

ARICA Y PARINACOTA  
GOBIERNO REGIONAL

DEJA SIN EFECTO RESOLUCION EXENTA QUE  
INDICA, Y APRUEBA POLITICAS DE SEGURIDAD  
2011-2012, PROGRAMA MEJORAMIENTO DE  
GESTIÓN

RESOLUCION EXENTA Nº 1959

ARICA, 30 NOV 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 Nº 427 de fecha 28 de marzo de 2011 que aprueba las políticas de seguridad 2011-2012, del Programa de Mejoramiento de Gestión; 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 Nº 1, 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; la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; Ley Nº 20.481, de 2010, que establece los Presupuestos del Sector Público del año 2011; lo dispuesto en la Resolución Nº1600, de 2008, que establece normas sobre exención de trámite de Toma de Razón; y las facultades que envisto como Intendente (S) del Gobierno Regional de Arica y Parinacota.

**CONSIDERANDO:**

La necesidad de definir políticas en el Servicio que permitan resguardar y contribuir al logro de los objetivos estratégicos del Gobierno Regional de Arica y Parinacota

**RESUELVO:**

1. **DEJESE SIN EFECTO**, la Resolución Exenta Nº 427 de fecha 28 de marzo de 2011 que aprueba las Políticas de Seguridad 2011-2012, del Programa de Mejoramiento de Gestión, del Gobierno Regional de Arica y Parinacota.
2. **Apruébese** las Políticas de Seguridad 2011-2012, del Programa de Mejoramiento de 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.
3. En cumplimiento a lo dispuesto en el artículo 6, inciso segundo, de la Resolución Nº 1.600, de 2008, de la Contraloría General de la República, se inserta el convenio mandato aprobado, que es del siguiente tenor:

**"POLITICA DE SEGURIDAD 2011 – 2012, GOBIERNO REGIONAL DE ARICA Y PARINACOTA**

**1. ASPECTOS GENERALES.**

Los computadores y la red proporcionan accesos y recursos, dentro del ámbito del Gobierno Regional de Arica y Parinacota y permiten la comunicación con usuarios en todo el mundo. Este privilegio acarrea responsabilidades a los usuarios, que deberán respetar los derechos de los otros usuarios, la integridad del sistema y de los recursos físicos, así como respetar las leyes y regulaciones vigentes.

Los motivos para la redacción de esta política, son los siguientes:

### **1.1. Necesidad.**

Los usuarios de los recursos informáticos, de a red del Gobierno Regional son responsables de no abusar de los recursos y de mantener el respeto a los derechos de los otros usuarios. Esta política aporta una serie de recomendaciones y líneas de actuación para formalizar el uso correcto de los sistemas de información y comunicación y la aplicación de buenas prácticas.

### **1.2. Objetivos de la Política.**

- Identificar amenazas a la información que permite continuidad de las acciones del negocio y tomar acciones mitigantes sobre ellas.
- Formular procedimientos de control y resguardo de los recursos físicos e informáticos del Servicio
- Asegurar la infraestructura informática para que facilite la realización de las acciones básicas del Servicio.
- Definir procedimientos de acceso, respaldo, copiar y compartir información entre usuarios de la red.
- Difundir los derechos de privacidad o protección de la propiedad intelectual.
- Definir las responsabilidades que supone el uso de los recursos y de las consecuencias de su abuso
- Definir un Plan de Comunicación que permita difundir los alcances y buenas prácticas asociadas a la seguridad de la información institucional.
- Definir los responsables de los activos de información y los mecanismos de auditoría y control.

Elaborar los procedimientos asociados al Sistema Unificado de Gestión de la Calidad.

### **1.3. Resumen.**

Los usuarios del Gobierno Regional de Arica y Parinacota que utilizan la infraestructura TIC (Tecnologías de la Información y Comunicación), deberán respetar la integridad de los recursos basados en los sistemas de información; evitar actividades destinadas a obtener accesos no autorizados o suplantación de identidad. Deberán respetar los derechos de los otros usuarios. No acaparar en exceso los recursos compartidos con otros usuarios y respetar las políticas de licencias de software. Esta política se deberá aplicar a la red, los equipos conectados a ella y a toda la información contenida en los equipos.

## **2. ÁMBITO DE LA APLICACIÓN.**

### **2.1. Agentes a los que se aplica esta política.**

Se deberá aplicar a todos los usuarios de la red del Servicio y que hagan utilización de los recursos expuestos en el siguiente apartado. Es importante consignar, que se aplicará también a cualquier otra entidad externa que utilice los recursos informáticos del Gobierno Regional.

### **2.2. Recursos a los que se refiere esta política.**

Son todos aquellos sistemas de información, sean éstos individuales o compartidos, y estén o no conectados a nuestra red. Se aplicará a todos os equipos (estaciones de trabajo, Notebooks, Netbooks, servidores, etc.) e infraestructura de comunicaciones que

sean propiedad o estén administrados por la Unidad de Informática del Servicio. Esto incluye terminales, computadores personales, estaciones de trabajo, servidores y periféricos asociados, así como el software, independiente de que se use para gestión administrativa, económica, investigación u otros. De forma específica, se podrán redactar políticas y recomendaciones de buen uso de servicios e infraestructuras, como por ejemplo:

- Servicios informáticos (correo electrónico, Web, multimedia, sistemas, etc.)
- Buen uso de la infraestructura de redes y del acceso a internet.
- Acceso a servidores con datos de carácter personal.
- Incidencias de seguridad.
- Videos conferencias.

### **2.3. Aspectos legales.**

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. Por ello, el Gobierno Regional, podrá ser requerido por los órganos administrativos pertinentes para que proporcione los registros electrónicos o cualquier otra información relativa al uso de los sistemas de información.

Esta política se sitúa dentro del marco legal jurídico definido por la Leyes y Decretos siguientes:

- Ley 19.223 que regula: “Tipifica figuras penales relativas a la informática”.
- Artículo 1: El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena del presidio menor en su grado medio a máximo. Si como consecuencia de estas conductas se afectasen los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.
- Artículo 2: El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en el sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.
- Artículo 3: El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.
- Artículo 4: El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quién incurre en estas conductas es el responsable del sistema de información, la pena aumentará en su grado.

Asimismo, forma parte integrante de este documento la normativa vigente en el país referido a las Tecnologías de la Información.

- Norma Chilena de Seguridad NCh 2777 hace referencia a los controles de la seguridad informática.
- Ley 19.223: Tipifica delitos informáticos.
- 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.
- DS 100/2006: Fija características mínimas obligatorias que deben cumplir los sitios WEB de los Órganos de la Administración del Estado.
- Ley 19.880: Bases y Procedimientos Administrativos, se refiere a acceso a información personal y privacidad.
- Decreto 26/2001: Reglamento sobre el Secreto o Reserva de los Actos y Documentos de la Administración del Estado.

#### **2.4. Actualización de la Política.**

Esta política, tendrá como plazo de actualización, revisión y de integración de nuevas normativas, cada 3 años.

### **3. DEFINICIONES.**

#### **3.1. Definición de Seguridad:**

Se entiende como la preservación de la Calidad de información contenida en el sistema de información del Servicio.

Para ello se requiere que sea confiable de tal manera que garantice la accesibilidad sólo a aquellas personas autorizadas, sea íntegra para salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento, se encuentre disponible cada vez que lo requieran. Que sea auditable para que todos los eventos sean registrados para su control posterior, se evite duplicidad, y se resguarde sólo información original, se pueda verificar el envío y recepción de información evitando que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió, que cumpla con las leyes, normas, reglamentaciones o disposiciones Legales vigentes.

#### **3.2. Responsable Administrativa del Equipamiento a su Carga.**

Responsable de los equipos informáticos que haya instalado en el Servicio y estén a su cargo. Este acto se registra al momento de firmar el acta de recepción del equipamiento entregado.

#### **3.3. Administrador del Sistema.**

Responsable de la gestión y administración de los sistemas a su cargo y de supervisar el cumplimiento de la política de uso de los mismos. Será generalmente, el informático a cargo del sistema bajo su responsabilidad.

#### **3.4. Responsable Administrativo de los recursos informáticas del Servicio.**

Esta responsabilidad será del Jefe o Encargado de la Unidad de Informática.

#### **3.5. Usuarios.**

Toda aquella persona que utilice los recursos informáticos del Gobierno Regional de Arica y Parinacota.

### **3.6. Encargado de Seguridad.**

Es quien se debe encargar de dirigir las medidas y acciones para hacer cumplir esta Política, así como de su interpretación, control de cumplimiento y resolución de los problemas relativos a la misma.

## **4. POLÍTICAS DE USO.**

En este punto se plantean una serie de recomendaciones que pretenden regular el buen uso, disponibilidad y nivel de servicio de los recursos informáticos del Servicio. Aquellas personas que de forma reiterada o deliberada o por negligencia las ignoren o las infrinjan, **se podrán ver sujetas a las actuaciones técnicas (para minimizar los efectos de la incidencia)** o disciplinarias que se estimen oportunas. En cualquier caso, será responsabilidad de los Jefes de División y Unidad de Informática dar la difusión necesaria a esta Políticas para que sean conocidas por todos los usuarios de la red del Servicio.

### **4.1. Sobre la integridad y disponibilidad de los recursos.**

Los usuarios deberán respetar la integridad de los recursos y sistemas de información. Para esto, se enumeran una serie de recomendaciones:

- Un usuario no debe tratar de intervenir o eliminar el PC asignado por el Servicio (hardware o configuración del SO), software o periféricos que estén asignados a otros usuarios, sin la debida autorización.
- Los usuarios no deberán entorpecer o absorber recursos compartidos de tal forma que impidan a otros usuarios realizar sus tareas de forma eficiente. Esto incluye, al menos, lo siguiente:
  - El envío a través de correo electrónico de cartas encadenadas o mensajes excesivamente voluminosos o con muchos destinatarios, ya sean locales o ajenos al Servicio.
  - Uso de programas que puedan saturar los servidores o la red. En cualquier caso, se deberá solicitar con la suficiente antelación al responsable informático.
  - Modificación no autorizada de privilegios o permisos.
  - Intentos de desactivar servidores o cortar el funcionamiento de la red.
  - Intento de realizar cualquier tipo de daño (físico o lógico) a las herramientas informáticas del Servicio: equipos, aplicaciones, documentos, etc.
- Los usuarios no deberán intencionadamente desarrollar o usar programas cuyo objetivo sea dañar otras máquinas o acceder a recursos restringidos (malware, virus, troyanos, puertas traseras, etc.). deberán controlar que no se le infecte su equipo con este tipo de software, para lo cual la Unidad de Informática dispondrá del software apropiado para la eliminación de programas maliciosos. Los usuarios de la red, no deben utilizar los enlaces de red para otros usos que no sean los permitidos en las "Recomendaciones de Uso de la Red" o los propios necesarios para el desempeño de su actividad.

### **4.2. Sobre accesos no autorizados y suplantación de identidad.**

Los usuarios no deberán tratar de conseguir accesos a sistemas o recursos a los que no estén autorizados y tampoco permitir o facilitar que otros lo puedan hacer. Los usuarios deberán respetar los derechos del resto de los funcionarios del Servicio. La mayoría de los sistemas de uso compartido proporcionan mecanismos para proteger los datos e información privada de posibles consultas por parte de otros. El o los intentos de saltarse estos mecanismos para conseguir acceso no autorizado a información calificada como personal, supondrá una violación de esta Política e incluso del marco legal señalado en el numeral 2.3.

Los administradores de sistemas que estén autorizados podrán acceder, exclusivamente, por motivos de mantenimiento y/o seguridad, a aquellos ficheros de usuarios que permitan al administrador detectar, analizar y seguir las trazas de una determinada sesión o conexión. En cualquier caso, el administrador de sistema tiene el deber de guardar secreto sobre el contenido de los ficheros de los usuarios, no estando autorizado a permitir que terceros puedan acceder a los mismos. En el supuesto que una política interna expresamente lo autorice, el administrador podrá permitir el acceso a terceros (Jefes de División, Departamento) a determinados archivos de otros usuarios, debiendo contar en todo caso, con la autorización respectiva.

- Los usuarios de los recursos informáticos del Servicio, no deberán acceder a computadoras, aplicaciones, datos o información o redes para las que no estén debidamente autorizados. Tampoco deberán permitir de forma intencionada que otros lo hagan, independientemente de que el recurso pertenezca o no al Servicio. No está permitido realizar de forma intencionada, acciones cuyo propósito sea la obtención de contraseñas de otros usuarios sin el consentimiento de éstos.
- Cualquier defecto o anomalía que se descubra en el sistema o en su seguridad se debe reportar con la mayor brevedad posible a la Unidad de Informática, quién será la encargada de investigar y proponer soluciones al problema. Todo usuario que haya sido autorizado a usar una cuenta mediante un sistema de login/password, será responsable de mantenerla en secreto y no darla a conocer a nadie más sin la autorización del administrador del sistema. Es el usuario el que siempre será responsable de lo que se ejecute en el sistema desde esa cuenta. Los funcionarios deberán evitar compartir recursos (archivos, directorios, etc.) sin el mecanismo de seguridad necesario y disponible en cada sistema operativo y/o aplicaciones que garanticen la seguridad de su equipo y la red.

#### **4.3. Sobre uso de infraestructura de comunicaciones.**

No se podrá instalar ningún servicio informático (correo electrónico, servidores web, FTP, etc.) sin la autorización expresa de la Unidad de Informática y con la designación de un administrador del sistema al interior del Servicio.

No se podrá realizar la conexión, desconexión o reubicación de equipos o cambios de configuración de los mismos sin la autorización expresa de la Unidad de Informática.

Está prohibido la instalación de dispositivos y tarjetas de acceso remoto, módems, RDSI, ADSL, routers o cualquier otro dispositivo de comunicaciones en ordenadores o red sin la autorización expresa de la Unidad de Informática.

Queda prohibida la conexión de equipos de comunicaciones para intercambio de información entre ordenadores del Servicio y otros ajenos a dicha red.

Está prohibido el uso de la red y computadores para conseguir acceso no autorizado a cualquier computador.

Está prohibido instalar o ejecutar en cualquier punto de la red informática (ordenadores o software de red) programas o ficheros que traten de descubrir información distinta de la del propio usuario, en cualquier elemento de la red. Esto incluye sniffer, escaneadores de puertos, etc.

No se podrá facilitar a un tercero, a través de la red del Servicio, a la infraestructura de comunicaciones propias de este Servicio, es decir, no se podrá proporcionar tránsito a terceros, salvo obtención del consentimiento, previamente solicitado, del Jefe del Servicio.

Se debe evitar la circulación de información comercial, con excepción de respuestas a peticiones expresas de información sobre productos o servicios de interés para las actividades habituales del Servicio.

No se tendrá acceso a la destrucción, manipulación o apropiación indebida de la información que circule por la red. Se evitará el consumo excesivo de los recursos por parte de cualquier usuario. Se deberá respetar el derecho de privacidad de los diferentes usuarios de la red.

**La infraestructura de la red del Servicio, nunca deberá ser utilizada, bajo ningún concepto, para lo siguiente:**

- Transmisiones de información o acto que viole la legislación vigente en la República de Chile.
- Fines privados o personales, con o sin ánimo de lucro.
- Fines lúdicos.
- Fines no estrictamente relacionados con las actividades propias del Servicio.
- Creación o transmisión de cualquier tipo de información que sea ofensiva, obscena o indecente.
- Transmitir información difamatoria de cualquier tipo, sea contra entidades o personas.
- Divulgación de información que viole los derechos de propiedad intelectual.
- Usar cualquier aplicación de la cual se sepa que su uso pueda suponer una disfunción de la red.

#### **4.4. *Sobre las licencias de software y "copyrights".***

Los usuarios y administradores deberán respetar las condiciones deben respetar las condiciones de licencia y copyright del software que usen en sus equipos.

- Todo software adquirido por el Gobierno Regional de Arica y Parinacota (licencias computadores o licencias para instalación en servidores centrales) deberá estar debidamente licenciado y la responsabilidad de esto recaerá en el Encargado de la Unidad de Informática, o el responsable del Servicio que haya autorizado su adquisición.
- Todo software que se use para fines administrativos, deberá estar debidamente licenciado, con un número de licencias que se corresponda con el número de usuarios simultáneos. Por supuesto, podrá usarse en equipos del Servicio software "libre" (Open Source, freeware, etc.).
- Todo software que se use y que esté protegido con copyright no puede ser copiado, salvo con la autorización del propietario. No se podrán usar los medios que el Servicio pone a disposición de su comunidad para copiar software protegido o romper las protecciones del mismo.
- Además del software, toda otra información que también posea derechos de autor, que esté en formato electrónico y que haya sido obtenida de otro equipo, se debe usar de acuerdo con la legislación vigente.
- En general, los PC de los usuarios en el Servicio no se habilita la posibilidad de instalar software. Si se detecta que se ha instalado algún software en los equipos, así como el uso del mismo, se deberán cumplir con las obligaciones y requisitos que se deriven de su instalación y utilización.

En ningún caso, los usuarios podrán permitir que ninguna persona lleve a cabo la instalación en sus equipos de software que no esté debidamente licenciado. El incumplimiento de estas obligaciones por parte de los usuarios, dará lugar a la aplicación de las medidas preventivas, correctivas y disciplinarias previstas en la presente Política y, en su caso, al ejercicio de las acciones legales pertinentes.

## 5. LOS ADMINISTRADORES DEL SISTEMA Y SUS RESPONSABILIDADES.

Como ya se ha mencionado, cada usuario de hará responsable del buen uso del equipamiento y la red que el Servicio pone a su disposición. Pero hay determinados recursos (servidores, aplicaciones, base de datos, etc.) cuyo uso o explotación es compartido por un grupo de usuarios. Estos recursos deberán tener un responsable administrativo (que asumirá competencias organizativas) y un administrador del sistema, que será nombrado por el responsable administrativo y que se encargará de las tareas técnicas de funcionamiento del recurso en cuestión.

### 5.1. *La administración de los recursos globales.*

Corresponde a la Unidad de Informática el papel de Administrador de los Sistemas para los recursos informáticos globales del Servicio. El administrador del sistema (en este caso la Unidad de Informática) deberá organizarse y realizar las acciones y esfuerzos necesarios para:

- Prevenir y evitar robos, pérdidas o cualquier daño físico a los componentes del sistema.
- Respetar todos los acuerdos y licencias relativos al hardware y software que sean aplicables al sistema.
- Tratar la información almacenada en el sistema de la forma apropiada y adoptar las precauciones y medidas para proteger la seguridad de los datos, red y equipos según lo especificado en el marco legal vigente y los compromisos adquiridos.

Las medidas de seguridad se dimensionarán en función de la importancia y criticidad de los recursos que se quieran proteger. Dar publicidad a las distintas políticas y recomendaciones de uso de los servicios. Garantizar los procedimientos de recuperación de la información y del sistema en los servidores bajo su responsabilidad. Colaborar con otros administradores de sistemas de otras entidades (por ejemplo otros ministerios), para resolver los problemas causados en las mismas desde máquinas bajo el dominio del Servicio.

Para cumplir esta Política, el administrador del sistema cuenta con medios restringidos (herramientas y personal) y la autorización mediante nombramiento de tipo profesional con las competencias técnicas adecuadas para tomar medidas razonables que garanticen el buen funcionamiento de los recursos para la colectividad y su seguridad. El administrador del sistema puede, temporalmente y con el consentimiento (cuando sea posible) del Responsable Administrativo o del Encargado de Seguridad, suspender los privilegios de acceso o conexión si lo estima necesario o apropiado para mantener la integridad y disponibilidad del sistema o de la red.

A parte de todas las actividades relacionadas en el punto anterior, el administrador del sistema debe procurar:

- Implantar y hacer cumplir en su ámbito de actuación la Política y normas generales, así como las particulares de ámbito.
- Coordinar y colaborar con la Unidad de Informática en el uso de los recursos globales.
- Mantener actualizados y seguros los sistemas bajo su responsabilidad. Será el Responsable Administrativo quién deba responder ante incidentes e incumplimientos de la Política por parte del sistema local.

### 5.2. *El Encargado de Seguridad.*

El Servicio deberá nombrar a una persona, llamada Encargado de Seguridad, quién ya fue nombrado por medio de Resolución N° 1346 de fecha 27 de octubre de 2010, quien es el responsable de redactar estas Políticas, proponer las medidas y acciones para hacer

cumplirla, así como de su interpretación, control de cumplimientos y resolución a los problemas relativos de la misma:

- Redactar la Política de Seguridad: será responsable de la redacción de la Política de Seguridad del Servicio.
- Interpretación de la Política: Responsable de la interpretación de esta política, de la resolución de los problemas y conflictos con otras políticas y situaciones especiales.
- Cumplimiento de la Política: en los casos en que incurran violaciones a esta Política, el Encargado de Seguridad estará autorizado a trabajar en colaboración con las correspondientes unidades administrativas para su resolución.
- Control y monitorización: será responsable de diseñar la arquitectura y medidas de seguridad, la implantación de herramientas y técnicas y su grado de cumplimiento y ajuste a esta Política.
- Colaborar con el responsable del Programa de Mejoramiento a la Gestión de Seguridad de la Información.
- Para asuntos legales derivados del incumplimiento de estas normas, se consultará con la Asesoría Jurídica.

## **6. LAS CONSECUENCIAS DEL MAL USO DE LOS RECURSOS.**

### **6.1. Colaboración de los usuarios.**

Los usuarios, cuando se les solicite, deberán colaborar con los administradores de sistemas, en la medida de sus posibilidades, en cualquier investigación que se haga sobre mal uso de los recursos, aportando la información que se les requiera.

### **6.2. Acciones correctivas y preventivas.**

Si los administradores del sistema (generales o locales) detectan la existencia de un mal uso de los recursos y éste procede de las actividades o equipo de un usuario determinado, se podrá tomar cualquiera de las siguientes medidas para proteger a los otros usuarios, redes o equipos:

- Notificar la incidencia al usuario o responsable del sistema.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el usuario ante la autoridad competente.
- Con el permiso del Encargado de Seguridad y la debida justificación, inspeccionar ficheros o dispositivos de almacenamiento del usuario implicado.
- Informar a los superiores u Órganos del Gobierno correspondiente de lo sucedido.

### **6.3. Medidas disciplinarias.**

En caso de ser necesario, corresponderá al Jefe de Servicio la adopción de medidas disciplinarias hacia el o los usuarios infractores de esta Política, una vez informado por el Encargado de Seguridad.

## 7. CORREO ELECTRÓNICO.

El gobierno Regional de Arica y Parinacota, a través de su Unidad de Informática entrega una herramienta para poder comunicarse entre sus usuarios internos y con el resto del mundo.

Será responsabilidad de cada usuario mantener el resguardo y respaldo de su cuenta de correo. La Unidad de Informática no se hace responsable por pérdidas de información.

El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y cancelación de la misma. En el anexo ***“Correo Electrónica del Gobierno Regional – Políticas 2011 - 2012”*** podrá conocer más y revisar las buenas prácticas de su uso.

Una vez completado el proceso de activación del servicio, el usuario se responsabiliza de mantener la confidencialidad de su contraseña y cuanta y de todas las actividades que se efectúen por el uso de éstas.

### 7.1. ***Compromisos mínimos de los Funcionarios/Usuarios.***

- a) Notificar inmediatamente a la Unidad de Informática de cualquier uso no autorizado de su contraseña o cuenta o de cualquier otro fallo de seguridad.
- b) Asegurarse de que su cuenta sea cerrada al final de cada sesión.
- c) Su cuenta y contraseña son personales e intransferibles, por tal razón para todos los efectos, sus uso se presume proviene del usuario registrado.

### 7.2. ***Listos de Correos.***

Los servicios de mensajería instantánea o foros de discusión son herramientas que facilitan la comunicación entre las personas, así como la difusión de información a varios interlocutores de una sola vez.

Para esto, el Gobierno Regional de Arica y Parinacota dispone de una lista de correo cerrada que contienen a todos los usuarios que trabajan en el Servicio.

El modo de trabajo consiste en que desde el programa de correos que el usuario disponga, éste mandará el correo a la dirección de la lista. Para más antecedentes, consultar anexo ***“Correo Electrónica del Gobierno Regional – Políticas 2011 – 2012”***.

### 7.3. ***Lectura del Correo Electrónica.***

La Unidad de Informática entrega a los usuarios del Servicio herramientas para poder facilitar el trabajo tanto al interior como desde el exterior. En el anexo ***“Correo Electrónica del Gobierno Regional – Políticas 2011 – 2012”***, se menciona las formas de trabajo y buenas prácticas que se deben cumplir para que este servicio este operativo un 100% para todos los usuarios del Servicio.

### 7.4. ***Maneja de Archivos Adjuntas y Tamaño.***

El tamaño máximo del archivo adjunto es de 10 Mg. Al sobrepasar esa capacidad el correo no se podrá enviar, quedando pendiente en la bandeja de salida y mostrando un error. Para más antecedente consultar anexo ***“Correo Electrónica del Gobierno Regional – Políticas 2011 2012”***.

Este recurso que proporciona el Servicio no debe ser utilizado para actividades personales que no tengan relación con las propias del desempeño laboral. En estos casos el soporte informático no está obligado a prestar soporte. No se debe de usar este servicio para fines comerciales, salvo autorización expresa del Jefe de División de Administración y Finanzas. En cualquier caso, el uso comercial que se haga debe estar relacionado con las actividades del Servicio y suponer información relevante para los usuarios de la red.

## 8. CUENTAS DE USUARIO.

### 8.1. Creación.

Cada persona que trabaja en el Gobierno Regional posee una cuenta de usuario y de Correo Electrónico. La creación de las cuentas de usuarios, son realizadas por la Unidad de Informática, previa autorización por parte del Departamento de RR.HH. Esta autorización es entregada vía correo electrónico al siguiente correo: [nuevo.usuario@gorearicayparinacota.gov.cl](mailto:nuevo.usuario@gorearicayparinacota.gov.cl).

En este correo se deberá indicar en el **asunto** el siguiente texto: "Creación de nueva cuenta GORE". Además en el cuerpo deberá venir la siguiente información:

- Nombre completo del nuevo usuario, indicando claramente sus dos nombres y dos apellidos.
- RUT.
- Indicar la jefatura directa del nuevo funcionario y dependencia funcional.

La información de la creación del nuevo funcionario es informada directamente al involucrado y vía correo electrónico a la jefatura directa.

### 8.2. De la Password o clave secreta.

Al momento de crear al usuario, éste es creado con una clave genérica o clave por defecto.

En caso que el usuario no recuerde su clave podrá solicitar a la Unidad de Informática la creación de una nueva clave, volviendo a asignársele la clave por defecto.

La Unidad de Informática no tiene acceso a la password que utiliza el usuario, sólo está capacitado técnicamente para poder cambiar dicha clave.

El cambio de clave sólo lo puede realizar directamente el usuario, si otra persona pide el cambio la Unidad de Informática negará dicha solicitud, salvo que venga visado por la jefatura de la DAF. Para mayor antecedente consultar el anexo "**Cuentas de Usuario**".

### 8.3. Del cambio de la Password o clave secreta.

Para el cambio de clave, se dispone de herramientas para efectuar esta tarea. El cambio de clave deberá programarse para que sea cambiado a lo menos cada 2 meses y de esta manera mantener una buena práctica sobre la seguridad de las cuentas.

Para mayor antecedente consultar el anexo "**Cuentas de Usuario**".

## 9. SERVICIO DE NAVEGACIÓN WEB.

El Gobierno Regional de Arica y Parinacota entrega las herramientas para que exista una comunicación que no tenga fallas (en la medida de lo posible de sus recursos) para que los usuarios naveguen a sitios internos y externos en el marco de sus labores normales y cotidianas al interior del Servicio.

La Unidad de Informática monitorea constantemente el tráfico de la red, como una tarea cotidiana teniendo como misión la de velar por un buen servicio a sus usuarios. Resultado de este trabajo se puede dar la situación que se encuentre tráfico que supere los márgenes de bajada o subida de información.

Frente a este tema se toman medidas para garantizar una navegación lo más expedita y rápida posible.

Una de las medidas que se toma es que se bloqueen algunos sitios que presentan alto tráfico en la red y que no guardan relación con el trabajo cotidiano al interior del Servicio.

Otra instancia de bloqueo de sitios es cuando los jefes directos indican explícitamente a la Unidad de Informática que se bloquee tal sitio para usuarios en particular o una página dada.

También se utiliza el criterio de palabras para bloquear sitios (por ejemplo la palabra sexo).

Para mayor antecedente ver anexo *“Navegación en Internet”*.

Se puede dar el caso que se esté bloqueando una página que en un momento dado tiene que ser utilizada excepcionalmente por los usuarios. En ese caso será el jefe directo del funcionario o funcionarios el cuál se comunicará con el Jefe de la DAF y éste en conjunto con el Encargado de la Unidad de Informática verán la factibilidad de la utilización de esas páginas sin transgredir la seguridad de la red.

El Gobierno Regional cuenta con un firewall (corta fuego) de hardware el cual es el encargado de monitorear y restringir el acceso a ciertas páginas, administrador por la Unidad de Informática.

Los usuarios que sean sorprendidos en prácticas de navegación que no son acordes al trabajo, serán sancionados con la restricción total de navegación en su equipo (no incluye correo electrónico), previo informe al jefe directo del funcionario.

Si la Unidad de Informática sorprende en acciones reiteradas al usuarios, tendrá la facultad de restringir todo acceso vía web, esto será notificado al Jefe de División de la DAF y al jefe directo del funcionario.

Una de las funciones cotidianas de los funcionarios la Unidad de Informática es velar por el buen funcionamiento de la navegación en Internet. Cuando se detecta que un computador está haciendo mal uso de los recursos, se procederá a tomar cualquiera de las siguientes medidas para proteger a los otros usuarios, la red u otros equipos:

- Notificar la incidencia al usuario o responsable del sistema.
- Suspender o restringir el acceso o uso de los servicios mientras dure la investigación. Esta suspensión podrá ser recurrida por el usuario ante la autoridad competente.
- Con el permiso del Encargado de Seguridad y la debida justificación, se podrán inspeccionar ficheros o dispositivos de almacenamiento del usuario implicado.
- Informar a los superiores u Órganos de Gobierno correspondiente de lo sucedido.

## 10. SOPORTE Y SOFTWARE INSTALADOS EN LOS EQUIPOS.

El Gobierno Regional de Arica y Parinacota entrega las estaciones de trabajo 100% operativas para las tareas cotidianas de los usuarios. Cuando exista una tarea que requiera de algún software especial, éste es instalado por la Unidad de Informática, manteniendo las restricciones del numeral 4.4.

Para los detalles de los software instalados, consultar el anexo *“Software instalados por el GORE”*. En este anexo se detalla claramente todos los software que instala el Servicio y a los cuales la Unidad de Informática y su soporte entregan soluciones. Por lo tanto quedan excluidos de soporte todos aquellos programas que no estén expresamente indicados.

Está estrictamente prohibida la instalación de software por parte de los usuarios u otra apersona que no pertenezca a la Unidad de Informática. La instalación deberá estar acorde con los software permitidos por el Servicio.

Si la Unidad de Informática, en su tarea de verificación de software instalados en cada estación de trabajo, se encuentra con algún tipo de software **no oficial**, se procederá a la desinstalación de dicho software de forma inmediata.

Si algún funcionario requiere la instalación de un software específico, el interesado conversará con el Encargado de la Unidad de Informática para establecer si procede a dicha petición. Si la solicitud es aprobada, se tiene que entregar el medio magnético con el programa y la respectiva licencia del programa a la Unidad de Informática, quién será la encargada de realizar las pruebas de compatibilidad con los programas ya instalados en los computadores. Si no existe problema, se procederá a la instalación del software en el equipo deseado.

## 11. RESPALDO DE INFORMACIÓN.

La Unidad de Informática, al momento de crear la cuenta de los usuarios, deberá asignar un disco virtual a cada uno de ellos en el servidor, para que de esta manera los usuarios puedan respaldar la información atinente al trabajo del Servicio.

Este disco virtual o volumen se encuentra etiquetado con la letra Z: (doble click en Mi Pc). En esta carpeta (Z:) los usuarios tendrán la responsabilidad de ingresar todos los documentos que él estime son de importancia para su trabajo cotidiano.

La Unidad de Informática respaldará en forma periódica dicha carpeta, no obstante el usuario podrá pedir un respaldo de su información en medio magnético para su propio resguardo.

Se vuelve a mencionar que la información almacenada en el volumen Z: **será de exclusiva responsabilidad de cada usuario**. La Unidad de Informática sólo respaldará los documentos ingresados en estas carpetas.

Quedan excluidos todos los archivos del tipo mp3 o algún otro formato de música o imágenes, como fotografías y cualquier archivo que no sea de índole institucional. En esta instancia el usuario podrá identificar ante la Unidad de Informática si existe algún archivo de este tipo que no corresponda a música sino a una grabación de otra índole y en cuyo caso podrá almacenar dicha información en este volumen.

Para más antecedente consultar el anexo ***“Respaldo de Información”***.

## 12. TAREAS Y COMPETENCIAS QUE TIENE LA UNIDAD DE INFORMÁTICA.

Dentro de las actividades cotidianas de la Unidad de Informática se encuentran las siguientes:

- Monitoreo constante del tráfico en la red del Servicio.
- Administración y monitoreo del servicio de correo electrónico institucional.
- Soporte a usuarios en el ámbito informático en general.
- Soporte a usuarios respecto a la administración de servicios de telefonía (instalación, habilitación, cambios, registros de programación de teléfonos, tarifador, etc.)
- Soporte al sitio Web o sistemas que el Servicio habilite o desarrolle.

## 13. POLITICAS DE SEGURIDAD.

### 13.1. Alcance y campo de aplicación.

Este documento que forma parte de la Política General del Gobierno Regional de Arica y Parinacota, se basa en el Decreto N° 83, donde se establecen las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos de los Órganos de la Administración del Estado. Las exigencias y recomendaciones previstas en esta norma, tiene por finalidad garantizar estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico entre los órganos de la Administración del Estado. Para ello se aplicarán las

disposiciones contenidas en el capítulo 3 de la norma NCh 2777, con las adecuaciones necesarias para ser aplicadas al interior del Servicio.

### **13.2. Seguridad perimetral.**

Para este caso el Gobierno Regional cuenta con un firewall de hardware el cual monitorea el tráfico y los sitios visitados o que se han querido visitar por parte de los usuarios. Este firewall de hardware cuenta con un antivirus propio así como un antispam. También cumple las veces de servidor proxy.

### **13.3. Seguridad física de acceso a las dependencias informáticas.**

Se deberá contar con una puerta que restrinja el acceso a la Unidad a más tardar a diciembre de 2011. El acceso deberá contar con una botonera con clave que será manejada sólo por los funcionarios de esa dependencia y otra clave que estará a cargo del encargado de servicios generales y se podrá usar sólo en caso de emergencia, la que será cambiada cuando haya sido utilizada.

### **13.4. Seguridad de acceso a Data Center.**

El Data Center del Gore se encuentra en el segundo piso del Edificio principal cerca de las dependencias de la Unidad de Informática. Su acceso es restringido, teniendo llave sólo los funcionarios de la Unidad de Informática. Para el año 2011 se espera poder cambiar su puerta de acceso así como implementar una botonera con clave para su acceso.

### **13.5. Seguridad de Servicio Informáticos.**

Los sistemas críticos se encuentran en los servidores del Gobierno Regional. Éstos cuentan con fuentes de poder redundantes y con arreglo de discos en modalidad raid.

### **13.6. Seguridad Política de escritorio limpio.**

Es importante proteger la información institucional reservada, sobre todo cuando las oficinas son visitadas frecuentemente por proveedores, consultores, clientes, personal de limpieza y otros compañeros de trabajo. Para este caso, se considera como una buena práctica mantener su escritorio lo más limpio y organizado posible. Si está desordenado, es muy probable que usted no se dé cuenta de que le falta algo o bien pudo desaparecer.

Se recomienda siempre guardar los documentos de importancia y en especial materiales de almacenamiento tales como discos externos portátiles, pen drives, notebooks, netbooks, PDAs, etc., en un lugar seguro. En el caso que se utilice notebooks, asegúrelos físicamente con cables para evitar robos. Se recomienda como buena práctica activa, el bloqueo automático de su computador al alejarse del puesto de trabajo.

No mantenga a la vista datos sensibles, que puedan vulnerar su seguridad en el uso del PC, como por ejemplo nombre de usuario, clave, direcciones IP, contratos, etc.

### **13.7. Seguridad de Clima a Data Center.**

El Data Center del Gobierno Regional cuenta con un equipo de aire acondicionado de 26 BTU de potencia, el que permite mantener una temperatura adecuada tanto para los servidores como para la central telefónica que se encuentra en el lugar.

Se hace necesario la adquisición de otro equipo de climatización de similares característica y que funcione cuando el principal se deteriore o bien cuando esté en mantención. La compra de un nuevo equipo será incluido en el presupuesto para el año 2012.

**13.8. Seguridad respecto a la energía eléctrica.**

En el Data Center se cuenta con una Ups de 3000 V lo que permite una autonomía de aproximadamente 10 minutos. Para este año se consideró la compra de una unidad por la antigüedad que tiene la que se está utilizando.

**13.9. Seguridad a nivel de usuario.**

Todos los funcionarios del GORE que requieran, podrán tener acceso a los servicios informáticos. Todos los usuarios de la red del Servicio deberán ser autenticados para el acceso a los sistemas institucionales y a los recursos de la red.

A nivel de PC se provee de un antivirus licenciado y que es actualizado contra el sitio corporativo del proveedor una vez al día. Además está programado un escaneo a la semana para los equipos.

**13.10. Seguridad para la navegación a Internet.**

Todos los funcionarios tienen la posibilidad de utilizar los servicios de Internet, sin embargo el servicio se entrega con algunas restricciones a páginas que son consideradas como peligrosas para la estabilidad de los servicios informáticos en general.

Se restringe el acceso a servicios tipo P2P, chat, radios online o TV. Estos bloqueos son para proteger el buen uso del ancho de banda, además de evitar posibles contagios de virus por parte de los funcionarios del Servicio.

**13.11. Seguridad de Servicio de Correo Electrónico.**

El servicio de correo electrónico institucional es administrador y provisto por la Unidad de Informática del Gobierno Regional. Ellos son quienes entregan las claves de acceso y se preocupa del uso eficiente y buenas prácticas. Como se considera un servicio crítico para la institución se tiene las siguientes medidas de seguridad, el firewall posee un detector de spam (llamado a veces información publicitaria no solicitada). Antes de ser depositado en la casilla correspondiente, el e-mail es verificado por el firewall. Esta medida no evita el 100% de ingreso de spam, pero si minimiza su ingreso.

**14. DIFUSIÓN DE LA POLÍTICA DE SEGURIDAD.**

El Responsable del Área de Recursos Humanos o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad

Funcionarios antiguos: ésta será transmitida periódicamente (1 vez por semestre) vía correo institucional a todos los usuarios. Además se realizará una capacitación anual que estará contenida en el Programa Anual de Capacitación.

Funcionarios nuevos (Contratas y Plantas): se incorporan los contenidos en el Programa de Inducción, aprobado por Resolución Exenta N° 1784 de 2009.

Personal que presta servicios a honorarios: se incorporará la siguiente cláusula a su Contrato: “La persona contratada por un periodo de al menos 1 año deberá, por razones de buen servicio, incorporar los procedimientos y deberes validos respecto a la seguridad de la información que han sido aprobados por el Servicio”. Debiendo por obligación participar en al menos una capacitación que difunda la política de seguridad del Servicio.

El canal donde siempre estará publicada la política de seguridad es el sitio web del Gobierno Regional de Arica y Parinacota.

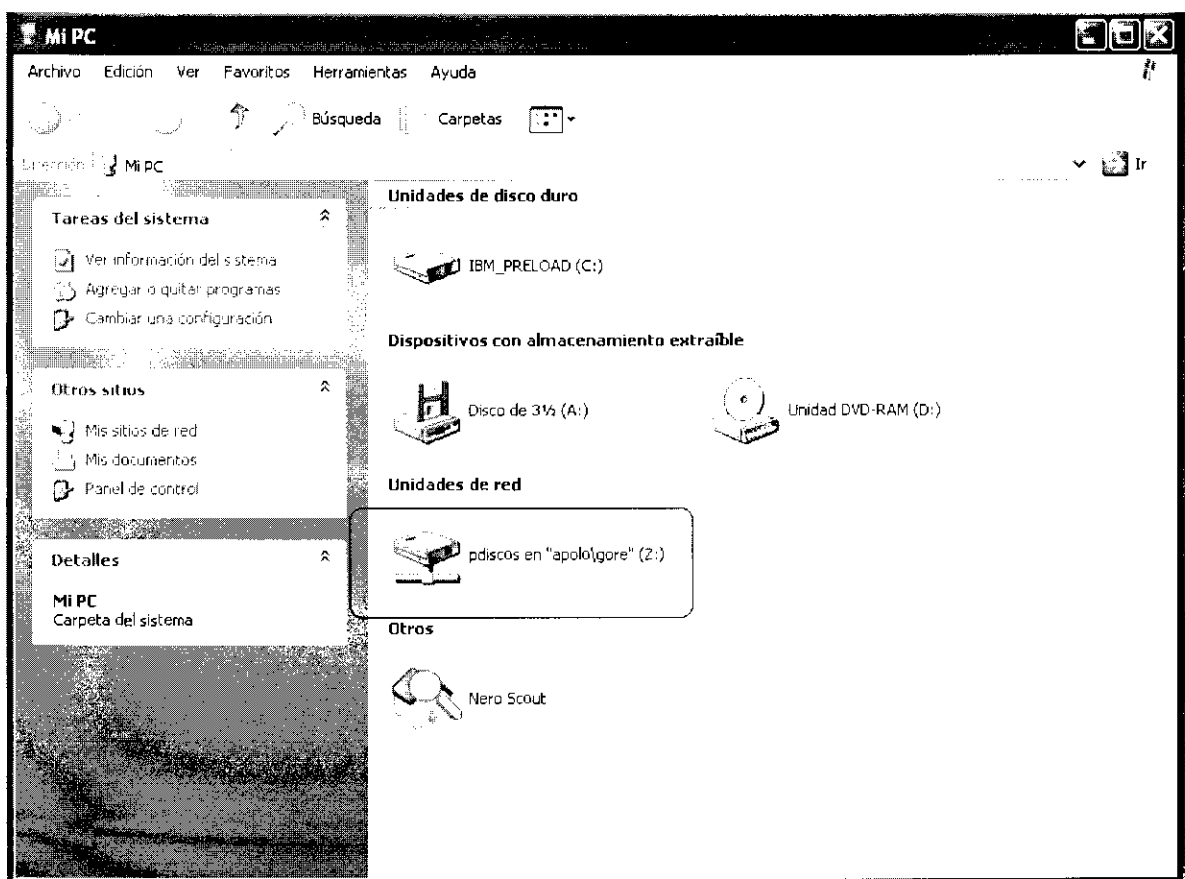
Se realizarán como parte de la mantención de las medidas de seguridad, 2 capacitaciones al interior del Servicio y con el Comité de Seguridad.

## ANEXOS

### **Respaldo de Información**

Pasos para realizar el respaldo de información sólo de datos de los usuarios del GORE. La información permitida para ser guardada es: documentos Word, Excel, Power Point, documentos PDF, Project. No se considera o no se permitirá respaldar información de tipo música (MP# u otro formato), fotos y videos.

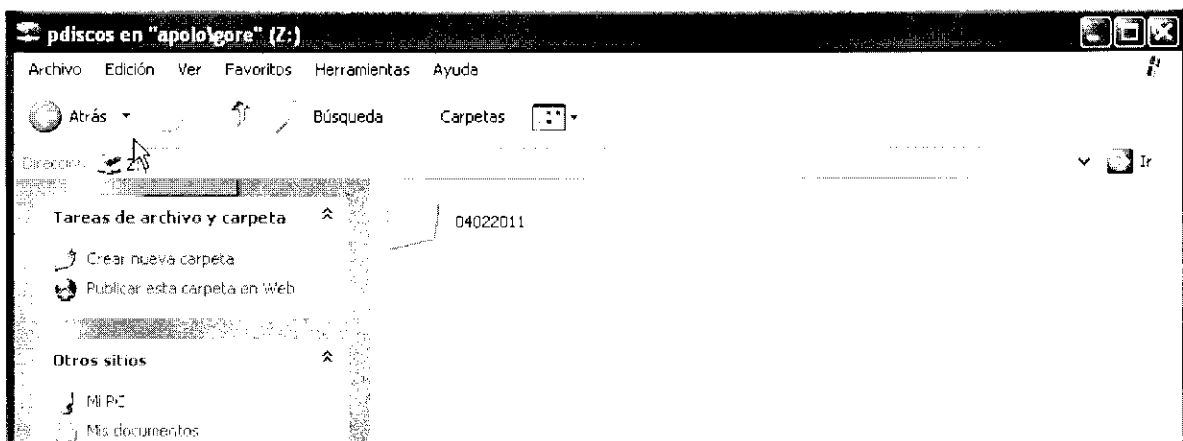
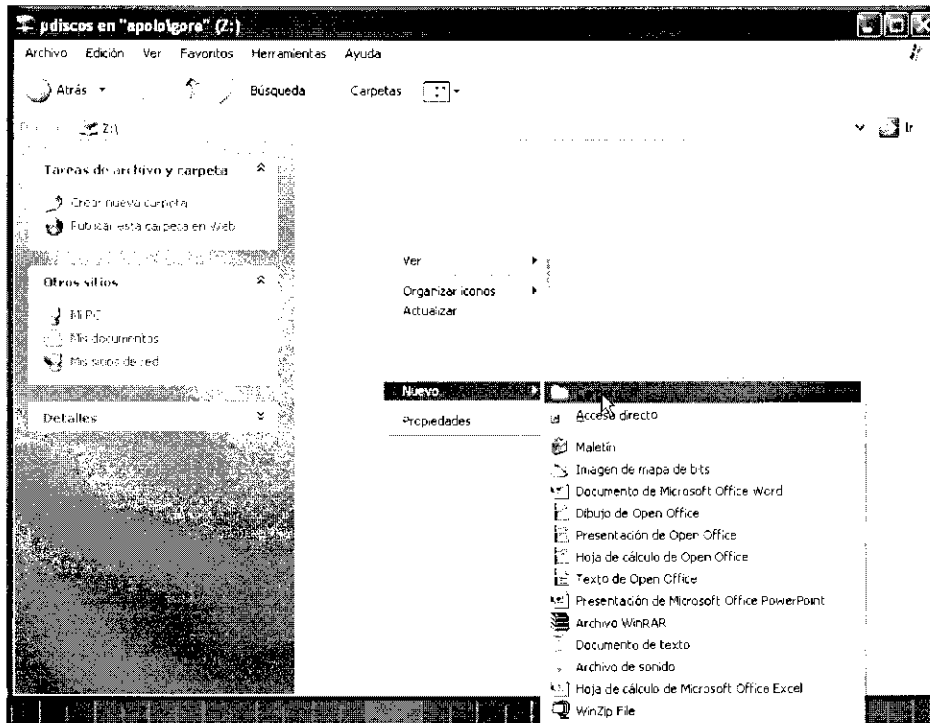
La siguiente pantalla muestra la ventana cuando hacemos doble click sobre el ícono Mi Pc.



En esta ventana se observa un volumen Z: Esta es la carpeta del servidor donde el funcionario deberá respaldar su información a lo menos una vez a la semana.

Se reitera, que es exclusiva responsabilidad del funcionario realizar el respaldo de su información.

Se sugiere a los usuarios que al momento de realizar un respaldo, creen una carpeta nueva la que tendrá de nombre la fecha del respaldo. (ver figura)



La carpeta creada será respaldada por la Unidad de Informática y se eliminará del volumen Z: De esta manera se mantendrá espacio suficiente para que los funcionarios realicen sus respaldos.

### **Correo Electrónico Gobierno Regional**

Para este fin la Unidad de Informática entrega dos herramientas para que los usuarios puedan trabajar desde las instalaciones del Gobierno Regional como desde cualquier punto con acceso a Internet, facilitando de esta forma a tarea de seguimiento de sus labores vía web.

La Unidad de Informática configura el servicio de correo de tal forma que al momento de abrir el correo en las estaciones de trabajo a su cargo, limpia la casilla del servidor, quedando este último vacío. Solo se accesa vía web para ver los correos que han llegado después de cerrar la aplicación local.

Las dos formas de trabajo con el correo electrónico son los siguientes:

- Vía Web.
- Outlook Express (trabajo interno o local).

La forma en que se utilizan estos lectores es la siguiente.

#### **VÍA WEB.**

Es la manera de leer los correos que están llegando al servidor de correos desde fuera de la estación de trabajo asignada. Para acceder a ellos se puede hacer de dos maneras: a través del Sitio del Gobierno Regional de Arica y Parinacota y luego pinchando el ícono "CORREO WEB" o bien digitando directamente en la barra del navegador "[webmail.garearicayparinacata.cl](http://webmail.garearicayparinacata.cl)".

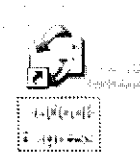
#### **VÍA EQUIPOS DE ESCRITORIO.**

La Unidad de Informática sólo admite la instalación del software de lectura de correo OUTLOOK EXPRESS de su versión 6 en adelante, lo que significa que cualquier otra herramienta de este tipo no será aprobado por la Unidad y tampoco se le dará soporte. Para este año 2011 se instalará en todos los equipos del Servicio el software MS OUTLOOK el cual se encentra licenciado, uniformando de esta manera la herramienta en cuestión.

La Unidad de Informática configura el la aplicación en cada equipo que tiene acceso directo a la red del Servicio.

Se reitera que el soporte es exclusivo sobre este software, dejando claro que no se hará soporte para ningún otro cliente de lectura de correo.

El software Outlook Express es muy sencillo de utilizar. Para acceder a los correo de forma local, se debe hacer doble click sobre el ícono que se encuentra en el escritorio y que como se mencionó anteriormente se encuentra configurado para acceder a la cuenta del usuario. (ver figura).



Se abrirá una ventana la cual muestra los correos del usuario y aquellos que están llegando.

#### **MANEJO DE ARCHIVOS ADJUNTO Y TAMAÑO.**

Se podrán adjuntar lo siguientes tipo de archivos:

- Todos los creados en Office y OpenOffice
- Imágenes del tipo JPEG.
- Documentos PDF
- Archivos RAR o ZIP.

Queda prohibido el envío de archivos con extensión EXE o extensión COM. Si el usuario tiene dificultades para el envío de un archivo adjunto y que este dentro de los permitidos, deberá comunicarse con la Unidad de Informática y hacer presente su problema.

El tamaño máximo del documento adjunto no podrá superar los 10 Mg. En caso que el archivo pese más de este tamaño, se tendrá que ajustar al tamaño para el tipo de restricción existente.

#### **CUOTA DE CORREO.**

Cada funcionario, al momento de ser creado como usuario del correo electrónico recibe una cuota para poder recibir correos. Esta cuota comprende tanto los archivos enviados como los recibidos y los archivos adjuntos que estos traigan. El tamaño de la cuota es de 2 Giga de información. Para aquellos funcionarios que sólo utilizan el correo vía web, es exclusiva responsabilidad de ellos ir eliminando los correo antiguos para de esta forma asegurarse que su casilla de correo tendrá capacidad para seguir recibiendo correos.

En relación al software Outlook Express, éste también posee una cuota de trabajo y que es de 2 Giga en su bandeja de entrada. Para liberar espacio en la bandeja de entrada, se recomienda la creación de carpetas y el traslado a ellas de los correos entrantes.

### **LISTAS DE CORREOS**

Los servicios de mensajería instantánea o foros de discusión son herramientas que facilitan la comunicación entre las personas, así como la difusión de información a varios interlocutores de una sola vez, por ello, conviene tener en cuenta una serie de comportamientos a la hora de usar estos medios.

Por otra parte, el sustento legal de estas políticas está refrendado en el artículo 25 del DS 83, donde se deben impartir instrucciones respecto del uso seguro del correo electrónico.

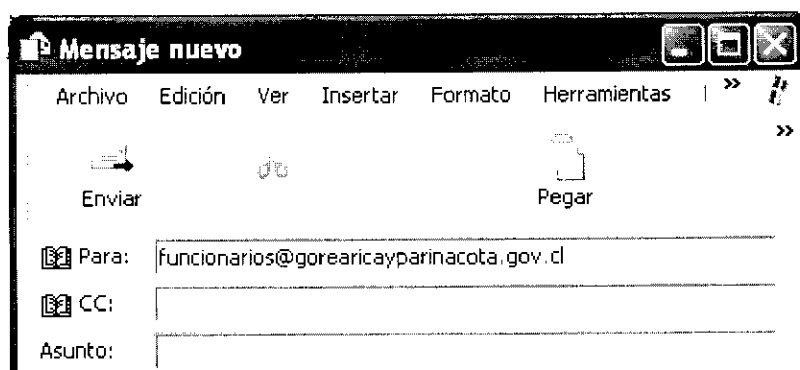
- a) Se debe considerar que el correo electrónico es vulnerable en la medida que no se conserven las medidas mínimas de buenas prácticas en el uso de este medio de comunicación.
- b) Se debe considerar que algunos tipos de archivos adjuntos recibidos en el correo electrónico pueden resultar altamente peligrosos, en especial los ejecutables o .exe que en su apertura o instalación pueden generar problemas.
- c) La password de acceso entregada por la Unidad de Informática es genérica para todas las cuentas de correo, es su responsabilidad cambiarla y generar una password segura.
- d) Nunca debe dejar la clave de acceso al correo electrónico en un papel y expuesta a ser vista. Se recomienda memorizar la clave ya que alguien puede suplantar su identidad.
- e) Genere password segura.
- f) La Unidad de Informática recomienda que para sus actividades personales NO utilice el correo electrónico institucional, para ello, el Servicio da las facilidades de no bloquear los servicios de correo tipo WEB MAIL.
- g) Usted como responsable en el uso del correo electrónico no puede utilizar este medio para el envío de correos difamatorios, uso para hostigamiento o acoso, compras no autorizadas, etc.
- h) No se deben usar estas utilidades para el envío de mensaje con contenidos fraudulentos, ofensivos, obscenos o amenazantes.

Las listas de correos se deben usar sólo para enviar mensajes relacionados con la finalidad de las mismas.

El gobierno Regional de Arica y Parinacota a través de su Unidad de Informática, cuenta con una lista única en la que figuran todos los funcionarios que tienen acceso a la red del Servicio. Es responsabilidad de la Unidad de Informática mantener actualizada esta lista.

El correo electrónico de esta lista es: [funcionarios@gorearicayparinacota.gov.cl](mailto:funcionarios@gorearicayparinacota.gov.cl)

El modo de uso de esta lista consiste en que desde el programa de correo Outlook Express, deberá ingresar en el campo "Para" la dirección de correo mencionada en el párrafo anterior. (ver figura)



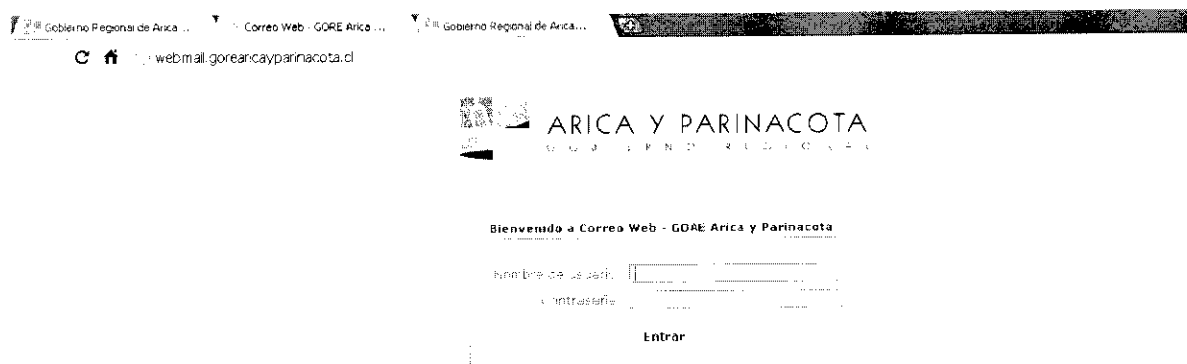
## **DEL BUEN USO DEL CORREO.**

1. Es responsabilidad del usuario mantener la confidencialidad del password.
2. Cada cuenta tendrá un espacio (cuota) que será establecida por la Unidad de Informática.
3. Es responsabilidad del usuario depurar su cuenta periódicamente para que exista espacio disponible, tanto en su casilla como en su equipo local.
4. La vigencia de la cuenta comprende el período de compromiso de trabajo con el Gobierno Regional.
5. La cuenta de correo electrónico es proporcionar apoyo en las actividades de los usuarios en su trabajo diario en el Servicio.
6. Es responsabilidad del usuario hacer buen uso de su cuenta, entendiendo por buen uso:
  - El empleo de su cuenta con fines propios del trabajo del Servicio.
  - Leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.
  - El uso de un lenguaje apropiado en sus comunicaciones.
  - Respetar las reglas de "Conducta en Internet" para las comunicaciones.
  - No permitir que segundas personas hagan uso de su cuenta.
7. Está estrictamente prohibido.
  - Uso de la cuenta para fines comerciales.
  - Mandar o contestar cadenas de correo.
  - Enviar SPAMS de información (correo basura), o enviar anexos (attachments) que pudieran contener información nociva para otros usuarios como virus o pornografía.
  - Usar la cuenta de otro usuario.
  - Utilizar como repositorio para documentos del tipo Word, pdf, Excel, etc.

## **CAMBIO DE PASSWORD DEL CORREO**

La Unidad de Informática genera la cuenta de correo con una clave genérica. Esta clave es entregada al usuario y es responsabilidad de éste realizar el cambio.

Este cambio se realiza a través del Sitio del Gobierno Regional en el ícono de CORRE WEB. Al pinchar se abre una ventana (ver figura)



En esta pantalla se debe ingresar el nombre de usuario y la clave entregada por la Unidad de Informática. Se ingresa a la pantalla del correo WEB. Ahí se debe seleccionar la opción CONFIGURACION.....

Remitente	Fecha	Tamaño
pamela cousins hurtubia	Dom 10:55	5,3 MB
Transparencia y Probidad	Sáb 21:38	51 KB
Pamela Díaz Rodriguez	Vie 17:51	58 KB
cmcomponentes	Vie 17:28	7,0 MB
Oracle	Vie 16:52	84 KB

Al ingresar a configuración se mostrará una pantalla la cual en su parte superior presenta una pestaña "CONTRASEÑA". Al hacer click en ella se abrirá otra ventana en dónde podrá cambiar la clave.

Sección

Interfaz de usuario

Vista de buzón

Composición de mensajes

**Cambiar Contraseña**

Contraseña Actual:

Contraseña Nueva:

Confirmar Contraseña:

**Guardar**

Se debe ingresar la clave actual y luego la nueva clave y confirmarla. Realizado este paso la clave ha sido cambiada y será su responsabilidad mantenerla secreta. Se recuerda a los funcionarios que en caso de olvido de la clave, la Unidad de Informática sólo podrá generar la clave genérica y el usuario deberá volver a realizar los pasos anteriores.

Para cambiar la clave en la estación de trabajo (Outlook Express), el usuario deberá ingresar al correo y presionar el ícono de "enviar y recibir". En ese momento se desplegará una ventana en la que le solicita ingresar la nueva contraseña.

### Cuentas de Usuario

Cada persona que trabaja en el Gobierno Regional posee una cuenta de usuario de inicio de sesión y de correo electrónico. Ambas cuentas son generadas por la Unidad de Informática, previa autorización del Departamento de RR.HH. Esta autorización es entregada vía correo electrónico indicando en el asunto el siguiente texto: **"Creación de nueva cuenta GORE"**.

En dicho correo se debe indicar:

- Nombre completo del nuevo usuario.
- RUN
- Indicar la jefatura directa del nuevo funcionario
- Su ubicación física.

La información de la creación del nuevo funcionario es informada directamente al nuevo usuario y vía correo electrónico a la jefatura directa.

#### ***De la password o clave secreta.***

En primera instancia, la Unidad de Informática crea la cuenta de inicio de sesión con una clave por defeco. En caso de que el usuario no recuerde su clave, éste podrá solicitar una nueva clave a la Unidad de Informática, generando la calve por defecto una vez más.

La Unidad de Informática no tiene acceso a la clave generada por el usuario, sólo está capacitada para generar una nueva clave.

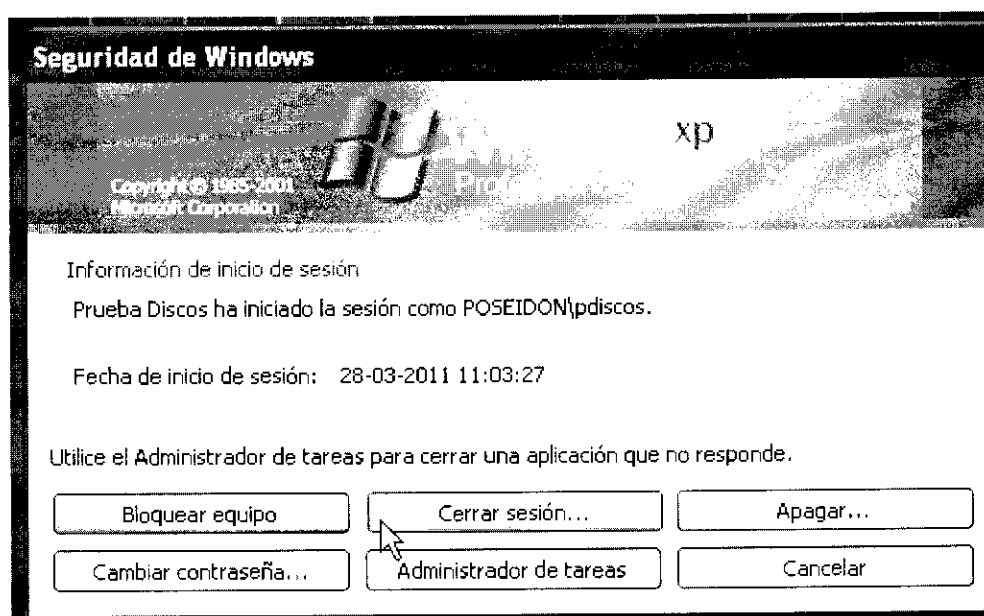
El cambio de clave sólo puede hacerlo el usuario directamente. Si otra persona pide el cambio, la Unidad de Informática negará dicha solicitud, salvo que venga visado por la jefatura de la DAF.

#### ***Del cambia de la password o clave secreta.***

Al momento de iniciar la sesión por primera vez, el sistema le solicitara realizar el cambio de la contraseña. El usuario deberá ingresar la contraseña actual y luego la nueva contraseña y confirmarla.

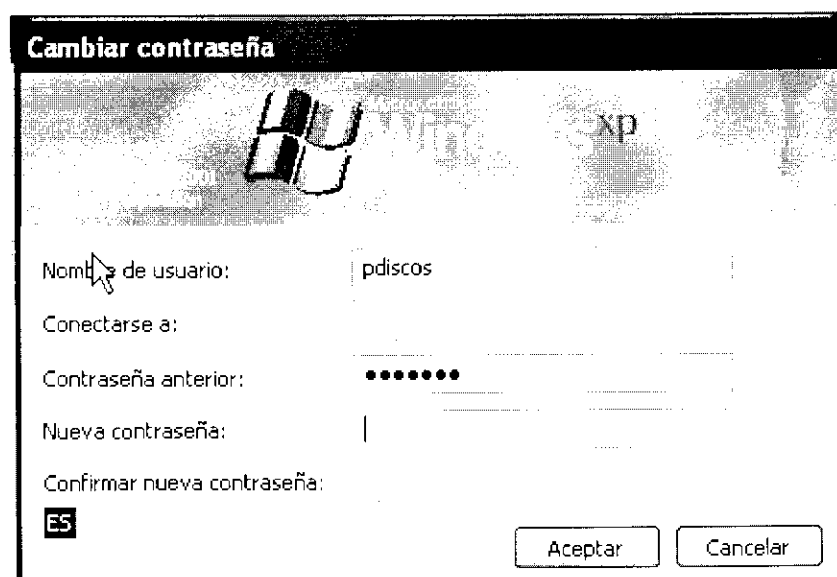
Realizado este paso el usuario deberá utilizar la nueva contraseña cuando inicie sesión en su equipo.

Si el usuario desea cambiar su contraseña, por temor a que alguien se la haya descubierto, deberá realizar lo siguiente: una vez ingresada a su sesión debe presiona las teclas CTRL + ALT + SUPR. El sistema le mostrara una ventana con varias opciones. Entre ellas la que dice "CAMBIAR CONTRASEÑA". El usuario deberá pinchar sobre esa opción y realizar el cambio de la contraseña. (ver figura).



Con el fin de prevenir que su clave sea conocida por alguna persona, el sistema le solicitará a lo menos cada dos meses cambiar su contraseña, no pudiéndose repetir contraseñas anteriores sino hasta después de 4 veces realizado este cambio.

La siguiente figura muestra la pantalla cuando se inicia por primera vez la sesión en Windows. En ella se observa la solicitud de cambiar la contraseña.



La nueva contraseña debe contener a lo menos 6 caracteres.

#### - **Navegación en Internet**

Los sitios bloqueados en general son:

- Para escuchar música y radios en línea.
- Bajar y subir archivos a la red Internet (rapidshare, flizashare, et.)
- Sitios del tipo P2P (emule, Lime, Ares, etc.)
- Ver videos en línea o diferidos.
- Juegos en línea.
- Ver televisión en línea.
- Ver pornografía.
- Sitios que permitan Messenger, chat, blogs, sitios de intercambio social, redes sociales.
- Sitios que salten política de seguridad antes descritas.

#### - **Software Instalado en Gobierno Regional**

La Unidad de Informática es la encargada de revisar y actualizar los software y hardware instalados al interior del Servicio y que se utilizan para el trabajo diario.

En cuanto al software instalado, la tarea de investigación y prueba de nuevas herramientas, genera un conocimiento, el cual es aplicado luego, al entregar soporte a los distintos usuarios del Servicio. Por esta razón es que se instala y da soporte solamente a estos software, dado que el ámbito es muy grande y no se puede abarcar en todos los programas.

La Unidad de Informática a través de su soporte, tiene como objetivo el entregar soporte de primera línea cuando éste es requerido.

Los sistemas que utiliza y que son instalados por la Unidad de Informática en los equipos de trabajo, son los siguientes:

- Sistema Operativo: Windows XP Pro.
- Browser de navegación: Mozilla Firefox, Internet Explorer, Google Chrome.
- Software de ofimática: Office 2007, OpenOffice .
- Lectura de Correo: Outlook Express, MS Outlook.
- Manejo de archivos compactados: WINRAR, WINZIP.
- Lectura de archivos PDF: Adobe Acrobat Reader.
- Grabación de archivos: Nero Smart Suite.”

**ANÓTESE Y COMUNÍQUESE**

  
XIMENA VALCARCE BECERRA  
INTENDENTA (S)  
GOBIERNO REGIONAL DE ARICA Y PARINACOTA

MPS/ASL/rdo

**DISTRIBUCION:**

- 1.- Responsables de PMG
- 2.- DAF y RR.HH.
- 3.- Jefes de División
- 4.- Oficina de Partes