Gobierno de Chile

Servicio Gobierno Regional
Magallanes y Antártica Chilena

RESOLUCIÓN EX. (G.R.) Nº 132 /

MAT : REEMPLAZA Y APRUEBA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN DEL SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTÁRTICA CHILENA.

PUNTA ARENAS, 30 DE AGOSTO DE 2011

VISTOS:

1. Lo dispuesto en los artículos 6, 7, 110 y siguientes de la Constitución Política de la República;
2. La Resolución Nº 1.600 del 30.10.08, de la Contraloría General de la República que fija normas sobre exención de trámite de toma de razón;
3. Lo dispuesto en el D.F.L. Nº 1/19.175 de 2005 que fijó el texto refundido de la Ley Nº 19.175, sobre Gobierno y Administración Regional;
4. El D.F.L. Nº 1/19.653, de 2000, del Ministerio Secretaría General de la Presidencia, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575 del 05.12.86., Orgánica Constitucional de Bases Generales de la Administración del Estado;
5. La Ley Nº 19.880, publicada en el D.O. el 29 de Mayo de 2003, del Ministerio Secretaría General de la Presidencia de 2002, que establece las bases de los procedimientos administrativos que rigen los actos de los Órganos de la Administración del Estado.
6. La Ley Nº 20.285, de fecha 11 de agosto de 2008, Ley Sobre Acceso a la Información Pública; y su reglamento;
7. La Resolución Exenta (G.R.) Nº38 de fecha 30.03.2011, del Sr. Intendente Regional (s) que aprueba Política General de Seguridad de la Información;
8. La Resolución Exenta (G.R.) Nº115 de fecha 25.07.2011, del Sr. Intendente Regional que nombra Encargado de Seguridad de Información de este Servicio;
9. Los antecedentes tenidos a la vista;

CONSIDERANDO:

1. Que, a través de lo dispuesto en el visto Nº 7, de la presente resolución, se aprueba actual Política General de Seguridad de la Información;
2. Que, con la finalidad de dar cumplimiento a requerimiento del PMG Sistema de Seguridad de la Información;
3. Que, en este contexto, es necesario reemplazar la actual Política General de Seguridad de la Información dado que no está de acuerdo a los lineamientos propuestos por el PMG Sistema de Seguridad de la Información;
4. Que, en virtud de lo anteriormente expuesto;

RESUELVO:

1. **REEMPLÁCESE Y APRUÉBESE** la "Política para el Acceso a la Información Pública y Gestión de Documentos y Archivos" del Servicio de Gobierno Regional de Magallanes y Antártica Chilena, la que entrará en vigencia a contar del 01 de septiembre del año 2011, en términos que a continuación se señalan:

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Política General de Seguridad de la Información

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1. Introducción

1.1. Objetivos

La Política General de Seguridad de la Información tiene los siguientes objetivos:

- Establecer mecanismos apropiados que garanticen la seguridad de los activos de información del Servicio de Gobierno Regional.

- Representar los intereses de la Dirección Ejecutiva del Servicio, con respecto a la administración y utilización, que los usuarios internos y/o externos deben hacer de los activos de información de la Organización, así como de las medidas que se deben adoptar para la protección de dichos recursos.

- Propender a nivel institucional, la cultura de la seguridad de la información y la comprensión de sus responsabilidades sobre ésta.

- Especificar las medidas esenciales de seguridad de la información que el Servicio debe adoptar, para resguardarse apropiadamente contra amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la información, ocasionando alguna de las siguientes consecuencias:
  - Pérdida o mal uso de los activos de información.
  - Pérdida de imagen Institucional.
  - Pérdida de información sensible.

- Difundir al interior del Servicio, aquellos lineamientos facilitadores para la adopción de acciones apropiadas relacionadas con la seguridad de la información.

1.2. Alcances y Limitaciones

Esta política se aplica a todos quienes trabajen en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena, cualquiera sea su calidad contractual, incluyendo a personal perteneciente a terceras empresas, sean éstas Públicas y/o Privadas, y que no necesariamente presten servicios directamente relacionados con el Servicio.

Incluye todos los activos de información que el Servicio posea en la actualidad o en el futuro, de manera que la no mención explícita en la presente política no es argumento suficiente para no proteger activos de información que se encuentren en otras formas. La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en videos o registros de audio de una conversación.

La presente política adopta su base de contenidos, a partir de las buenas prácticas definidas en el estándar Nch-ISO 27001 y de los requisitos legales, normativos y contractuales relativos a la seguridad de la información, que sean aplicables a la organización, como el Decreto Supremo 83 de fecha 03 de junio de 2004 del Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

1.3. Definiciones

Se presenta a continuación, un listado de definiciones de los conceptos que se requiere conocer para dar un cumplimiento apropiado a la política:

- **Activo de Información:** son todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
- **Autenticación:** proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
- **Confidencialidad:** aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.
- **Contenido del documento:** información, ideas y conceptos que un documento expresa.
- **Continuidad del negocio:** continuidad de las operaciones de la institución.
- **Disponibilidad:** aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.
- **Documento electrónico:** toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.
  Ejemplos de documentos electrónicos:
  - **Documentos públicos:** aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
  - **Documentos reservados: aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter.**
  - **Documentos secretos:** los documentos que tienen tal carácter de conformidad a la Ley 20.285 sobre Acceso a la Información, artículos 21 a 23.
- **Seguridad del Documento electrónico:** Actividades realizadas para preservar la Confidencialidad, Integridad y Disponibilidad de 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.
- **Ejecutivo:** autoridad dentro de la institución.
- **Identificador formal de autenticación**: mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.
- **Incidentes de seguridad**: situación adversa que amenaza o pone en riesgo un sistema informático.
- **Información**: contenido de un documento electrónico.
- **Integridad:** salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.
- **Política de seguridad:** conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.
- **Repositorio:** estructura electrónica donde se almacenan documentos electrónicos.
- **Riesgos:** amenazas de impactar y vulnerar la seguridad del activo de información y su posibilidad de ocurrencia.
- **Sistema informático:** conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de realizar procesamiento y/o transferencia de información.
- **Usuario**: entidad o individuo que utiliza un sistema informático.

2. Responsabilidades Generales

- **Comité de Seguridad:** En su calidad de tal, el Comité de Seguridad responde ante la Dirección Ejecutiva, por la existencia y cumplimiento de las medidas orientadas a mantener un nivel de seguridad de la información acorde con las necesidades del Servicio y los recursos disponibles.
- **Encargado de Seguridad:** Es el representante del Ejecutivo en la definición y aplicación de los criterios de seguridad de la información en el Servicio, para lo cual:
  - Debe validar que los activos de información son identificados y valorizados apropiadamente por sus Propietarios, y que éste valor se mantiene actualizado en el tiempo.
  - Debe analizar permanentemente el nivel de riesgo existente, proponiendo al Ejecutivo soluciones efectivas.
  - Una vez autorizada la implementación de las medidas de protección, debe coordinar con los supervisores respectivos su materialización correcta y oportuna.
  - Además es el responsable de mantener actualizadas las políticas de seguridad y de difundirlas al personal del Servicio y a terceros.
- **Funcionarios del Servicio**: Tiene la responsabilidad de cumplir con lo establecido en este documento y aplicarlo tanto en su entorno laboral, como fuera de éste. Además, tiene la obligación de alertar de manera oportuna y adecuada por los canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.
- **Propietario de la Información:** Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos. Debe participar activamente en la definición del valor de la información para el Servicio, de manera que se puedan definir los controles apropiados para protegerla.
- **Custodio de la Información:** Es cualquier persona que mantiene bajo su responsabilidad, información de la cual no es el Propietario. Es responsable de aplicar las medidas de seguridad que se definan de acuerdo al valor de los activos. En esta categoría se encuentra:
  - El personal encargado de los sistemas de tecnologías de información que crean, procesan o modifican la información del Servicio y sus usuarios externos.
  - El personal que tiene acceso a información del Servicio y sus usuarios externos.

3. Adhesión a la Política

1. La presente política y los estándares y procedimientos que tenga asociados, deben ser cumplidos por todo el personal, sin excepción.
2. El Encargado de Seguridad debe monitorear el cumplimiento de la presente política, reportando los resultados a la Dirección Ejecutiva, semestralmente.
3. La Dirección Ejecutiva del Servicio se reserva el derecho de revocar a los usuarios el privilegio de acceso a la información y a las tecnologías que la soportan.
4. La Dirección Ejecutiva del Servicio se reserva el derecho de tomar medidas disciplinarias en contra del personal que falte a lo aquí dispuesto.
5. La Dirección Ejecutiva debe realizar revisiones anuales al contenido de las políticas de seguridad para garantizar su vigencia.

4. Protección de la Información

1. La Dirección Ejecutiva del Servicio reconoce que la seguridad de la información es un objetivo del Servicio, que debe ser impulsado y apoyado por todos los miembros de la organización.
2. La información es un activo valioso que debe ser protegido de manera consistente con los objetivos del Servicio, y los requerimientos legales, normativos y contractuales que sean aplicables.
3. Se debe tener presente que no es posible eliminar el riesgo, sólo reducir la probabilidad de ocurrencia o sus consecuencias, por lo tanto las medidas que se definan para proteger la información deben ser determinadas en base a un análisis previo que considere el costo beneficio de aplicarlas en relación con los riesgos existentes.
4. Periódicamente se deben realizar análisis de riesgos sobre los activos, de manera que se definan controles de seguridad apropiados al valor de los activos de información.

5. Apoyo Dirección Ejecutiva

1. La Dirección Ejecutiva del Servicio debe destinar los recursos necesarios para asegurar que todo el personal reciba entrenamiento permanente en seguridad de la información, de acuerdo a su función y rol en la organización.
2. La Dirección Ejecutiva del Servicio debe destinar los recursos necesarios para gestionar de manera correcta y oportuna la Seguridad de la Información en la organización.
3. Los riesgos que se identifiquen deberán ser gestionados por la Dirección Ejecutiva de manera que sean llevados a un nivel aceptable para el Servicio. Para esto podrán ser aceptados, eludidos, transferidos o mitigados.
4. Para aquellos riesgos que no sean aceptables, deberán tomarse las medidas de protección apropiadas, las cuales serán sometidas a la aprobación de la Dirección Ejecutiva para asegurar que:

    - Son suficientes para llevar el riesgo a un nivel apropiado.
    - Tienen un costo apropiado al beneficio que aportan.
    - Reciben los recursos y el apoyo necesarios para su implementación.

6. Clasificación de la Información

1. Los propietarios de la información deben clasificar la información que esté bajo su responsabilidad en “Confidencial”, “Uso Interno” o “Pública”, de acuerdo a su importancia para el Servicio.
2. Toda la información que no haya sido clasificada debe considerarse como de “Uso Interno” de manera que reciba los niveles de protección acordes a esta clasificación.

3. El Encargado de Seguridad debe preocuparse de que la información reciba una clasificación apropiada, de manera que las medidas de protección que se apliquen corresponden a las necesidades reales del negocio.
4. Por cada uno de los niveles de clasificación establecidos, se deben definir medidas de protección específicas, las que serán aplicadas por todo el personal.

7. Uso de Activos de Información

1. Todo uso de activos de información debe ser para propósitos del Servicio de acuerdo a las políticas, estándares y procedimientos que se definan y considerando criterios de buen uso.
2. El Servicio no permite el uso personal de los activos de información.
3. Los usuarios de activos de información:
   - No deben divulgar información del Servicio ni de sus usuarios externos, que haya sido clasificada como “Confidencial” o de “Uso Interno”, salvo que hayan sido expresamente autorizados por el Propietario de la Información, quien deberá hacerse responsable de esta divulgación. Está prohibido que los usuarios saquen información de las dependencias de la organización si no han sido específicamente autorizados.
   - Deben solicitar autorización por escrito al Propietario de la Información, cuando necesiten proporcionar información “Confidencial” o de “Uso Interno” a terceros. La entrega de esta información se realizará suscribiendo acuerdos de confidencialidad con el tercero y aplicando los controles específicos que se definan.
   - Deben cumplir con todos los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deberán mantenerse alineadas con las leyes vigentes.
   - Deben proteger sus elementos de control de acceso, como contraseñas, dispositivos y otros, ya que son individuales, intransferibles y de responsabilidad única de cada funcionario.
   - Deben reportar a un nivel apropiado y lo antes posible, cualquier incidente que ponga en riesgo la seguridad de la información para que se tomen las medidas necesarias.

8. Normas que componen la Política

Son parte de esta política los siguientes dominios establecidos en la NCh-ISO 27001, los cuales abarcan activos de información que interesa proteger.

1. Norma de Funciones, Responsabilidades y Organización de Seguridad de la Información.
2. Norma de Gestión de Activos.
3. Norma de Seguridad de Recursos Humanos.
4. Norma de Seguridad Física y Ambiental.
5. Norma de Gestión de las Comunicaciones y Operaciones.
6. Norma de Gestión de Acceso.
7. Norma de Gestión de Incidentes de Seguridad de la Información.
8. Norma de Adquisición, Desarrollo y Mantenimiento de Seguridad de la Información.
9. Norma de Gestión de Continuidad del Negocio.
10. Norma de Cumplimiento.
11. Política de Seguridad de la Información.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Funciones, Responsabilidades y Organización de la Seguridad de la Información

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1 Introducción

1.1 Declaración Institucional

El Servicio de Gobierno Regional de Magallanes y Antártica Chilena reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente los valores generales de seguridad de la información que deben permanecer a través del tiempo para el cumplimiento por parte de todos los funcionarios, sea cual fuere su calidad jurídica.

1.2 Objetivo

El objetivo de la Norma de Funciones, Responsabilidades y Organización es definir las actividades de los distintos participantes, establecer un marco referencial para iniciar y controlar la implementación de la seguridad de la información por parte de la Primera Autoridad Regional, con el fin de delimitar las responsabilidades de cada ente.

1.3 Ámbitos de aplicación

Todos los Activos de Información contenidos en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.4 Vigencia

Esta Norma de Funciones, Responsabilidades y Organización entrará en vigencia a partir del **01 de septiembre de 2011.**

1.5 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.6 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2 Funciones y responsabilidades

Para una adecuada protección de la información del Servicio se establecen las funciones y responsabilidades que se detallan a continuación.

2.1 Funciones Definidas

Para la protección de la información se identifican las siguientes funciones en el Servicio:

2.1.1 Comité de Seguridad de la Información

El Comité de Seguridad de la información estará formado por:

- Intendente Regional
- Jefes de División
- Jefe Dpto. Servicios Generales
- Jefe Unidad de Fortalecimiento Institucional
- Jefe Unidad de Tecnología, Información y Comunicaciones
- Asesor Jurídico
- Encargado de Seguridad de la Información
- Representante Departamento Gestión de Personal
- Representante Comité Paritario
- Representante Funcionarios

El comité de Seguridad se encarga de definir y establecer los lineamientos generales de seguridad y aprobar la política, normas y demás definiciones en lo que respecta a seguridad de la información. Deberá revisar y verificar el cumplimiento de lo anterior, asegurando su continuidad, idoneidad, eficiencia y efectividad. Cuando por unanimidad lo consideren necesario o cuando ocurran cambios significativos en la seguridad de la información, podrá convocar a la Unidad de Auditoria a fin de revisar el enfoque de implementación de seguridad de la información en el Servicio. Será este quien comunique los lineamientos generales de seguridad, definidos por la alta dirección, publicando y difundiendo la política, normas y demás definiciones en lo que respecta a seguridad de la información.

2.1.2 Encargado de Seguridad de la Información

Es el representante del Servicio en materias de Seguridad de la Información, encargado del desarrollo inicial de la Política de Seguridad, control e implementación de la misma, así como también de velar por su correcta aplicación. Deberá coordinar la respuesta a incidentes que afecten a los activos de información institucionales, así como establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

2.1.3 Propietario/Dueño de Datos

Se establece como Propietario de Datos, a todos los Jefes de División, Jefes de Departamento y Jefes de Unidad del Servicio, quienes tienen la autoridad y responsabilidad respecto a los activos de información correspondiente a su área de trabajo. La función principal de un Propietario de Datos es establecer (verificar y confirmar) y autorizar controles para asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información. De ser necesario, el dueño de la información

puede delegar algunas actividades y tareas operativas a otro funcionario del Servicio, preferentemente de su respectiva área (Custodio).

2.1.4 Custodio de Datos

Se establece como custodio de datos al responsable de asistir a un Propietario/dueño de la información en mantener la confidencialidad, integridad, disponibilidad y privacidad de los activos de información del Servicio. La delegación a un tercero debe ser aprobada y autorizada por el Propietario de Datos e informada al comité de Seguridad del Servicio. La propiedad y responsabilidad de los datos no puede ser delegada a un tercero.

Se establecen como Custodios de la Información a:

- Al responsable de los archivos centralizados de la información en medios escritos;
- Los usuarios finales que conserven en su poder los medios de información;
- El o los responsables del sitio donde se encuentren los equipos de procesamiento centralizado, de comunicación y/o almacenamiento.

2.1.5 Administrador de Seguridad

Dentro de la función de Administrador de Seguridad, existen 3 clasificaciones:

- Administrador de Sistemas/Equipos

  El Administrador de Sistemas debe tener a su cargo la administración de la seguridad de cada uno de los equipos, sistemas, aplicaciones y/o servicios donde se procese información.

- Administrador de Seguridad Física

  El Administrador de Seguridad Física debe tener a su cargo la administración de la seguridad física de las distintas instalaciones y áreas sensibles del Servicio, que albergan información, equipamiento y los sistemas de procesamiento de información del Servicio.

- Administrador de Seguridad del Personal

  El Administrador de Seguridad del Personal debe tener a su cargo el establecimiento de las medidas de seguridad asociadas a los procesos de evaluación y selección de personal, capacitación, entrenamiento y sensibilización del personal en temas asociados a la seguridad de la información; con el objetivo de reducir y/o prevenir los riesgos de error humano, fraudes, robo o uso inadecuado de las instalaciones e información del Servicio.

Dichos Administradores de Seguridad tienen a su cargo la administración de la seguridad de la información del área que le corresponda. Cada administrador deberá implantar las medidas dictadas por el Jefe Superior del Servicio y / o el Comité de Seguridad del Servicio, las cuales dependerán del área en la que habitualmente desempeña sus labores.

2.1.6 Funcionarios y Usuarios de los recursos en general

Un Usuario (Funcionario o externo) es un individuo asignado a un rol, que está autorizado a acceder a los activos de información del Servicio.

2.2 Responsabilidades

2.2.1 Comité de Seguridad de la Información

- El Comité deberá reunirse a lo menos cuatro veces por año (trimestralmente) para tratar temas referentes a la Seguridad de la Información al interior del Servicio; o cuando la situación lo amerite.
- Deberá aprobar la política, normas y demás definiciones en lo que respecta a seguridad de la información en el Servicio.
- Promover la consideración de la seguridad en todos los Planes y Proyectos de Sistemas de Información del Servicio.
- El comité deberá verificar y revisar el cumplimiento de esta política, asegurando su continuidad, idoneidad, eficiencia y efectividad.
- Revisará a través de auditores externos o internos, el enfoque e implementación de seguridad de la información en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena, cuando por unanimidad lo consideren necesario o cuando ocurran cambios significativos en la seguridad de la información.
- Se encargará de definir los lineamientos generales de seguridad que regirán en el Servicio.
- Será quien comunique los lineamientos generales de seguridad, publicando y difundiendo la política, normas y demás definiciones en lo que respecta a seguridad de información.
- Deberá definir las estrategias que se seguirán en el Servicio sobre temas específicos de seguridad de la información y aprobar las principales iniciativas para incrementar la seguridad de la información.
- Monitorear cambios significativos en la exposición de los recursos de la información frente a las amenazas más importantes.
- Revisar y monitorear los incidentes relativos a la seguridad.

2.2.2 Encargado de Seguridad de la Información

- Representante del Servicio, quien debe apoyar la función de seguridad e incentivarla localmente.
- Tener a su cargo el desarrollo inicial de las Políticas de seguridad al interior del Servicio, el control de su implementación, y velar por su correcta aplicación.
- Coordinar la respuesta a incidentes que afecten a los activos de información institucional.
- Debe incentivar y darle importancia requerida en el Servicio al Comité de Seguridad de la Información.
- Debe apoyar las estrategias que el Comité de Seguridad defina que se seguirán en el Servicio sobre temas específicos de seguridad de la información e iniciativas para incrementar la seguridad de la información.
- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
- Debe incentivar que se revisen y monitoreen los incidentes relativos a la seguridad.
- Velar por la efectiva aplicación de la Política General de Seguridad de Información.
- Levantar temas y propuestas de políticas y/o normativas al Comité de Seguridad.

2.2.3 Propietario / Dueño de Datos

- Identificar toda la información y procesamiento de la misma que corresponde a su área de responsabilidad cualquiera sea su forma y medio de conservación.

- Clasificar todos los datos de su propiedad de acuerdo al grado de criticidad de los mismos.
- Documentar y actualizar periódicamente la clasificación de datos efectuada.
- Velar por la seguridad de sus datos, procurando la correcta aplicación de mecanismos orientados a la mitigación de riesgos.
- Es el responsable de la información y de los procesos que la manipulan, sean estos manuales, mecánicos o electrónicos.
- Debe participar activamente en la definición del valor de la información para el negocio, de manera que se puedan definir los controles apropiados para protegerla.
- Autorizar los distintos accesos para que el personal pueda utilizar de manera apropiada los datos de acuerdo con sus respectivas funciones de trabajo.

2.2.4 Custodio de Datos

- Cumplir con las actividades y tareas que le han sido delegadas por el Propietario de Datos.
- Llevar un adecuado registro de los usuarios permitidos a acceder a su información.
- Conservar las llaves y/o combinaciones para acceder a los activos de información considerados como confidencial/restringida o de carácter reservado.
- Disponer la custodia de las claves de mayor riesgo de los equipos/servicios/aplicaciones conservadas en sobre cerrado.
- Definir los eventos de seguridad adicionales que considere necesario para la protección de su información.
- Desarrollar los procedimientos necesarios para cumplir con las normas definidas y lineamientos exigidos por el Propietario de Datos.

2.2.5 Administrador de Seguridad

Se establecen las siguientes responsabilidades para los diferentes Administradores de Seguridad, las que se detallan a continuación:

- Administrador de Sistemas/Equipos
  - Administrar todas las solicitudes de creación, baja y modificación de usuarios y sus respectivos perfiles para los equipos y aplicaciones.
  - Mantener actualizada una lista de todos los usuarios con permisos de acceso en los equipos y sistemas bajo su dominio.
  - Asistir a los usuarios en las tareas relacionadas con la protección de los datos.
  - Verificar periódicamente que solamente los usuarios autorizados tengan acceso a los equipos y sistemas.
  - Implementar todas las medidas de seguridad definidas que apliquen a los equipos/sistemas bajo su dominio.
  - Analizar e informar cualquier evento que atente contra la seguridad de la información.
  - Investigar y mantenerse actualizado con respecto a nuevas amenazas, posibles ataques y riesgos que pueden afectar los equipos y/o sistemas bajo su dominio.
  - Implementar y velar por una adecuada definición y operación de mecanismos, herramientas y procedimientos de seguridad.
- Administrador de Seguridad Física
  - Entrenar al personal para su correcta conducta y respuesta a posibles incidentes de seguridad física.
  - Implementar las medidas de seguridad física definidas para la protección de información e instalaciones de procesamiento y equipamiento del Servicio.
  - Procurar que las instalaciones de procesamiento de información crítica o sensible del Servicio estén ubicadas en áreas protegidas y resguardadas por un perímetro restringido.

- Implementar controles para la seguridad del equipamiento contra posibles incidentes de seguridad, tales como: incendio, robo, etc.
- Mantener un registro de los incidentes de seguridad física ocurridos en el Servicio, impactos, soluciones implementadas.
- Asistir al Comité de Seguridad en el diseño, definición e implementación de medidas de seguridad física orientadas a la protección de la información, instalaciones y equipamiento del Servicio.

- Administrador de Seguridad del Personal
  - Apoyar en la definición e implementación de los controles asociados a los procesos de selección y evaluación del personal previo a su contratación.
  - Resguardar y custodiar la documentación de antecedentes del personal en general, y verificar su buen uso.
  - Mantener permanentemente informado al Comité de Seguridad respecto de los temas relativos a la seguridad del personal.
  - Identificar riesgos de seguridad en el ámbito de seguridad del personal, y evaluar oportunamente medidas de seguridad necesarias para su posterior implementación.
  - Apoyar al Comité de Seguridad en el desarrollo e implementación de los programas de difusión, sensibilización y capacitación a los usuarios, con relación a las normativas de seguridad de la información, riesgos, responsabilidades, entre otros.

2.2.6 Funcionarios y Usuarios de los recursos en general

- Cumplir con la Política General de seguridad de la Información, Normas, Procedimientos, y demás definiciones de seguridad de la información implementadas en el Servicio.
- Emplear los activos tecnológicos y de información del Servicio solamente para fines propios del mismo.
- Poner en conocimiento del Encargado de Seguridad cualquier situación detectada que pueda poner en peligro la seguridad de la información.

ANEXO A

Estructura del Comité de Seguridad de la Información.

Cargo	Titular	Suplente
Intendente Regional	Arturo Storaker	Designado por él
Jefe DAF	Luis Sáez	Javier Nahuelquen
Jefe DAC	Veronica Peragallo	Iván Ulloa
Jefe DDR	Lorena Silva	José Velásquez
Jefe Dpto. Servicios Generales	Oscar Sierpe	Myriam Leiva
Jefe UFI	Lionel Silva	Claudia Villarroel
Jefe UTIC	Juan Carlos Chávez	Mónica Barría
Encargado de Seguridad	Javier Nahuelquen	Luis Sáez
Asesor Jurídico	Ruth Bravo	Sandra Sánchez
Rep. Gestión de Personal	Karina Andrade	Héctor Díaz
Rep. Comité Paritario	Ana Celia Navarro	Ximena Ramírez
Rep. Funcionarios	Juan Mauricio Muñoz	José Márquez

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Gestión de Activos

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1 Introducción

1.1 Objetivo

El objetivo de la Norma de Gestión de Activos es identificar los activos del Servicio y documentar la importancia de los mismos, definir las actividades de los distintos participantes y establecer un marco referencial para controlar la gestión de activos en relación a la seguridad de la información al interior del Servicio.

1.2 Ámbitos de aplicación

Todos los Activos contenidos en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.3 Vigencia

Esta Norma de Gestión de Activos entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información
- Manual de Procedimientos para el control del Activo Fijo
- Manual de Procedimiento Gestión de Archivos
- Política de Recursos Humanos

2 Funciones y responsabilidades

Para una adecuada protección de la información del Servicio se establecen las funciones y responsabilidades que se detallan a continuación.

2.1 Funciones Definidas

Para la protección de los Activos se identifican las siguientes funciones en el Servicio:

2.1.1 Encargado de Inventario

El Encargado de Inventario ejecutará las acciones administrativas relativas a los bienes muebles de uso. Será designado por la Jefatura de la División de Administración y Finanzas siendo comunicada la designación formalmente a través del Jefe del Departamento de Servicios Generales.

El Encargado de Inventario operará el Sistema Informático de Control del Activo Fijo.

2.1.2 Encargado de Archivo Central

El Encargado de Archivo Central tendrá por función velar por el ordenamiento, protección, uso y resguardo del Archivo Central del servicio, de conformidad a la normativa vigente.

2.1.3 Encargado de Archivo de Oficina

El Encargado de Archivo de Oficina tendrá por función velar por el ordenamiento, protección, uso y resguardo del Archivo de Oficina, de conformidad a la normativa vigente.

2.1.4 Administrador de Sistemas y Plataforma

El Administrador de sistema y plataforma tendrá como función velar por el correcto funcionamiento, acceso, uso y resguardo de la Plataforma Informática del servicio; así como también velar por el correcto funcionamiento, acceso, uso y resguardo de los Sistemas Informáticos.

2.1.5 Encargado de Activos de Personal

El encargado de activos de Personal tendrá como función velar por el correcto uso, resguardo y protección de los Activos de Información de carácter funcionario como ser calificaciones, anotaciones, carpeta funcionaria, etc.

2.1.6 Funcionarios y/o Usuarios de Activos

Tendrán por función velar por el correcto uso y resguardo de los Activos que le hayan sido encomendados en el Servicio.

2.2 Responsabilidades

2.2.1 Encargado de Inventario

- El Encargado de Inventario será responsable de ejecutar las acciones administrativas relativas al uso de los bienes muebles.
- El Encargado de Inventario operará el Sistema Informático de Control del Activo Fijo.
- Será responsable de identificar todos los Activos de carácter Bien Mueble del Servicio.
- Elaborar y mantener un inventario de todos los Activos de carácter Bien Mueble del Servicio.
- Revisar y monitorear los incidentes relativos a la seguridad de dichos activos.
- Deberá desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con esquema de clasificación establecido por el Servicio.

2.2.2 Encargado de Archivo Central

- El Encargado de Archivo Central será responsable de velar por el ordenamiento, protección, uso y resguardo del Archivo Central del Servicio, de conformidad a la normativa vigente.
- Asegurar que la información reciba un nivel de protección apropiado.

- Clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para el Servicio.
- Será responsable de implementar los procedimientos adecuados para el etiquetado y manejo de la información de acuerdo a la normativa vigente.
- Deberá definir procedimientos de manejo seguro que incluyan procesamiento, almacenamiento, transmisión, desclasificación y destrucción.
- Definirá los procedimientos de la cadena de custodia y el registro de cualquier incidente de seguridad relevante.
- Será responsable de la capacitación en materias de manejo de archivos y seguridad de los mismos a los encargados de archivo de oficina.

2.2.3 Encargado de Archivo de Oficina

- El Encargado de Archivo de Oficina tendrá la responsabilidad de velar por el ordenamiento, protección, uso y resguardo del Archivo de Oficina.
- Clasificar todos los datos de su área de acuerdo al grado de criticidad de los mismos.
- Documentar y actualizar periódicamente la clasificación de datos efectuada.
- Velar por la seguridad de sus datos, procurando la correcta aplicación de mecanismos orientados a la mitigación de riesgos.

2.2.4 Administrador de Sistemas y Plataforma

- Controlar que la solicitud de creación, acceso, modificación haya sido autorizada por los Propietarios de los Datos.
- Controlar que la solicitud de baja de los usuarios, haya sido requerida por los responsables autorizados.
- Dejar constancia en formulario de su revisión e ingreso al sistema realizado.
- Controlar la información de las cuentas de usuarios que están en proceso como aquellas ya procesadas.
- Mantener adecuadamente resguardada la información de seguridad definida en el sistema de administración de usuarios y recursos.
- Recibir los computadores devueltos según procedimiento definido, y respaldar y borrar los archivos de trabajo que se generaron en el computador, al momento de la desvinculación de un funcionario, o el cambio de funciones dentro del Servicio.
- Mantener los inventarios detallados de los recursos de hardware instalados dentro y fuera del centro de procesamiento de datos y la descripción de su localización.
- Solicitar la reparación de hardware que, al momento de revisar o recibir se amerite que lo necesita.
- Solicitar las actualizaciones de hardware y/o software que estime necesarias para el buen funcionamiento del Servicio.
- Entregar el hardware solicitado y autorizado, según procedimientos definidos para el efecto.
- Administrar y resguardar los laptops que no estén asignados.
- Solicitar la reparación o mantención del equipamiento móvil (proyectores VGA, notebooks, netbooks, ipad, etc.) que, al momento de recibirlos lo requieran.
- Mantener el equipamiento móvil individualizado y con los sellos que corresponda.
- Mantener listado actualizado de los usuarios que tienen equipamiento móvil asignado.
- Entregar el equipamiento móvil solicitado y autorizado y recibir el equipamiento devuelto.

2.2.5 Encargado de Activos de Personal

- Realizar inducción a la Funcionarios nuevos respecto de la Política General de Seguridad del Servicio, incluidas normas y procedimientos asociados.
- El encargado de activos de Personal velará por el correcto uso, resguardo y protección de los Activos de Información de carácter funcionario como ser calificaciones, anotaciones, carpeta funcionaria, etc.

- Deberá informar al Comité de seguridad de cualquier detección de falta a la Política que pueda poner en riesgo los activos bajo su responsabilidad.
- Proponer las medidas de mitigación adecuadas.

2.2.6 Funcionarios y Usuarios de los recursos en general

- Cumplir con la Política General de seguridad de la Información, Normas, Procedimientos, y demás definiciones de seguridad de la información implementadas en el Servicio.
- Emplear los activos tecnológicos y de información del Servicio solamente para fines propios del mismo.
- Poner en conocimiento del Encargado de Seguridad cualquier situación detectada que pueda poner en peligro la seguridad de la información.

2.3 Recursos Físicos

2.3.1 Uso de Computadores de Escritorio

2.3.1.1 Provisión de recursos computacionales

La provisión de recursos computacionales será realizada exclusivamente por la División de Administración y Finanzas a través de su Unidad de Tecnología, Información y Comunicaciones.

2.3.1.2 Asignación de Computadores de Escritorio

Siempre que se le entregue un computador de escritorio a un usuario deberá quedar una constancia escrita y firmada por el receptor del equipo que consigne al menos el número de SGR de la CPU y del monitor, así como el software instalado.
Deberá existir un procedimiento que defina todo lo que se le debe instalar (como base) a un equipo antes de su asignación en función del cargo.

2.3.1.3 Administración de los Computadores de Escritorio

La administración de los computadores de escritorio del Servicio estará a cargo de Unidad de Tecnología Información y Comunicaciones, el cual deberá:

- Recibir los computadores devueltos según el procedimiento definido, y respaldar y borrar los archivos de trabajo que se generaron en el computador, al momento de la desvinculación de un funcionario, o del cambio de funciones dentro de la organización.

- Mantener los inventarios detallados de los recursos de hardware instalados dentro y fuera de los centros de procesamiento de datos y las descripciones de su localización.

- Solicitar la reparación o mantención de los computadores que, al momento de recibirlos, se estime lo necesitan.

- Solicitar las actualizaciones del hardware y/o software que contienen los computadores.

- Entregar los computadores solicitados y autorizados, según los procedimientos definidos para este efecto.

2.3.1.4 Medidas de Seguridad

Los equipos y dispositivos computacionales que cambien de asignación deben entregarse sin información de uso restringido. Se deberá respaldar la información con presencia y autorización del dueño de información del área, entregando copia al usuario y guardando copia en la Unidad de Tecnología, Información y Comunicaciones y debe borrarse la información del computador antes de la reasignación, asegurándose que ésta no pueda ser accedida o leída.

Configurar las estaciones de trabajo para que activen en forma automática el uso de protector de pantalla con contraseña, después de 15 minutos de inactividad.

Es responsabilidad de los usuarios no modificar las configuraciones de protección de pantalla implantadas por la Unidad de Tecnología, Información y Comunicaciones.

No dejar disquetes, pendrives u otras unidades de almacenamiento olvidados en los computadores.

Los usuarios deben procurar cuidar los elementos computacionales que les son asignados para su uso.

2.3.1.5 Conductas inapropiadas en el uso de Computadores

Los sistemas computaciones están asignados y habilitados para uso en la gestión del negocio del Servicio de Gobierno Regional de Magallanes y Antártica Chilena. Se consideran conductas inapropiadas:

- Las actividades de lucro personal.

- La desinstalación o inhabilitación consciente de las aplicaciones/configuraciones de seguridad del computador, por ejemplo del antivirus, claves de ingreso, entre otros.

- La instalación de software no autorizado por la Unidad de Tecnología, Información y Comunicaciones.

- La modificación de la configuración del sistema operativo u otras aplicaciones que formen parte del software operativo básico del equipo.

- Mover el equipo fuera del área designada.

- Abrir el equipo y/o cambiar el hardware o dispositivos que lo componen.

2.3.2 Uso de Computadores Portátiles

2.3.2.1 Asignación de laptops

Los laptops son herramientas de trabajo que el Servicio de Gobierno Regional pone a disposición de sus funcionarios para el desempeño de sus funciones y su uso está restringido a las personas a las cuales se les asignó.

En ningún caso podrán facilitarlo a terceros.

Los laptops podrán ser asignados permanente o temporalmente al funcionario o colaborador mientras desempeñe labores para el Servicio.

La asignación de equipos se realizará previa solicitud por escrito del Jefe Directo del asignatario en cuestión

Los laptops deben estar identificados con un logotipo que señale que el equipo es utilizado por el Servicio de Gobierno Regional y que indique el número de teléfono de la Unidad de Tecnología, Información y Comunicaciones del Servicio. Esto ayudará a disuadir a las personas con intenciones de hurtar los equipos para revenderlos y ayudará también, en caso de extravío a recuperarlos.

A cada usuario, junto con el laptop, se le hará entrega de elementos de seguridad para su protección, tales como un bolso diseñado y construido especialmente para el transporte seguro del equipo y un mouse si se requiriese.

Siempre que se le entregue un laptop a un usuario, este deberá firmar un Acta de Entrega en donde indique las características del equipo y responsabilice al usuario por su cuidado y protección. La Unidad de Tecnología, Información y Comunicaciones guardara las actas firmadas por los usuarios.

2.3.2.2 Administración de los laptop

La administración de los laptop del Servicio de Gobierno Regional estará a cargo de la División de Administración y Finanzas a través de la Unidad de Tecnología, Información y Comunicaciones, y las principales funciones referidas a esta responsabilidad serán:

- Almacenar y resguardar los laptops que no estén asignados.

- Solicitar la reparación o mantención de los laptops que, al momento de recibirlos lo requieran.

- Solicitar las actualizaciones del hardware y/o software que contienen los laptops.
- Mantener los laptops individualizados y con los sellos que correspondan.

- Mantener el inventario actualizado de los laptops que administra, con los detalles del hardware y software que tienen.

- Mantener un listado actualizado de los usuarios que tienen laptops asignados, indicando el equipo, y sus partes, fecha de entrega, fecha de devolución (si corresponde), identificación completa del usuario.

- Entregar los laptops solicitados y autorizados y recibir los laptops devueltos.

- Los laptops que cambien de asignación deben entregarse sin información de uso restringido. Se deberá respaldar la información con presencia y autorización del dueño de información del área entregando una copia a éste y almacenando copia en Unidad de Tecnología de Información y Comunicaciones y debe borrarse la información del laptop antes de la reasignación, asegurándose que ésta no pueda ser accedida o leída.

- Solicitar el aumento o recambio de equipos según las necesidades de los usuarios.

2.3.2.3 Medidas de Seguridad

Almacenar los laptops nuevos o no asignados en gabinetes con llave u oficinas con acceso controlado.

El laptop deberá mantenerse siempre con contraseña al nivel de la BIOS activa, es decir, previo al inicio de las funciones básicas del equipo deberá ingresarse una clave, y ésta deberá ser conocida por el superior del funcionario al cual le ha sido asignado el equipo.

Dicha contraseña deberá cumplir con las características de seguridad definidas por la Unidad de Tecnología, Información y comunicaciones para tal efecto.

El laptop deberá contar con contraseña del sistema operativo para iniciar la sesión de trabajo.

El usuario debe asegurarse de que su equipo cuenta con el software antivirus definido por el Servicio.

El usuario no podrá estar conectado a otra red o computador, mientras se encuentre conectado a la red del Servicio de Gobierno Regional.

En caso de viajes fuera del área en que normalmente residen los equipos portátiles, éstos deben ser llevados como equipaje de mano a fin de prevenir pérdidas o daños.

Todo proveedor externo que tenga la posibilidad de manipular la información contenida dentro de un laptop, deberá firmar un contrato de confidencialidad con el Servicio.

Los laptops que tengan que ser trasladados por mantención y reparación deben entregarse sin información restringida ni confidencial, cuando la tecnología lo permita.

Se deberá respaldar la información con presencia y autorización del usuario que tiene asignado el laptop quedándose él con el respaldo y una copia en la Unidad de Tecnología, Información y Comunicaciones, luego, se debe borrar la información del equipo antes del traslado, asegurándose que ésta no pueda ser accedida o leída. La información mantenida en el laptop es de responsabilidad del usuario.

2.3.2.4 Conductas inapropiadas en el uso de laptop

Los sistemas computacionales están asignados y habilitados para uso en la gestión del negocio del Servicio de Gobierno Regional. Se consideran conductas inapropiadas:

- Las actividades de lucro personal.

- La desinstalación o inhabilitación consciente de las aplicaciones/configuraciones de seguridad del laptop, por ejemplo del antivirus.

- La instalación de software no autorizado por la Unidad de Tecnología, Información y Comunicaciones.

- La modificación de la configuración del sistema operativo u otras aplicaciones que formen parte del software operativo básico del equipo.

- Abrir el equipo y/o cambiar el hardware o dispositivos que lo componen.

2.3.2.5 Responsabilidades del usuario

Es obligación del usuario, cuidar el equipo asignado y no exponerlo a riesgos innecesarios, por ejemplo: calor extremo, golpes, derramamiento de líquidos, hurto, etc.

Al momento de recibir un laptop, debe verificar que éste no presenta alteraciones o daños físicos.

Utilizar correctamente, y en todo momento que sea requerido, los elementos de seguridad que le sean entregados para proteger el laptop.

El usuario deberá administrar correctamente su información dentro del equipo, de tal forma que al momento de respaldarla y eliminarla del laptop, no comprometa archivos del sistema.

El usuario deberá respaldar a lo menos una vez al mes la información contenida en el laptop, evitando grabar en el disco local del equipo.

2.3.3 Uso de otros recursos asignados

2.3.3.1 Impresoras

El recurso impresora debe ser utilizado sólo para soportar las operaciones del Servicio de Gobierno Regional.

Cada usuario es responsable de los documentos que imprime en las impresoras compartidas como en las individuales.

Luego de imprimir, el usuario debe retirar de inmediato los documentos de la impresora. Aquellos documentos que permanezcan luego de concluida la jornada laboral, podrán ser destruidos.

En aquellos casos en los que la impresora no imprima inmediatamente un documento, tomarse el tiempo para averiguar la causa, antes de volver a dar un comando de impresión.

Si por error se imprime algo no deseado y que puede contener información confidencial, ésta deberá ser destruida, por ejemplo, mediante el uso de máquina trituradora de papeles.

Si por problemas de confiabilidad de información o tecnología de la impresora del área, se requiere un equipo de impresión local, la aceptación del requerimiento será definido en conjunto con el Jefe Directo correspondiente y el Jefe de la División de Administración y Finanzas. Independiente de lo anterior, se llevará a cabo un control de las impresiones que se realicen por dicho dispositivo.

Se debe propender al uso racional del recurso de impresión. Si por razones de servicio, es necesario imprimir grandes volúmenes de información, estos deberán hacerse en las horas de menor demanda del servicio (horas de almuerzo, a última hora de la tarde, etc.)

2.3.3.2 Fotocopiadoras

Las fotocopiadoras deben ser utilizadas sólo con fines relativos al Servicio.

No está permitido su uso para fotocopiar textos de estudio, cuadernos u otros documentos personales.
Luego de fotocopiar un documento, el usuario debe retirar de inmediato los documentos de la fotocopiadora. Aquellos documentos que permanezcan luego de concluida la jornada laboral podrán ser destruidos.

2.3.3.3 Fax

El fax debe ser utilizado sólo con fines relativos al Servicio.

Deberá evitarse el envío de información confidencial por este medio y sólo podrá ser usado cuando exista la certeza de que el destinatario lo recibirá y no será leído por terceros.

Para el envío de fax al exterior, es conveniente utilizar siempre un mismo formato o carátula de fax.

En cuanto a la recepción de fax, si se sabe de su envío, se sugiere:

- Solicitar a la persona que enviará el fax, consignar en el mismo el nombre del destinatario del Servicio de Gobierno Regional, para evitar confusiones.

- Indicar a la persona el horario de trabajo del Servicio, para (en lo posible) evitar que llegue información en otros horarios y quede expuesta en la máquina de fax.

- Preocuparse de retirar los fax recibidos oportunamente.

Sin perjuicio de lo anterior, siempre deberá haber un responsable de las máquinas de fax, que distribuya y/o avise lo que llega a los destinatarios.

2.3.3.4 Teléfonos Móviles

Los teléfonos móviles asignados por el Servicio deberán ser usados para los fines a los que fueron destinados.

El Servicio se reserva el derecho de informar a todo el personal los números asignados a cada funcionario y es el Servicio la que a través de su línea ejecutiva asigna o retira estos servicios.

Evitar compartir información confidencial o propia del Servicio en conversaciones por el teléfono móvil, a no ser que se tenga la certeza de que la tecnología no permite ser interceptada.

Está prohibido el uso de las llamadas de cobro revertido y será de costo del usuario responsable, todas las llamadas recibidas en los equipos móviles.

Está prohibido hacer llamadas personales desde el extranjero con los equipos móviles del Servicio.

Todo funcionario que tiene asignado un teléfono móvil es responsable por el equipo y las llamadas que se realicen del mismo.

El incumplimiento por parte del usuario del buen uso de este servicio, ocasionará la suspensión de éste en forma temporal o definitiva. Sin desmedro de las acciones que la Primera Autoridad estime pertinentes al caso.

2.3.3.5 Teléfonos y Líneas Telefónicas

Los teléfonos deberán ser usados principalmente para asuntos de trabajo. Las llamadas telefónicas personales deben restringirse a los mínimos razonables acordes con las circunstancias.

No dejar sobre el escritorio o en áreas visibles códigos de acceso sensibles del sistema telefónico del Servicio que permiten realizar llamadas internacionales y a teléfonos móviles.

Emplear y resguardar las claves de acceso a los buzones de mensajes de voz.

Evitar compartir información confidencial o propia del Servicio en conversaciones por el teléfono, a no ser que se tenga la certeza de que la tecnología no permite ser interceptada.

Aquellos teléfonos autorizados para realizar llamadas internacionales y a teléfonos móviles deberán permanecer restringidos a través del uso de claves, y serán desbloqueados por el responsable al momento de efectuar las llamadas.

Todo funcionario que tiene asignado un teléfono fijo es responsable por el equipo y las llamadas que se realicen del mismo.

Está prohibido el uso de las llamadas de cobro revertido y será de costo del funcionario responsable, todas las llamadas recibidas en los equipos fijos.

2.3.4 General

Todos los funcionarios y colaboradores del Servicio de Gobierno Regional tienen la obligación de proteger y resguardar la información sensible y confidencial del Servicio, ya sea que ésta se encuentre en equipos y recursos provistos por el mismo o en dispositivos de propiedad de los usuarios, tales como Discos Duros Externos, Pendrive, etc.

Los funcionarios del Gobierno Regional velarán por que los bienes muebles de uso de propiedad fiscal sean adecuadamente registrados, administrados y protegidos, y pondrán en su uso el mismo cuidado e interés que el dedicado a los de su propiedad privada.

2.3.4.1 Concepto y Clasificación de los bienes

Bienes Muebles son aquellos que pueden trasladarse de lugar sin que pierdan su individualidad.
Bienes Muebles Fiscales son aquellos bienes que han sido adquiridos por los Servicios de la Administración del Estado, ya sea por adquisición directa, donación o proyectos.

Los Bienes Muebles Fiscales se clasifican en:

Bienes de Consumo: Son los que se extinguen o destruyen por su uso natural.
Bienes de Uso: Son aquellos que no se extinguen por el empleo de ellos según su naturaleza.

La administración de los bienes muebles de uso, corresponderá al Jefe de la División de Administración y Finanzas.

Todo bien mueble de uso estará a cargo de un funcionario, normalmente su usuario directo. El funcionario responsable de los bienes velará por su adecuado uso y mantención.

Los bienes poseen los siguientes movimientos o estados de inventario:

- **Alta o Entrada:** Es la operación que registra la incorporación de un bien mueble al Sistema de Control del Activo Fijo. Una vez ingresado un bien y autorizada el alta, se le asignará una Codificación Única de Inventario, que el bien mantendrá durante toda su vida útil.
- **Baja o Salida**: Es la operación que registra la eliminación de un bien mueble del Sistema de Inventario.
- **Traslado:** Corresponde a la transferencia de un bien desde un Centro de Costos a otro. Implica una Baja en el Centro de Costos de origen y un Alta en el Centro de Costo de destino.

Las facultades para autorizar y suscribir los actos administrativos que aprueban las altas, bajas y traslados de bienes muebles de uso en el Servicio, se encuentra delegada en la jefatura de la División de Administración y Finanzas.

2.3.4.2 Procedimiento para el Alta

Corresponderá efectuar la operación de Alta al funcionario encargado de inventario del Servicio.

Una vez obtenido el Número de la Solicitud de Inventario, lo anotará en la factura o guía de despacho correspondiente, conjuntamente con el número correlativo del bien dentro de la Solicitud.

En los casos de compras centralizadas de bienes muebles de uso, tales como equipos computacionales y accesorios, en los que generalmente la unidad compradora es la Unidad de Tecnología, Información y Comunicaciones, éste remitirá los bienes de destino con un memorándum, en el que se identificará el bien en cuestión, y adjuntará copia o fotocopia de la factura de compra, la que será el documento sustentatorio para efectuar el Alta.

Terminado el proceso de Alta, el Encargado de Inventario emitirá un Certificado de Alta, el que firmará y archivará.

2.3.4.3 Procedimiento para la Baja

La Jefatura de la División Administración y Finanzas que estime que ciertos bienes son prescindibles, los ofrecerá a otros Unidades o Departamentos. Si no hay interesados internos, la Jefatura de la División Administración y Finanzas informará a otras instituciones eventualmente receptoras la existencia de bienes prescindibles para el Servicio. Las instituciones eventualmente receptoras deben ser entidades de interés social y sin fines de lucro u otras entidades del Estado.

2.3.4.4 Hoja Mural de Inventario

En cada oficina o recinto en que se depositen bienes inventariables, deberá existir una Hoja Mural en la que constará una relación de todos los bienes existentes en el recinto.

Esta Hoja Mural será emitida por el Encargado de Inventario a cada funcionario con bienes inventariables asignados y deberá reemplazarse cada vez que se modifique por alta, baja o traslado de bienes.

Si no ha habido movimiento, deberá actualizarse una vez al año, a lo menos.

Firmarán esta Hoja, el Funcionario Responsable de los bienes, normalmente el usuario de ellos; el Jefe del Centro de Costos y el Encargado de Inventario del Servicio.

2.3.4.5 Identificación de los bienes

Todos los bienes muebles de uso deberán ser identificados mediante la adhesión o escritura del código de inventario que emita el Encargado de Inventario del Servicio.

Este código será único e irrepetible.

2.3.5 Gestión de Archivos y Documentos

2.3.5.1 Directrices Generales

Los documentos generados por mandato del Servicio de Gobierno Regional de Magallanes y Antártica Chilena a personas naturales y jurídicas externas, se consideran parte integrante del patrimonio.

Los documentos son únicos, en tanto cada trámite es producto de una acción administrativa. El hecho de ser únicos y constituir una fuente primaria de información y prueba jurídica de ello, demanda cuidados especiales de conservación.

Los documentos deberán estar organizados y la información accesible para su uso, en instalaciones adecuadas y bajo dirección de un funcionario de la misma repartición, nombrado especialmente para tal cometido, el cual se denominará “*encargado de archivos”.*

Esta persona tendrá un equipo de apoyo, “encargados de archivo de oficina” quienes serán responsables de los archivos de cada División, Departamento o Unidad.

Todos los documentos oficiales ORIGINALES, generados por el Servicio, deberán ser archivados en la Oficina de Partes.

No obstante en conocimiento que la División de Análisis y Control de Gestión confecciona sus propios Oficios, denominados Oficios DAC, éstos (originales) deberán quedar en manos de dicha División.

Así mismo las Actas de Sesiones Ordinarias, Actas de Sesiones Extraordinarias y Oficios Despachados confeccionados por el Consejo Regional, todos originales, deberán quedar en manos de dicho Consejo Regional.

Los documentos de carácter personal y/o privados no deben ser conservados en conjunto con los institucionales.

Ante el cese de funciones de un funcionario del Servicio, se debe confeccionar un acta de entrega o de traspaso de la documentación asociada a la gestión del funcionario que se retira.

En los casos de documentación correspondiente a procesos cerrados y que cumpla con las condiciones para su incorporación al Archivo Central, se debe proceder a su procesamiento para su traspaso correspondiente.

2.3.6 Activos de Personal

2.3.6.1 Inducción

Un nuevo funcionario ingresado a la institución, en calidad de planta o contrata, deberá recibir programas de inducción como máximo dentro de los primeros siete días hábiles a la fecha de su incorporación.

Esta inducción constará de a lo menos dos de tres componentes:

a) Aplicación Manual de Inducción
b) Inducción a cargo de la Unidad de Gestión de Personal
c) Inducción al cargo de su Jefe Directo en el lugar de trabajo

2.3.6.2 Aspectos Generales

La institución propicia el respeto a las personas, la tolerancia a la diversidad de opinión, credo religioso e ideológico, la solidaridad y el trabajo en equipo.

La institución velará por la salud ocupacional, la prevención de riesgos laborales de sus funcionarios, propiciando condiciones y medio ambiente de trabajo libre de riesgos para la salud física y mental de las personas.

La Institución propiciará la comunicación permanente suficiente y oportuna al personal, respeto a sus derechos laborales y previsionales, los beneficios de bienestar, las obligaciones y prohibiciones que establecen las leyes vigentes, entre otros.

La Organización procurará el mejoramiento del entorno laboral, el clima organizacional, el desarrollo personal y laboral, dentro de los lineamientos estratégicos definidos.

La Unidad de Gestión de Personal velará por el uso adecuado de la información personal de los funcionarios pertenecientes al Servicio, resguardando adecuadamente dichos activos de información.

Solo personal autorizado y bajo la supervisión de la Unidad de Gestión de Personal podrá tener acceso a la información contenida en los archivos de dicha unidad.

Se deberá mantener un listado actualizado de los funcionarios con sus datos personales y la información crítica que estos manejan dentro del Servicio, que será administrado por la Unidad de Gestión de Personal.

Será la Unidad de Gestión de Personal la encargada de velar por el correcto uso y funcionamiento de los relojes control del Servicio.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Seguridad de Recursos Humanos

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1 Introducción

1.1 Objetivo

Los objetivos de la Norma de Seguridad de Recursos Humanos:

- Establecer mecanismos específicos para el control adecuado de candidatos potenciales a cargos del Servicio de Gobierno Regional, para reducir el riesgo de error humano, el mal uso de recursos, robo y fraude.
- Reducir los daños ocasionados por incidentes de seguridad y mal funcionamiento.
- Asegurar que los funcionarios estén conscientes de las amenazas de la seguridad de la información y que se comprometan con la Política General de Seguridad de la Información, en lo que a su trabajo normal se refiere.

1.2 Ámbitos de aplicación

Todos los Activos de Información contenidos en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.3 Vigencia

Esta Norma de Seguridad de Recursos Humanos entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información
- Política de Recursos Humanos

2 Aspectos Generales

El Servicio de Gobierno Regional debe velar por la seguridad de sus activos de información asociados a los recursos humanos, es por esto que se deben realizar procesos de selección para los potenciales postulantes y en especial para aquellos trabajos que manejen información sensible.

Los antecedentes de los candidatos deben ser validados:

- Usando los contactos de referencia de empresas anteriores para confirmar experiencia.
- Buscando antecedentes que respalden la veracidad del currículo, mediante confirmación de credenciales académicas y profesionales, así como de los documentos de identidad presentados.
- Comprobando los antecedentes financieros y penales.
- Realizando evaluaciones psicológicas.

Los roles y responsabilidades en la seguridad deben ser documentados para cada cargo. Esta documentación debe incluir las responsabilidades relacionadas con la seguridad de la información, así como la responsabilidad en la protección de los recursos de información relevantes. Estas condiciones de trabajo deben quedar documentadas en el contrato de trabajo respectivo.

El personal debe tener presente desde el momento de su contratación su responsabilidad en la Seguridad de la Información.

Durante el proceso de inducción y antes de acceder a activos de la organización, el nuevo funcionario debe tomar conocimiento de las políticas de seguridad, así como en lo que respecta a requerimientos de seguridad, responsabilidades legales y controles en uso, tratamiento de incidentes, herramientas de trabajo y uso de aplicaciones. Además deberá firmar un acuerdo de confidencialidad. Esta norma deberá hacerse extensiva a funcionarios actualmente en servicio.

La responsabilidad por la seguridad de la información debe ser una obligación laboral diaria de todos los funcionarios.

El Jefe de Servicio debe impartir instrucciones claras para la seguridad de los documentos electrónicos, respecto de las siguientes materias:

- Uso de sistemas informáticos, con énfasis en prohibición de instalación de software no autorizado, documentos y archivos guardados en el computador.
- Uso de la red interna, uso de Internet, uso del correo electrónico, acceso a servicios públicos, recursos compartidos, servicios de mensajería y comunicación remota, y otros.
- Generación, transmisión, recepción, procesamiento y almacenamiento de documentos electrónicos.

Será responsabilidad de la Unidad de Gestión de Personal reportar incidentes de seguridad relacionados con activos de información de personal.

El Encargado de Seguridad debe informar a través de la Unidad de Gestión de Personal, a los funcionarios, la existencia de peligros potenciales para la seguridad de la información en su entorno de trabajo. De la misma manera se deberá informar la existencia de medidas para minimizar los riesgos asociados.

Se deberá entrenar a los funcionarios del Servicio, en los procedimientos de seguridad de la información, en el uso correcto de los equipos de procesamiento de la información y de los dispositivos de seguridad física y ambiental, para minimizar los posibles riesgos en la seguridad.

Cuando sea necesario, el entrenamiento debe hacerse extensivo a personal de terceros que deban realizar actividades que involucren acceso a información de carácter sensible para la organización.

Periódicamente se debe hacer reforzamiento del entrenamiento en seguridad para mantener actualizados a los funcionarios.

Antes del finiquito de un empleado, toda la información de la organización que estaba en su custodia debe ser retenida o recolectada para prevenir su divulgación no autorizada.

El personal del Servicio deberá portar una identificación que acredite su calidad funcionaria, durante su permanencia en el centro de labores. Dicha Credencial deberá ser requerida al momento del cese de funciones.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Seguridad Física y Ambiental

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

Contenido

1. Introducción

1.1 Objetivo

Las disposiciones han sido establecidas con el fin de prevenir los riesgos de accidentes del trabajo o enfermedades profesionales que pudieran afectar a los funcionarios del Servicio de Gobierno Regional y contribuyendo así a mejorar y aumentar la seguridad del personal en el Servicio. Por otro lado se establecen disposiciones para el personal en materias de Seguridad de todos los activos de información del Servicio.

Los objetivos de la Norma de Seguridad Física y Ambiental:

- Impedir el acceso no autorizado, daños o interferencias a los activos de información dentro de la organización.
- Prevenir pérdidas, daños o compromiso de los bienes e interrupción de las actividades del Servicio.
- Evitar que sean robados o se comprometa la información de los equipos que la procesan.
- Evitar riesgos y accidentes del personal que puedan causar pérdidas de activos de información.

1.2 Ámbitos de aplicación

Todos los Activos de Información contenidos en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.3 Vigencia

Esta Norma de Seguridad Física y Ambiental entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información
- Reglamento Interno de Orden, Higiene y Seguridad

2. Aspectos Generales

Todos los activos físicos clasificados como críticos deben ser protegidos de accesos no autorizados, en áreas seguras y controladas.

El Servicio debe establecer controles que protejan la información y los activos físicos que la procesan, de la divulgación, modificación o robo por personas no autorizadas.

Los equipos deben ser ubicados en lugares protegidos de modo de reducir el riesgo de accesos no autorizados y de amenazas tales como fuego, inundaciones, terremotos, explosiones, levantamientos civiles o cualquier otro tipo de siniestro.

Se deben proteger los equipos, según el nivel de sensibilidad que tengan asignado, de fallas y otras interrupciones causadas por falta de mantención de los equipos de soporte, cortes de energía eléctrica y variaciones de voltaje y trabajos realizados por terceros.

Los trabajos realizados por terceros deberán entregar toda la documentación relacionada con proyectos y mantenciones del equipamiento de la Organización.

El cableado de energía y telecomunicaciones que transporta datos o soporta servicios de información debe ser protegido de intercepciones o daño.

La instalación y mantención de cables de energía y líneas de telecomunicaciones, debe ser realizada por personal calificado, que sigan los estándares de calidad y seguridad de la industria y que cuenten con la certificación pertinente.

El equipamiento debe ser correctamente mantenido de modo de asegurar continuidad, disponibilidad e integridad.

Los equipos no deben salir de las instalaciones del Servicio sin la debida autorización.

Se deben tomar medidas de seguridad para el equipamiento que se utilice fuera de la organización, tomando en cuenta los diferentes riesgos asociados.

Todos los funcionarios con oficinas personales deben asegurar el cierre de las puertas cuando estas oficinas no estén en uso, de manera que sólo el personal autorizado pueda tener acceso a ellas.

Toda persona ajena al Servicio, debe exhibir en un lugar visible una identificación que indique su calidad de visita.

Nunca se debe realizar visitas de público a los centros de datos e instalaciones de comunicaciones (áreas seguras en general).

Los funcionarios no deben fumar, comer o beber, en áreas seguras, sala de servidores, áreas sensibles, donde se ubiquen equipos computacionales.

El personal del Servicio debe mantener el debido resguardo y reserva de la ubicación física de su sala de equipos y áreas sensibles.

Los funcionarios deben mantener sus escritorios y áreas de trabajo ordenadas, sin documentación sensible a la vista con el objetivo de que ésta no quede al alcance de personas malintencionadas.

Los dispositivos utilizados para imprimir o copiar información sensible, tales como impresoras, fotocopiadoras o máquinas de fax, deben ubicarse dentro de áreas seguras o bajo la supervisión de algún funcionario designado. También se deberá propender a incorporar mecanismos de seguridad en sus accesos.

El equipamiento que realiza labores de procesamiento de información crítica (servidores), debe tener medidas de seguridad adecuada o especial acorde con su criticidad.

3. Obligaciones

Todos los funcionarios del Servicio de Gobierno Regional, estarán obligados a tomar cabal conocimiento del reglamento interno de higiene y seguridad y a poner en práctica las normas y medidas contenidas en él.

Todo funcionario estará obligado a registrar la hora exacta de llegada y de salida del Servicio, esto por efecto de los posibles accidentes del trayecto.

Todos los funcionarios deberán respetar las siguientes normas de higiene en el Servicio a fin de evitar condiciones que puedan ocasionar enfermedades, contaminaciones y atraer moscas y roedores.

Mantener los lugares de trabajo libres de restos de comida, etc., los que deberán ser depositados exclusivamente en los receptáculos habilitados para tales efectos.

De acuerdo a las disposiciones legales vigentes, el Servicio está obligado a proteger a todo su personal de los riesgos del trabajo, entregándole al funcionario cuya labor la requiera, sin costo alguno, pero a cargo suyo y bajo su responsabilidad los elementos de protección del caso. Si es que fuera necesario, de acuerdo a eventuales actividades.

El funcionario deberá usar el equipo de protección que proporciona el Servicio cuando el desempeño de sus labores así lo exija. Será obligación del funcionario dar cuenta en el acto a su jefe inmediato cuando no sepa usar el equipo o elemento de protección.

Los elementos de protección que se reciban son de propiedad del Servicio, por lo tanto, no pueden ser enajenados, canjeados o sacados fuera del recinto de la faena, salvo que el trabajo así lo requiera.

Para solicitar nuevos elementos de protección, el funcionario está obligado a devolver lo que tenga en su poder. En caso de deterioro o pérdida culpable o intencional, la reposición será del cargo del funcionario.

Todo funcionario deberá informar en el acto al Jefe de inmediato si su equipo de protección ha sido cambiado, sustraído, extraviado o se ha deteriorado, solicitando su reposición.

El funcionario deberá conservar y guardar los elementos de protección personal que reciba en el lugar y en la oportunidad que indique el jefe inmediato o lo dispongan las Normas de Seguridad o Reglamentos.

Los Jefes Inmediatos serán directamente responsables de la supervisión y control del uso oportuno y correcto de los elementos de protección y del cumplimiento de las normas.

Las maquinarias y equipos del tipo que sean deberán ser manejadas con los elementos de protección requeridos, con el propósito de evitar la ocurrencia de accidentes del trabajo.

El o los funcionarios que usen escalas deberán cerciorarse de que estén en buenas condiciones. No deberán colocarse en ángulos peligrosos, ni afirmarse en suelos resbaladizos, cajones o tablones sueltos.

Los funcionarios deberán preocuparse y cooperar con el mantenimiento y buen estado de funcionamiento y uso de maquinarias, herramientas e instalaciones en general. Deberán asimismo preocuparse de que su área de trabajo se mantenga limpia, en orden, despejada de obstáculos, esto para evitar accidentes o que se lesione cualquiera que transite a su alrededor.

Las vías de circulación interna y/o de evacuación deberán estar permanentemente señaladas y despejadas, prohibiéndose depositar en ellas elementos que puedan producir accidentes, especialmente en caso de siniestros.

Los lugares de trabajo deberán mantenerse limpios y ordenados evitando los derrames de cualquier líquido, grasa u otra sustancia que pueda producir resbalones o caídas.

Al término de cada jornada el funcionario deberá procurar dejar despejada su área, ordenada y sin excedentes de materiales inutilizados.

El almacenamiento de los desechos y basura se harán en lugares designados específicamente por los jefes superiores, no pudiendo los funcionarios improvisar los lugares de depósito, ni mucho menos atochar las vías de circulación.

Todo funcionario que sufra un accidente, dentro o fuera del Servicio, por leve o sin importancia que el parezca, debe dar cuenta en el acto a su Jefe Inmediato.

Todo funcionario está obligado a colaborar en la investigación de los accidentes que ocurran en el Servicio Gobierno Regional. Deberá avisar a su Jefe Inmediato cuando tenga conocimiento o haya presenciado cualquier accidente acaecido a algún compañero, aún en el caso que éste no lo estime de importancia o no hubiese sufrido lesión. Igualmente, estará obligado a declarar en forma completa y real, los hechos presenciados o de que tenga noticias, cuando la Institución lo requiera.

El funcionario que padezca alguna enfermedad o que note que se siente mal, si el malestar afecta su capacidad y por ende su seguridad en el trabajo deberá poner esta situación en conocimiento de su Jefe Inmediato, para que éste proceda a tomar las medidas que el caso requiere.

Los avisos, letreros y afiches de seguridad deberán ser leídos por todos los funcionarios, quienes deberán cumplir con sus instrucciones.

Los mismos avisos, carteles, afiches, deberán ser protegidos por todos los funcionarios quienes deberán impedir su destrucción, debiendo avisar a la autoridad competente de su falta con el fin de reponerlos.

El funcionario debe conocer exactamente la ubicación de los equipos extintores de incendio del sector en el cual desarrolle sus actividades, como asimismo conocer la forma de operarlos, siendo obligación de todo Jefe velar por la debida instrucción del personal al respecto.

Todo funcionario que observe un amago, inicio o peligro de incendio, deberá dar alarma inmediata y se incorporará al procedimiento establecido por el Servicio para estos casos.

El acceso a los extintores deberá mantenerse despejado de obstáculos.

4. Prohibiciones

Ingresar al lugar de trabajo o trabajar en estado de intemperancia, prohibiéndose terminantemente entrar bebidas alcohólicas al establecimiento, beberla o darla a beber a terceros.

Fumar o encender fuegos en los lugares que se hayan señalado como prohibidos.

Comer o preparar alimentos en el lugar de trabajo, a menos que las circunstancias lo ameriten.

Alterar el registro de hora de llegada propia o de algún funcionario o el registro de hora de salida y tratarse por propia cuenta las lesiones que haya sufrido en algún accidente.

Permanecer en los lugares de trabajo después del horario sin autorización del Jefe Inmediato.

Negarse a proporcionar información en relación con determinadas condiciones de trabajo y de su seguridad o acerca de accidentes ocurridos.

Romper, rayar, retirar o destruir avisos, carteles, afiches, instructivos, reglamentos acerca de la seguridad e higiene.

Usar calzado inadecuado que pueda producir resbalones o torceduras.

Lanzar objetos de cualquier naturaleza que estén dentro del recinto del Servicio, aunque éstos no sean dirigidos a persona alguna.

Trabajar en altura, conducir vehículos motorizados de cualquier tipo, padeciendo de vértigos, mareos o epilepsia; trabajar en faenas que exigen esfuerzo físico, padeciendo insuficiencia cardíaca o hernia, o de ejecutar trabajos o acciones similares sin estar capacitado o autorizado para ello.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Gestión de las Comunicaciones y Operaciones

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1 Introducción

1.1 Objetivo

El objetivo de la Norma de Gestión de las comunicaciones y operaciones es asegurar la operación correcta y segura de los medios de procesamiento de la información, establecer responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

1.2 Ámbitos de aplicación

Todos los Activos de Información contenidos en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.3 Vigencia

Esta Norma de Funciones, Responsabilidades y Organización entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2 PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES

2.1 Lineamientos y Control

Será la Unidad de Tecnología, Información y Comunicaciones, la responsable de explicitar y difundir los siguientes antecedentes e información,

- Los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos;
- Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado;
- Las buenas prácticas para protegerse de los riesgos asociados a la obtención de archivos y software a través de las redes de telecomunicaciones, o por otros medios, indicando qué medidas de protección se deberán aplicar. Para los efectos de reducir el riesgo de negligencia o mal uso deliberado de los sistemas deberán aplicarse políticas de segregación de funciones. Asimismo, deberán documentarse los procedimientos de operación de sistemas informáticos e incorporarse mecanismos periódicos de auditorías de la integridad de los registros de datos almacenados en documentos electrónicos.
- Realizar copias de respaldos de la información y las aplicaciones críticas para la misión de la institución en forma periódica
- La periodicidad con que se realizarán los respaldos de los computadores personales de la institución que estén asignados a usuarios, deberá explicitarse y no podrá ser menor a 1 respaldo anual;
- La periodicidad con que se realizarán los respaldos de los sistemas informáticos y los equipos no contemplados en el punto anterior, utilizados en el procesamiento o almacenamiento de documentos, deberá calendarizarse anualmente de acuerdo a su criticidad.
- Deberá garantizarse la disponibilidad de infraestructura adecuada de respaldo, para asegurar que éstos estén disponibles incluso después de un desastre o la falla de un dispositivo. Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen los requisitos estipulados en los planes de continuidad institucionales;
- Deberá almacenarse en una ubicación remota, un nivel mínimo de información de respaldo, junto con registros exactos y completos de las copias de respaldo y los procedimientos documentados de restablecimiento. Esta instalación deberá estar emplazada a una distancia tal que escape de cualquier daño producto de un desastre en el sitio principal. En ámbitos críticos para la institución, se deberán almacenar al menos tres generaciones o ciclos de información de respaldo;
- Los respaldos deberán cumplir con un nivel apropiado de protección física de los medios, consistente con las prácticas aplicadas en el sitio principal. Los controles asociados a los dispositivos del sitio de producción deberán extenderse para abarcar el sitio de respaldo.
- Deberán consignarse plazos de retención de los respaldos de la institución, así como cualquier necesidad de realización de respaldos que estén permanentemente guardados, y
- Deberán utilizarse medios y condiciones físicas de almacenamiento que garanticen una vida útil concordante con los plazos definidos en el punto precedente.

2.2 Gestión de la entrega del servicio de terceros

Se deberá implementar y mantener el nivel apropiado de seguridad de la información y la entrega del servicio en línea con los acuerdos de entrega de servicios de terceros.

2.2.1 Entrega del servicio

- La entrega de servicios por parte de un tercero deberá incluir los acuerdos de seguridad pactados, definiciones del servicio a prestar y aspectos de la gestión del mismo.
- En caso de que el acuerdo implique abastecimiento externo, el servicio debiera planear las transiciones necesarias (de información, medios de procesamiento de la información y cualquier otra cosa que necesite transferirse), y se deberá asegurar que se mantenga la seguridad a través del periodo de transición.
- Se deberá asegurar que la tercera persona mantenga una capacidad de servicio suficiente junto con los planes de trabajo diseñados para asegurar que se mantengan los niveles de continuidad del servicio después de fallas importantes o un desastre.

2.2.2 Monitoreo y revisión de los servicios de terceros

- Será la División, Departamento o Unidad receptora del servicio prestado, la encargada de monitorear los niveles de desempeño para chequear adherencia con los acuerdos;
- Solicitará y revisará reportes de servicio producidos por terceros.
- Proporcionará información sobre incidentes de seguridad de la información relacionados con servicios de terceros.
- El Servicio deberá mantener el control y visibilidad general suficiente en todos los aspectos de seguridad con relación a la información confidencial o crítica o los medios de procesamiento de la información que la tercera persona ingresa, procesa o maneja.

2.3 Protección contra el código malicioso

El Servicio deberá tomar precauciones para evitar la introducción de códigos maliciosos

2.3.1 Controles contra códigos maliciosos

- Se prohíbe la utilización de cualquier Software no autorizado por la Unidad de tecnología, información y Comunicaciones (UTIC).
- Se realizarán por parte de UTIC, revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos críticos , investigando formalmente la presencia de cualquier activo no aprobado o enmiendas no autorizadas.
- UTIC instalará y actualizará regularmente el Software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria.
- UTIC instalará y monitoreara un Antivirus para evitar el ingreso de virus dañinos a los sistemas críticos del Servicio.

2.4 Respaldo o Back-UP

El Servicio deberá mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

Se establecerán procedimientos de rutina para tomar copias de respaldo de la data y practicar su restauración oportuna.

Se considerará los siguientes ítems para el respaldo de la información:

- La Jefaturas de División deberán definir el nivel necesario de respaldo de la información;
- UTIC producirá registros exactos y completos de las copias de respaldo y procedimientos documentados de la restauración;
- la extensión (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos debiera reflejar los requerimientos de criticidad del Servicio, para la operación continua de la organización;
- Las copias de respaldo se almacenarán en un lugar apartado, a la distancia suficiente como para escapar de cualquier daño por un desastre en el local principal; dicha responsabilidad recaerá en la División de Administración y Finanzas.
- Los medios de respaldo se deberán probar regularmente por parte de UTIC para asegurar que se pueda confiar en ellos para usarlos cuando sea necesario en caso de emergencia;
- Los procedimientos de restauración se deberán chequear y probar regularmente por UTIC para asegurar que sean efectivos y que pueden ser completados dentro del tiempo asignado en los procedimientos operacionales para la recuperación;

2.5 Gestión de Seguridad de la Red

El Servicio deberá asegurar la protección de la información en redes y la protección de la infraestructura de soporte.

La Unidad de Tecnología, Información y comunicaciones implementará controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados. En particular, se consideraran los siguientes ítems:

- La responsabilidad operacional para las redes se deberá separar de las operaciones de cómputo;
- Se establecerán las responsabilidades y procedimientos para la gestión del equipo remoto, incluyendo el equipo en las áreas del usuario;
- Se establecerán controles especiales para salvaguardar la confidencialidad y la integridad de la data que pasa a través de las redes públicas o privadas;
- Se deberán aplicar registros de ingreso y monitoreo apropiados para permitir el registro de las acciones de seguridad relevantes;
- Las actividades de gestión deberán estar estrechamente coordinadas para optimizar el servicio a la organización y para asegurar que los controles sean aplicados consistentemente a través de la infraestructura de procesamiento de la información.;

2.6 Gestión de Medios Removibles

Si ya no son requeridos, los contenidos de los medios re-usables que no son removidos de la organización no deberán ser recuperables;

Se deberá establecer los procedimientos para identificar los ítems que requieren de una eliminación segura;

Cuando sea posible se deberá registrar la eliminación de ítems confidenciales para mantener un rastro de auditoría.

El Comité de Seguridad del Servicio establecerá los procedimientos para el manejo y almacenaje de información para proteger esta información de una divulgación no-autorizada o mal uso.

3 Uso de Internet

3.1 General

- La navegación por Internet se realizará mediante la aplicación que la Unidad de Tecnología, Información y Comunicaciones especifique e instale en los computadores de los usuarios. Si un usuario requiere por motivos técnicos de alguna aplicación que requiera utilizar otro navegador, deberá solicitar autorización expresa de la Unidad de Tecnología, Información y Comunicaciones.

- La Unidad de Tecnología, Información y Comunicaciones es la única autorizada a cambiar la configuración de la conexión a Internet, es decir, de los navegadores que utilizan los usuarios.

- La Unidad de Tecnología, Información y Comunicaciones es responsable de que todos los navegadores tengan deshabilitado cualquier elemento que genere una vulnerabilidad en la seguridad de la conexión.

- La conexión a Internet en las instalaciones del Servicio será a través de él o los servidores de la red del Servicio, ninguna conexión a Internet deberá realizarse a través de módem ú otro medio de acceso a Internet distinto al que provee el Servicio.

- En caso de establecerse conexiones a través de otros medios éstas deben ser previamente autorizadas y registradas por la Unidad de Tecnología, Información y Comunicaciones.

- Se debe controlar la introducción de virus en forma intencional o bien accidentalmente a través de archivos bajados de Internet. Los virus pueden degradar el servicio y la disponibilidad de los sistemas, o puede también generar la pérdida o corrupción de datos, requeridos para la mantención de las operaciones vitales del Servicio.

- Si el usuario incurriese en conductas prohibidas en el uso de la conexión Internet será motivo suficiente para cancelar este privilegio y aplicar las medidas disciplinarias generales que estipule el reglamento correspondiente.

3.2 Usos permitidos de Internet

Se otorgará el uso Internet como herramienta para soportar las actividades del Servicio necesarias para llevar a cabo de mejor manera sus funciones de trabajo.

El uso aceptable de Internet, incluye:

- Comunicación entre funcionarios y no funcionarios para fines de la institución,
- Comunicación con los clientes actuales y potenciales clientes,
- Soporte técnico de la Unidad de Tecnología, Información y Comunicaciones para bajar actualizaciones (parches).
- Revisión de sitios web de posibles proveedores para obtener información de los productos y obtener referencia regulatoria e información asociada a las funciones, además de recursos.
- Uso para fines personales, respetando normas de buenas conductas que permitan optimizar el uso del tiempo disponible y que no entorpezcan las labores habituales.
- El acceso a Internet está sujeto a normas éticas de buen uso de los recursos, las que deberán ser observadas por los usuarios y administradores de este servicio.
- Si por motivos de trabajo un usuario requiere bajar software desde Internet, éste deberá pedir a la Unidad de Tecnología, Información y Comunicaciones, la autorización necesaria para evitar violaciones a acuerdos de licencia de software, así como para evitar introducir

a la red del Servicio algún tipo de código malicioso (virus, troyanos). En cualquier caso, sólo la Unidad de Tecnología, Información y Comunicaciones está facultada para realizar la instalación.

3.3 Usos prohibidos de Internet

- Internet no debe usarse para distraer tiempo de las funciones para cuales ha sido contratado.
- Se prohíbe la utilización de Internet para fines ajenos al Servicio, tales como:
  - Realizar actividades personales que puedan generar costos adicionales al Servicio.
  - Realizar actividades políticas, religiosas u de otra índole que no sean propias de las funciones del usuario.
  - Comprometer información del Servicio de Gobierno Regional.
  - Involucrar el nombre e imagen del Servicio en actividades fraudulentas o ilegales a través de Internet, incluyendo enviar y recibir material que transgreda los derechos de autor y acuerdos de licencias.
  - Distribuir intencionalmente información falsa o difamatoria que podría deteriorar la reputación del Servicio de Gobierno Regional ante posibles acciones legales o de otro tipo, debido al mal uso de Internet.
  - Bajar, adquirir, almacenar, distribuir o imprimir información ilegal, pornográfica, o descriptiva en forma negativa de razas, sexo, política o creencias religiosas.
  - Bajar material registrado (Copyright). Toda reproducción de material disponible en Internet debe ser hecha sólo con el permiso escrito del autor o propietario del documento.
  - Bajar de Internet, instalar o ejecutar programas tendientes a detectar, reconocer y explotar vulnerabilidades de la red interna o de los sistemas de seguridad del Servicio. (Por ejemplo; programas para realizar cracking de contraseñas).
  - Utilizar el nombre del Servicio de Gobierno Regional, en instancias públicas o privadas no teniendo autorización para ello. Por ejemplo chat, foros, news, etc.
  - Bajar de Internet gráficos, MP3, música, imágenes o videos que degraden de alguna manera el servicio, a menos que exista un uso en el Servicio específico, explícito, para tal material.

3.4 Asignación y revocación de acceso a los servicios de Internet

Se debe revocar toda cuenta de usuario que permanezca inactiva por un período prolongado de tiempo.

El otorgamiento de los servicios Internet (e-mail, Navegación, Protocolo de transferencia de archivos (FTP), Telnet) deberán ser provistos de acuerdo a las necesidades del Servicio, así la administración de la red se reservará el derecho de agregar o suprimir servicios.

Se deberá revocar el acceso a Internet de los usuarios en los siguientes casos:

- El usuario deja de trabajar en Servicio de Gobierno Regional
- El usuario ha incurrido en conductas prohibidas en el uso de Internet.

En el caso de existir mal uso del recurso, se aplicarán al usuario las sanciones tipificadas en el Reglamento Interno.

3.5 Control de acceso a Internet y Monitoreo

El Servicio de Gobierno Regional se reserva el derecho de emplear herramientas que le permitan monitorear, registrar y filtrar los accesos de los usuarios a Internet, cuyos resultados podrán ser utilizados para los fines que se estimen convenientes.

Se dispondrá de los recursos necesarios que permitan verificar y controlar el cumplimiento de las normas y velar así por la seguridad de los recursos y sistemas del Servicio de Gobierno Regional.

La administración se reserva el derecho de examinar el Log de conexiones a la web, directorios de archivos personales y cualquier otra información almacenada sobre los computadores del Servicio de Gobierno Regional, en cualquier momento y sin aviso, como parte de un programa de auditoría. Dicha revisión será con el objeto de asegurar el cumplimiento de las políticas internas.

La Unidad de Tecnología, Información y Comunicaciones deberá proveer las herramientas necesarias para bloquear páginas de Internet que el Servicio de Gobierno Regional considere no apropiadas (ej.: con contenido pornográfico, con software para vulnerar las redes y sistemas, etc.). Adicionalmente, las herramientas deberán permitir entregarle un mensaje de advertencia al usuario cuando intente ingresar a páginas definidas como prohibidas por el Servicio.

4 Uso del Correo Electrónico 

4.1 General

El correo electrónico es conveniente, rápido y efectivo para comunicarse con los otros funcionarios, proveedores y clientes del Servicio de Gobierno Regional.

No obstante, el correo electrónico debe emplearse en forma adecuada, debido a que cualquier declaración o mensaje irresponsable o sensible en un correo electrónico puede ser utilizado en contra del funcionario y del Servicio de Gobierno Regional. Asimismo, comentarios de críticas hacia otras personas, bajo ciertas circunstancias, pueden llegar a constituir algún tipo de acoso o discriminación.

El estar conectado al correo electrónico aumenta el riesgo de transferir (en forma no autorizada) información o archivos del Servicio de Gobierno Regional y viceversa.

4.2 Usos permitidos de los servicios de correo electrónico

El correo electrónico debe ser utilizado únicamente para soportar las actividades del Servicio necesarias para llevar a cabo de mejor manera sus funciones de trabajo.

El uso aceptable del correo se basará fundamentalmente en la comunicación entre funcionarios y no funcionarios para fines del Servicio. Se acepta el uso eventual para fines personales, siempre y cuando éste no interfiera con las actividades del Servicio de Gobierno Regional, además no se viole ninguna otra política, disposición, pauta o norma de este acuerdo o cualquier otro acuerdo del Servicio de Gobierno Regional.

Sólo la Unidad de Tecnología, Información y Comunicaciones puede utilizar el correo electrónico para advertir sobre virus o su posible existencia en los computadores personales, habiendo verificado la autenticidad de la fuente de información.

4.3 Usos prohibidos de los servicios de correo electrónico

Los usos prohibidos del correo electrónico son, entre otros:

- Suscribirse a páginas de humor o transmitir imágenes inapropiadas. El contenido de los mensajes no debe ser injurioso, ofensivo o irrespetuoso, ni debe hacer referencia a temas filosóficos, políticos, religiosos, de sexo u otros que por su contenido se aparten de temas propios del Servicio.
- Envío de cadenas o mensajes que impliquen el reenvío de mensajes o campañas de tipo solidario.
- Uso del sistema de correo electrónico para asuntos de caridad o comerciales ajenos al Servicio.
- Manejar o participar en actividades políticas, comprometer información del Servicio de Gobierno Regional, estar involucrado en actividades fraudulentas o distribuir intencionalmente información falsa o difamatoria.
- Difundir por correo electrónico al interior del Servicio de Gobierno Regional, noticias que provengan de Internet o de otros medios, o tomar información de dicha red dándola por cierta.
- Enviar material confidencial del Servicio de Gobierno Regional a personas no autorizadas a conocer o poseer dicha información.
- Uso de copias ocultas en el envío de correos con información confidencial.
- Re-enrutar en forma automática el mail del Servicio a una cuenta de correo privada.
- Uso de mensajería instantánea (Yahoo Messenger, MSN Messenger etc.) durante la jornada de trabajo, a menos que la necesidad del Servicio así lo requiera y se autorice a nivel de jefatura el uso de uno en particular.
- Chatear con personas ajenas al Servicio, durante la jornada laboral.
- Las cuentas de usuario no puede utilizarse para difundir, visualizar o almacenar anuncios personales o comerciales, ofertas de servicios, promociones u otra información similar.

4.4 Consideraciones

- Las comunicaciones realizadas por este medio serán consideradas formales.
- En la comunicación por correo se deberán mantener las mismas reglas de cortesía y formalidades de la información escrita, aplicando también todas las reglas semánticas y ortográficas.
- Toda comunicación fuera del Servicio de Gobierno Regional, debe incluir la siguiente cláusula de confidencialidad:

> *“Este mensaje es una comunicación privada. En caso de recepción accidental por terceras personas, sírvase remitir toda copia al emisor inmediatamente.*
> *La privacidad de esta comunicación goza de protección legal. En consecuencia, está prohibido leer, conservar, copiar, divulgar o transmitir todo o parte de este mensaje a personas diferentes de su destinatario legal su emisor original.*
>
> *This message is a private communication. In case of accidental receipt by other than those addressed, refer all copies to sender. Sender and addressee are entitled to legal protection for the privacy of this communication. Therefore, it is strictly forbidden to read, keep, and copy, publish or transmit this message, or any portion of it, to persons different than the addressee or the initial sender.”*

- Cualquier documento o archivo que se adjunte a un mensaje, deberá estar libre de virus.
- Será responsabilidad del área emisora del mensaje la revisión mediante antivirus. Las áreas receptoras de mensajes infectados con virus o sospechosos deberán abstenerse de abrirlos y deberán informar a la Unidad de Tecnología, Información y comunicaciones.

- No se deben enviar correos electrónicos con archivos adjuntos superiores a lo establecido por la Unidad de Tecnología, Información y comunicaciones.
- Se recomienda precaución en la manipulación de archivos ejecutables que vengan adjuntados en los correos electrónicos.
- Si el origen del correo electrónico es desconocido, no ejecute o abra ningún archivo adjuntado antes de que éste sea revisado por personal de la Unidad de Tecnología, Información y comunicaciones.
- Cuando se incluya el mensaje original en una respuesta, se sugiere eliminar toda información accesoria que no esté relacionada con el contenido de la respuesta. En estos casos queda estrictamente prohibido introducir modificaciones a los mensajes anteriores sin advertir por escrito esa circunstancia.
- Cada usuario es responsable de mantener un óptimo uso de su cuenta para permitir la correcta recepción de mensajes, para lo cual deberá realizar los respaldos necesarios y eliminar el correo antiguo.
- Para los comunicados masivos, en caso de que el receptor considere necesario contestar al emisor, está debe realizarse sólo al emisor, y no a todos los destinatarios del mail.
- Los correos deberán contener el siguiente pie de firma institucional:

Nombre del Funcionario
Cargo del Funcionario
Servicio de Gobierno Regional
Magallanes y Antártica Chilena
(56-61) telefono directo
www.goremagallanes.cl

4.5 Otorgamiento de acceso a los servicios de correo electrónico

- En los casos que corresponda, se debe otorgar acceso a los servicios de correo a aquellos funcionarios no contratados (part - time) por períodos definidos, los que pueden ser reactivados de acuerdo a las necesidades de sus labores. Esto previa autorización de la Unidad de Tecnología, Información y Comunicaciones.
- En el caso de personal externo, se deberán incluir las cláusulas de esta norma en el contrato de prestación de servicios.
- Las cuentas de correo que por su naturaleza deban permanecer como cuentas genéricas deben ser excepcionales, (previo consentimiento del Administrador de Sistemas) deberán siempre estar re-enrutadas a alguien que aparezca como responsable.
- Tratar de evitar el uso de cuentas genéricas de correo. En caso de requerirse, tratar de que éstas sean utilizadas sólo para recibir información y no permitan enviar mensajes. Toda respuesta debe emanar de la cuenta personal del responsable.
- Cuando la ausencia prolongada sea una “ausencia programada”, por ejemplo un permiso o vacaciones, se deberá dejar en el correo una respuesta automática que señale el período de ausencia y un número de teléfono del reemplazante para comunicarse en casos urgentes o importantes.
- Las cuentas de correos de usuarios que dejen de pertenecer a la organización, serán bloqueadas, respaldadas y posteriormente eliminadas, no permitiendo bajo ningún punto de vista que estás sean enrutadas a otros correos. Además, se eliminará el acceso a dichas cuentas desde fuera de la red del Servicio.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Gestión de Acceso

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1 Introducción

1.1 Objetivo

El objetivo de la Norma de Gestión de Acceso es asegurar una adecuada administración de las autorizaciones y contraseñas de los usuarios a los activos tecnológicos y de información del Servicio de Gobierno Regional.

1.2 Ámbitos de aplicación

Todos los Activos de Información contenidos en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.3 Vigencia

Esta Norma de Funciones, Responsabilidades y Organización entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2 Administración de cuentas de usuarios y perfiles de acceso

2.1 Administración de los accesos

El proceso de la administración de los accesos de usuarios a los recursos informáticos debe estar regulado y supervisado por:

- Los Administradores de Sistemas y Plataformas de cada uno de los recursos,
- Propietario de Datos
- El Jefe de División, Departamento o Unidad, para la creación y eliminación de usuarios.

Los usuarios para ser autorizados a acceder a los recursos informáticos deben cumplir los siguientes pasos:

2.1.1 Solicitud de acceso

La solicitud de los accesos debe ser requerida por el Jefe de División, Departamento o Unidad, solicitante con a los menos 1 día hábil de anticipación.

La Jefatura que está solicitando, deberá identificar los recursos específicos a los cuales el usuario requiere acceder. Recursos tales como:

- Red del Servicio de Gobierno Regional
- equipo de procesamiento
- una aplicación específica
- base de datos
- servicios
- menús y/o funcionalidades
- lista de autorizaciones
- objetos
- grupos
- dominios
- otros recursos que deben identificarse puntualmente
- equipos
- licencias
- otros.

Se debe tener en cuenta que debe existir una adecuada segregación de funciones, desde un punto de vista de control interno, de acuerdo con la función administrativa del usuario, la criticidad de los datos y la oposición de intereses.

En el caso de los traspasos de cargos, el Jefe de División, Departamento o Unidad deberá informar del cambio al Propietario de Datos pertinente quien deberá evaluar si los permisos otorgados con anterioridad deben o no continuar vigentes.

2.1.2 Acceso a los recursos en cada uno de los equipos

El acceso a los recursos de los equipos debe ser autorizado por el Propietario de los Datos para los cuales se está solicitando acceso.

Como principio general, el usuario sólo debe tener acceso a los recursos indispensables para realizar su tarea.

La asignación de permisos a los recursos solicitados debe ser ejecutada por el Administrador de Sistemas correspondiente y deberá contar con las aprobaciones de accesos.

2.2 Uso de formularios para Altas, Bajas y Modificaciones

Para solicitar creaciones, bajas o modificaciones de cuentas de usuarios a los sistemas y a los datos se deberá utilizar el medio que la Unidad de Tecnología, Información y Comunicaciones disponga, el que deberá ser completado por el Jefe de División, Departamento o Unidad solicitante y enviado por la vía que se publique a la Unidad de Tecnología, Información y Comunicaciones.

2.3 Bajas de usuarios

El Jefe de División, Departamento o Unidad respectivo debe informar la baja de los usuarios que ya no presten servicios en sus respectivas funciones, enviando el formulario correspondiente a la Unidad de Tecnología, Información y Comunicaciones, a partir de la fecha de vigencia de la desvinculación o cambio de cargo.

Adicional a lo anterior, el Departamento de Gestión de Personal debe comunicar mensualmente, a través de un listado, a los Administradores de Sistemas de los distintos ambientes y sistemas, los nombres de los usuarios que ya no pertenecen al Servicio, para que estos realicen un control efectivo de los usuarios habilitados.

2.4 Administración de cuentas especiales

Si un usuario requiere de una cuenta especial (de altos privilegios), ésta deberá ser autorizada por el Comité de Seguridad de Información y ejecutado por la Unidad de Tecnología, Información y Comunicaciones

El Comité de Seguridad de Información deberá identificar las cuentas de usuarios de mayor riesgo de cada uno de los sistemas.

Los Administradores de Sistemas son los responsables de definir las cuentas con máximos privilegios en las aplicaciones para acceder en situaciones de emergencia, identificando a las personas que pueden acceder a las mismas.

Las contraseñas de estas cuentas deben permanecer en un sobre cerrado, en un lugar de acceso restringido.

La responsabilidad por la administración y custodia de las contraseñas correspondientes a las cuentas de mayor riesgo recae en la Unidad de Tecnología, Información y Comunicaciones.

2.5 Responsabilidades del Administrador de Sistemas

Los Administradores de Sistemas son responsables de:

- Controlar que la solicitud de creación, acceso, modificación haya sido autorizada por los Propietarios de los Datos.
- Controlar que la solicitud de baja de los usuarios, haya sido requerida por los responsables autorizados, Jefes de Unidad, Propietarios de los Datos y Recursos Humanos.
- Dejar constancia en el formulario de su revisión y del ingreso al sistema realizado.

- Controlar la información de las cuentas de usuarios que están en proceso como aquellas ya procesadas.
- Mantener adecuadamente resguardada la información de seguridad definida en el sistema inherente a la administración de usuarios y recursos.

2.6 Perfiles de Acceso de los Usuarios

Los perfiles de accesos son el conjunto de atribuciones y privilegios a los cuales tiene acceso una cuenta de usuario o grupo de usuarios.

Los Propietarios de los Datos deben revisar en forma periódica los perfiles de usuario del personal vigente y realizar una actualización de éstos cada vez que ocurra un cambio en la definición de funciones.

La responsabilidad de asignar un determinado perfil a un usuario corresponderá al Propietario de Datos.

El Propietario de Datos deberá considerar lo siguiente:

- Realizar un constante análisis de las funciones del personal del Servicio dentro de los activos de información bajo su responsabilidad.
- El perfil de usuario (Función que desempeña el usuario) debe ser solicitado formalmente por el Jefe de División, Departamento o Unidad directo al Propietario de Datos.
- Los perfiles de usuario deberán estar acorde a las funciones de cada rol dentro de la Organización.
- No asignar mayores privilegios a un usuario que las descritas por función.
- Asegurar que los accesos de todos los usuarios se otorguen teniendo en cuenta el grado de necesidad de conocimiento/uso que deban tener los mismos sobre los datos. Los accesos deben ser otorgados brindando a los usuarios los mínimos privilegios necesarios para poder tener un adecuado manejo sobre los datos, teniendo en cuenta el grado de sensibilidad y criticidad de los mismos conjuntamente con el principio de oposición de intereses entre las distintas funciones.
- Cualquier cambio en los perfiles de usuario debe ser validado ante el Propietario de Datos por el Jefe de División, Departamento, o Unidad especificando las razones del cambio.
- Minimizar la generación y el uso de perfiles de usuario con máximos privilegios o similares. Para ello se deben implementar las facilidades brindadas por los sistemas para la creación de perfiles personalizados. Todos los usos de estos tipos de perfiles deben ser revisados por el Administrador de Sistemas correspondiente.
- Asegurar que ningún usuario pueda introducir, extraer o modificar información de los sistemas informáticos por vías no autorizadas. Esto incluye todo tipo de software ilegal o copias no autorizadas de software legal.
- Restringir el acceso de los usuarios de producción a los productos y/o utilitarios que permitan la alteración no autorizada de datos y/o programas.
- Monitoreo y revisión de los servicios de terceros

2.7 Cuentas de usuario

Las cuentas de usuario deben cumplir con los requerimientos que se detallan a continuación:

- Cada persona debe tener una única identificación de su cuenta personal de usuario en todos los sistemas / equipos del Servicio.
- La identificación de la cuenta personal debe corresponder a una nomenclatura estándar predefinida.

- La identificación de cuentas especiales, también debe corresponder a una nomenclatura estándar predefinida.

2.8 Utilización de las cuentas de usuario

Se prohíbe a los usuarios la utilización de cuentas genéricas y compartir su cuenta con otros usuarios. En caso de requerir compartir o emplear cuentas genéricas, éstas deberán ser autorizadas por el Jefe correspondiente y tendrán acceso sólo de visualización.

3 Administración de contraseñas

Para una adecuada administración de las contraseñas a los recursos informáticos, a través de un sistema de control de accesos, debe tenerse en cuenta las siguientes consideraciones:

3.1 Compromiso del usuario

Todo usuario debe efectuar un compromiso de responsabilidad y confidencialidad del uso de su cuenta de usuario, de la respectiva contraseña asignada y de la información de los sistemas informáticos a los que acceda.

Cada vez que un usuario tenga que cambiar su contraseña, el sistema le debe arrojar un mensaje de compromiso de confidencialidad (siempre y cuando se dispongan de las herramientas automáticas que lo permitan).

3.2 Administración de contraseñas de cada usuario

Toda cuenta de usuario debe tener asociada obligatoriamente una contraseña.

Cada vez que un usuario sea creado en un recurso de la organización, se deberá definir una contraseña única, la cual será otorgada por el Administrador de Sistemas del sistema correspondiente. Esta contraseña de carácter personal, deberá ser cambiada obligatoriamente en el primer acceso realizado por el usuario.

Todas las contraseñas deben cumplir con los siguientes requisitos (siempre y cuando se dispongan de las herramientas automáticas que lo permitan):

- Deben permanecer encriptadas y residir en archivos ocultos y protegidos.
- No deben ser visibles por pantalla al momento de ser ingresadas.
- Deben ser definidas con una longitud mínima de ocho (8) posiciones.
- Debe contener letras y números (ser alfanumérica).
- No deben ser en blanco.

Para la generación de contraseñas se debe seguir la siguiente metodología de combinación de datos:

- La contraseña no debe ser igual a la identificación personal (User_ID) ni tampoco ser demasiado obvias.
- El Administrador de Sistemas debe comunicar al usuario la contraseña (cuando se le otorgue por primera vez).

- En caso de que el Administrador de Sistemas lo crea conveniente debe utilizar adicionalmente procedimientos de llamado y re llamado para asegurarse la identidad del usuario al que le transfiere la contraseña.

Para el cambio de las contraseñas deben considerarse los siguientes requisitos:

- Exigir el cambio automático, la primera vez que el usuario ingresa al sistema o recurso.
- Exigir el cambio automático, al menos cada cuarenta y cinco (45) días.
- Ser distinta por lo menos de las últimas cinco (5) contraseñas anteriores.
- Permitir ser cambiadas toda vez que el usuario lo requiera.
- Para aquellos equipos de procesamientos que contienen información confidencial del Servicio, incluyendo servidores y estaciones de trabajo, se deben establecer contraseñas de BOOT o Encendido (aquella que aparece cuando recién se prende el computador o servidor). ***Las contraseñas de encendido deben guardarse en sobre cerrado bajo la responsabilidad del Jefe de Área correspondiente.***

3.3 Bloqueo de cuentas

Toda cuenta de usuario que haya intentado el acceso al sistema en forma fallida y consecutiva 3 veces, debe ser automáticamente bloqueada. La misma sólo debe ser reconectada, por el Administrador de Sistemas correspondiente. Para las cuentas especiales de mayor riesgo, la reconexión debe ser documentada por el Administrador de Sistemas y comunicada a la Unidad de Tecnología, Información y Comunicaciones.

Toda cuenta de usuario que no haya accedido al sistema por 60 días corridos debe bloquearse y se deben iniciar los procesos de autorización necesarios para darla de baja definitivamente.

Se debe bloquear la cuenta de usuario durante los permisos o ausencias que excedan de 15 días corridos. Para ello el usuario o su respectivo Jefe directo deberán informar, a través de un mail a la Unidad de Tecnología, Información y Comunicaciones, las fechas durante las cuales se producirá la ausencia.

El bloqueo deberá permanecer hasta la fecha que se indique en la comunicación para el usuario responsable de la misma, luego de lo cual debe asignársele una nueva contraseña con cambio obligatorio al próximo ingreso.

3.4 Cuenta de Reemplazo de Funciones

Cada vez que un usuario deba reemplazar a otro en sus funciones por un periodo definido, se debe crear una cuenta que identifique al usuario reemplazante y al reemplazado y debe tener una fecha de expiración definida desde su creación. Por otra parte la cuenta reemplazada debe bloquearse siguiendo lo descrito en el punto 3.3 de esta norma. La Unidad de Tecnología, Información y Comunicaciones creará la cuenta de reemplazo sobre la base de un documento que respalde dicha operación, esto es un memorando de reemplazo.

3.5 Registro de eventos en el sistema

Se debe implementar, en el sistema de control de accesos, el registro automático de todos los eventos relacionados con la seguridad, de acuerdo a lo estipulado por la “*Norma de Monitoreo y Manejo de Incidentes de Seguridad”* y específicamente para las cuentas de acceso de mayor riesgo.

3.6 Pantalla inicial de acceso a los equipos

Se debe implementar, de manera automática en el sistema, un mensaje al momento de ingresar el usuario al equipo de procesamiento. El mensaje debe manifestar que los sistemas están disponibles para los propósitos de gestión autorizados por el Servicio en las normas respectivas. El mensaje deberá recordar al usuario el compromiso de responsabilidad y confidencialidad de la respectiva contraseña asignada y de la información a la que accede. Dicho mensaje deberá permanecer en pantalla el tiempo suficiente como para que el usuario pueda leerlo en su totalidad.

3.7 Desconexión

Se debe desconectar toda sesión activa cuando la estación de trabajo no verifique uso durante un tiempo determinado, siempre y cuando se dispongan de las herramientas automáticas necesarias para hacerlo.

3.8 Uso de Carpetas Compartidas

Los usuarios son responsables de la información sensible a la que tienen acceso y deben evitar almacenarla en carpetas compartidas, debido a que cualquier usuario que esté conectado a la red puede tener acceso a dicha carpeta y hacer mal uso de ésta.

En caso de requerir compartir la información con otros usuarios, corresponderá aplicar controles de acceso a las carpetas definiendo las cuentas de usuarios con permiso de acceso, y proteger los archivos a ser compartidos con contraseña. Sólo deben compartir la contraseña con aquellos usuarios que requieren acceder a la información.

3.9 Compromiso de Confidencialidad

Todo usuario o funcionario, al momento de recibir una cuenta de usuario y contraseña, deberá firmar un compromiso de confidencialidad que incluya a lo menos el siguiente texto:

Como parte integrante del Servicio de Gobierno Regional, declaro que conozco toda la normativa del Servicio en relación a la Seguridad de la Información en los equipos informáticos a los que tengo acceso y me comprometo a:

- *No divulgar cualquier información obtenida de los sistemas aplicativos ni utilizarla para cualquier fin contrario a los intereses del Servicio.*
- *No revelar ni compartir las contraseñas otorgadas para mi cuenta de usuario.*
- *Aceptar las responsabilidades sobre el uso de mi cuenta de usuario.*
- *Conservar toda información en los equipos centralizados de procesamiento de datos del Servicio. Soy enteramente responsable en cuanto al resguardo y protección de la información guardada en mi estación de trabajo.*
- *Modificar la contraseña al momento que me fuera entregada por primera vez y cada vez que la misma sea restituida por el Administrador de Sistemas.*

3.10 Pantalla inicial de acceso a los equipos

Leyenda que debe aparecer al iniciar una conexión:

ATENCIÓN:

“Todos los sistemas están habilitados para uso en la gestión del negocio del Servicio de Gobierno Regional y regulados por políticas del mismo.
Por requerimientos de Seguridad, las actividad del sistema están sujetas a monitoreo, resguardando los derechos de confidencialidad de las comunicaciones personales.
Se recuerda el compromiso de responsabilidad y confidencialidad de sus claves y de la información a la que accede.”

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Gestión de Incidentes en la Seguridad de la Información

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1. Introducción

1.1 Objetivos

- La presente norma tiene como objetivos:
  - Establecer procedimientos operativos para gestionar las debilidades y problemas de seguridad.
  - Reducir los daños ocasionados por incidentes de seguridad y mal funcionamiento.

1.2 Alcances y Limitaciones

- Esta norma se aplica a todos los usuarios de Activos de Información del Servicio de Gobierno Regional de Magallanes y Antártica Chilena.

1.3 Vigencia

Esta Norma de Gestión de Incidentes en la Seguridad de la Información entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2. Aspectos Generales

Se deben establecer responsabilidades y procedimientos formales para el reporte, respuesta y análisis posterior de los incidentes de seguridad.

Todos los incidentes que puedan afectar la seguridad de la información, deben ser informados inmediatamente al Encargado de Seguridad para que se tomen las medidas correspondientes.

Siempre que se sospeche de una intrusión en un computador, éste debe ser desconectado inmediatamente de la red.

Todo el personal que trabaje en la operación de sistemas debe poseer documentación y estar capacitado en procedimientos que especifiquen claramente cómo debe ser manejada la seguridad de la información cuando ocurran incidentes.

Siempre que se sospeche de un acceso no autorizado a un sistema o se tenga la certeza de que está ocurriendo, el personal debe reportarlo inmediatamente al Encargado de Seguridad, para que personal capacitado pueda tomar las acciones correspondientes.

Se deben definir los responsables del manejo de los incidentes en los sistemas de información, además se les debe conceder la autoridad para llevar a cabo esta labor.

Se deberán enviar reportes periódicos de incidentes de seguridad al comité de seguridad del Servicio.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Adquisición, Desarrollo y Mantenimiento en los Sistemas de Información

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1. Introducción

1.1 Objetivos

- La presente norma tiene como objetivo:
  - Asegurar una adecuada protección en el diseño, desarrollo, mantención y adquisición de los programas de aplicación del Servicio que se utilizan para apoyar las funciones críticas del mismo.

1.2 Alcances y Limitaciones

- Esta norma se aplica a todas las acciones asociadas al desarrollo, mantención y adquisición de software que apoyan las funciones críticas del Servicio.

1.3 Vigencia

Esta Norma de Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2. Aspectos Generales

El Servicio debe velar porque el aspecto de seguridad esté incorporado en los sistemas de información, esto incluye la infraestructura y las aplicaciones. Los requisitos de seguridad deben ser identificados y acordados antes del desarrollo de los sistemas de información.

Se deben establecer los requisitos para los nuevos sistemas de información especificando de manera formal, los requerimientos de controles de seguridad.

Se deben prevenir pérdidas, modificaciones o mal uso de los datos de usuarios en las aplicaciones de los sistemas, utilizando controles y seguimientos de auditorías o registros de actividad.

Durante la etapa de desarrollo de los sistemas se debe evaluar la necesidad incorporar controles criptográficos que protejan la confidencialidad e integridad de la información que se considere en riesgo.

Se deben tomar acciones para asegurar que todo el software desarrollado y las actividades de mantenimiento de software cumplen con las políticas, estándares y procedimientos definidos en el Servicio.

Se debe controlar el acceso a archivos de sistemas y a códigos fuentes de programas.

Se deben establecer procedimientos para proteger los datos de prueba de los sistemas.

El Servicio debe definir procedimientos que controlen y definan la instalación de software operacional en los sistemas.

El Servicio debe procurar que la integridad del software que se encuentra en producción no se vea afectada por el proceso de desarrollo y mantención de sistemas, manteniendo un apropiado nivel de seguridad.

El Servicio debe establecer estándares para las metodologías de desarrollo y para los lenguajes de programación, los que podrán ser diversos.

Los cambios en los sistemas deben ser controlados por un procedimiento formal de control de cambios.

Todos los proyectos de desarrollo de sistemas realizados con personal interno o solicitados a terceros, deben ser programados con los lenguajes aprobados y definidos en los estándares de programación del Servicio.

Durante el desarrollo de los sistemas se deben establecer controles y procedimientos de seguridad para validar toda la información sensible procesada por los sistemas de información del Servicio.

Sobre el desarrollo de software a través de outsourcing se deben definir responsabilidades de supervisión y monitoreo por el Servicio o por órganos de control.

Los requerimientos de software y hardware se deben realizar a través de la Unidad de Tecnología, Información y Comunicaciones.

El responsable de sistemas, debe planificar y organizar la utilización de los recursos, para un uso eficiente y responsable, alineándolos con los requerimientos del Servicio.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Gestión de la Continuidad del Negocio

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1. Introducción

1.1 Objetivos

- La presente norma tiene como objetivos:
  - Mantener la integridad y la disponibilidad de los activos de información o minimizar su pérdida en el caso de falla de sistemas, desastre o suceda algún otro hecho que resulte en la pérdida de datos.
  - Establecer medidas que mitiguen las interrupciones de las actividades del Servicio debido a los efectos de fallas o desastres.

1.2 Alcances y Limitaciones

- Esta política se aplica a todo los procesos de negocio que involucran información sensible del Servicio.

1.3 Vigencia

Esta Norma de Gestión de Continuidad del Negocio entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2. Aspectos Generales

El Servicio preparará, actualizará y probará periódicamente los planes de recuperación que provean las acciones alternativas que los funcionarios utilizarán para mantener la continuidad de las operaciones en el caso de que se produzca una interrupción de las actividades regulares consideradas críticas. Esto debe ser coordinado con los planes de continuidad existentes.

La gestión de la seguridad debe incluir controles que permitan identificar y disminuir los riesgos, además de limitar las consecuencias de daños de incidentes.

Se debe considerar la contratación de seguros que formen parte del proceso de continuidad.

Se deben manejar estándares para desarrollar, mantener y documentar los planes de continuidad del negocio y los planes de contingencia tecnológica.

El Servicio revisará y preparará periódicamente una evaluación del grado de criticidad de todos los sistemas multiusuario.

Se debe preparar un plan de recuperación, el que debe ser actualizado periódicamente y especificar las facilidades que les serán proporcionadas a los funcionarios de manera que puedan continuar con sus labores en el evento de una interrupción.

El Servicio documentará los planes de continuidad y de sistemas.

Cada plan de continuidad debe especificar las condiciones para su activación y las responsabilidades para cada uno de sus componentes. La responsabilidad de activación del plan de continuidad recae en el Encargado de Seguridad.

Después de que se haya realizado un análisis de riesgo, se debe efectuar un análisis que especifique el período máximo por el que el Servicio puede continuar con sus actividades sin el funcionamiento de los servicios críticos, según esto debe evaluar las acciones a seguir.

Los planes de contingencia y de los sistemas de información deben ser accesibles en todo momento y estar disponibles tanto en el sitio principal como el de contingencia.

Se deben probar y actualizar anualmente los planes y procesos de contingencia.

Si las actividades financieras críticas del Servicio pueden ser realizadas de forma manual, se debe establecer un plan de contingencia adicional considerando esta alternativa, y que sea permanentemente actualizado.

Periódicamente el personal responsable de la seguridad de la información debe verificar la disponibilidad de los números de teléfonos de los funcionarios involucrados en la ejecución de las actividades de recuperación en contingencia, de los proveedores de servicios y entidades afectadas.

Se deben revisar y actualizar al menos anualmente los roles y responsabilidades de los planes de contingencia y de recuperación.

SERVICIO DE GOBIERNO REGIONAL DE MAGALLANES Y ANTARTICA CHILENA

Norma de Cumplimiento

Historia de Revisiones					
Rev.	Descripción del Cambio	Realizado Por	Visado Por	Aprobado por	Vigencia Desde
0	Versión Inicial	Encargado de Seguridad	Comité de Seguridad de la Información	Intendente Regional	30/05/2011
1.0	Versión Modificada	Unidad Fortalecimiento Institucional	Encargado de Seguridad de la Información Comité de Seguridad de la Información	Intendente Regional RES.EX.(GR) N° 132 del 30-08-2011	01/09/2011

.

Contenido

1. Introducción

1.1 Objetivos

La presente política tiene como objetivos:

- Consolidar la seguridad de la información dentro del Servicio, a través de mecanismos de administración por parte de las áreas, grupos e individuos asignados a cada función.
- Definir en forma clara las responsabilidades de cada funcionario en el contexto de la seguridad de la información.

1.2 Alcances y Limitaciones

Esta política se aplica a todos quienes trabajen en el Servicio de Gobierno Regional de Magallanes y Antártica Chilena, cualquiera sea su calidad contractual, incluyendo a personal perteneciente a terceras empresas, sean éstas Públicas y/o Privadas, y que no necesariamente presten servicios directamente relacionados con el Servicio.

Incluye todos los activos de información que el Servicio posea en la actualidad o en el futuro, de manera que la no mención explícita en la presente política no es argumento suficiente para no proteger activos de información que se encuentren en otras formas. La política cubre toda la información impresa o escrita en papel, almacenada electrónicamente, trasmitida por correo o usando medios electrónicos, mostrada en videos o registros de audio de una conversación.

La presente política adopta su base de contenidos, a partir de las buenas prácticas definidas en la norma NCH-ISO27001 y de los requisitos legales, normativos y contractuales relativos a la seguridad de la información, que sean aplicables a la organización, como el Decreto Supremo 83 de fecha 03 de junio de 2004 del Ministerio Secretaría General de la Presidencia, que aprueba Norma Técnica para los órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.

1.3 Vigencia

Esta Norma de Cumplimiento entrará en vigencia a partir del **01 de septiembre de 2011.**

1.4 Responsables

Todos los funcionarios del Servicio de Gobierno Regional de Magallanes y Antártica Chilena son responsables del cumplimiento de esta norma.

1.5 Documentos Relacionados

- Política de Seguridad del Servicio
- Todas las Normas de la Política General de Seguridad de la Información

2. Aspectos Generales

El Servicio de Gobierno Regional de Magallanes y Antártica Chilena debe conformar un equipo de trabajo ejecutivo para gestionar, evaluar y resolver sobre materias relacionadas a la Seguridad de la Información, el que se denominará “Comité de Seguridad de la Información”. Este Comité podrá estar incorporado en algún otro comité que tenga el mismo nivel de resolución.

Se crea el rol de “Encargado de Seguridad de la Información”, quien debe promover, evaluar y fiscalizar las medidas de seguridad aprobadas por la Primera Autoridad Regional.

El rol del Encargado de Seguridad podrá ser asumido por una persona jerárquicamente independiente de las unidades organizacionales existentes o podrá ser asignado a alguna persona que no comprometa éticamente las funciones que desempeña.

El Comité de Seguridad de la Información debe reunirse al menos cada tres meses para revisar el estado de la seguridad de la información del Servicio, aprobar y revisar los proyectos de seguridad de la información, aceptar nuevas políticas o modificaciones a las existentes.

El Servicio, a través del Encargado de Seguridad, debe establecer medidas de seguridad para prevenir, detectar y responder oportunamente ante posibles daños a la Seguridad de la Información.

El Encargado de Seguridad debe establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos en forma periódica.

La Primera Autoridad Regional debe definir el nivel de riesgo aceptable para los riesgos que se identifiquen y deberá determinar las acciones a tomar para gestionarlo, a través de alguna de las siguientes alternativas:

- Evitarlo: Cambiando la manera de operar.
- Mitigarlo: Reducir su probabilidad de ocurrencia o las consecuencias: a través de controles apropiados.
- Transferirlo: A otra instancia, como un tercero o seguros.
- Retenerlo: Aceptar el riesgo y vivir con él.

El Encargado de Seguridad debe preocuparse de que exista claridad y formalidad respecto de los Propietarios de la Información, como por ejemplo, quién es el responsable de la base de datos, archivos principales y cualquier recopilación de información.

Cualquier cambio en el estado contractual del personal debe ser comunicado inmediatamente por el área responsable a los administradores de sistemas. Encargado de seguridad y personal de seguridad física, para que puedan implementar las restricciones de acceso a la información que correspondan.

Política de Seguridad de la Información

El Servicio de Gobierno Regional de Magallanes y Antártica Chilena reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente los valores generales de seguridad de la información que deben permanecer a través del tiempo para el cumplimiento por parte de todos los funcionarios, sea cual fuere su calidad jurídica.

Dichos valores son:

- ***Integridad y Exactitud***

  Toda la información y todas las transacciones deben encontrarse libre de errores y/o irregularidades de cualquier índole.

- ***Legalidad***

  Toda la información y los medios o elementos que la contienen, procesen y/o transporten, deben cumplir con las reglamentaciones legales vigentes.

- ***Autorización***

  Toda la información debe cumplir con los niveles de autorización correspondientes para su utilización, ejecución y divulgación, y que todas las transacciones de los procesos administrativos tengan las correspondientes autorizaciones para su ejecución.

- ***Disponibilidad***

  La información y la capacidad de su procesamiento deben ser resguardados y poder recuperarse de forma rápida y completa ante cualquier hecho contingente que interrumpa la operatoria o dañe las instalaciones, medios de almacenamiento y /o equipo de procesamiento.

- ***Confidencialidad***

  Toda la información (física y electrónica) y sus medios de procesamiento y/o conservación deben estar protegidos del uso no autorizado o revelaciones accidentales, errores, fraudes, sabotaje, espionaje, violación de la privacidad y otras acciones que pudieran perjudicarla.

- ***Salvaguarda Física***

  Todos los medios de procesamiento y/o conservación de información deben contar con medidas de protección física que eviten el acceso y/o utilización indebida por personas no autorizadas. La información debe ser mantenida de manera tal que se asegure su conservación.

- ***Propiedad***

  Todos los derechos de propiedad sobre la información deben estar adecuadamente establecidos.

REVISADO POR	VISADO POR	APROBADO POR
Javier Manuelquen Muñoz Encargado de Seguridad de la Información	Luis [illegible] Martínez Representante Comité de Seguridad de la Información.	Arturo Storaker Molina INTENDENTE REGIONAL RES.EX.(GR) 132 del 30-08-2011

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE, Arturo Storaker Molina, Intendente Región de Magallanes y Antártica Chilena, Ruth Bravo Rodríguez, Asesor Jurídico Servicio de Gobierno Regional.

Lo que transcribo a Ud. para su conocimiento.

SERVICIO GOBIERNO REGIONAL MAGALLANES Y ANTÁRTICA CHILENA

RUTH BRAVO RODRIGUEZ
ASESOR JURÍDICO
SERVICIO GOBIERNO REGIONAL

LSM/lsg

DISTRIBUCIÓN:

1. Gabinete Intendencia Regional de Magallanes y Antártica Chilena.
2. Jefe División Administración y Finanzas.
3. Jefe División de Análisis y Control de Gestión.
4. Jefe División de Desarrollo Regional.
5. Encargado de Seguridad de la Información.
6. Jefe Unidad de Auditoría Interna.
7. Asesor Jurídico.
8. Funcionarios Servicio Gobierno Regional.
9. Archivo.