ARICA Y PARINACOTA
GOBIERNO REGIONAL

APRUEBA INSTRUCTIVO DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN DEL GOBIERNO REGIONAL DE ARICA Y PARINACOTA.

RESOLUCIÓN EXENTA Nº 2331 **/2011**

ARICA, 30 DIC 2011

VISTO: La Resolución Exenta Nº233 de fecha 21 de febrero de 2011 que designa funcionarios responsables del Programa de Mejoramiento de Gestión año 2011; La Resolución Exenta N° 427 de fecha 28 de marzo de 2011 que aprueba Políticas de Seguridad de la Información; Las leyes Números 19.553, 19.882 y 20.212; el Decreto Supremo Número 475 del 6 de mayo de 1998, del Ministerio de Hacienda; el Decreto con Fuerza de Ley Nº29, de 2004, que fija el texto refundido, coordinado y sistematizado de la Ley Nº18.834, sobre Estatuto Administrativo; el Decreto con Fuerza de Ley Nº1, de 2005, que fija el texto refundido, coordinado y sistematizado de la Ley Nº18.757, Orgánica Constitucional de Bases Generales de Administración del Estado; el Decreto con Fuerza de Ley Nº1, de 2005, que fija el texto refundido, coordinado, sistematizado y actualizado de la Ley Nº19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; el Decreto Ley Nº573, de 1974, sobre Estatuto de Gobierno y Administración Interiores del Estado; Ley Nº20.175, que crea la Región XV de Arica y Parinacota y Provincia del Tamarugal, en la Región de Tarapacá; la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; el Decreto Supremo Nº258, del 11 de Marzo de 2010, del Presidente de la República, sobre nombramiento de Intendente Titular en la Región de Arica y Parinacota; lo dispuesto en la Resolución Nº1600, de 2008, que fija el texto refundido, coordinado y sistematizado de la Resolución Nº55, de 992, de la Contraloría General de la República, que establece normas sobre exención de trámite de toma de razón; Ley Nº20.481, de 2010, que establece los Presupuestos del Sector Publico del año 2011; y las facultades que envisto como Intendente del Gobierno Regional de Arica y Parinacota.

CONSIDERANDO:

1. La necesidad de establecer procedimientos de control interno en el Servicio que permitan definir limites de seguridad, resguardar los activos entre ellos la información y contribuir al logro de los objetivos estratégicos del Gobierno Regional de Arica y Parinacota
2. La necesidad de dar cumplimiento al Sistema de Seguridad de la Información 2011 en su fase de implementación.

RESUELVO:

1.- APRUÉBASE el instructivo de activos de la información, del Programa de Mejoramiento de la Gestión, del Gobierno Regional de Arica

y Parinacota, la que se llevará a efecto conforme a lo dispuesto en el presente instrumento, el cual se entiende parte integrante de la presente Resolución.

2.- En cumplimiento de lo señalado en el Artículo 6 de la Resolución N° 1600 de 2008, de la Contraloría General De La República, se insertan los citados Anexos, que por medio de este acto se aprueban, cuyo texto, es el siguiente:

INSTRUCTIVO
INVENTARIO DE ACTIVOS DE LA INFORMACIÓN
GOBIERNO REGIONAL DE ARICA Y PARINACOTA

División de Planificación y Desarrollo Regional

Diciembre de 2011

I.- Resumen Ejecutivo

En el marco del proceso de Modernización del Estado, el cual tiene como objetivo central realizar las adecuaciones necesarias, tanto en la estructura institucional del aparato estatal, como en la manera en que estas instituciones "hacen las cosas", aumentando la eficacia y eficiencia en sus funciones de modo de servir mejor a la ciudadanía.

En este contexto, en el año 1998, con la implementación de la ley Nº 19.553, se inició el desarrollo de Programas de Mejoramiento de la Gestión (PMG) en los servicios públicos, asociando el cumplimiento de objetivos de gestión a un incentivo en las remuneraciones de los funcionarios.

A partir del año 2010, el PMG incluye al sistema de **"Seguridad de la Información"**, dentro del área de Calidad de Atención a Usuarios, cuya asistencia y validación están a cargo de la Subsecretaría del Interior y la Dirección de Presupuestos.

La información es un bien que, como otros bienes de la organización, tiene gran valor y necesita ser protegida en forma apropiada. La Seguridad de la Información protege a dicha información de una gran gama de amenazas con el fin de asegurar la continuidad de las operaciones, minimizar el daño de la institución y maximizar la eficiencia y las oportunidades de mejora de la gestión de la organización.

Esta puede existir de muchas formas, pudiendo ser:

- Impresa o escrita en papel
- Almacenada electrónicamente
- Transmitida por correo o medios electrónicos
- Mostrada en películas o en una conversación

Cualquier forma que tome la información, los dispositivos a través de los cuales es compartida y almacenada, siempre debe estar protegida en forma adecuada.

La Seguridad de la Información se logra mediante la implementación de un adecuado conjunto de controles, que pueden traducirse en políticas, procedimientos, prácticas, estructuras organizacionales y funciones de software. Se necesita establecer estos controles para asegurar que se cumplan los objetivos específicos de seguridad de la organización.

Bajo estos alcances, el presente instructivo es una guía que tiene por objetivo brindar orientación y apoyo para inventariar la seguridad de la información del Gobierno Regional de Arica y Parinacota.
En este contexto, el instructivo incorpora un análisis de las principales brechas detectadas al interior del Gobierno Regional, así como la identificación y valorización de los activos de información, sus principales procedimientos, clasificación y agrupamiento. De esta forma el Sistema de la Seguridad de la Información permitirá asegurar la calidad, disponibilidad y oportunidad de la información.

II.- Utilidad del Sistema de Seguridad de la Información

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

III.- La Gestión de los Activos de Información

El objetivo de la gestión de los activos es implementar y mantener una apropiada protección de los activos institucionales. Todos los activos deben ser inventariados y contar con un propietario nombrado.

Los propietarios deben identificar todos los activos y deben asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección de los activos.

Adicionalmente se debe asegurar que la información reciba un nivel de protección adecuado. **La información debe ser clasificada para indicar la necesidad, prioridades y grado de protección esperado en su manejo.**

La información puede ser pública o secreta –también se denomina "reservada"- (Ley 20.285), y contar con diferentes grados de importancia dentro de la institución.
Algunos activos pueden requerir un nivel de protección adicional o manejo especial dependiendo de su criticidad y riesgo. Se debe utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales.

IV.- Definición de Activos de Información

Los **Activos de Información** corresponden a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.

De esta forma podemos distinguir 3 niveles básicos de activos de información:

- La Información propiamente tal, en sus múltiples formatos (papel, digital, texto, imagen, audio, video, etc.)
- Los Equipos/Sistemas/infraestructura que soportan esta información
- Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

Dado que los activos de información poseen valor para la organización necesitan, por tanto, ser protegidos adecuadamente para que el "negocio" o la misión institucional no se vean perjudicados. Esto implica identificar riesgos, detectar vulnerabilidades y establecer los controles de seguridad que sean necesarios, tanto a nivel de gobierno institucional y de gestión de procesos, como a nivel de tecnologías de la información utilizadas.

El Sistema de Seguridad de la Información (SSI) establece distintos controles tanto a nivel de gobierno y gestión, como de tecnologías de la información, con el objeto de garantizar que los activos de información cumplan con preservar las siguientes condiciones:

- **La Integridad**: La información está completa, actualizada y es veraz, sin modificaciones inapropiadas o corrupción.
- **La Confidencialidad**: La información está protegida de personas/usuarios no autorizados.
- **La Disponibilidad**: Los usuarios autorizados pueden acceder a las aplicaciones y sistemas cuando lo requieran para utilizar la información apropiadamente al desempeñar sus funciones.

Según el Decreto Supremo N° 83 del 12 de enero de 2005 del Ministerio Secretaría General de la Presidencia (desde ahora en adelante DS-83), la Norma Chilena Oficial NCh-ISO 27001.Of2009 (desde ahora en adelante NCh ISO 27001), como también lo establecido en la Ley N° 20.285, y otras normativas presentes en el SSI del PMG, las exigencias y recomendaciones que se proveen, presentan desafíos en cuanto a la necesidad de garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución de información, por lo que es necesario que cada uno de los órganos del Estado cumpla con estas normativas a través de la implantación de un Sistema de Seguridad de la Información.
En este contexto, el activo esencial es la información que maneja el sistema; o sea los datos, y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos, y los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los soportes de información que son dispositivos de almacenamiento de datos.
- El equipamiento auxiliar que complementa el material informático.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citados.

Activos de la Información

Para facilitar el manejo y mantenimiento del inventario los activos se pueden distinguir diferentes categorías de los mismos:

- **Datos:** Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.

- **Aplicaciones:** El software que se utiliza para la gestión de la información.

- **Personal:** En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general,

todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.

- **Servicios:** Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).

- **Tecnología:** Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.)

- **Instalaciones:** Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.)

- **Equipamiento auxiliar:** En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.) Cada uno de los activos que se identifiquen debe contar con un responsable, que será su propietario. Esta persona se hará cargo de mantener la seguridad del activo, aunque no necesariamente será la que gestione el día a día del mismo.

Los pasos a realizar para la realización del inventario de activos serán:

- Identificación de activos dentro de los grupos definidos
- Relaciones de dependencia
- Valoración

Tipos y Códigos de los Activos:

- [S] Servicios
- [D] Datos / Información
- [SW] Aplicaciones (software)
- [HW] Equipos informáticos o Tecnología (hardware)
- [COM] Redes de comunicaciones
- [SI] Soportes de información
- [AUX] Equipamiento auxiliar
- [L] Instalaciones
- [P] Personal

V.- Valorización de los Activos de Información

Una vez identificados los activos, el siguiente paso a realizar es la valorización, Es decir, hay que estimar qué valor tienen para la organización, cual es su importancia para la misma. Para calcular este valor, se considera cual puede ser el daño que puede suponer para la organización que un activo resulte dañado en cuanto a su disponibilidad, integridad y confidencialidad.

Esta valoración se hará de acuerdo con una escala cualitativa. En este sentido, la escala establece que los rangos de riesgos en caso de pérdida de la información son bajo, medio, alto.

Riesgo de los Activos	Escala de Valorización		
Perdida de los contenidos legales de los datos	Alto	Medio	Bajo
Reducción del rendimiento de la actividad.	Alto	Medio	Bajo
Efecto negativo en la reputación.	Alto	Medio	Bajo
Pérdidas económicas.	Alto	Medio	Bajo
Trastornos en el negocio.	Alto	Medio	Bajo

V.- Cuadro de identificación de los Activos

Tipo de Activo	
Código	
Descripción	
Propietario	
Responsable Directo del Activo	
Utilidad de la Información	
Respaldos Complementarios Existentes	
Valorización	
Riesgo	
Observaciones	

V.I.- Ejemplo de Cuadro de Identificación de los Activos

Tipo de Activo	Datos/Información
Código	D
Descripción	Archivadores con convenios de transferencias FIC-2011
Propietario	Departamento de Desarrollo económico y Social – Unidad FIC / DIPLADE.
Responsable Directo del Activo	Juan Pérez Diaz
Utilidad de la Información	Cada proyecto FIC posee un archivador con el convenio de transferencia de recursos, resolución que lo aprueba, ficha de aprobación de informes técnicos y oficios recibidos y respondidos.
Respaldos Complementarios Existentes	El proyecto posee un respaldo digital en PDF con sus respectivos convenios y resoluciones en el PC del Sr. Juan Pérez D. profesional del Departamento de Desarrollo Económico.
Riesgo del Activo	Perdida de los contenidos legales de los datos.
Valorización	Alto
Observaciones	

Reglamento de Utilización y Resguardo de los Activos de Información

Artículo Primero: De la identificación de los Activos de Información

- Cada Funcionario deberá utilizar el cuadro de identificación de activos adjunto en el presente instructivo, con la finalidad de actualizar en forma permanente los activos de información que posee cada área de responsabilidad o propietario.

Artículo Segundo: Respaldos de los Activos de Información

- Cada activo inventariado deberá contar con una copia en papel y archivo digital, el cual deberá estar debidamente identificado, con la finalidad de contar con los respaldos correspondientes en caso de pérdida, robo u otro incidente que genere menoscabo de los activos inventariados.

Artículo Tercero: de la forma de almacenamiento de los activos de información

- Cada activo identificado e inventariado deberá ser almacenado en áreas seguras dentro del recinto, oficina o área de trabajo, con su correspondiente identificación y correcto almacenamiento.

- Cada activo deberá contener los respectivos códigos de uso, códigos de licitación, códigos BIP u otros que identifique al activo, situación que a su vez debe acompañar el año de ejecución correspondiente y centro de responsabilidad.

- Cada activo debe contar con copia digital, la cual deberá contar con una carpeta en el computador del usuario debidamente identificada.

Artículo Cuarto: de la transmisión de los datos vía correo electrónico

- Todo correo electrónico que sea emitido por los funcionarios del Gobierno Regional, desde la cuenta institucional, deberá identificar claramente el contenido de la información enviada, la firma o identificación del funcionario y en el caso que la información adjunta sea de carácter institucional, legal o de alto contenido técnico deberá ser enviada con copia a la jefatura correspondiente.

Artículo Quinto: Procedimiento de etiquetado de los activos de información

- Cada archivador, correo electrónico, oficios, memos, respaldos en CD, u otros datos de carácter legal y técnico deberán ser etiquetados con logo corporativo del Gobierno Regional, código respectivo del estudio, proyecto o programa e identificar la unidad responsable.

Artículo Sexto: De la Destrucción de los activos de información

- Cada vez que se eliminen datos o información que este respaldada debidamente en formato papel y digital y/o en sus respectivos archivadores o archivos digitales, podrán ser eliminados sólo con la aprobación de la Jefatura correspondiente.

- La información destruida deberá ser depositada en los basureros del área de trabajo. En este sentido, la información eliminada deberá estar en formato

inutilizable, con la finalidad de que no pueda ser alterada, utilizada o leída en su totalidad por terceros.

Artículo Séptimo: de la formalidad en caso de pérdida o rodo de los activos de información.

- En caso de pérdida, robo u otra situación que menoscabe los activos de información inventariados por las áreas de responsabilidad, se deberá informar con un memo interno, en un plazo no superior a los 3 días hábiles al coordinador de Seguridad del Gobierno Regional, con la finalidad de respaldar formalmente dicha situación.

Artículo Octavo: De la distribución del Instructivo

- El presente instructivo deberá ser distribuido en un ejemplar para cada funcionario del Gobierno Regional en el plazo de 7 días hábiles a contar de la fecha de formalización de la resolución exenta que aprueba el instructivo de activos de la información.

ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE

GOBIERNO DE CHILE
INTENDENTE
REGION ARICA Y PARINACOTA

JOSÉ DURANA SEMIR
INTENDENTE
GOBIERNO REGIONAL DE ARICA Y PARINACOTA

MPS/CGM/ASL/asl
DISTRIBUCION:
1. DAF, DACOG, DIPLAN; Funcionarios (sitio web y correo institucional); Oficina de partes; Dpto. Jurídico.