Ministerio de Vivienda y Urbanismo

Gobierno de Chile

APRUEBA POLÍTICA DE SEGURIDAD DE LA INFORMACION PARA EL SERVIU REGION DE AYSÉN.

RESOLUCION EXENTA 831

COYHAIQUE, 19 MAY 2011

VISTOS:

a. Lo dispuesto en el D.L. N° 1.305, de 1975 que reestructura y regionaliza el Ministerio de Vivienda y Urbanismo;

b. Lo dispuesto en el D.S. N° 83, (MINSEGPRES), de 2004 que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos;

c. Lo dispuesto en la Norma Chilena Nch W 2.777, (IN N), de 2003 sobre código de práctica para la gestión de seguridad de la información;

d. Lo dispuesto en la Resolución Exenta N° 4.287, (V. Y U.), de 2005 que fija Políticas para el uso de Correo Electrónico Institucional;

e. Lo dispuesto en la Resolución Exenta N° 5.033, (V. Y U.), de 2005 que aprueba la Política de uso de la Red Informática Interna para el Ministerio de Vivienda y Urbanismo; sus Secretarías Regionales Ministeriales y de los Servicios de Vivienda y Urbanización;

f. Lo dispuesto en la Resolución Exenta N° 6710, (V. Y U), de 2007 que establece la política de uso del Servicio Institucional de Mensajería Instantánea;

g. Lo dispuesto en la Resolución Exenta N° 831, (V. Y U.), de 2006 que aprueba la Política de Licenciamiento de Software para el MINVU;

h. La Resolución Exenta N° 072, (SERVIU Región de Aysén), de 2010 mediante la cual se designa a la Encargada de Seguridad de la Información;

i. La Resolución Exenta N° 456, (SERVIU Región de Aysén), de 2011 mediante la cual se complementa Resolución Exenta N° 072, (Serviu Región de Aysén), de 2010 mediante la cual se establecen las funciones de la Encargada de Seguridad de la Información;

j. La Resolución Exenta N° 1929, (V. Y U.), de 2011 que aprueba la Política de la Seguridad de la Información para el Ministerio de Vivienda y Urbanismo;

k. La Resolución N° 1.600, de 2008 de la Contraloría General de la República, que fija las normas sobre exención del trámite de toma de razón;

l. Las facultades que me confieren el D.S. 355 de 1976. de V. y U,y el D.S N° 140 fecha 23/12/2010, ambos del MINVU, que me designa como Director Serviu Región de Aysén; y

TENIENDO PRESENTE:

a. Que el Comité de Ministros de Desarrollo Digital y la Secretaria de Desarrollo Digital, comprende la incorporación de Tecnologías de Información en las Comunicaciones de los órganos de la Administración del Estado, con el fin modernización del estado mediante el desarrollo de e-gobierno.

b. Que se han dictado una serie de normas técnicas entre las que se encuentra el Decreto Supremo N° 83 de 2005, del Ministerio Secretaria General de la Presidencia, que aprueba norma técnica para los organismos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos, y la Norma ISO 27000 (NCh-ISO 27001.Of2009), que proporcionan un marco de gestión de la seguridad de la Información utilizable por cualquier tipo de organización, pública o privada.

c. Las políticas internas de Uso de la Red Institucional, de Correo Electrónico, de Licenciamiento de Software y de uso de Servicio Institucional de Mensajería Instantánea, sancionadas en las Resoluciones Exentas (V. Y U) N° 5033 de 2005, N° 4287 de 2005, N° 831 de 2006 y N° 6710 de 2007.

d. Que, de conformidad con lo previsto en el articulo 11 del Decreto Supremo N ° 83, es necesario establecer Política de seguridad de la Información y en el control A.5.1.1. de la norma ISO 27001, es necesario aprobar un documento de Política de Seguridad; dicto lo siguiente

RESOLUCIÓN:

1. Apruébase la Política de Seguridad de la Información para el SERVIU Región de Aysén. Por el Texto adjunto en esta Resolución.
2. Establécese la obligación de la Encargada de Seguridad de la Información del Serviu Región de Aysén de efectuar la difusión de la Política fijada por este instrumento, así como realizar todas las acciones tendientes a su implementación y velar por su estricto cumplimiento.
3. Se deja constancia que la presente Resolución no irroga gastos para el presupuesto de este Serviu.

ANÓTESE, NOTIFÍQUESE, CÚMPLASE Y ARCHÍVESE.

MINISTERIO DE VIVIENDA Y URBANISMO DIRECTOR SERVIU REGION DE AYSEN

PEDRO SADE BARRIA
ARQUITECTO
DIRECTOR SERVIU REGION DE AYSEN

PSB/PRF/IIM/GIH/CDM/ENC/GNZ
DISTRIBUCION A :
- Jefes Departamentos (5)
- Delegación Provincial Aysén
- Unidad de Gestión de la Calidad
- Contralor Regional
- Oficina de partes.

1. DECLARACIÓN INSTITUCIONAL

El Serviu Región de Aysén promueve y apoya el cumplimiento del DS N° 83, lo que implica un compromiso de proteger los activos de la información institucionales de las amenazas, riesgos, etc.
Así como también de desarrollar y ejecutar un Plan de acción de mejora continua de modo de asegurar una adecuada gestión de la seguridad de la información en sus diferentes ámbitos de aplicación.

2. TERMINOS Y DEFINICIONES

2.1. SEGURIDAD DE LA INFORMACIÓN

2.1.1. **Confidencialidad:** Se garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma.

2.1.2. **Integridad:** Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

2.1.3. **Disponibilidad:** Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

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

2.1.5. Sistemas 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.

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

2.1.7. Activos de la Información: Corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

2.1.8. 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 del Servicio.

2.1.9. 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.

2.1.10. COMITÉ DE SEGURIDAD DE LA INFORMACION: El comité de Seguridad de la información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Servicio, destinado a garantizar el apoyo manifiesto de la autoridad a las iniciativas de seguridad.

2.1.11. RESPONSABLE DE LA SEGURIDAD INFORMATICA: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y asesorar en materia de seguridad de la información a los integrantes del Servicio que así lo requieran.

2.1.12. INCIDENTES DE SEGURIDAD: Un incidente de seguridad es un evento adverso en un activo de la información, 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.

3. OBJETIVOS DE LA GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

- Proteger los activos de información.

- Catastrar y Clasificar los activos de información que son parte de los procesos estratégicos de la institución, con el fin de asegurar su disponibilidad ante cualquier evento.

- Analizar el impacto de los riesgos identificados en los procesos estratégicos de la institución, permitiendo elaborar planes de contingencia que disminuyan su ocurrencia.

- Entrenar al personal del SERVIU Región de Aysén en el correcto uso de la plataforma tecnológica de la institución, a través de jornadas de capacitación enfocadas en la seguridad de la información.

- Adoptar y difundir las Políticas de Seguridad de la Información existentes en el MINVU al SERVIU Región de Aysén, así como fomentar el desarrollo de procedimientos regionales que abarquen los aspectos de la ISO 27.000.

4. ALCANCE

Esta Política se Seguridad de la información se aplica en todo el ámbito del Servicio, 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.
Es decir, esta política define las directrices de la Seguridad de la Información para todas las unidades de trabajo, secciones, departamentos, delegación provincial y prestadores de servicio externos en el SERVIU Región de Aysén, que permitan preservar la confidencialidad, integridad y disponibilidad de la información. Los ámbitos de acción relacionados con el contenido de la política son el uso de Internet y correo electrónico, uso de software autorizado en la plataforma tecnológica de la institución, uso de servicios de mensajería, uso adecuado de los recursos informáticos, obligaciones y responsabilidades de los usuarios/as.

5. AMBITO DE APLICACIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

El ámbito de aplicación de la Política de Seguridad contempla los Dominios contenidos en la Nch-ISO 27002.2009 y que son los siguientes:

- Organización de la seguridad de la información: Orientado a administrar la seguridad de la información dentro del Servicio y establecer un marco gerencial para controlar su implementación.
- Gestión de Activos: Destinado a mantener una adecuada protección de los activos del Servicio.
- Seguridad asociada a los recursos humanos: Orientado a reducir los riesgos de error humano, comisión de ilícitos contra el Servicio o uso inadecuado de las instalaciones.
- Seguridad física y del ambiente: Destinado a impedir accesos no autorizados, daños e interferencia a las unidades, departamentos e información del Servicio.
- Gestión de las comunicaciones y operaciones: Dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y medios de comunicación.
- Control de acceso: Orientado a controlar al acceso lógico a la información.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: Orientado a garantizar que la seguridad sea una parte integral de los sistemas de información y se incluya en la etapa de formulación del software.

- Gestión de incidentes de la seguridad de la información: Destinado a asegurar que las debilidades y eventos de seguridad de la información asociados a sistemas de información son comunicados de manara de permitir tomar acciones correctivas a tiempo.
- Gestión de continuidad del negocio: Dirigido a considerar los aspectos de la seguridad de la información de la gestión de la continuidad operativa de manera de hacer frente a las interrupciones de las actividades institucionales y proteger los procesos críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.
- Cumplimiento: Orientado a evitar los incumplimientos de cualquier ley, estatuto, regulación u obligación contractual legal y de cualquier requisito de seguridad a los cuales puede estar sujeto el diseño, operación, uso y gestión de los sistemas de información.

6. REQUISITOS DE CUMPLIMIENTO

El SERVIU Región de Aysén en cumplimiento con el Decreto Supremo N° 83 para los órganos de la Administración del Estado, debe cumplir con los articulas N° 36 y N° 37, los cuales indican que se deberá cumplir con las disposiciones contenidas en el capítulo 3 de la Norma Chilena 2777 de "Tecnología de la Información -Código de práctica para la gestión de la información". El propósito del cumplimiento de esta norma, es alcanzar el Nivel avanzado de seguridad.

7. PRIVACIDAD

El SERVIU Región de Aysén se reserva el derecho de monitorear, duplicar, grabar y/registrar la información referente al uso que hacen los usuarios de los recursos tecnológicos, con o sin su notificación, esto incluye al correo electrónico, acceso a Internet, acceso a archivos, inicios de sesión de red o cambios en los niveles de acceso.

8. DIFUSIÓN DE LA POLITICA

Una vez aprobada la Política de Seguridad de la Información por la alta dirección de la institución, ésta será dada a conocer a través de correo electrónico a todos los funcionarios del Servicio. Además, trimestralmente se realizarán envíos de correos informativos con tópicos específicos de la política a los funcionarios del SERVIU Región de Aysén. Además, la Política de Seguridad de la Información se dará a conocer a las partes externas relevantes.
Por otra parte se hará entrega de la Política de Seguridad a los funcionarios/as que ingresen al Servicio.

9. REVISIÓN Y EVALUACIÓN PERIODICA

La política de Seguridad de la Información deberá ser redactada por la Encargada de Seguridad de la Información, quién en conjunto al Comité de Gestión de Seguridad y Confidencialidad de la Información serán los responsables de mantenerla y revisarla anualmente. Los cambios en la política serán el reflejo de cambios en los estándares, incidentes de seguridad, nuevas vulnerabilidades o nuevos procesos y/o servicios en la infraestructura técnica u organizacional.
Reevaluándose en forma periódica, a lo menos cada 3 años. El Serviu región de Aysén reevaluará la Política de información cada tres años.

10. POLÍTICAS SEGURIDAD DEFINIDAS POR EL MINVU APLICABLES EN EL SERVIU REGION DE AYSÉN

10.1. Resolución N° 4287 FIJA Políticas para uso de correo electrónico en el Minvu.
10.2. Resolución N° 5033 aprueba Políticas de uso de red informática interna del Minvu.
10.3. Resolución N° 6710 establece Política de uso de SIMI (servicio institucional de mensajería instantánea).
10.4. Resolución N° 831 aprueba Política de licenciamiento de software para el Minvu.

11. ROLES Y RESPONSABILIDADES

11.1. Comité de Gestión de Seguridad y Confidencialidad de la Información del Serviu Región de Aysén.

Procederá a revisar y proponer a la máxima autoridad del Servicio 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 afecten a los recursos de información frente a las amenazas más importantes; 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; garantizar que la seguridad sea parte del proceso de planificación de la información; promover la difusión y apoyo a la seguridad de la información dentro del servicio y coordinar el proceso de administración de la continuidad de las actividades del Serviu Región de Aysén.

El Comité estará compuesto por funcionarios/as del Serviu Región de Aysén, que sean representantes estratégicos en las distintas áreas del servicio, por lo que a lo menos estará compuesto por:

- Jefes de Departamento
- Delegado/a Provincial de Puerto Aysén
- Contralor/ra Interno
- Encargado/a SIAC
- Encargado/a unidad de Gestión de la Calidad
- Encargado/a de Seguridad de la Información Serviu Región de Aysén.

11.2. Encargado/a de Seguridad de la Información Serviu Región de Aysén

Tiene las siguientes responsabilidades:

- Desarrollar, documentar y mantener las Políticas de Seguridad de la información y velar por su correcta aplicación al interior del SERVIU Región de Aysén
- Establecer puntos de enlace con el Encargado de Seguridad de la Información del MINVU y SERVIUS Regionales, que le permitan estar al tanto de las tendencias, normas, decretos y métodos de seguridad pertinentes.
- Liderar las soluciones a los eventuales incidentes de seguridad computacionales
- Ser parte del Comité de Gestión de Seguridad y Confidencialidad de la Información del SERVIU Región de Aysén.
- Proponer al Comité de Gestión de Seguridad y Confidencialidad de la Información los procedimientos y el Programa de trabajo necesarios para cubrir las actividades asociadas a su Rol.
- Validar y proponer al Comité de Gestión de Seguridad y Confidencialidad de la Información los Planes de Contingencia para asegurar la continuidad de operaciones informáticas criticas para la Institución
- Administrar y coordinar diariamente el proceso de Seguridad Informática
- Establecer en conjunto con el Comité de Gestión de Seguridad y Confidencialidad de la Información del SERVIU Región de Aysén, la difusión de las Políticas de Seguridad definidas.

- Investigar y proponer, software y hardware existente en el mercado que apoyen las tareas de seguridad de la plataforma computacional del SERVIU Región de Aysén.
- Mantener constantemente informada a la jefatura, de cualquier vulnerabilidad detectada dentro de la plataforma computacional del SERVIU Región de Aysén.
- Garantizar el cumplimiento de las políticas, estándares, procedimientos o guías contenidas en las políticas internas de seguridad.

Se debe estimular una aproximación multidisciplinaria a la Seguridad de la Información, como por ejemplo, involucrar la cooperación y colaboración de los directivos, usuarios, administradores, diseñadores, personal de seguridad y especialistas con experiencia en áreas tales como gestión de seguros y riesgos

11.3. Propietario de la Información.

Los propietarios de la información son los Jefes de Departamento y/o Área de las unidades de negocio, quienes son responsables de los bienes de información que se generan y se utilizan en las operaciones de su unidad. Las áreas de negocio deben ser conscientes de los riesgos, de tal forma que sea posible tomar decisiones para disminuirlos, Entre las responsabilidades de los propietarios de información se tienen:

- Clasificar la información y Revisión periódica de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos del negocio.
- Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- Determinar los criterios y niveles de acceso a la información.
- Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
- Determinar los requerimientos de copias de respaldo para la información que les pertenece.
- Tomar las acciones adecuadas en caso de violaciones de seguridad.
- Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.
- Pueden delegar sus responsabilidades en sus subrogantes, sin embargo el propietario se mantiene como el último responsable de la seguridad del bien.
- Los niveles de autorización se deberían definir claramente y documentar.

11.4. Custodio de información.

Son responsables de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su administración.

11.4.1. División Informática Minvu

- Administración de los accesos a nivel de red (sistema operativo)
- Administrar accesos a nivel de bases de datos.
- Administrar los accesos a archivos físicos de información almacenada en medios magnéticos, ópticos o impresos.
- Implementar controles definidos para los sistemas de Información, incluyendo investigación e implementación de actualizaciones de seguridad de los sistemas en coordinación con el Departamento de Administración y Finanzas.
- Desarrollar procedimientos de autorización y autenticación.
- Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de información que custodia.
- Investigar brechas e incidentes de seguridad.
- Entrenar a los funcionarios en aspectos de seguridad de información en nuevas tecnologías o sistemas implantados bajo su custodie.
- Asistir y administrar los procedimientos de respaldo, recuperación y plan de continuidad de sistemas.

11.4.2. **Oficina de Partes Serviu Región de Aysén:** Quien es responsable de la administración diaria de la seguridad de los respaldos físicos de los actos administrativos y de toda la comunicación oficial de la autoridad y directivos del Serviu Región de Aysén.

11.4.3. **Departamento de Administración y Finanzas:** Quien es responsable de la administración diaria de la seguridad de los respaldos físicos de los pagos y egresos efectuados por el Serviu Región de Aysén.

11.4.4. **Usuario:** Quien es la persona que utiliza información producida por los departamentos, delegación provincial y unidades del Serviu Región de Aysén como parte de su trabajo frecuente.
Funciones y Responsabilidades:

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas, cuando así se le indique.
- Reportar violaciones de la seguridad de información al Encargado de Seguridad de la Información.
- Asegurar el ingreso de información adecuada a los sistemas.
- Acatar las políticas de seguridad del MINVU y del Serviu región de Aysén.
- Utilizar la información únicamente para los propósitos autorizados.

11.5. Proceso de Autorización para las Instalaciones de Procesamiento de Información

El Departamento de Administración y Finanzas del SERVIU Región de Aysén, está encargado de controlar y autorizar la instalación de nuevos centros de procesamiento de información que se requieran implementar, entendiéndose como centro de procesamiento nuevos puntos de red, nuevas dependencias con conexión a red, nuevos servidores de procesamiento de información, nuevos servicios de red, entre otros.

11.6. Cooperación entre Organizaciones

Debe existir una red de contactos que facilite la cooperación entre el SERVIU Región de Aysén, el MINVU, la Secretaría Regional Ministerial y otros Servicios de Vivienda y Urbanización regionales, como también con las otras Instituciones del Estado y del sector privado, con el objetivo de que la cadena de procesos que permiten brindar servicios al SERVIU Región de Aysén sea segura y confiable, no sólo en sus procesos internos sino que también se requiere que las operaciones que se realizan con otras instituciones también lo sea.
Intercambio de Información: La División de Informática debe establecer niveles de servicio para la comunicación con las instituciones con las cuales actualmente intercambie información y debe definir Estándares de interoperatibilidad para los proyectos de desarrollo que garanticen un nivel mínimo de seguridad, estas definiciones deben ser extrapoladas a los desarrollos de sistemas que se externalizan con terceros.
Servicios externos: Se deben crear nexos formales que permitan la cooperación entre las instituciones privadas y el SERVIU Región de Aysén, para que los servicios contratados tengan una base sustentable ante contingencias.
Comunidad informática: El sitio Web de la Comunidad informática Gubernamental (wwwe2gcl) debe ser considerado como sitio oficial de comunicación gubernamental para el intercambio de información, experiencias y herramienta de trabajo.

12. SEGURIDAD DEL ACCESO DE TERCEROS

El acceso de un tercero a las instalaciones del SERVIU Región de Aysén donde se realiza el procesamiento de la información, debe estar basado en un contrato formal, el cual debe contener todos los requisitos de seguridad para garantizar el cumplimiento de las políticas, normativas y procedimientos de seguridad previamente establecidos por el SERVIU Región de Aysén.

13. EXTERNALIZACIÓN

En todos los proyectos donde se haya externalizado la responsabilidad del procesamiento de Información del SERVIU Región de Aysén, se debe establecer un contrato para asegurar el cumplimiento de todos los requisitos de seguridad definidos por el SERVIU Región de Aysén, ya sean Políticas de Seguridad, Metodologías para los Proyectos Tecnológicos, Normativas, Procedimientos, Controles de Seguridad u otros.

14. POLÍTICA DE CLASIFICACION y CONTROL DE BIENES INFORMATICOS

El objetivo de esta Política es mantener una protección apropiada de los bienes informáticos del SERVIU Región de Aysén
Se define como Bien Informático a cualquier componente tecnológico, sea este de hardware o software, y servicios que participan en la gestión de los procesos de la institución.
La designación de responsables de los bienes informáticos, permite mantener y administrar dichos recursos adecuadamente, por esta razón es necesario identificar los usuarios de todos los bienes informáticos, delimitando las responsabilidades sobre aquellos de asignación personal y/o por unidad de negocio

14.1. RESPONSABILIDAD DE LOS BIENES INFORMATICOS

El Departamento de Administración y Finanzas del SERVIU Región de Aysén, tiene las siguientes responsabilidades

14.1.1. Responsabilidad del Área de Explotación de Sistemas

Tiene la Responsabilidad de mantener

- **Bienes de Información**, tales archivos de datos, procedimientos de apoyo y operación, planes de continuidad, planes de recuperación de la información respaldada.
- **Bienes Físicos**, tales como Hardware para Servidores, Rack de Servidores, Equipos de comunicación, tales como Router(s), Switch(s), Firewal/(s) y Appliance en General.
- Servicios, tales como Servicio de Mensajería, Servicio de Administración de Red, Servicio de Monitoreo, Servicio de Operación e Infraestructura de red.

14.1.2. Responsabilidad del Área de Soporte Técnico Computacional

Tiene la Responsabilidad de mantener

- **Bienes de Información**, tales como material de entrenamiento, procedimientos de operación, transferencia de información del usuario cuando sea pertinente, licencias de software y medios magnéticos asociados.
- **Bienes Físicos** Equipamiento computacional en general (equipos de escritorio, equipos portátiles, Impresoras, Plotters y similares).
- **Servicios:** Servicio de Soporte preventivo y correctivo en Terreno.

14.1.3. Responsabilidad de la Sección de Servicios Generales

Tiene la Responsabilidad de mantener:

- **Bienes físicos:** Red eléctrica, infraestructura y mantención de edificio.
- **Servicios** Red Eléctrica, Telefonía y otros similares

14.2. CLASIFICACION DE LA INFORMACION

La información se debe clasificar para determinar prioridad y su grado de protección, ya que puede tener un grado de sensibilidad y criticidad variable algunos pueden adquirir un nivel adicional de protección o manipulación especial. Se debe usar un sistema de clasificación para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manipulación.

- **Decretos Supremos** Son actos administrativos dictados por el Presidente de la República en ejercicio de sus atribuciones y con formalidades legales, ya sea para ejecutar una ley o para realizar la administración del Estado que le está confiada. En el primer caso se denominan Decretos Reglamentarios o simplemente reglamentos y en el segundo caso, se denominan Decretos Supremos.
- **Decretos Exentos:** Se llaman Decretos Exentos aquellos que no están sujetos al trámite de Toma de Razón por parte de la Contraloría General de la República (CGR), En algunos casos se exige que estos decretos se envíen para su registro a la CGR
- **Resoluciones:** Son actos administrativos, emanados de las autoridades superiores del Ministerio, de las SEREMI y de los SERVIU, en ejercicio de sus funciones administrativas, de acuerdo a las facultades que les conceden la ley y los reglamentos orgánicos de los respectivos servicios.
- **Oficios:** Son aquellas comunicaciones escritas en las cuales se tratan materias del Servicio, derivadas del funcionamiento administrativo, técnico u operativo Los oficios se clasifican en Ordinarios, Secretos y Reservados.

15. SEGURIDAD DEL PERSONAL

15.1. SEGURIDAD EN LA DEFINICION DEL TRABAJO Y RECURSOS

Los estándares relacionados al personal deben ser aplicados para asegurar que los funcionarios sean seleccionados adecuadamente antes de ser contratados, puedan ser fácilmente identificados mientras formen parte del SERVIU Región de Aysén y que el acceso sea revocado oportunamente cuando un funcionario es desvinculado o trasladado. Adicionalmente deben desarrollarse los mecanismos necesarios para asegurar que el personal esté consciente de todas sus responsabilidades administrativas y acciones que aplican respecto del cargo y rol que le toca desempeñar, según se expresa en el Estatuto Administrativo que rige para los funcionarios públicos. Esta política se aplica a todos los funcionarios, personal Contrata, honorarios, outsourcing y proveedores.

Los empleados son el activo más valioso de la Institución, sin embargo, un gran número de problemas de seguridad pueden ser causados por descuido o desinformación, por ende se deben implementar procedimientos para manejar estos riesgos y ayudar al personal del SERVIU Región de Aysén a crear un ambiente de trabajo seguro.

Deben tomarse las medidas de precaución cuando se contrata, traslada y desvincula a los funcionarios. Para esto se deben implementar controles que permitan asegurar a comunicación oportuna de los cambios del personal y los requerimientos de acceso a recursos informáticos como aplicaciones, herramientas de escritorio, PC, etc. a los responsables de la administración de los Servicios de Información.

15.1.1. Acuerdo de Confidencialidad

Se debe confeccionar un acuerdo de confidencialidad de la información o de no divulgación entre el SERVIU Región de Aysén y sus funcionarios, agentes públicos, personal a honorarios y prestadores de servicio como parte de los términos y condiciones iniciales de empleo. Todos los usuarios correspondientes a terceras personas que requieran acceder a información y no estén cubiertos por un contrato, deberán firmar un acuerdo de confidencialidad antes de que tengan acceso a los equipos de procesamiento de información.

15.1.2. Términos y Condiciones de Contratación

El SERVIU Región de Aysén debe incluir en los términos y condiciones de contratación, la responsabilidad que tienen los funcionarios, agentes públicos, personal a honorarios y prestadores de servicio con relación a la seguridad de la información perteneciente al SERVIU Región de Aysén. Estas medidas deben notificarse a los involucrados, de manera tal de que se cumplan (a lo menos) las leyes relacionadas con los derechos de propiedad y las Políticas de seguridad informática del SERVIU Región de Aysén.

15.2. RESPUESTA A LOS INCIDENTES DE SEGURIDAD Y MAL FUNCIONAMIENTO

Los incidentes de seguridad y mal funcionamiento asociado a las Tecnologías de la Información deberán ser notificados al Departamento de Administración y Finanzas a través de la Sección Servicios Generales y Adquisiciones, quienes deberán mantener y aplicar los procedimientos operativos necesarios, los cuales serán aplicados ante la solicitud de asistencia de algún usuario. Todos los reportes asociados a incidentes o deficiencias de seguridad, deberán ser registrados por esta área, quienes deberán revisar, corregir y generar un informe con la solución implementada. Esta, información permitirá analizar el mal funcionamiento o incidentes recurrentes o de alto impacto. A su vez, esta base de conocimiento se tomará en cuenta en los procesos de revisión continua de la Política de Seguridad. Cualquier incidente que no pueda ser resuelto a nivel regional, deberá ser reportado a la División de Informática a través de la Mesa de Ayuda a Usuarios del MINVU.

15.2.1. Procesos Disciplinarios

Se debe aplicar un proceso disciplinario formal para los funcionarios, personal a honorarios y contratos de prestaciones de servicios que hayan violado las políticas y procedimientos de seguridad, avalado por la normativa vigente y Estatuto Administrativo según corresponda. Será el Comité de Seguridad y Confidencialidad de la Información del SERVIU Región de Aysén quienes deberán notificar al Director Regional o al Contralor Interno de la institución, para que ordene la investigación sumaria correspondiente y los integrantes del comité podrán actuar como órgano consultivo o perito en el proceso.

16. SEGURIDAD FISICA Y DEL AMBIENTE

16.1. AREAS SEGURAS

16.1.1. Perímetro de Seguridad Físico

El equipamiento computacional del SERVIU Región de Aysén debe protegerse físicamente de las amenazas, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables.

16.2. SEGURIDAD DE LOS EQUIPOS

16.2.1. Ubicación y Protección de los Equipos

El equipamiento debe mantenerse alejado de riesgos, peligros ambientales y oportunidades de acceso a personal no autorizado, por ende:

Se deben minimizar los riesgos tales como el fuego, el agua, la humedad, polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, radiación electromagnética, el hurto y robo.

Se deben monitorear las condiciones ambientales para identificar aquellas que podrían afectar adversamente la operación.

Se debe mantener actualizada una normativa de uso del equipamiento en la sala de servidores, visible para todas las personas que acceden a ella.

16.2.2. Suministro de Energía Eléctrica

La sala de servidor:
Deben proveer un suministro de energía eléctrica adecuado, conforme con las especificaciones del fabricante.
Deben estar protegidas ante fallas de energía y otras anomalías eléctricas.
Deben ser provistas de continuidad del suministro eléctrico para lo cual el SERVIU Región de Aysén debe contar con un servicio interrumpido de energía eléctrica (UPS).
Se debe verificar regularmente que los equipos de suministro interrumpido de energía eléctrica (UPS) tengan una capacidad de carga adecuada, y se encuentren operativos.

16.2.3. Seguridad del Cableado

Las líneas de energía eléctrica y telecomunicaciones en las instalaciones de procesamiento de información, deben estar sujetas a protección adecuada.
El cableado de redes se debe proteger de la intervención o daño de personas no autorizadas, mediante canaletas porta cables o equivalente.
Los cables de energía eléctrica deben estar separados de los cables de comunicación, para evitar interferencias.

16.2.4. Mantenimiento de los Equipos

Todo el equipamiento computacional debe tener su mantenimiento de acuerdo a las especificaciones e intervalos de servicios recomendados por el proveedor.
Solamente el personal autorizado por el Departamento de Administración y Finanzas y Soporte Técnico debe realizar la mantención del equipamiento computacional.
Se debe mantener un registro de todas las fallas y de los mantenimientos correctivos y preventivos.

16.2.5. Seguridad de los equipos fuera de la organización

Los equipos y dispositivos pertenecientes al SERVIU Región de Aysén que se ocupen fuera de las instalaciones de la Institución, no se deben dejar desatendidos en lugares públicos.

16.2.6. Seguridad en la eliminación de ítems en desuso o reuso de equipos

Para no comprometer la información sensible contenida en los equipos en desuso o reuso, se debe eliminar físicamente, borrar o sobrescribir.
Si se trata de un dispositivo de almacenamiento, se debe revisar para asegurar que cualquier dato sensible o licencie de software se haya respaldado o sobrescrito antes de la eliminación
En cuanto a los DVD, CD, Cinta en desuso, se deben destruir físicamente.

17. GESTION DE LAS OPERACIONES Y COMUNICACIONES

17.1. RESPONSABILIDAD Y PROCEDIMIENTO DE LAS OPERACIONES

17.1.1. Procedimientos de Operación Documentados

El Departamento de Administración y Finanzas debe mantener documentados y actualizado todos los procedimientos de operación con instrucciones detalladas para la ejecución de cada trabajo efectuado. Estos procedimientos deberán ser validados y aprobados por el Jefe del Departamento de Administración y Finanzas.
La documentación de los procedimientos debe ser desarrollada considerando los procedimientos documentados elaborados por la División de Informática del MINVU.

17.5. SEGURIDAD Y MANIPULACION DE DISPOSITIVOS

El SERVIU Región de Aysén debe contar con un procedimiento para la gestión de dispositivos computacionales, que permita a lo menos almacenar dispositivos en un lugar y ambiente seguro. Junto con esto, debe contar con el mecanismo de autorización de baja de especies para dispositivos en desuso (contenido en el OS. W 577/1978). Adicionalmente, todos los dispositivos que contengan información sensible deben ser administrados por el Área de Soporte Técnico Computacional, quien deberá garantizar que los dispositivos que ya no se necesiten, se eliminen sin riesgo, aplicando los procedimientos de Solicitud de Baja y Autorización de Salida de Especies, previamente establecidos por la División Administrativa del MINVU.

17.5.1. Seguridad de la Documentación de Sistema

Los manuales de operaciones, manual de usuario, estructuras de datos, procedimientos y otros, correspondientes a información de sistemas y/o servicios tecnológicos utilizados por el SERVIU Región de Aysén, deben estar almacenados de manera segura. Para que así sea, los dueños de dicha información deberán solicitar al Departamento de Administración y Finanzas los respaldos y resguardos necesarios.

17.6. INTERCAMBIOS DE INFORMACION y SOFTWARE

El intercambio de información que realice el SERVIU Región de Aysén con otras instituciones públicas o privadas, deberá ser controlado mediante un "Acuerdo de Intercambio de Información y Software", el cual deberá considerar:

- Normas técnicas y mecanismos de seguridad para el intercambio de información.
- Niveles de servicios.
- Responsabilidades.

17.6.1. Seguridad de los Dispositivos en Tránsito

Para evitar el acceso no autorizado a la información, el mal uso o corrupción durante el transporte físico o electrónico, se deben utilizar mecanismos de empaquetamientos suficientes como para proteger los contenidos de cualquier posible daño físico u electrónico durante el tránsito, tales como:

- Contenedores con llave.
- Empaque con detección de manipulación.
- Firma electrónica.

17.6.2. Seguridad en el Comercio Electrónico

Para proteger los sistemas del SERVIU Región de Aysén que utilicen software de terceros, que permitan el comercio electrónico (Asociado a pagos electrónicos vía tarjetas de crédito y débito bancarias, transferencias bancarias, Servipag, Tesorería General de la República y otros), se deberán considerar controles de autenticación, autorización, información de precio, registro de transacciones, verificación y sistema de pago, para protegerse de fraudes y responsabilidades.

Para ello es necesario generar convenios con socios comerciales mediante contratos de servicios.

Los sistemas de comercialización del SERVIU Región de Aysén deben divulgar entre los clientes los términos del negocio.

Los aspectos anteriores deben considerar la utilización de técnicas criptográficas.

17.6.3. Seguridad del Correo Electrónico

EL SERVIU Región de Aysén debe mantener un sistema de correo electrónico que incluya toda la seguridad necesaria para evitar riesgos tales como: vulnerabilidades, accesos no autorizados, denegación de servicio, comprobación de origen despacho entrega y aceptación.

17.1.2. Control de Cambio de Operación

Los cambios en las instalaciones y sistemas de procesamiento de información deben ser controlados por el Área de Explotación de Sistemas del MINVU, ya que los cambios de ambiente operacional pueden impactar las aplicaciones. Este control debe considerar llevar:

- Registros de cambios significativos
- Evaluación del impacto
- Se deben comunicar los cambios a todas las personas que sean pertinentes.
- Procedimiento para recuperar la condición inicial y abortar los cambios no exitosos

17.1.3. Procedimiento de Gestión de Incidentes

Se deben mantener los procedimientos de gestión a lo menos para los siguientes tipos de incidentes potenciales de seguridad:

- Procedimiento ante problemas de fallas de comunicación en la red WAN.Procedimiento ante fallas de comunicación con entidades externas.Procedimiento de corrección ante fallas del Portal institucional y aplicaciones

Procedimientos de corrección de problemas en la Infraestructura de red, correo electrónico, así como también en las aplicaciones contenidas en Microsoft SharePoint.

17.1.4. Separación de Instalaciones de Desarrollo y Operaciones

El Departamento de Administración y Finanzas a través del Área de Explotación de Sistemas MINVU, deberá gestionar las restricciones de acceso para los distintos ambientes de trabajo: "Ambiente de Desarrollo, de Pruebas y de Producción". Estas restricciones de utilización deberán ser respetadas por todos los individuos que interactúan con dichos ambientes.

17.2. ACEPTACION y PLANIFICACION DEL SISTEMA

El Área de Explotación de Sistemas MINVU, debe monitorear y hacer proyecciones de los requerimientos futuros, con el objeto de disponer de una adecuada capacidad de proceso y almacenamiento. Estas proyecciones deben tomar en cuenta los nuevos negocios y les requisitos del sistema. Los nuevos sistemas que se implementen en el SERVIU Región de Aysén deben cumplir con las etapas establecidas en las Fases de desarrollo de la "Metodología DINFO-MINVU", que está orientada a optimizar la calidad de los productos de Tecnologías de Información.

17.3. PROTECCION CONTRA SOFTWARE MALICIOSO

El Departamento de Administración y Finanzas debe implementar y mantener los controles necesarios para la prevención y detección de software malicioso, para ello debe contar a lo menos con:

- Sistemas de protección perimetral de la red del SERVIU Región de Aysén. Sistema de antivirus y control de malware en estaciones de trabajo y servidores. Control de la ejecución efectiva de las indicaciones contenidas en **la "POLÍTICA DE LICENCIAMIENTO DE SOFTWARE PARA EL MINVU".**

17.4. GESTION DE LA RED

El Departamento de Administración y Finanzas debe implementar controles para resguardar la integridad y confidencialidad de los datos que contienen los Sistemas del SERVIU Región de Aysén, así como los datos contenidos en los Sistemas de mensajería.

17.6.4. Sistemas Disponibles Públicamente

El Departamento de Administración y Finanzas, debe revisar que los sistemas y servicios del SERVIU Región de Aysén que serán accesibles a través Internet, cumplan con las legislaciones y normativas vigentes tales como: DS N°100, DS N°83 y DS N°81, previo a que el sistema o la aplicación se encuentre disponible públicamente.