ARICA Y PARINACOTA

APRUEBA POLITICA DE SEGURIDAD DEL GOBIERNO REGIONAL

RESOLUCION EXENTA N° 2319

ARICA, 31 DIC 2013

VISTOS:

1. El Memorándum N° 29, de fecha 31 de diciembre de 2013, de la Jefa(s) de la Administración y Finanzas al Departamento Jurídico del Gobierno Regional de Arica y Parinacota.
2. El Decreto con Fuerza de Ley N° 1 de 2000, de la Secretaria General de la Presidencia, que fijó el texto refundido, coordinado y sistematizado de la ley N° 18.575, Orgánica Constitucional de Bases Generales de Administración del Estado; el Decreto con Fuerza de Ley N° 1 de 2005, que fijó el texto refundido, coordinado, sistematizado y actualizado de la ley N° 19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; lo dispuesto en el artículo 61 de la Ley N° 19.880, que establece Bases de los Procedimientos Administrativos que rigen los Actos de los Órganos de la Administración del Estado; el Decreto Ley N° 1.263, de 1975, Orgánico de Administración Financiera del Estado; lo dispuesto en la Resolución N° 1.600, de 2008, de la Contraloría General de la República, que establece normas sobre la exención del trámite de toma de razón; y las facultades que invisto como Intendente(S) del Gobierno Regional de Arica y Parinacota.

CONSIDERANDO:

La petición planteada por la Jefa(S) de la Administración y Finanzas del Gobierno Regional de Arica y Parinacota, señalada en el numeral 1 del presente instrumento.

RESUELVO:

1. **APRUÉBASE** Política de Seguridad de Información del Gobierno Regional de Arica y Parinacota.

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 la Política de Seguridad, que por medio de este acto se aprueban, cuyo texto, es el siguiente:

Gobierno Regional Arica y Parinacota: Política de Seguridad

HISTORIAL DE CAMBIOS

NOMBRE DEL FICHERO	VERSIÓN	RESUMEN DE CAMBIOS PRODUCIDOS	FECHA
GORE - Politica de Seguridad_v01.doc	2.00	Segunda versión.	03/12/2013

CONTROL DE DIFUSIÓN

RESPONSABLE: Encargado de la Unidad Informática, Encargado de Seguridad.

DISTRIBUCION: Gobierno Regional de Arica y Parinacota

INDICE

1 Objeto 2

2 Alcance 2

3 Legislación y Normativas de referencia 3

4 Principios de la Seguridad de la Información 3

5 Objetivos de Seguridad 4

6 Responsabilidad de la Política de Seguridad 4

7 Organización de la Seguridad de la Información 5

7.1 Comité de Seguridad de la Información 5

7.1.1 Funciones del Comité de Seguridad 5

7.2 Composición del Comité de Seguridad 5

7.3 Roles, funciones y responsabilidades en materia de seguridad 6

7.3.1 Encargado de Seguridad de la Información 6

7.3.2 Responsable del Sistema de Información 6

7.3.3 Administradores de los Sistemas 7

7.3.4 Otras responsabilidades 7

7.3.4.1 Responsable de Seguridad Física ..... ¡Error! Marcador no definido.

7.3.4.2 Responsable del Área de Recursos Humanos ..... ¡Error! Marcador no definido.

7.3.4.3 Responsables Legales ..... ¡Error! Marcador no definido.

7.3.4.4 Auditores Internos (o externos) ..... ¡Error! Marcador no definido.

7.4 Organización y funcionamiento ..... ¡Error! Marcador no definido.

8 Obligaciones del personal ..... ¡Error! Marcador no definido.

9 Asesoramiento especializado en materia de seguridad de la información ¡Error! Marcador no definido.

10 Formación y Concienciación ..... ¡Error! Marcador no definido.

11 Estructura de la Documentación de Seguridad ..... ¡Error! Marcador no definido.

12 Revisiones, distribución y cumplimiento ..... ¡Error! Marcador no definido.

13 Aprobación y entrada en vigor ..... ¡Error! Marcador no definido.

1 Objeto

El presente documento define y establece los principios que conforman la Política Seguridad de la Información del Gobierno Regional de Arica y Parinacota, para garantizar en la mejor medida de lo posible la confidencialidad, integridad y disponibilidad de sus sistemas de información, de las comunicaciones y de los servicios con el fin de proporcionar a los ciudadanos y a los propios usuarios del Gobierno Regional, unos servicios fiables, de calidad y de confianza para permitirles el ejercicio de derechos y el cumplimiento legal a través de estos medios.

Establece el compromiso del Gobierno Regional con la seguridad de los Sistemas de Información, definiendo los objetivos y criterios básicos para el tratamiento de la misma, sentando los pilares del marco normativo de seguridad de esta institución y la estructura organizativa y de gestión que velará por su cumplimiento.

2 Alcance

La presente Política es aplicable a toda la información y activos de información del Gobierno Regional que la soportan, incluyendo todas las personas y terceras empresas o instituciones que de una forma u otra acceden a ellos, independientemente de su situación física, dentro o fuera de las instalaciones del organismo. Afecta por tanto, y son de aplicación directa a todos los sistemas, aplicaciones, servicios, información y ubicaciones del Gobierno Regional, incluyendo al personal implicado en su tratamiento.

Se entenderá la Seguridad, como un proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información, quedando excluidas cualquier tipo de actuaciones puntuales o de tratamiento coyuntural.

La Política de Seguridad expuesta en el presente documento sirve de referencia, en ningún momento pretenden ser una política absoluta, pudiendo estar sometida a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad marcados por el Gobierno Regional.

Debe ser conocida y cumplida por todo el personal del Gobierno Regional, independientemente del puesto, cargo y responsabilidad dentro del mismo.

3 Legislación y Normativas de referencia

Se aplicará las leyes y normativas chilenas, en relación con protección de datos personales, propiedad intelectual y uso de herramientas Informáticas, así como las que puedan ir surgiendo en el futuro al respecto.

Esta Política se sitúa dentro del marco legal jurídico definido por las Leyes y Decretos siguientes:

- Ley 19.223: Tipifica figuras penales relativas a la informática.
- Ley 17.336: Sobre propiedad intelectual.
- Ley 19.628. Sobre la protección de la vida privada o protección de datos de carácter personal.
- Ley 19.812: Sobre protección de la vida privada.
- Ley 19.799: Sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.
- Ley 18.168: General de Telecomunicaciones.
- Ley 19.927: Ley contra la Pedofilia.
- DS 77/2004: Aprueba Norma Técnica sobre Eficiencia de la Comunicaciones Electrónicas entre Órganos de la Administración del Estado y entre éstos y los ciudadanos.
- DS 81/2004: Establece las características mínimas obligatorias de interoperabilidad que deben cumplir los documentos electrónicos en su generación, envío, recepción, procesamiento y almacenamiento.
- DS 83/2004: Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad del Documento Electrónico.
- DS 93: Aprueba Norma Técnica para minimizar la recepción de mensajes electrónicos no deseados en las casillas electrónicas de los Órganos de la Administración del Estado y de sus funcionarios.
- DS100/2006: Fija características mínimas obligatorias que deben cumplir los sitios Web de los Órganos de las Administración del Estado.
- Ley 19.880: Bases y Procedimientos Administrativos, se refiere a acceso a la información personal y privacidad.
- Decreto 26/2001: Reglamento sobre el Secreto o Reserva de los Actos y Documentos de la Administración del Estado.
- Norma Chilena de Seguridad NCh 2777 con referencia a los controles de seguridad.

La presente Política de Seguridad queda desarrollada además en Políticas, Normativas o Procedimientos clasificados como de "Uso Interno" e incluso de tipo "Reservados Secreto".

4 Principios de la Seguridad de la Información

Los principios que conforman la **Política de Seguridad de la Información** son:

- La información que posee y trata el Gobierno Regional tiene un valor muy importante para el propio organismo, por lo tanto es primordial protegerla.

- La información debe ser protegida contra accesos y alteraciones no autorizados, manteniéndola confidencial e íntegra en todo momento.

- La información debe estar disponible, permitiendo su acceso autorizado, siempre que sea necesario.

- La Seguridad de la Información es responsabilidad de todos. Todas las personas que tienen acceso a la información del Gobierno Regional deben protegerla, por lo que deben estar adecuadamente formadas y concienciadas

- La Seguridad de la Información no es algo estático, por lo que debe ser constantemente controlada y periódicamente revisada.

- La información relativa a las personas y ciudadanos que trate el Gobierno Regional pertenece a ellos y no a la Administración conforme a la normativa en protección de datos de carácter personal y de la protección de la vida privada.

- Todos aquellos activos (infraestructura, soportes, sistemas comunicaciones, etc.) donde la información reside, viaja o es procesada, deben estar adecuadamente protegidos

- Las medidas de seguridad que se implanten deben estar en proporción a la criticidad de la información que protejan y a los daños o pérdidas que se pueden producir en ella. En todo momento se seguirán, como mínimo, las medias de seguridad impuestas por el DS 83/2004 como Norma Técnica para los Órganos de la Administración del Estado.

- El tratamiento de datos de carácter personal debe estar siempre de acuerdo con las leyes aplicables en cada momento, siendo especialmente importante la Ley 19.628 Sobre Protección de la Vida Privada.

5 Objetivos de Seguridad

El Gobierno Regional define los siguientes **objetivos de seguridad**:

- Proteger los recursos de Información y la tecnología para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad y disponibilidad de los mismos 24 horas al día durante los 365 días del año.
- Minimizar la probabilidad de ocurrencia de incidentes, así como reducir su frecuencia y duración de los mismos, en especial los incidentes a través de Internet y de los Sistemas de Información puestos a disposición de los ciudadanos.
- Mantener la presente Política de Seguridad actualizada, realizando al menos, una revisión anual para confirmar y asegurar su vigencia y nivel de eficacia.
- Incluir, en los planes de formación del personal al servicio del Gobierno Regional acciones formativas y de concienciación relativas a la Seguridad de la Información y a la protección de datos de carácter personal.
- Cumplimiento de la Norma NCh 2777 a través de la implantación de diversos proyectos a corto, medio y largo plazo.

Los Objetivos de Seguridad representan, y se han tenido en cuenta como la base y dirección para el establecimiento de la presente Política de Seguridad de manera que se mantenga alineada con ellos.

6 Responsabilidad de la Política de Seguridad

La responsabilidad general y última de la presente Política de Seguridad recae sobre el Gobierno Regional de Arica y Parinacota.

La Resolución Exenta nº 428/2011 crea un Comité de Seguridad de la Información como responsable de implementar la Política de Seguridad, así como de aplicar sus Políticas de Seguridad individuales para permitir resguardar y contribuir al logro de los objetivos del Gobierno Regional.

7 Organización de la Seguridad de la Información

7.1 Comité de Seguridad de la Información

Para la gestión de la Seguridad de la Información, se crea el Comité de Seguridad de la Información, dentro del ámbito de la presente Política formado por un equipo multidisciplinar que coordinará las actividades y controles de seguridad establecidos en el Gobierno Regional y que vela por el cumplimiento de la normativa vigente, interna y externa, en materia de seguridad.

7.1.1 Funciones del Comité de Seguridad

Son funciones del Comité de Seguridad:

- Supervisar la programación del trabajo y los plazos para el cumplimiento de los objetivos de seguridad.
- Supervisar que se logran los objetivos con la documentación y evidencia que se requiera.
- Aprobar la Política de Seguridad, establecer los criterios de revisión de la misma, revisarla, distribuirla y velar por su cumplimiento
- Promover y respaldar los planes de acción e iniciativas que garanticen la implantación de la Política de Seguridad en todo el Gobierno Regional
- Establecer los requisitos de seguridad que se deben cumplir a nivel organizativo, técnicos y de control de los sistemas y servicios, de su disponibilidad y otros que permitan alcanzar los objetivos de Seguridad identificados
- Garantizar que la seguridad forma parte del proceso de planificación de la gestión de la información y como proceso integral constituido por todos los elementos técnicos, humanos, materiales y organizativos relacionados con los sistemas de información.
- Aprobar los nombramientos de responsables y responsabilidades en materia de Seguridad de la Información
- Valorar el grado de conformidad de los procedimientos implantados en el Gobierno Regional con las normas definidas en la Política, estableciendo planes de mejora para aquellos que requieran de una modificación para su total conformidad
- Aprobar los procedimientos que se definan para dar cumplimiento a las normas y políticas individuales derivadas de la Política de Seguridad
- Acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.
- Verificar que todas las acciones llevadas a cabo en materia de Seguridad sean compatibles o se encuentren respaldadas por la Política de Seguridad
- Promover la realización de auditorías periódicas que permitan verificar el cumplimiento de las obligaciones de las Administraciones en materia de seguridad.
- Mantener contactos periódicos con grupos, otras entidades, organismos, foros, etc. que resulten de interés en el ámbito de la Seguridad de la Información, compartiendo experiencias y conocimiento que ayuden a mejorar y mantener su seguridad
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades de cada área.
- Respaldar los planes estratégicos en materia de seguridad definidos por el Gobierno Regional.
- Valorar y evaluar los recursos necesarios para dar soporte al proceso de planificación e implantación de la seguridad en el Gobierno Regional, priorizando las actuaciones en materia de seguridad cuando los recursos sean limitados
- Los que el Gobierno Regional determine.

7.2 Composición del Comité de Seguridad

Los miembros nominativos que componen el Comité de Seguridad son los funcionarios asignados en la Resolución Exenta Nº 428/2011.

7.3 Roles, funciones y responsabilidades en materia de seguridad

7.3.1 Encargado de Seguridad de la Información

Funcionario nombrado que asume la responsabilidad de que los servicios y sistemas de información del Gobierno Regional se mantengan con el mayor grado de seguridad, atendiendo a los principios de:

- Confidencialidad: la información del Gobierno Regional sólo debe poder ser conocida por las personas autorizadas para ello.
- Integridad: la información asociada a los servicios del Gobierno Regional no debe ser alterada por personas no autorizadas.
- Disponibilidad: garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma siempre que lo requieran.

Sus funciones son:

- Elaborar y supervisar el cumplimiento de la presente Política, y de sus normas, políticas y procedimientos derivados
- Asesorar en materia de seguridad de la información a los integrantes del Gobierno Regional que así lo requieran
- Coordinar la interacción con otros organismos especializados y unidades administrativas en caso de que se incurra en violaciones de la presente Política.
- Tomar conocimiento y supervisar la investigación y monitorización de los incidentes de seguridad
- Establecer las medidas de seguridad, adecuadas y eficaces para cumplir los requisitos de seguridad establecidos por el Gobierno Regional y la normativa vigente.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
- Preparar los temas a tratar en las reuniones del Comité de Seguridad, aportando información puntual para la toma de decisiones
- Responsable de la ejecución directa o delegada de las decisiones del Comité de Seguridad.
- Diseñar la arquitectura y medidas de seguridad, la implantación de herramientas y técnicas, su grado de cumplimiento y ajuste a la presente Política.

En aquellos sistemas de información que por su complejidad, distribución, separación física de sus elementos o números de usuarios se necesitara de personal adicional para llevar a cabo las funciones de Encargado de la Seguridad de la Información, el Encargado de Seguridad podrá designar cuantos Encargados de Seguridad Delegados considere necesarios. Los Encargados de Seguridad Delegados se harán cargo, en su ámbito, de todas aquellas acciones que delegue el Encargado de Seguridad de la Información teniendo dependencias funcionales directas de él.

7.3.2 Responsable del Sistema de Información

Personal designado cuyas responsabilidades son:

- Desarrollo, operación y mantenimiento del Sistema de Información durante todo su ciclo de vida, de sus especificaciones, instalación y verificación de su correcto funcionamiento.
- Garantizar que las medidas de seguridad se integren adecuadamente dentro del marco general de seguridad.
- Elaborar los procedimientos operativos de seguridad de los sistemas de información.
- Elaborar los Planes de Continuidad de los Sistemas de Información

El Responsable del Sistema podrá acordar la suspensión del manejo de determinada información o la prestación de un cierto servicio si es informado de deficiencias graves de seguridad que pudieran afectar a la satisfacción de los requisitos establecidos. Esta decisión deberá ser acordada con los responsables de la información afectada, del servicio afectado y el Encargado de Seguridad antes de ser ejecutada.

En aquellos sistemas que por su complejidad, distribución, separación física de elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Responsable de Sistema, el Gobierno Regional podrá designar cuantos Responsables de Sistemas Delegados considere necesario.

La designación y delegación de funciones en los Responsables de Sistemas Delegados corresponde al Responsable de Sistemas, sin perjuicio de que la responsabilidad final siga recayendo sobre el Responsable del Sistema.

Los Responsables de Sistemas Delegados se harán cargo en su ámbito, de todas aquellas acciones que delegue el Responsable del Sistema relacionadas con la operación, mantenimiento, instalación y verificación del correcto funcionamiento del Sistema de Información, así como también tendrán dependencia funcional directa con el Responsable del Sistema que es a quién reportan.

7.3.3 Administradores de los Sistemas

Persona designada, dependiente del Responsable del Sistemas o del Encargado de Seguridad, cuyas funciones son las siguientes:

- Implementar, gestionar y mantener las medidas de seguridad aplicables al Sistema de Información
- Gestionar, configurar y actualizar, en su caso, el hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información
- Gestionar las autorizaciones concedidas a los usuarios del sistema, en particular, los privilegios concedidos, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado
- Aplicar los Procedimientos Operativos de Seguridad
- Aprobar los cambios en la configuración vigente de los sistemas de información
- Asegurar que los controles de seguridad establecidos son cumplidos estrictamente
- Asegurar que los procedimientos aprobados para manejar los sistemas de información son aplicados
- Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes
- Informar al Encargado de Seguridad de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad y con los sistemas de información
- Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

En el caso de que determinados sistemas de información que por su complejidad, distribución, separación física de sus elementos o número de usuarios se necesite personal adicional para llevar a cabo las funciones de Administrador de Sistemas, se podrán designar Administradores de Sistemas Delegados.

7.3.4 Otras responsabilidades

7.3.4.1 Responsable de Seguridad Física

Personal designado cuyas responsabilidades son implantar las medidas de seguridad relativas a la seguridad física de las instalaciones del Gobierno Regional y dentro de las determinadas por el Encargado de Seguridad, informando a éste de su grado de implantación, eficacia e incidentes.

7.3.4.2 Responsable del Área de Recursos Humanos

Personal designado encargado de notificar a todo el personal que ingrese en el Gobierno Regional de sus obligaciones respecto al cumplimiento de la Política de Seguridad de la Información y de todas las normas y procedimientos que de ella surjan.

7.3.4.3 Responsables Legales

Personal designado encargado de verificar el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos, u otra documentación del Gobierno Regional en lo que se refiere a la Seguridad de la

Información. Informará y notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad de la Información del Gobierno Regional.

7.3.4.4 Auditores Internos (o externos)

Responsables de practicar auditorías periódicas sobre los sistemas de información, debiendo informar de sobre el cumplimiento de las especificaciones y medidas de Seguridad de la Información establecidas en la presente Política y por las normas, procedimientos y prácticas que de ella surjan.

Esta responsabilidad podrá ser delegada puntualmente a personal ajeno al Gobierno Regional.

7.4 Organización y funcionamiento

El Comité de Seguridad se reunirá con carácter ordinario, al menos una vez cada tres meses, pudiéndose reunir de manera extraordinaria, por razones de urgencia y causa justificada, en periodos inferiores.

De toda documentación de funcionamiento del Comité de Seguridad quedará constancia en registro electrónico.

8 Obligaciones del personal

Todos los miembros del Gobierno Regional tiene la obligación de conocer y cumplir la presente Política de Seguridad, las normativas, políticas y procedimientos derivados de la misma, siendo responsabilidad del Comité de Seguridad disponer de los medios necesarios para que la información llegue a los afectados.

9 Asesoramiento especializado en materia de seguridad de la información

El Encargado de Seguridad de la Información será el encargado de coordinar los conocimientos y las experiencias disponibles en el Gobierno Regional con el fin de proporcionar ayuda en la toma de decisiones en materia de seguridad, pudiendo obtener asesoramiento de otros organismos.

10 Formación y Concienciación

El objetivo es lograr la plena conciencia respecto a que la Seguridad de la Información afecta a todos los miembros del Gobierno Regional y a todas las actividades llevadas a cabo en él. A estos efectos, el Gobierno Regional propondrá y organizará sesiones formativas y de concienciación para que todas las personas que intervienen en el proceso y sus responsables jerárquicos tengan una sensibilidad hacia los riesgos que se corren.

11 Estructura de la Documentación de Seguridad

La documentación relativa a la Seguridad de la Información estará clasificada en cuatro niveles de manera que cada documento de un nivel se fundamenta en los de nivel superior.

Los niveles de documentación que se establecen son:

- Primer nivel: **Política de Seguridad de la Información**
  De obligado cumplimiento
  La responsabilidad de aprobación será competencia del Comité de Seguridad.
  Se trata de un documento de tipo "Público".
- Segundo nivel: **Normativas, Políticas y Procedimientos de Seguridad**
  De obligado cumplimiento de acuerdo al ámbito organizativo, técnico o legal correspondiente.

La responsabilidad de aprobación de los documentos redactados en este nivel será competencia del Encargado de Seguridad bajo la supervisión del Comité de Seguridad.
Se trata de documentos de tipo "Uso Interno".

- Tercer nivel: **Procedimientos Técnicos y Operativos de Seguridad**.
  Procedimientos técnicos orientados a resolver las tareas, consideradas críticas por el perjuicio que causaría una actuación inadecuada, de seguridad, desarrollo, mantenimiento y explotación de los sistemas de información.
  La responsabilidad de aprobación de estos procedimientos técnicos es responsabilidad de los Responsables de los Sistemas de Información correspondiente, bajo la supervisión del Encargado de Seguridad. En caso de que los procedimientos afectaran a varios sistemas de información será responsabilidad del Encargado de Seguridad el aprobarlo.
  Se trata de documentos de tipo "Reservado Secreto".
- Cuarto nivel: **Informes, registros y evidencias electrónicas**.
  Informes técnicos: documentos de carácter técnico que recogen el resultado y las conclusiones de un estudio o una evaluación.
  Registros de actividad o alertas de seguridad: documentos de carácter técnico que recogen amenazas y vulnerabilidades de los sistemas de información.
  Evidencias electrónicas: generadas durante toda la fase del ciclo de vida del sistema de información.
  La responsabilidad de que existan este tipo de documentos es de cada uno de los Responsables de los Sistemas de Información en su ámbito.
  Se trata de documentos de tipo "Reservado Secreto".

12 Revisiones, distribución y cumplimiento

El Comité de Seguridad velará por la revisión, distribución y cumplimiento de la presente Política de Seguridad.

La revisión de la Política, de las políticas, normas y procedimientos derivados de ella se realizará al menos una vez al año, así como cada vez que ocurran cambios significativos en los elementos del Sistema de Información que puedan afectarle directa o indirectamente, distribuyéndose a todo el personal afectado.

La versión más actualizada de la Política de Seguridad, sus políticas, normativas y procedimientos asociados y derivados de ella se publicarán en la Intranet del Gobierno Regional.

13 Aprobación y entrada en vigor

La presente Política de Seguridad queda propuesta por el Comité de Seguridad y aprobada por Resolución Exenta del año 2013, y hasta que sea reemplazada por una nueva Política de Seguridad.

ANOTESE, COMUNIQUESE Y PUBLIQUESE EN LA PAGINA WEB DEL SERVICIO.

PATRICIO LOPEZ BERRIOS
INTENDENTE(S)
GOBIERNO REGIONAL DE ARICA Y PARINACOTA

MPS/jmg
DISTRIBUCION:
1. DAF.
2. Unidad Informática
3. Oficina de partes.
4. Dpto. Jurídico.