.
- Se deberán cambiar los identificadores cuando existan indicios de un posible compromiso del identificador o del sistema, para realizarlo el funcionario deberá comunicar al jefe de Departamento de Informática y Sistemas Computacionales por medio de correo electrónico.
- El funcionario deberá cambiar a lo menos una vez al año sus claves.

No basarse en condiciones obvias o de fácil deducción a partir de datos relacionados con la persona, por ejemplo, nombres, números telefónicos, cédula de identidad, fecha de nacimiento; estén libres de caracteres idénticos consecutivos o grupos completamente numéricos o alfabéticos.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un funcionario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los funcionarios deben cumplir las directivas que se impartan a tal efecto.

8.3 Control de Acceso a la Red

8.3.1 Política de Utilización de los Servicios de Red

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

8.3.2 Autenticación de Funcionarios para Conexiones Externas

El Encargado de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizarán una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

8.3.3 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 de Punta Arenas. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas y verificadas.

8.3.4 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.

8.3.5 Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Encargado de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente, por escrito, por el Director(a) de cada Departamento Municipal, quien esté a cargo del personal que lo solicite y por el Director(a) de Servicios Generales. Asimismo, se definirán las pautas de utilización de Internet para todos los funcionarios.

8.3.6 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.

8.4 Control de Acceso al Sistema Operativo

8.4.1 Identificación Automática de Equipos

El Encargado de Seguridad de la Información junto con el jefe del Departamento de Informática y Sistemas Computacionales realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

8.4.2 Sistema de Administración de Contraseñas

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.
b) Permitir que los funcionarios 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 8.2.1 "Uso de Contraseñas".
d) Imponer cambios en las contraseñas en aquellos casos en que los funcionarios mantengan sus propias contraseñas, según lo señalado en el punto "Uso de Contraseñas".
e) Se forzará obligatoriamente por medio del mismo sistema a los funcionarios 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 funcionario, 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 unidireccional.
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.

8.4.3 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.

8.4.4 Alarmas Silenciosas para la Protección de los Funcionarios

Se considerará la provisión de alarmas silenciosas para los funcionarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Encargado de Seguridad de la Información junto con el jefe de Departamento de Informática y Sistemas Computacionales.

8.4.5 Suspensión de equipos por Tiempo Muerto

El Encargado de Seguridad de la Información, junto con los Propietarios de la Información de que se trate definirán bajo qué tiempo desean que el equipo pase a estado de suspensión, la cual, el equipo queda protegido por contraseña. Las mismas se "apagarán" después de un periodo definido de inactividad.

Para los computadores, se implementará una contraseña, la cual la define el Propietario del equipo computacional y su información, con esto se evita el acceso no autorizado, pero no cierra las sesiones de aplicación o de red.

Además, se debe registrar la contraseña en formato físico y debe ser entregada en sobre cerrado a su jefatura para su resguardo.

8.4.6 Subdivisión de Redes

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados. Para esto se definirán *y* documentarán los perímetros de seguridad que sean convenientes. Estos perímetros se implementarán mediante la instalación de "gateways" con funcionalidades de "firewall" o redes privadas virtuales, para filtrar el tráfico entre los dominios (Ver 8.4.8. Control de Conexión a la Red *y* 8.4.9. Control de Ruteo de Red) *y* para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos (Ver 8.1. Administración de Acceso a Funcionarios).

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos *y* los requerimientos de acceso (Ver 8.1. Administración de Acceso a Funcionarios), el Responsable del Departamento de Informática y Sistemas Computacionales evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados (Ver 8.4.8. Control de Conexión a la Red y 8.4.9. Control de Ruteo de Red) para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad Informática, el esquema más apropiado a implementar.

8.4.7 Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El Responsable de Seguridad Informática definirá procedimientos para solicitar y aprobar accesos a Internet.

Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los funcionarios.

Se evaluará la conveniencia de generar un registro de los accesos de los funcionarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. MANUAL - POLÍTICA – REGLAMENTOS

Dicho control será comunicado a los funcionarios de acuerdo a lo establecido en el punto 5.1.1.3 "Compromiso de Confidencialidad". Para ello, el Responsable de Seguridad Informática junto con el Responsable del Departamento de Informática y Sistemas Computacionales analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de "firewalls", "proxies", etc.

8.4.8 Control de Conexión a la Red

Sobre la base de lo definido en el punto "Requerimientos ", se implementarán controles para limitar la capacidad de conexión de los funcionarios. Dichos controles se podrán implementar en los "gateways" que separen los diferentes dominios de la red (Ver 8.4.6. Subdivisión de Redes). Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.

8.4.9 Control de Ruteo de Red

En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Municipio de Punta Arenas, 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. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros, autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

8.4.10 Seguridad de los Servicios de Red

El Responsable de Seguridad Informática junto con el Responsable del Departamento de Informática y Sistemas Computacionales definirá las pautas para garantizar la seguridad de los servicios de red de la Municipalidad de Punta Arenas, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.
- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de segundad. Dicha configuración será revisada periódicamente por el Responsable de Seguridad Informática.

8.5 Control de Acceso a las Aplicaciones

8.5.1 Restricción del Acceso a la Información

Los funcionarios de sistemas municipales, tendrán acceso a la información sensible de la Municipalidad de Punta Arenas 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.

8.5.2 Aislamiento de los Sistemas Sensibles

El sistema sensible definido por la Municipalidad de Punta Arenas es el servidor, ya que procesan todos los datos que apoyan a los sistemas municipales a que cumplan sus funciones, este servidor se encuentra aislado de todo contacto humano no autorizado. Este servidor cuenta con un computador dedicado a las tareas de manejo de bases de datos y especificaciones para respaldos entre otros.

8.6 Monitoreo del Acceso y Uso de los Sistemas

8.6.1 Registro de Eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del funcionario, 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.

8.6.2 Monitoreo del Uso de los Sistemas

8.6.2.1 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 funcionarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los funcionarios conocerán el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá por correos electrónicos masivos que determinadas actividades pueden ser objeto de control y monitoreo (Ver 11.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información y 5.1.3. Compromiso de Confidencialidad).

8.6.2.2 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.

8.7 Política sobre el cumplimiento de requisitos Legales

8.7.1 Cumplimiento de requisitos legales.

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.

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. Los funcionarios únicamente podrán utilizar material autorizado por la municipalidad. La Municipalidad solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordados y lo dispuesto por la normativa vigente. La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales. Se deberán tener presente la siguiente norma:

Ley de Propiedad Intelectual, LEY 17336 DE PROPIEDAD INTELECTUAL

Derecho de propiedad intelectual del software

El software es considerado una obra intelectual que goza de la protección de la Ley 17336 de Propiedad Intelectual.

Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción. Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El responsable de Seguridad Informática, en conjunto con jurídico, analizarán los términos y condiciones de cumplimiento con las licencia de software y la prohibición del uso de software no autorizado , implementando los siguientes controles:

a) 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.
b) 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.
c) Mantener un adecuado registro de activos.
d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f) Verificar que sólo se instalen productos con licencia y software autorizado.
g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
i) Utilizar herramientas de auditoría adecuadas.
j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

9. DESARROLLO Y MANTENIMIENTO DE SISTEMAS

a) Generalidades

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos. Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Asimismo, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software

b) Objetivo

Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los sistemas y en la infraestructura de base en la cual se apoyan. Definir los métodos de protección de la información crítica o sensible.

c) Alcance

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 el Organismo en donde residan los desarrollos mencionados.

d) Responsabilidad

El Responsable de Seguridad Informática junto con el Propietario de la Información y la Unidad de Auditoría Interna, definirán los controles a ser implementados en los sistemas desarrollados internamente o por terceros, en función de una evaluación previa de riesgos. El Responsable de Seguridad Informática, junto con el Propietario de la Información, definirá en función a la criticidad de la información, los requerimientos de protección mediante métodos criptográficos. Luego, el Responsable de Seguridad Informática definirá junto con el Responsable del Área de Sistemas, los métodos de encriptación a ser utilizados.

Asimismo, el Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir los procedimientos de administración de claves.
- Verificar el cumplimiento de los controles establecidos para el desarrollo y mantenimiento de sistemas.
- Garantizar el cumplimiento de los requerimientos de seguridad para el software.
- Definir procedimientos para: el control de cambios a los sistemas; la verificación de la seguridad de las plataformas y bases de datos que soportan e interactúan con los sistemas; el control de código malicioso; y la definición de las funciones del personal involucrado en el proceso de entrada de datos.

El jefe del Departamento de Informática y Sistemas Computacionales, propondrá para su aprobación por parte del superior jerárquico que corresponda, la asignación de funciones de "implementador" y

"administrador de programas fuentes" al personal de su área que considere adecuado, cuyas responsabilidades se detallan en el presente capítulo. Asimismo, verificará el cumplimiento de las definiciones establecidas sobre los controles y las medidas de seguridad a ser incorporadas a los sistemas. El Área de Sistemas propondrá quiénes realizarán la administración de las técnicas criptográficas y claves.

El Responsable del Área de Administración incorporará aspectos relacionados con el licenciamiento, la calidad del software y la seguridad de la información en los contratos con terceros por el desarrollo de software. El Responsable del Área Legal participará en dicha tarea.

9.1 Requerimientos de Seguridad de los Sistemas

9.1.1 Análisis y Especificaciones de los Requerimientos de Seguridad

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

9.2 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.

9.2.1 Política de Utilización de Controles Criptográficos

Se utilizarán controles criptográficos en los siguientes casos:

a) Para la protección de claves de acceso a sistemas, datos y servicios.
b) Para la transmisión de información clasificada, fuera del ámbito del Municipio.
c) 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

9.2.2 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.

9.2.3 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.

9.2.4 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.

9.3 Seguridad de los Procesos de Soporte

9.3.1 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.

9.3.2 Restricción del Cambio de Paquetes de Software

La modificación de paquetes de software suministrados por proveedores, previa autorización del jefe del Departamento de Informática y Sistemas Computacionales, 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.

9.3.3 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.

9.3.4 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 establecido, etc.
D. Verificación del cumplimiento de las condiciones de seguridad contempladas en el punto anterior.
E. Acuerdos de custodia de las fuentes del software (y cualquier otra información requerida) en caso de quiebra de la tercera parte.

10. GESTION DE LA CONTINUIDAD DE LA MUNICIPALIDAD

a) Generalidades

La administración de la continuidad de las actividades es un proceso crítico que debe involucrar a todos los niveles de la Municipalidad de Punta Arenas. El desarrollo e implementación de planes de contingencia es una herramienta básica para garantizar que las actividades de la Municipalidad puedan restablecerse dentro de los plazos requeridos.

Dichos planes deben mantenerse actualizados y transformarse en una parte integral del resto de los procesos de administración y gestión, debiendo incluir necesariamente controles destinados a identificar y reducir riesgos, atenuar las consecuencias de eventuales interrupciones de las actividades de la Municipalidad y asegurar la reanudación oportuna de las operaciones indispensables.

b) Objetivo

Minimizar los efectos de las posibles interrupciones de las actividades normales de la Municipalidad de Punta Arenas(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.

Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro. Maximizar la efectividad de las operaciones de contingencia de la Municipalidad de Punta Arenas con el establecimiento de planes que incluyan al menos las siguientes etapas:

- **Notificación / Activación:** Consistente en la detección y determinación del daño y la activación del plan.
- **Reanudación:** Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
- **Recuperación:** Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

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

c) Alcance

Esta Política se aplica a todos los procesos críticos identificados de la Municipalidad.

d) Responsabilidad

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia.

Los Propietarios de la Información (Ver en Punto 3.1.2 Asignación de Responsabilidades en Materia de Seguridad de la Información) y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Identificar las amenazas que puedan ocasionar interrupciones de los procesos *y/o* las actividades de la Municipalidad.
- 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 de la Municipalidad de Punta Arenas.
- Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Municipalidad de Punta Arenas.

Los Responsables de Procesos revisarán periódicamente los planes bajo su incumbencia, como así también identificar cambios en las disposiciones relativas a las actividades del Municipio aún no reflejadas en los planes de continuidad. Los administradores de cada plan verificarán el cumplimiento de los procedimientos implementados para llevar a cabo las acciones contempladas en cada plan de continuidad.

El Comité de Seguridad de la Información tendrá a cargo la coordinación del proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de información de la Municipalidad frente a interrupciones imprevistas, lo cual incluye las siguientes funciones: Identificar y priorizar los procesos críticos de las actividades de la Municipalidad de Punta Arenas.

- Asegurar que todos los integrantes de la Municipalidad de Punta Arenas comprendan los riesgos que la misma enfrenta, en términos de probabilidad de ocurrencia e impacto de posibles amenazas, así como los efectos que una interrupción puede tener en la actividad del Organismo.
- Elaborar y documentar una estrategia de continuidad de las actividades de la Municipalidad de Punta Arenas consecuente con los objetivos y prioridades acordados.
- Proponer planes de continuidad de las actividades de la Municipalidad de Punta Arenas de conformidad con la estrategia de continuidad acordada.
- Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
- Coordinar actualizaciones periódicas de los planes y procesos implementados.
- Considerar la contratación de seguros que podrían formar parte del proceso de continuidad de las actividades de la Municipalidad de Punta Arenas.
- Proponer las modificaciones a los planes de contingencia.

10.1 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 de Punta Arenas 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 de Punta Arenas y no limitándose a los equipos computacionales municipales.

10.2 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 garantizar la continuidad de las actividades de la Municipalidad de Punta Arenas.

10.3 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 emergencias existentes.

11. CUMPLIMIENTOS

a) Generalidades

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales. Los requisitos normativos y contractuales pertinentes a cada sistema de información deben estar debidamente definidos y documentados.

El Área Legal de la Municipalidad de Punta Arenas, será responsable de encuadrar jurídicamente la formulación e implementación de la política.

b) Objetivos

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al funcionario o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.
- 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.
- Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo. Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
- Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la Municipalidad.

c) Alcance

Esta Política se aplica a todo el personal de la Municipalidad de Punta Arenas, cualquiera sea su situación de revista. Asimismo, se aplica a los sistemas de información, normas, procedimientos, documentación y plataformas técnicas de la Municipalidad de Punta Arenas y a las auditorías efectuadas sobre los mismos.

d) Responsabilidad

El Responsable de Seguridad Informática cumplirá las siguientes funciones:

- Definir normas y procedimientos para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual y a la conservación de registros.
- Realizar revisiones periódicas de todas las áreas de la Municipalidad a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.
- Verificar periódicamente que los sistemas de información cumplan la política, normas y procedimientos de seguridad establecidos.
- Garantizar la seguridad y el control de las herramientas utilizadas para las revisiones de auditoría.

El Responsable del Área Legal de la Municipalidad de Punta Arenas, con la asistencia del Responsable de Seguridad Informática cumplirán las siguientes funciones:

- Definir y documentar claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información.
- Redactar un Compromiso de Confidencialidad a ser firmado por todo el personal.

Los Responsables de Unidades Organizativas velarán por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos en la presente Política, dentro de su área de responsabilidad.

Todos los funcionarios de los mandos medios y superiores conocerán, comprenderán, darán a conocer, cumplirán y harán cumplir la presente Política y la normativa vigente.

11.1 Cumplimiento de Requisitos Legales

11.1.1 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.

11.1.2 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.

11.1.2.1 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:

a) 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.
b) 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.
c) Mantener un adecuado registro de activos.
d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Verificar que sólo se instalen productos con licencia y software autorizado.
f) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
g) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
h) Utilizar herramientas de auditoría adecuadas.
i) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

11.1.3 Protección de los Registros de la Municipalidad

Los registros críticos del Municipio de Punta Arenas 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.

11.1.4 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.

11.1.5 Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

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

11.1.6 Regulación de Controles para el Uso de Criptografía

Al utilizar firmas digitales o electrónicas, se deberá considerar lo dispuesto por la Ley 19.699 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.

11.1.7 Recolección de Evidencia

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

11.2 Revisiones de la Política de Seguridad y la Compatibilidad Técnica

11.2.1 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.

11.2.2 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.

11.3 Consideraciones de Auditorías de Sistemas

11.3.1 Controles de Auditoría de Sistemas

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.

11.3.2 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.

I. MUNICIPALIDAD DE PUNTA ARENAS
SECRETARIA MUNICIPAL

11.4 Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en las presente Políticas de Seguridad conforme a lo dispuesto por las normas estatutarias y reglamentarias convencionales que rigen al personal municipal, y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Municipios pertinentes.

12. POLÍTICA DE TRABAJO A DISTANCIA Y TELETRABAJO

a) Generalidades

La Municipalidad de Punta Arenas, por intermedio de su Comité de Seguridad de la Información y través de esta política entrega las características mínimas obligatorias de seguridad de la información, confidencialidad, integridad y disponibilidad, para abordar el trabajo a distancia y teletrabajo.

Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones u conexión a otros equipos dentro de la entidad.

Se denomina teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante esos medios.

En este contexto se incorpora esta modalidad de trabajo bajo la ley vigente[1] e introduce consideraciones de ciberseguridad para que estas labores se desempeñen sin poner en riesgo la información de la empresa ni los activos de información en general.

b) Objetivos

Los objetivos que busca esta política son los siguientes:

- Definir las condiciones y las restricciones del uso del trabajo a distancia y del teletrabajo.
- Establecer medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia o de teletrabajo.

c) Alcance

Esta política se aplica a todos los funcionarios y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Municipalidad de Punta Arenas. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

Esta política rige independientemente del lugar en el trabajador presta sus servicios a la organización, total o parcialmente, e indistintamente de la modalidad de trabajo ya sea "presencial", "a distancia", "teletrabajo" u otra, en las condiciones que establezca la legislación vigente.

Esta política gobierna la seguridad de la información de todos los procesos estratégicos de la Municipalidad de Punta Arenas.

d) Roles y Responsabilidades

Las responsabilidades se encuentran definidas en la política de la organización de la seguridad de la información.

e) Vigencia y Actualización

La Política se considera vigente desde la fecha de su aprobación por parte de la autoridad, documento que será revisado y actualizado cada dos años o cuando el Comité de Seguridad de la Información lo determine, o toda vez que se produzca un cambio significativo que modifique el nivel de riesgo presente de la Municipalidad de Punta Arenas.

La Política deberá ser revisada por el Comité de Seguridad de la Información.

[1] Ley N° 21.220 https://www.bcn.cl/leychile/navegar?idNorma=1143741

Entre los cambios que hacen necesaria la revisión de las políticas, se debe destacar:

- Cambios en las leyes o reglamentos que afecten a la Municipalidad de Punta Arenas.
- Incorporación o modificaciones relevantes de procesos críticos de la Municipalidad de Punta Arenas.
- Cambios significativos al soporte tecnológico.
- Modificaciones en la estructura de la organización.
- Cambios significativos en los niveles de riesgo a que se expone la información.
- Cambios relevantes en las Definiciones Estratégicas.
- Ajustes necesarios producto de Estados de Excepción Constitucional.
- Ajustes necesarios para proteger las infraestructuras críticas.

Las revisiones que se efectúen a la Política de General de Seguridad de la Información deben considerar tanto la actualidad de ella, como su eficacia, eficiencia y cumplimiento.

f) Revisión del cumplimiento

El Comité de Seguridad de la Información, anualmente, asignará la responsabilidad de ejecutar un proceso formal de revisión del cumplimiento a cargo de una o varias unidades organizacionales, pudiendo optar también por una revisión independiente interna o una externa ejecutada por una tercera parte.

Además, este Comité determinará la metodología y los alcances que estime necesarios para cumplir los objetivos estratégicos de revisión y cumplimiento de las políticas y su mejora continua.

g) Control de documentos

Los documentos requeridos por el Comité de Seguridad de la Información deben protegerse y controlarse. Con este objetivo, las acciones necesarias a implementar son:

- Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.
- Registrar los cambios o actualizaciones de los documentos una vez que son aprobados por el Comité de Seguridad de la Información, incorporando Tabla en Capitulo final en cada documento.
- Se deberá controlar el uso no intencionado de documentos obsoletos.
- En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo con los procedimientos aplicables a su clasificación.

h) Difusión

El mecanismo de difusión de la Política será a través de la Intranet, circulares informativas, correos electrónicos masivos o cualquier otro medio que el Comité de Seguridad de la Información estime pertinente, procurando apoyar la sensibilización con infografías que faciliten la comprensión de esta por todos los usuarios en general.

12.1 Trabajo A Distancia y Teletrabajo

Por la complejidad y transversalidad del concepto se implementa una política específica y las medidas que apoyan la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia y de teletrabajo.

a) Definiciones estructurales:

Las definiciones fundamentales que se tendrán en consideración en todas las políticas en las que se integre el concepto de "trabajo a distancia" o "teletrabajo" serán las establecidas en la Ley N°21.220:

Trabajo a distancia:
Es trabajo a distancia aquel en el que el trabajador presta sus servicios, total o parcialmente, desde su domicilio u otro lugar o lugares distintos de los establecimientos, instalaciones o faenas de la empresa.

Teletrabajo:
Se denominará teletrabajo si los servicios son prestados mediante la utilización de medios tecnológicos, informáticos o de telecomunicaciones o si tales servicios deben reportarse mediante estos medios.

b) Condiciones del uso del trabajo a distancia y del teletrabajo

Cada unidad organizacional establecerá:

- Que funcionarios están en condiciones de realizar trabajo a distancia o teletrabajo.
- Que roles son los que se considerarán dentro de los posibles de incorporar.
- Que información o sistemas son lo que necesitan (previa validación con el Departamento de Informática y Sistemas Computacionales)

El Departamento de Informática y Sistemas Computacionales, establecerá:

- Que servicios estarán disponibles para teletrabajadores.
- Los tipos de servicios de red y aplicaciones.
- Los esquemas de identificación, autenticación y autorización, es decir, cómo deben identificarse los teletrabajadores, autenticarse y recibir la autorización antes de acceder a los recursos de la empresa.
- Especificaciones de equipos y software: ¿hay algún dispositivo específico o producto de software que deba implementarse en el equipo del teletrabajador? (por ejemplo, firewall, pendrive encriptado o software de encriptación).
- Integridad y confidencialidad: cómo debe protegerse la conexión desde el equipo remoto (es decir, VPN) y cómo deben protegerse los datos en dicho equipo.
- Pautas de mantenimiento: ¿cómo debe ser la configuración equipo del teletrabajador?.
- Directrices del usuario: que aclaren el papel del usuario en la protección de los recursos de la empresa, por ejemplo, uso apropiado de los recursos; el usuario no debe modificar las configuraciones de seguridad; utilizar de software antivirus; almacenamiento de datos corporativos en unidades locales; uso de encriptación herramientas.

El comité de Seguridad de la Información deberá velar por que se cumplan las siguientes exigencias normativas:

- Los requisitos de seguridad para las comunicaciones, considerando la necesidad de contar con acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la que se accederá y que se traspasará por el enlace de comunicaciones y la sensibilidad del sistema interno;
- La provisión de acceso a un escritorio virtual que evite el procesamiento y el almacenamiento de información en equipos de propiedad privada;
- La amenaza del acceso no autorizado a la información o a los recursos de parte de otras personas que utilizan el recinto, es decir, la familia y los amigos;
- El uso de redes domésticas y los requisitos o restricciones en la configuración de los servicios de redes inalámbricas;

- Las políticas y procedimientos para evitar disputas en cuanto a los derechos de propiedad intelectual desarrollados en equipos de propiedad privada;
- Acceso a equipos de propiedad privada (para verificar la seguridad de la máquina durante una investigación), lo que se puede evitar por legislación;
- Acuerdos de licenciamiento de software que pueden hacer que las organizaciones se hagan responsables del software de cliente en estaciones de trabajo de propiedad privada de empleados o de usuarios externos;
- Requisitos de protección de malware firewall (cortafuegos).

Las pautas y disposiciones que se deberán incluir son:

- Una definición del trabajo permitido, las horas de trabajo, la clasificación de información que se puede tener y los sistemas y servicios internos que se autoriza al teletrabajador a acceder;
- La provisión de equipos de comunicación idóneos, incluidos los métodos para proteger el acceso remoto;
- La provisión de soporte y mantenimiento de hardware y software;
- Procedimientos para el respaldo y la continuidad en el negocio;
- Auditoría y monitoreo de seguridad;
- Revocación de autoridad y derechos de acceso y la devolución de los equipos cuando concluyen las actividades de teletrabajo.

c) Consideraciones del uso del trabajo a distancia y del teletrabajo

Las principales consideraciones que deberán contemplar los jefes de cada una de las unidades organizacionales son:

- Analizar los privilegios que necesitará el teletrabajador para aplicarlos bajo el principio de los mínimos privilegios (en cuanto al acceso a la plataforma de Sistemas de la Municipalidad de Punta Arenas) para funcionar.
- Educación del usuario: los usuarios deben conocer y entender los posibles riesgos de la información asociados con el teletrabajo, cómo se abordan esos riesgos y el papel del usuario en minimizando los riesgos.
- Medidas que apoyen la seguridad para proteger la información a la que se accede, procesa o almacena en los sitios de trabajo a distancia o de teletrabajo.

d) Modo de operación

La activación del trabajo remoto deberá estar previamente autorizada por el jefe de la unidad correspondiente y los usuarios definidos deberán tener sus anexos de contrato firmados y validados por sus jefaturas correspondientes y con su equipamiento de trabajo debidamente asignado.

e) Consejos preventivos para teletrabajo

- Habilitar una zona dentro de tu hogar con suficiente espacio para contener los equipos y materiales de trabajo.
- Aislar los ruidos externos y los propios de la casa
- Controlar la iluminación, temperatura y ventilación de lugar definido.
- Es conveniente disponer de luz natural, esta disminuye el riesgo de fatiga visual.
- Evite consumir alimentos y líquidos cerca del su equipo, podría dañarlo.
- Evite cableado eléctrico suelto, fíjelo cosa de evitar accidentes.
- Utilice pausas de trabajo para consumir alimentos.

- A modo de "mejores prácticas" se deben promover e implementar las siguientes medidas de seguridad, asociadas al uso de computadores utilizados bajo modalidad de teletrabajo:

  - Usar protector de pantalla con clave cuando el computador no esté en uso.
  - No dejar Pendrive/Flash Drive olvidados en los computadores.
  - Bloquear puertos USB del equipo para periféricos de almacenamiento externos. Es importante mencionar que en caso de excepciones previamente autorizadas podrán ser habilitados para tal efecto en forma temporal.
  - El usuario debe asegurarse de que su equipo cuenta con el software antivirus, el cuál debe ser actualizado por lo menos una vez por semana.
  - El usuario es responsable de copiar, en forma periódica, los archivos de trabajo que residan en su PC; para ello, deberá copiarlos en One Drive que estará disponible en la red para estos efectos.

f) Instalación de Software Base

A todo equipo, antes de ser asignado para trabajo remoto, se le deberá instalar el siguiente software base:

- Sistema operativo cliente debidamente licenciado y aprobado por la entidad.
- Drivers internos y de periféricos utilizados en la organización.
- Actualizaciones, probadas en la organización.
- Software de ofimática debidamente licenciado.
- Antivirus corporativo.
- Cliente Firewall activo.
- Aplicaciones requeridas y utilizadas por la organización.
- Visualizador de PDF de ser requerido.
- Browser actualizado, como navegador de Internet.
- Acceso VPN requerido.
- Software especializado para acceso remoto.
- Software especializado para realización de video conferencia o teleconferencias.
- Control de dirección "MAC".

Una vez que el computador tenga todo el software base instalado, pasará a llamarse Dispositivo para trabajo remoto y podrá ser asignado a un usuario.

g) Registro e inventario de equipos y software instalado

El Departamento de Informática y Sistemas de Comunicaciones es responsable de llevar un registro detallado de los recursos de hardware y software, instalados dentro y fuera de los centros de cómputo, y las descripciones de su localización. Para ello deberá existir un documento de Inventario del equipamiento, en el cual al menos deberá ser identificado:

- el modelo
- la serie del equipo si existiese
- su dueño
- el nivel de criticidad (alto, medio o bajo)
- el tipo de acceso que el usuario tendrá (local, remoto)
- N° de IP
- características del equipo (Ram, Espacio de Almacenamiento, CPU)
- otros antecedentes que sean importantes a considerar.

h) Cuidados especiales para trabajo remoto

- Protector de pantalla con clave activado y con tiempo de activación inferior a 5 minutos.
- Evitar navegar por sitios desconocidos.
- No descargue música, videos, películas o programas desde Internet.
- No instale ninguna aplicación en los equipos portátiles que no sea autorizada y supervisada por área de TI
- Evite ingresar a sitios desde publicidad en páginas web.
- Si el remitente de un mail no es seguro o es extraño, ¡Nunca abra los archivos adjuntos!
- Mantenga su antivirus actualizado.
- Revisiones periódicas (diarias) de su equipo para asegurar que esté actualizado (antivirus y sistema operativo).

i) Consideraciones especiales en trabajo remoto:

Contacte vía teléfono al Departamento de informática y Sistemas de Comunicaciones cuando:

- su equipo no se pueda conectarse a internet.
- su equipo no se pueda conectarse a alguna aplicación.
- su equipo no se encienda.
- su conexión VPN no funcione.

j) Aspectos mínimos para verificar la operatividad de la política

Normativa de protección del puesto de trabajo remoto.

o Informar al personal sobre la normativa de protección del puesto de trabajo fuera de la oficina llevando a cabo auditorías periódicas para asegurar su cumplimiento.

Relación de usuarios que disponen de la opción de trabajar en remoto.

o Llevar un control de las personas que, por su perfil dentro de la empresa o las características de su trabajo, tienen la opción de teletrabajar.

Procedimientos para la solicitud y autorización del teletrabajo.

o Redactar un documento donde se contemplen todas las cuestiones relativas al teletrabajo (duración del mismo, dispositivos facilitados, etc.), que será firmado por cada teletrabajador.

Periodo de implantación y pruebas.

o Valorar diferentes escenarios y configuraciones antes de habilitar el teletrabajo, contemplando todos los riesgos de seguridad.

Realizar pruebas de carga en escenarios simulados.

o Si existe un volumen considerable de empleados que van a teletrabajar al mismo tiempo, valorar la carga que esto ocasiona en los sistemas internos de la empresa.

Aplicaciones y recursos a los que tiene acceso cada usuario.

o Dar acceso a cada funcionario, solo a las aplicaciones y recursos necesarios para llevar a cabo su trabajo dependiendo de su perfil dentro de la organización. Detallar las aplicaciones permitidas, así como sus condiciones de uso. Valorar la inclusión del nuevo software solicitado por los empleados.

Acceso seguro.

o Gestionar las credenciales de acceso de los empleados forzando el uso de contraseñas robustas y su cambio periódico, además de incluir el doble factor de autenticación siempre que sea posible.

Configuración de los dispositivos de teletrabajo.

o Configurar los dispositivos utilizados por el funcionario para teletrabajar (sistema operativo, antivirus, control de actualizaciones, etc.)

Cifrado de los soportes de información.

o Implantar tecnologías de cifrado que protegen la información de posibles accesos malintencionados.

Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa.

o Elaborar las políticas que detallan a los empleados dónde deben guardar la información con la que trabajan en remoto.

Planificación de las copias de seguridad de todos los soportes.

o Comprobar regularmente que se realizan periódicamente y que pueden restaurarse.

Uso de conexiones seguras a través de una red privada virtual o VPN.

o Implementar una red VPN extremo a extremo que permite que la información que se intercambia entre los equipos de la organización viaje cifrada a través de Internet.

Aplicaciones de escritorio remoto siempre a través de una VPN.

o Para ofrecer un extra de seguridad y privacidad a las comunicaciones, solo se permite el uso de las aplicaciones de escritorio remoto bajo una VPN.

Virtualización de entornos de trabajo.

o Valorar la implementación de la virtualización como método para proporcionar a cada empleado su propio espacio de trabajo, eliminando los riesgos asociados al uso de un dispositivo físico.

Priorizar el uso de dispositivos corporativos.

o Elegir los dispositivos corporativos para teletrabajar, ya que cuentan con las políticas de seguridad que la empresa considera necesarias y tienen instalado el software preciso para realizar el trabajo de forma segura.

Conexión a Internet.

o Cuando no es posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utilizar la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi públicas.

o Uso de dispositivos personales Utilizando las configuraciones y conexiones permitidas y seguras al teletrabajar desde tus dispositivos personales.

Concienciar a los empleados antes de empezar a utilizar acceso remoto.

o Educar a los funcionarios en ciberseguridad antes de que comiencen a teletrabajar para que conozcan las políticas y las medidas que se llevaran a cabo en la empresa.

Cumplimiento Ley de Datos Personales.

o Educar a los empleados que manejan datos personales para la protección de los mismos durante el teletrabajo y realizar los cambios en los tratamientos para contemplar estas situaciones.

Aplicaciones de teleconferencia y colaborativas.

o Configurar estas aplicaciones para un uso seguro que permita que se respeten la privacidad y la propiedad intelectual de los participantes.

13. POLÍTICA DE DESTRUCCIÓN DE LA INFORMACIÓN

a) Generalidades

La Municipalidad de Punta Arenas, por intermedio de su Comité de Seguridad de la Información y través de esta política entrega las características mínimas obligatorias de seguridad de la información, confidencialidad, integridad y disponibilidad, para el proceso de destrucción de la información, los criterios aplicables, tipificación de documentos, digitalización, conservación y excepciones.

b) Definiciones

Destrucción de Documentos: La eliminación de documentos es el procedimiento mediante el cual se determina y ejecuta la eliminaciónfísica de la documentación de un archivo dentro de una Unidad.

Documentos Oficiales: son los que la legislación define como instrumentos públicos, o sea aquéllos autorizados con las solemnidades legales por el competente funcionario, como, por ejemplo: los decretos, las resoluciones y los oficios.

Documentos No Oficiales o Documentos en General: aquéllos que la legislación no considera como públicos, auténticos u oficiales, como, por ejemplo: copias y duplicados, memorándum, borradores, fotocopias o diarios, documentos sin firma o sin fecha.

Revisión Definitiva: Las inspecciones y auditorías realizadas por la Contraloría General de la República tienen el carácter definitivo desde el momento en que se emite el respectivo informe final que da cuenta de su resultado.

Copia Fiel: Es aquella reproducción de un documento, ya sea en forma física, digital u otra microforma, que cuenta con la certificación de ministro de fe correspondiente de que dicha copia guarda absoluta conformidad con el documento original.

Digitalización: La digitalización consiste en la transformación de la información analógica, propia de la naturaleza física, en información digital apta para ser tratada por aparatos computacionales, por ejemplo, la que se realiza a través de un dispositivo de escaneo o fotografía electrónica.

Microforma: Una imagen compactada o digitalizada de un documento original a través de una tecnología idónea para su almacenamiento, conservación, uso y recuperación posterior, y que además debe mantener en forma fiel, indeleble, legible e íntegra su calidad de documento. Las microformas tienen la calidad de copia fiel de un original en soporte papel incluso en sus imperfecciones, y para todos los efectos, tiene el mismo mérito del documento original.

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.

Principio de Equivalencia Funcional: Consiste en que los actos administrativos suscritos por medio de firma electrónica o convertidos a microforma serán válidos y producirán los mismos efectos que si se hubieren llevado a cabo en soporte de papel. Su aplicación no es más que la materialización del principio de igualdad ante la ley y su objetivo es la no discriminación con relación a los soportes, en cuanto a los efectos jurídicos, validez o fuerza obligatoria.

c) Objetivo General

Establecer directrices que permitan aplicar en forma eficiente, eficaz y efectiva los procesos de eliminación y digitalización de la documentación, teniendo en cuenta el ciclo de vida del documento y la normativa vigente. Este capítulo hace referencia a la forma en que se procederá con la eliminación de documento, y a la creación de digitalizaciones en caso de requerirse mantener respaldo de la documentación.

d) Objetivos Específicos

- Mejora de los espacios físicos internos de almacenamiento en las Unidades Municipales.
- Ordenamiento interno respecto de la documentación existente para dar mejor respuesta a la búsqueda de la documentación, para los procesos y gestión interna municipal.

e) Alcance

Esta política se aplica a todos los funcionarios y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Municipalidad de Punta Arenas. También se aplica a cualesquiera de sus relaciones con terceros que impliquen el acceso a sus datos, utilización de sus recursos o a la administración y control de sus sistemas de información.

f) Responsabilidades

Las responsabilidades se aplican a todos los funcionarios y terceras partes que tengan o no una relación directa o indirecta de acceso a la información que pueda afectar los activos de información de la Municipalidad de Punta Arenas.

13.1 Criterios Aplicables

La Contraloría General de la República, ha señalado que en virtud de los principios de eficiencia, eficacia e idónea administración de los medios públicos, previstos en los artículos 3° y 5° de la ley N° 18.575, que los órganos de la Administración del Estado pueden aprovechar las ventajas que les ofrece la aplicación de las leyes N°s. 18.845 -que establece sistemas de microcopia o micrograbación de documentos- y 19.799 -sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma-, a fin de que la obligación de conservar sus documentos, sea cumplida propendiendo al uso de sistemas electrónicos y digitales de generación, soporte y almacenamiento de información, en la medida que ello resulte procedente.

A su vez, en el dictamen N° 23.766 de 2008, se consideró la factibilidad de reemplazar el proceso de microfilm utilizado para copiar y archivar documentación de respaldo o derivada de la gestión que le compete desarrollar a las entidades públicas, por un sistema de tecnología más avanzada, como lo es la digitalización de documentos, en la medida que el método a emplear garantice, en términos equiparables a los documentos originales, la duración, legibilidad y fidelidad de las copias que se obtengan, como también la reproducción de las mismas, conforme al artículo 2° de la ley N° 18.845.

Igualmente, dado el principio de la equivalencia entre el soporte electrónico y el de papel, previsto en el artículo 1°, inciso segundo, de la ley N° 19.799, por el dictamen N° 81.069, de 2013, se concluyó que las reglas previstas por el ordenamiento en materia de conservación, archivo y eliminación de documentos de la Administración también resultan aplicables respecto de sus documentos electrónicos.

En ese mismo sentido, la Ley 21.180 para la Transformación Digital del Estado, recoge estos principios y los incorpora a través de la modificación de diversos cuerpos legales incorporando reformas que permiten avanzar en la digitalización de los procedimientos administrativos, entre ellos la promoción de la tramitación electrónica y que la microforma de documentos se pueda realizar través de medios digitales.

Para la ejecución de los procesos de destrucción documental deberá aplicarse un principio preventivo, ya que, en el caso de duda, la Unidad que pretenda iniciar el proceso de eliminación de algún documento, deberá contar con la aprobación de la unidad de Control Municipal, indicando o exhibiendo si es necesario los documentos consultados y los demás antecedentes que estime pertinentes para resolver la decisión de su conservación o eliminación.

También se podrá solicitar informe a la Dirección de Asesoría Jurídica, en aquellos casos que no estén claramente definidos por la ley o reglamentos aplicables. La solicitud de informe a la Dirección de Asesoría Jurídica debe indicar las razones que motivan su consulta, como los hechos que justifican la duda acerca la eliminación o conservación de los documentos consultados.

13.2 Organización de Documentos

En general, los documentos ya sea en soporte papel como aquellos que se encuentran en sus repositorios digitales deben clasificarse de acuerdo con las series documentales existentes y ordenarse cronológicamente por fecha, desde el antiguo hasta lo más reciente, y de acuerdo con la disposición numérica interna.

Al almacenar los documentos, estos se organizarán en forma separada según el tipo documental al que pertenezcan, a modo de ejemplo y sin que la enunciación sea taxativa:

- Decretos Alcaldicios Decretos registro SIAPER Resoluciones Reglamentos Ordenanzas
- Manuales
- Actas del Concejo Municipal Circulares
- Providencias Órdenes Internas
- Comunicaciones recibidas (Memorandos, oficios u otros). Comunicaciones enviadas (memorandos, oficios u otros). Libros de correspondencias.

13.3 Para La Conservación De Documentos En Soporte Papel

Para proteger los documentos que permanezcan en formato papel de su extravío o deterioro, se deben aplicar procedimientos que aseguren su integridad. Para ello, se debe recurrir al empaste, anillado, carpetas, archivadores o cualquier otro medio disponible en la unidad que permita su mejor conservación y búsqueda.

Respecto de los documentos oficiales, estos se deben mantener accesibles y en buen estado de conservación física, de acuerdo con las directrices que emita el Archivo Nacional en el ejercicio de sus funciones. Para estos fines deberá ser necesario que algún funcionario de la Municipalidad de Punta Arenas, sea el que deberá mantenerse actualizado respecto de los lineamientos de dicha institución.

El (la) Conservador(a) del Archivo Nacional podrá verificar las condiciones de conservación y organización de los documentos originales en soporte papel que se mantengan bajo nuestra custodia. El (La) Conservador(a) podrá delegar esta facultad en los (las) funcionarios(as) del Archivo Nacional que estime pertinente.

Periódicamente y para facilitar el caso de requerir ser llevadas a otra dependencia o bodega, los documentos deberán agruparse en cajas que permitan la colocación de un sello, con indicación del contenido, tipo de documento y fecha.

De requerir ser llevadas a bodegaje fuera de las dependencias de la unidad, las cajas deberán ser selladas y firmadas por el jefe de la unidad o por el funcionario a quien este designe, firma que debe pasar por el sello y la caja. Luego deberán fotografiadas por todos sus costados. Para estos efectos deberá levantarse un acta en la que se anotará el contenido y el nombre de el o los funcionarios encargados de sellar, firmar y de transportar a la bodega, además deberán adjuntarse las fotografías de la caja.

Cada vez que se requiera consultar los documentos en bodega por una unidad diferente a la que ordenó su archivo, deberá contar autorización expresa a la unidad originaria de los documentos, del alcalde o de la Administrador(a) Municipal.

En caso de encontrarse documentación oficial dañada en los archivos físicos de la Municipalidad de Punta Arenas, deberá priorizarse su conversión a microforma:

Documentación que se encuentra con daño que arriesga destrucción o ilegibilidad parcial o total:
Deberán convertirse prioritariamente a microforma aquellos documentos oficiales y aquellos que no siendo oficiales se requiera conservar, que se encuentren en estado de daño que arriesga su destrucción o ilegibilidad inminente. La microforma deberá realizarse en la situación en que se encuentre el documento, debiendo el ministro de fe dejar constancia de su apariencia, de las partes faltantes y de cualquier otro detalle que considere importante consignar.

Documentación que se encuentran en estado ilegible.
Son aquellos documentos que están en un muy mal estado de conservación física, ya que presentan severo daño físico y cuyo contenido es ilegible.

Tal circunstancia debiera ser notificada al funcionario encargado, con el fin de que se tomen las medidas administrativas correspondientes que permitan su reconstitución –si es posible– a través de copias fieles que existan del documento.

Documentación con daño por desastres:
Se trata de aquellos documentos que, por diversas circunstancias, tales como inundaciones, terremotos, lluvias, incendios, entre otros, quedan inutilizados, y que por tanto se debe proceder a su incineración para evitar su mal uso y otros efectos nocivos para la salud.

Sobre el particular, la Contraloría General de la República señala que dicha circunstancia es un imprevisto imposible de resistir y constituye un caso fortuito o de fuerza mayor, regulador por el artículo 45 del Código Civil. Por ende, se debe tener en consideración la jurisprudencia administrativa existente sobre la materia.

En este caso, el procedimiento que dará inicio previa consulta de la Unidad requirente a la Dirección de Asesoría Jurídica, para que pondere los antecedentes y emita el respectivo informe sobre la procedencia o no de su eliminación en el estado en que se encuentren.

La consulta que realice la Unidad requirente deberá contener de modo expreso y claro, si a juicio del solicitante, es necesaria su eliminación, y si está de acuerdo o no con su destrucción.

13.4 Digitalización Documental o Microforma de los Documentos Oficiales.

Este procedimiento se seguirá para la digitalización de los documentos municipales que tengan carácter oficial, como por ejemplo lo son los decretos, oficios y resoluciones en sus versiones originales. Igualmente deberán pasar a microforma aquellos documentos privados aprobados por la Municipalidad de Punta Arenas, como son por ejemplo los contratos y convenios, y todo aquel documento no oficial de

la Municipalidad respecto del cual la unidad a cargo, la Dirección de Cultura y/o la Dirección de Asesoría Jurídica estime que tiene un valor documental comprobable ya sea por su valor probatorio, cultural, histórico u otro que se especifique.

De acuerdo con la Ley N° 21.180, la microforma será el soporte que dé sustento al documento original en términos tales que éste pueda ser visto y leído con la ayuda de equipos visores o métodos análogos, digitales o similares; y pueda ser reproducido en copias impresas, esencialmente iguales al documento original. Para estos fines se seguirán las instrucciones de la Ley N° 18.845 y su reglamento.

Para que la digitalización tenga valor de copia fiel deberá contar con los siguientes elementos:

a) La imagen electrónica que representa el aspecto y contenido del documento en el soporte de origen. El documento por copiar debe ser el original, no se admite la microforma en base a fotocopias del original u otro tipo de reproducción.

b) Deberá contener, como metadatos obligatorios, a lo menos, la referencia a su condición de copia fiel de documento original en soporte papel; resolución de la captura; cantidad de páginas del documento original; fecha y hora de la diligencia; identidad del (de la) ministro(a) de fe y referencia al estado de conservación, elementos que compondrán el acta de apertura.

c) Deberá contar con firma electrónica avanzada del (de la) ministro(a) de fe.

El **acta de apertura** es el documento por el cual se deja constancia de la fecha de la diligencia, de la identidad del ministro de fe y de una declaración de éste relativa al estado de conservación del o de los documentos originales, con indicación de cualquier observación acerca de enmendaduras, raspaduras, adiciones, apostillas, entrerrenglonaduras y otras alteraciones que puedan apreciarse a simple vista en el documento original y que no se encontraren salvadas en éste. Este documento representa el inicio del proceso de microforma.

Una vez realizada la microforma deberá confeccionarse un **acta de cierre,** que es el documento emanado del ministro de fe, en la cual se estamparán la firma y un signo, sello o timbre indeleble y auténtico de dicho funcionario. Etapa de término del proceso de microforma. El original de ambas actas se mantendrá en el archivo o registro respectivo.

Los documentos digitalizados deberán almacenarse en ficheros individuales con indicación de su número de serie de documento y su materia, deberán organizarse forma ordenada en las carpetas que se dispongan en el servidor municipal que sirva de repositorio y también en un soporte digital físico (ejemplo: unidades pendrive, flash o disco).

De acuerdo con el dictamen N° 34.050 de 2016 confirmado por el dictamen N° E124197 de 2021 de la Contraloría General de la República, deberán remitirse al Archivo Nacional copia digital de las microformas de aquellos documentos por la Municipalidad que hayan cumplido cinco años de antigüedad desde su emisión.

13.5 De la Digitalización de documentos no oficiales

La digitalización de aquellos documentos municipales que no tengan el carácter de oficiales, y que a juicio de cada unidad merezcan su conservación deberá realizarse por la misma unidad municipal.

Será obligatorio para cada unidad, digitalizar los memorándums y otro tipo de comunicaciones internas propias que tengan bajo su archivo en soporte papel. Respecto de los antecedentes que acompañan a los memorándums deberá analizarse caso a caso la necesidad de digitalizarlos o no, teniendo especialmente a la vista si se trata de documentos respecto de los cuales consta que ya hayan sido digitalizados por otra unidad.

Asimismo, se requiere para la Oficina de Partes mantener la digitalización de todos los documentos recibidos.

Los documentos digitalizados deberán almacenarse en ficheros individuales con indicación de su número de serie y su materia, deberán organizarse forma ordenada en las carpetas que se dispongan en el servidor municipal que sirva de repositorio y también en un soporte digital físico (ejemplo: unidades pendrive, flash o disco).

13.6 Conservación Y Uso De Las Microformas

En la confección de las microformas que resulten de un proceso de digitalización de documentos originales en soporte papel, se deberá atender especialmente a que éstas mantengan sus calidades de documento y de archivo.

Se entiende por **calidad de documento** de la microforma el ser copia fiel de un original en soporte papel incluso en sus imperfecciones. La **calidad de archivo** se refiere a la condición de la microforma de mantener en forma fiel, indeleble, legible e íntegra su calidad de documento.

El Repositorio será responsabilidad del respectivo funcionario a cargo del archivo, sin perjuicio de la celebración de convenios de cooperación entre diferentes órganos o de la contratación de una empresa privada para que preste el servicio.

El Repositorio deberá garantizar que se respeten las normas sobre publicidad de los documentos, contenidas en la Ley 18.575 sobre Bases de la Administración del Estado y otras leyes especiales.

El Repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información en él contenida. Para ello la información deberá ser respaldada en copias de seguridad, bajo las siguientes características:

a) La información deberá ser respaldada con cada proceso de actualización de documentos.
b) Se deberá mantener una copia de seguridad en el lugar de operación de los sistemas de información y otra en un centro de almacenamiento de datos electrónicos especializado. Este centro de almacenamiento de datos electrónicos, que puede ser propio o provisto por terceros, deberá cumplir con condiciones tales como un estricto control de acceso, un completo y detallado registro de entrada y salida de respaldos, resguardo de la humedad, temperatura adecuada, control del riesgo de incendio y otras.
c) El esquema de respaldo deberá ser simple, basado en generación de copias acumulativas, con el objeto de mantener la historia de la información en el mínimo de versiones posibles.
d) La seguridad, integridad y disponibilidad del Repositorio deberán estar caracterizadas por:
    - Medidas de seguridad y barreras de protección, frente al acceso no autorizado de usuarios.
    - Contar con monitoreo y alarmas que se activen cuando ocurra un evento no autorizado o fuera de programación, para el caso de eventuales fallas de las medidas de seguridad al acceso.
    - La sustitución de la información, por la versión más reciente que se disponga, en el menor tiempo posible, en casos de alteración no programada de aquella.

- La existencia de un programa alternativo de acción que permita la restauración del servicio en el menor tiempo posible, en caso de que el Repositorio deje de operar por razones no programadas.

13.7 Destrucción de documentos oficiales.

La Municipalidad de Punta Arenas deberá adoptar las medidas necesarias para garantizar los documentos originales en soporte papel, aun cuando hayan sido pasados a microforma.

La destrucción física de las unidades o series documentales en soporte papel, deberá realizarse empleando cualquier método que garantice la imposibilidad de reconstrucción de los documentos y su utilización posterior. En atención a su impacto medio ambiental.

13.8 Destrucción de documentos no oficiales

Se instruye la destrucción de todos aquellos documentos que no tenga el carácter de oficiales, una vez cumplidos cinco años desde su generación, debiendo considerarse especialmente para estos efectos, aquellas fotocopias de documentos originales que ya se encuentren efectivamente digitalizados o convertidos en microforma, a disposición de todos los funcionarios.

Sin embargo, previo a la destrucción de documentos no oficiales que se encuentren archivados en las distintas unidades, la Dirección a cargo de dichos documentos deberá haber realizado el análisis de pertinencia sobre digitalizar previamente dichos documentos.

Asimismo, la eliminación solo podrá llevarse a cabo tras el correspondiente análisis de las características históricas, culturales, administrativas, jurídicas e informativas de la documentación, levantando un acta oficial de la eliminación en que consten que no concurren dichas características.

13.9 Procedimiento para la destrucción de documentos

Para la eliminación de documentos **no oficiales**, hay que considerar los siguientes pasos:

- Tener en cuenta los requisitos legales y criterios institucionales, distinguiendo especialmente el tipo de documento, si es que ya fue digitalizado o convertido en microforma y la importancia que puede haber adquirido su versión original en soporte papel con el transcurso del tiempo.

- Realizar un inventario de los documentos que serán eliminados, firmada por la jefatura de la Unidad correspondiente, y remitirlos a la Dirección de Control, a fin de que pueda revisar tal documentación y objetar tal eliminación si así lo estimare.

- De existir duda de la unidad a cargo de la documentación o de la Dirección de Control, se podrá excepcionalmente solicitar informe a la Dirección de Asesoría Jurídica, para aquellos casos que no estén claramente definidos por la ley o por los reglamentos aplicables. La solicitud de informe a la Dirección de Asesoría Jurídica debe indicar las razones que motivan su consulta, como los hechos que justifican la duda acerca la eliminación o conservación de los documentos consultados.

- Una vez obtenido el visto bueno de la Dirección de Control, la Unidad requirente puede continuar con el procedimiento.

- Se deberá realizar un **Acta de apertura** de eliminación, donde se expongan las circunstancias que concurren para la eliminación y los procedimientos llevados a cabo. El acta debe ser firmada por todos quienes participaron en el proceso de la selección de documentos a eliminar.

- Se debe tramitar el Decreto Alcaldicio que apruebe la destrucción, la que debe estar acompañada por el acta de inventario de la documentación seleccionada para eliminar más el acta de eliminación correspondiente.

- Una vez decretado se debe proceder a la eliminación física de la documentación mediante un mecanismo que garantice su total destrucción, la imposibilidad de reconstrucción de los documentos y su utilización posterior.

- Levantar un Acta de ejecución de la eliminación, donde conste como se llevó a cabo el proceso. Se recomienda incluir material visual (videos/fotografías). Dicha acta deberá ser suscrita por el Secretario Municipal.

- Se debe enviar copia del acta de ejecución de la eliminación a la Dirección de Control, junto a los demás antecedentes en formato digital.

13.10 Situaciones especiales en que no se debe destruir documentación

a) Al respecto se tienen presentes las disposiciones legales especiales y las instrucciones generales de la circular N° 28.704 de la Contraloría General de la República.

b) Es responsabilidad de la unidad a cargo de los documentos, que se respeten las disposiciones especiales que rijan sobre la materia, debiendo mantenerse actualizados constantemente sus procesos.

   A modo de ejemplo, indicamos las que existen respecto de los siguientes documentos:

   - **Actas Municipales:** Estas deberán conservarse y remitirse al Archivo Nacional, aquellas que tengan más de 60 años de antigüedad.

   - **Licencias Médicas y Documentos Previsionales:** La eliminación de documentos de carácter previsional se regula, a su vez, por las instrucciones que dicte o haya dictado la Superintendencia de Seguridad Social, en su calidad de autoridad técnica de control de las instituciones públicas de previsión y del Servicio Nacional de Salud (hoy Servicios de Salud), de que está investida en virtud de lo dispuesto en los artículos 3º y 27º de la Ley N° 16.395. En lo relativo a licencias médicas y documentación sobre Subsidios por Incapacidad Laboral, éstos se deben conservar durante 5 años desde su otorgamiento, al igual que la documentación de los servicios de bienestar del sector público. Los expedientes médicos, evaluaciones de invalidez, declaraciones de irrecuperabilidad, y dictámenes al respecto, se deben conservar en forma permanente.

     Estos se deberán conservar más allá de la total extinción de la obligación para el eventual examen de las operaciones a que refieran.

   - **Documentos con valor histórico o cultural:** Para estos efectos debe tener en especial consideración lo preceptuado en la circular N° 051, del 9 de febrero de 2009, sobre disposiciones y recomendaciones referentes a conservación, transferencia y eliminación de antecedentes, de la Dirección de Bibliotecas, Archivos y Museos, especialmente aquello referido en el punto V, sobre

"Eliminación de Documentos", N°1 "... está prohibida la destrucción de todo documento de valor histórico o cultural, aunque haya sido microcopiado o micrograbado. Se entiende que tiene tal carácter aquellos documentos pertenecientes a la Administración Pública respecto de los cuales el Conservador del Archivo Nacional ejerza el derecho de oposición a que se refiere el Artículo 6°- de la Ley Nº 18.845". Lo expuesto en relación con el artículo 6º, de la Ley N°18.845, de 1989.

Además, todo documento de la Municipalidad de Punta Arenas que hace identificable a la comuna, tales como Memorias Municipales, Catastros, Expedientes de la Dirección de Obras Municipales, Planos Reguladores, Ordenanzas, Reglamentos, Estudios u cualquier otro documento transcendental.

- **Documentación Indígena:** El Archivo General de Asuntos Indígenas, dependiente del Archivo Nacional, conservará los documentos oficiales que se generen en materia indígena. No existe norma que permita su destrucción, por lo que se debe conservar permanentemente.

- **Documentos de la deuda pública, especies valoradas u otros efectos:** Se eliminan dos años después del examen de la Contraloría General, trámite en el cual también debe intervenir el Contralor General o su delegado.

- **Libros, documentos y cuentas aprobadas:** Se incinera después de tres años desde su revisión definitiva, salvo que el Contralor General considere especial interés en conservarlo.

- **Documentos relativos a personal:** Puede prescindirse de aquellos que daten de cinco años si los antecedentes están registrados en libros o en tarjetas individuales físicos o digitales. Respecto de los documentos en soporte papel que debe registrar la Contraloría en el sistema SIAPER la Municipalidad de Punta Arenas los deberá mantener archivados formatos físicos, junto con los documentos o certificados oficiales que fueron registrados para estos efectos. Podrán eliminarse una vez convertidos a microforma y cumplido el plazo de 10 años desde que son microformados, según exige la ley.

- **Documentos representativos de obligaciones pendientes:** Estos documentos deberán ser conservados más allá de la total extinción de la obligación para el eventual examen de las operaciones a que se refieran. El destino definitivo de la documentación estará condicionado a los resultados de los exámenes que se practique.

- **Documentos de Fiscalía o Jurídicos:** Se pueden eliminar según reglas generales, previa autorización de la Dirección de Asesoría Jurídica en cada caso.

- **Documentos previsionales:** Éstos se deberán conservar más allá de la total extinción de la obligación para el eventual examen de las operaciones a que refieran.

- **Documentos tributarios:** La destrucción de documentos de carácter tributario se rige por las normas especiales contenidas, entre otras, en los artículos 17, inciso 2º y 97º, Nº16 del Código Tributario, y por las instrucciones que haya impartido o imparta al efecto el Servicio de Impuestos Internos.

- **Documentos de Oficina de Partes:** Los Decretos Alcaldicios, reglamentos, ordenanzas emitidas en soporte papel en sus versiones originales, deberán conservarse indefinidamente, mientras no hayan sido convertidas en microforma y no haya transcurrido el plazo legal de 10 años para destruirlos conforme a la ley. Para ello, se deberá adoptar las medidas necesarias en el legajo de

documentos para ser archivados, para facilitar sus consultas.

Respecto de los documentos recepcionados por oficina de partes, se recomienda su eliminación una vez cumplidos cinco años, siempre que hayan sido debidamente digitalizados.

- **Documentos relativos al Departamento Patentes Comerciales:** Se considera útil mantenerlos durante cinco años, una vez transcurrido este plazo, podrán ser eliminados del archivo los que presenten Término de Actividad Económica dentro de la comuna y/o traslado de la actividad comercial hacia otra comuna.

- **Documentos relativos a la Dirección de Tránsito y Transporte Público:** Los instrumentos consistentes básicamente en permisos de circulación y sus respectivos respaldos, corresponden a documentación que es objeto de revisión en auditorías al macroproceso de ingresos realizadas por la Contraloría General de la República, por lo que sólo procederá su eliminación, en caso de tal muestra haya sido examinada por el propio Órgano Contralor.

  En Cuanto a lo relativo a licencias de conducir, los oficios, memorándum y demás documentación administrativa, se deberán conservar al menos por 5 años. Las carpetas con antecedentes de los conductores deben mantenerse en forma definitiva. Las carpetas de contribuyentes que hayan fallecido se podrán eliminar, previa revisión interna contra la inscripción en el Registro Electoral y / o Registro Civil. Esta revisión deberá realizarse al 31 de diciembre de cada año.

- **Documentos relativos al Juzgado de Policía Local:** Conforme a lo dispuesto en el art. 2 de la Ley 20285, los Tribunales de Justicia se encuentran excluidos de la referida normativa, haciéndose aplicables su propio estatuto orgánico.

ANÓTESE, COMUNÍQUESE, y una vez hecho, **ARCHÍVESE.**

HERNÁN ALTAMIRANO ABURTO
ALCALDE (S)

JUAN CISTERNA CISTERNA
SECRETARIO MUNICIPAL (S)

HAA/RVC/JCC/DSO.-
DISTRIBUCIÓN:
- Dirección Servicios Generales
- Dirección Jurídica
- Antecedentes
- Archivo.-