ARICA Y PARINACOTA
GOBIERNO REGIONAL

APRUEBA INSTRUCTIVO DE SEGURIDAD FISICA Y AMBIENTAL DEL GOBIERNO REGIONAL DE ARICA Y PARINACOTA.

RESOLUCIÓN EXENTA Nº 2333 **/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 seguridad física y ambiental en el Servicio que permitan 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 seguridad física y ambiental, 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
SEGURIDAD FÍSICA Y AMBIENTAL
GOBIERNO REGIONAL DE ARICA Y PARINACOTA

PMG SSI

División de Planificación y Desarrollo Regional

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.

Bajo estos alcances, y con la finalidad de resguardar los activos de información del Gobierno Regional, resulta fundamental dotar de las condiciones físicas y ambientales para resguardar los activos de la institución.
Para ello, se ha diseñado el presente instructivo de seguridad física y ambiental, el objetivo de brindar un marco que minimice los riegos de daños e interferencias a la información y a las operacionales del Gobierno Regional. A su vez, pretende evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de procedimientos de seguridad.

Instructivo de Seguridad Física y Ambiental del Gobierno Regional

I.- Artículo Primero: Objetivos y Generalidades de la Seguridad Física y ambiental del Gobierno Regional

La seguridad física y ambiental brinda el marco para minimizar los riesgos de daños e interferencias a la información y a las operaciones del Gobierno Regional. Asimismo, pretende evitar al máximo los incidentes que puedan menoscabar los activos fijos y de información del Gobierno Regional, mediante el establecimiento de perímetros de seguridad.

Para el logro de esto el presente instructivo de seguridad física y ambiental tiene por objetivo:

1. Prevenir e impedir accesos no autorizados, daños e interferencia a las instalaciones e información del Gobierno Regional.

2. Proteger el equipamiento de procesamiento de información crítica del Gobierno Regional ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.

3. Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento que alberga la información del Gobierno Regional.

4. Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

Alcance

El presente instructivo se aplica a todos los recursos físicos relativos a los sistemas de información del Gobierno Regional; instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, u otros activos fijos o de información de propiedad de la institución.

II.- Artículo Segundo: el Perímetro de Seguridad del Gobierno Regional

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

El Gobierno regional utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas.

El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área de seguridad de acuerdo a la evaluación de riesgos efectuada.

Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:

a) Definir y documentar claramente el perímetro de seguridad.

b) Ubicar las instalaciones de procesamiento de información dentro del perímetro de un edificio o área de construcción físicamente sólida (por ejemplo no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción).

c) Verificar la existencia de un área de recepción atendida por personal. Si esto no fuera posible se implementarán los siguientes medios alternativos de control de acceso físico al área o edificio: (indicar otros medios alternativos de control). El acceso a dichas áreas y edificios estará restringido exclusivamente al personal autorizado.

d) Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

e) Extender las barreras físicas necesarias desde el piso (real) hasta el techo (real), a fin de impedir el ingreso no autorizado y la contaminación ambiental, por ejemplo por incendio, humedad e inundación.

f) Identificar claramente todas las puertas de incendio de un perímetro de seguridad. El Responsable de Seguridad llevará un registro actualizado de los sitios protegidos, indicando:

- Identificación del Edificio y Área.
- Principales elementos a proteger.
- Medidas de protección física.

III.- Artículo Tercero: De Los Controles de Acceso Físico

Las áreas protegidas del Gobierno Regional se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad, a fin de permitir el acceso sólo al personal autorizado.

Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a) Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.

Se utilizarán los siguientes controles de autenticación para autorizar y validar todos los accesos: (por ejemplo: personal de guardia con listado de personas habilitadas o por tarjeta magnética o inteligente y número de identificación personal, etc.). Se mantendrá un registro protegido para permitir auditar todos los accesos.

c) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

d) Revisar y actualizar cada los derechos de acceso a las áreas protegidas del Gobierno Regional, los que serán documentados y firmados por el Responsable de la Unidad Organizativa de la que dependa.

e) Revisar los registros de acceso a las áreas protegidas. Esta tarea la realizará la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información.

IV.- Artículo Cuarto: De la Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas, por ejemplo, filtración de agua desde otras instalaciones del Gobierno Regional.

Bajo estos alcances, se establecen las siguientes medidas de protección para áreas protegidas:

a) Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.
b) Establecer que los edificios o sitios donde se realicen actividades de procesamiento de información serán discretos y ofrecerán un señalamiento mínimo de su propósito, sin signos obvios, exteriores o interiores.
c) Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área protegida para evitar solicitudes de acceso, el cual podría comprometer la información.
d) Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia. Se agregará protección externa a las ventanas, en particular las que se encuentran en planta baja o presenten riesgos especiales.
e) Separar las instalaciones de procesamiento de información administradas por el Gobierno Regional de aquellas administradas por terceros.
f) Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.
g) Almacenar los materiales peligrosos o combustibles en los siguientes lugares seguros a una distancia prudencial de las áreas protegidas del Gobierno Regional.

V.- Artículo Quinto: Del Desarrollo de Tareas en Áreas Protegidas

Para incrementar la seguridad de las áreas protegidas, se establecen los siguientes controles y lineamientos adicionales. Esto incluye controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí:

a) Dar a conocer al personal del Gobierno Regional la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.
b) Evitar la ejecución de trabajos por parte de terceros sin supervisión.
c) Bloquear físicamente e inspeccionar periódicamente las áreas protegidas desocupadas.
d) Limitar el acceso al personal del servicio de soporte externo a las áreas protegidas o a las instalaciones de procesamiento de información sensible. Este acceso, como

el de cualquier otra persona ajena que requiera acceder al área protegida, será otorgado solamente cuando sea necesario y se encuentre autorizado y monitoreado. Se mantendrá un registro de todos los accesos de personas ajenas.

e) Pueden requerirse barreras y perímetros adicionales para controlar el acceso físico entre áreas con diferentes requerimientos de seguridad, y que están ubicadas dentro del mismo perímetro de seguridad.
f) Impedir el ingreso de equipos de computación móvil, fotográficos, de vídeo, audio o cualquier otro tipo de equipamiento que registre información, a menos que hayan sido formalmente autorizadas por el Responsable de dicho área o el Responsable del Área de Seguridad.
g) Prohibir beber y fumar dentro de las instalaciones de procesamiento de la información.

VI.- Artículo Sexto: De la Ubicación y Protección del Equipamiento y Copias de Seguridad

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

a) Ubicar el equipamiento en un sitio donde se minimice el acceso innecesario y provea un control de acceso adecuado.
b) Ubicar las instalaciones de procesamiento y almacenamiento de información que manejan datos clasificados, en un sitio que permita la supervisión durante su uso.
c) Aislar los elementos que requieren protección especial para reducir el nivel general de protección requerida.
d) Adoptar controles adecuados para minimizar el riesgo de amenazas potenciales, por: Robo o hurto, Incendio, Explosivos, Humo, Inundaciones o filtraciones de agua (o falta de suministro), Polvo, Vibraciones, Efectos químicos e Interferencia en el suministro de energía eléctrica.
e) Revisar regularmente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones de procesamiento de la información.
f) Considerar asimismo el impacto de las amenazas citadas en el punto d) que tengan lugar en zonas próximas a la sede del Gobierno Regional.

VII.- Artículo Séptimo: Del Mantenimiento de Equipos

El Gobierno Regional Deberá realizar el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática.
b) El Área de Informática mantendrá un listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
c) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
d) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
e) Registrar el retiro de equipamiento de la sede del Organismo para su mantenimiento.
f) Eliminar la información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

VIII.- Artículo Octavo: De la Seguridad de los equipos Fuera de las Instalaciones del Gobierno Regional

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito del Organismo, será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma.

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito del Gobierno Regional para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma. Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. Asimismo, se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Gobierno Regional, cuando sea conveniente.

IX.- Artículo Noveno: De las Políticas de Escritorios y Pantallas Limpias.

Los Funcionarios del Gobierno Regional deberán adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

Para ello, Se aplicarán los siguientes lineamientos:

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

X.- Artículo Decimo: 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:
-DAF, DACOG, DIPLAN; Funcionarios (sitio web y correo institucional); Oficina de partes; Dpto. Jurídico.