ARICA Y PARINACOTA

**APRUEBA NORMAS DE USO ACEPTABLE, GOBIERNO REGIONAL DE ARICA Y PARINACOTA**

**RESOLUCION EXENTA N°** 2322

**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** Normas de Uso Aceptable 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:

# NORMAS DE USO ACEPTABLE
# GOBIERNO REGIONAL DE ARICA Y PARINACOTA

## NOTA DE CONFIDENCIALIDAD

La información contenida en estas normas de seguridad y uso aceptable es confidencial y sólo puede ser utilizada por la institución a la cual se aplica y queda expresamente prohibido su uso para fines comerciales. Su clasificación es de USO INTERNO.

Las personas autorizadas para usar estas normas, la pueden copiar, modificar y reproducir únicamente para aquellos fines a los cuales está destinada.

Cualquier retención, difusión, distribución o copia de estas normas está prohibida y será sancionada por la Ley, como asimismo toda violación a esta nota de confidencialidad será motivo para radicar o solicitar una acción civil en su contra.

Firmas de los responsables.

| ELABORADO POR: | REVISADO POR | APROBADO POR |
|---|---|---|
| Alvaro López V. | Juan Carlos Rojas | José Durana Semir |
| _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ | _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ | _ _ _ _ _ _ _ _ _ _ _ |
| Encargado Unidad Informática | Encargado de Seguridad | Intendente |

## CONTROL DE VERSIONES

| *REVISIONES DEL DOCUMENTO* | | | | |
|---|---|---|---|---|
| **Nº Revisión** | ***Fecha Aprobación*** | ***Motivo de la revisión*** | **Páginas Modificadas** | **Autor** |
| 0(Cero) | 28.03.2011 | Elaboración y revisión inicial | Todas | A. López |
| 1 | 03.12.2013 | Modificación a Normas de Uso Aceptable (anteriormente llamado Políticas de Seguridad 2011-2012) | Todas | A. López<br>Consultora |

**INDICE**

## 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.

En el presente documento se plantean una serie de normativas 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.

Los motivos para la redacción de estas normas o políticas, son los siguientes:

### 1.1 Necesidad

Los usuarios de los recursos informáticos, de la 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 las Normas.

Lo que se plantea, es asegurar una infraestructura informática que facilite la realización de las misiones básicas del Servicio, como son la comunicación y tareas administrativas.

Los computadores, servidores y la red del Servicio, son tecnologías que permiten de forma eficiente el acceso y distribución de información.

Estas tecnologías nos permiten el acceder, copiar y compartir información con otros usuarios de la red, por lo que usuarios deben estar conscientes de sus derechos y de los demás, tales como la privacidad o protección de la propiedad intelectual. Este documento explica qué se considera un uso adecuado de la red y sistemas con relación a los derechos de otros. También se mencionará, las responsabilidades que supone el uso de estos recursos y de las consecuencias de su abuso.

## 2. ÁMBITO DE LA APLICACIÓN.

### 2.1 Agentes a los que se aplicas estas normas

Se deberá aplicar a todos los usuarios de la red del Servicio y que hagan utilización de los recursos expuestos en el siguiente apartado.

Estas normas también son de aplicación a cualquier otra entidad externa al Gobierno Regional que utilice los recursos informáticos del mismo.

### 2.2 Recursos a los que se refiere estas normas

Son todos aquellos sistemas de información, sean éstos individuales o compartidos, y estén o no conectados a la red del Gobierno Regional.

Se aplicará a todos los 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.

### 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.

Estas normas se sitúan dentro del marco legal jurídico definido por la Leyes y Decretos siguientes:

- Ley 19.223 que regula: "Tipifica figuras penales relativas a la informática".
- 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 las normas.

Estas normas o políticas de uso, tendrá como plazo de actualización, revisión y de integración de nuevas, una vez cada año.

## 3. DEFINICIONES.

**Activo**: conjunto o funcionalidad de un Sistema de información o relacionados con éste necesarios para que el Gobierno Regional funcione correctamente. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para el Gobierno Regional.

**Autenticidad:** Relativo a la credibilidad de la información. Manifiesta la garantía existente sobre la identificación del origen y destino de la información y sobre la autorización para que se transmita entre ellos.

**Confidencialidad:** Relativo a la garantía de que la información con acceso y divulgación restringida, ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.

**Disponibilidad:** Relativo a la garantía de que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera, en tiempo y forma.

**Incidente o incidencia:** Evento adverso en un sistema de información que compromete la confidencialidad, integridad, disponibilidad o confidencialidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes.

**Información**: toda comunicación o representación de conocimiento como datos, en cualquier forma y en cualquier medio, físico o digital.

**Integridad**: Relativo a la exactitud, unicidad, consistencia y totalidad de la información y los métodos de procesamiento.

**Legalidad:** referido al cumplimiento de las leyes, normas, reglamentos, ordenanzas o disposiciones a la que está sujeta el Gobierno Regional.

**Sistema de Información**: conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento transmisión y difusión de la información.

## 4. NORMA DE USO DE LOS MEDIOS TECNOLÓGICOS DEL SERVICIO

**Responsables y Personal:**

| | |
|---|---|
| **Responsable** | Encargo de Seguridad |

### 4.1 Objetivo

Esta norma se aplicará a todos los recursos tecnológicos que el Gobierno Regional posee y pone a disposición de los usuarios del mismo para su uso en el desempeño de sus funciones, ya sea dentro o fuera de las ubicaciones principales del Gobierno Regional y dentro y fuera del horario laboral establecido.

Estos recursos no incluyen los servidores y redes dedicados exclusivamente a los servicios del Gobierno Regional que se regirán por la *Normativa de Uso de la Infraestructura del Servicio*.

### 4.2 Premisas

Esta norma se basa en las siguientes premisas:

- Los medios tecnológicos son instrumentos que el Gobierno Regional pone a disposición de los trabajadores en el desempeño de sus funciones en el puesto de trabajo.
- El derecho legítimo del Gobierno Regional a controlar el uso de los medios tecnológicos que pone a disposición de los trabajadores
- Salvaguardar el derecho a la intimidad del trabajador

### 4.3 Correo electrónico

El Gobierno Regional pone a disposición de sus usuarios una cuenta de correo electrónico con el fin de poder comunicarse e intercambiar información en el desarrollo de sus funciones laborales.

El Gobierno Regional no realizará nunca, de forma rutinaria, monitorizaciones o inspecciones de los buzones de correo sin el consentimiento del titular de la cuenta asociada. No obstante, éstas se podrán única y exclusivamente cuando haya requerimientos judiciales.

La cuenta de correo podrá usarse para comunicaciones personales, siempre y cuando éstas no se realicen de manera abusiva y no interfieran de manera significativa en buen cumplimiento de sus funciones.

Se prohíbe el uso de cuentas de correo personales alojadas en servidores externos por el peligro de software malicioso (troyano, virus, gusanos, etc.) que pueden suponer, a excepción de personal autorizado.

#### *4.3.1 Características*

- Los usuarios son los únicos responsables de todas las actividades realizadas con sus cuentas de acceso al correo y su buzón asociado.
- Los mensajes de tipo personal están sujetos, así mismo a los términos y condiciones de esta normativa.
- Se realizarán copias de seguridad de los mensajes residentes en los buzones de los trabajadores con el único fin de garantizar su disponibilidad en caso de incidentes.
- Los buzones contarán con una capacidad máxima de 2Gb.
- El tamaño máximo de recepción o envío de un mensaje será de 10Mb. Se podrá ampliar temporalmente previa petición individual y justificada.
- Se filtrarán, detendrán y estudiarán automáticamente, mediante herramientas al efecto, aquellos correos entrantes o salientes que puedan representar peligro de algún tipo (conteniendo virus u otro tipo de software malicioso, SPAM, etc.). Para determinar su riesgo potencial, todos los correos serán examinados por estas herramientas, conforme a patrones definidos. Cuando un correo sea definitivamente detenido y desechado, se informará al trabajador, indicando el motivo.
- La password de acceso genérica entregada por la Unidad Informática deberá ser cambiada inmediatamente, siendo responsabilidad del Usuario el modificarla periódicamente y disponer de una password segura.
- Es responsabilidad del usuario mantener la confidencialidad del password.

#### *4.3.2 Uso Aceptable*

En general, la cuenta de correo electrónico se podrá usar libremente para:

- Intercambio de información con trabajadores del Servicio, así como a empresas, particulares externos u otros organismos, relacionada con el desempeño de las funciones del trabajador.

- Intercambio de información con fines particulares solamente de forma moderada y no abusiva.

- Cuando se envíen correos electrónicos a destinatarios múltiples, con carácter individual a cada uno de ellos, se realizará de forma que éstos puedan confirmar la identidad del origen del mensaje.

- El uso de lista de correos es específico para enviar mensajes relacionados con la finalidad de las mismas.

*4.3.3 Transmisión de información por correo electrónico*

Se podrá enviar información por correo electrónico, con los siguientes requerimientos:

- Información de tipo Pública: sin necesidad de cifrar y a cualquier destino.

- Información de Uso Interno: cifrada o sin cifrar, a todo el personal del Servicio y al personal externo autorizado o directamente relacionados con el desempeño de sus funciones y fines del Gobierno Regional.

- Información Reservada Secreta: solamente cifrada y al personal del Servicio y al personal externo que estén expresamente autorizados a acceder y tratar la información. Adicionalmente, se incluirá la información necesaria para que el destinatario pueda confirmar la identidad del remitente.

*4.3.4 Recepción de correo*

- Cualquier correo de procedencia totalmente desconocida y con contenido inapropiado y no solicitado, será eliminado de inmediato.

- Antes de abrir cualquier archivo adjunto a un correo se debe chequear contra virus y software malicioso. Se tendrá preconfigurada la herramienta a tal efecto, para que inspeccione el correo entrante en tiempo real.

- Cuando se reciba un correo por error, cuyo destino real era otra persona, se borrará sin hacer uso, en ningún sentido, del contenido de este, pudiendo si se estima oportuno, hacer saber el hecho al remitente.

*4.3.5 Uso no aceptable*

- Facilitar la cuenta de usuario a otras personas.

- No se permitirá el uso del correo electrónico para fines personales, en ningún caso, cuando:

    - Interfiera con el rendimiento del propio Servicio, o suponga un alto coste para el Gobierno Regional.

    - Interfiera en las labores propias del trabajador

- Enviar mensajes con direcciones no asignadas al trabajador o manipular las cabeceras de correo electrónico.

- En cuanto a la difusión de información utilizando listas de distribución, no se permite:

    - Utilizar las listas de distribución para envío de información ajena a las finalidades del Gobierno Regional.

    - Utilizar las listas de forma indiscriminada.

    - Incluir archivos de tamaño elevado y/o envío a listas de correo, para evitar la degradación del servicio de correo y el llenado involuntario de los buzones de los trabajadores

- Enviar archivos con extensión EXE o extensión COM.
- Participar en la propagación de correos en cadena.
- Ataques con objetivo de imposibilitar o dificultar el servicio de correo electrónico, distribuir de forma masiva grandes cantidades de mensajes.
- Difundir contenido inadecuado o ilegal (apología del terrorismo, programas piratas, pornografía infantil, amenazas, estafas, virus o código malicioso, discriminación por razones de sexo, discapacidad, raza, religión, etc.).
- Enviar contenido fuera de contexto en la participación en foros temáticos.
- Difusión a través de canales no autorizados.
- Suscripción indiscriminada a listas de correo.

*4.3.6 Advertencias legales*

En todas las comunicaciones por correo electrónico que realice el personal del Gobierno Regional hacia el exterior se incluirá al final del texto:

***La información incluida en el presente correo electrónico es CONFIDENCIAL, siendo para el uso exclusivo del destinatario arriba mencionado. Si usted lee este mensaje y no es el destinatario señalado, el empleado o el agente responsable de entregar el mensaje al destinatario, o ha recibido esta comunicación por error, le informamos que está totalmente prohibida cualquier divulgación, distribución o reproducción de esta comunicación, y le rogamos que nos lo notifique, nos devuelva el mensaje original a la dirección arriba mencionada y borre el mensaje. Gracias.***

*4.3.7 Anexos*

Se dispone del documento *Uso del Correo Electrónico del Gobierno Regional* como manual de uso del correo electrónico.

### 4.4 Servicio de Navegación Web (Internet)

El Gobierno Regional 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 funciones laborales, por ello pone a disposición de sus trabajadores conexión a Internet.

Se establecerán registros automáticos de las personas y procesos que usen Internet, quedando registrados los sitios concretos a los que accede a través de equipos de comunicaciones específicos para tal fin.

Los usuarios son los únicos responsables de todas las actividades realizadas en el uso de Internet.

*4.4.1 Uso aceptable*

Se podrá usar Internet para:

- Acceso a cualquier tipo de información relacionada con el desempeño de las funciones del trabajador.

*4.4.2 Uso no aceptable*

Queda prohibido el uso de Internet en los siguientes términos:

- Con fines particulares y en horario laboral, salvo momentos puntuales y sea estrictamente necesario.
- Juegos de entretenimiento, juegos de azar, concursos, subastas, etc.

- Descarga de software ilegal
- Cuando no estén estrictamente relacionadas con las funciones del trabajador, las siguientes actividades:
    - Descarga de cualquier tipo de software sin autorización del Encargado de Seguridad.
    - Descarga o visualización de videos, audios, etc.
    - Acceso a servicios como chat, IRC, telnet, ftp, videoconferencias,etc.
- En ningún caso, uso de programas "peer-to-peer" (P2P) para compartir archivos.
- Descargas continuadas de cualquier tipo de archivos o de volúmenes de información muy grandes que puedan degradar la conexión a Internet y por tanto afectar al resto de los trabajadores.
- Transmisiones de información o acto que viole la legislación vigente en la Republica de Chile.
- Transmitir información difamatoria de cualquier tipo, sea contra entidades o personas.
- Divulgación de información que viole los derechos de propiedad intelectual.

#### *4.4.3 Bloqueo de la navegación*

En el caso de que en un momento determinado el acceso a una página quede bloqueado por la Unidad Informática, el desbloqueo de la misma debe ser autorizado específicamente. Será el jefe directo del funcionario o funcionarios que deseen acceder al contenido de la misma quién lo comunicará al Jefe de la DAF para que éste, junto con el Encargado de Seguridad, estudien la factibilidad de la utilización de esa página sin transgredir la seguridad de la red del Servicio.

#### *4.4.4 Régimen disciplinario*

Aquellos usuarios que sean sorprendidos en prácticas de navegación no acordes a sus funciones laborales, serán sancionados con la restricción total de navegación de su equipo (a excepción del correo electrónico), previo informe al jefe directo del funcionario.

Si la Unidad de Informática sorprende en acciones reiteradas al usuario, tendrá la facultad de restringir todo acceso a vía Web, siendo notificado al Jefe de la División de la DAF y al jefe directo del funcionario.

Con el permiso del Encargado de Seguridad y la debida justificación, se podrán inspeccionar ficheros o dispositivos de almacenamiento del usuario.

### 4.5 Computadoras y periféricos

#### *4.5.1 Licencias de Software y Copyrights*

- Todo software adquirido por el Gobierno Regional (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.

*4.5.2 Uso aceptable*

Se permite el uso de **Computadoras (PC)** para:

- Realización de trabajos y actividades relacionadas con el desempeño de las funciones del trabajador
- Guardar información propiedad del usuario, relacionada con el desempeño de sus funciones. Esta carpeta deberá estar permanentemente autorizada a ser revisada por el antivirus corporativo. La información contenida en ella es responsabilidad del trabajador.

Sobre **periféricos**, está permitido:

- El uso del teléfono (fijo o móvil), impresoras, escáneres, plóteres, y demás periféricos para fines relacionados con el desempeño del trabajador, de forma no abusiva, y cuando sea estrictamente necesario, colaborando así a controlar el gasto y cuidar el medioambiente.

*4.5.3 Uso no aceptable*

No está permitido el uso de **Computadoras (PC)** para lo siguiente:

- Realizar trabajos particulares o con fines privados, durante el horario laboral.
- Modificación de la configuración física hardware de las estaciones sin autorización.
- Instalación de software libre no autorizado o de software no licenciado por el Gobierno Regional. La instalación autorizada de software siempre debe hacerse bajo la supervisión de la Unidad Informática.
- Instalación de cualquier paquete software que pueda causar un mal funcionamiento o degradación en la red o en los servicios del Gobierno Regional.
- Cambio en la configuración de las estaciones, excepto en aquellos valores que atañen directamente a la operatividad: configuración de pantalla, escritorio, valores de usuario, aplicaciones, etc. No está en ningún caso permitido cambiar la configuración de la red, así como el antivirus, cortafuegos personal o cualquier otro control de seguridad
- Instalación y uso de software orientado a conseguir privilegios en la red o realización de ataques a otros equipos (generadores de tráfico, escaneadores de puertos, escuchas de tráficos, etc.)
- Realizar la conexión, desconexión o reubicación de equipos o cambios de la configuración de los mismos sin la autorización expresa de la Unidad Informática.
- Guardar información como aplicaciones, ejecutables, etc. que sea ilegal o susceptible de contener software malicioso.

Así mismo, sobre **periféricos**, **no** está permitido:

- El uso abusivo del teléfono (fijo o móvil corporativo) para realizar llamadas particulares, entendiendo por abusivo la reiteración en valores altos en coste o duración de llamadas.
- El uso de las impresoras, escáneres, plóteres, y demás periféricos para trabajos o información particular dentro del horario laboral, o fuera de éste, de forma indiscriminada o sin autorización expresa.

#### *4.5.4 Anexos*

Se dispone del documento *Software instalados por el GORE* que detalla claramente todo el software que instala el Servicio y a los cuales la Unidad Informática y su soporte entregan soluciones. Por lo tanto quedan excluidos de soporte todos aquellos programas que no estén expresamente indicados en dicho documento.

### 4.6 Acciones correctivas y preventivas

Si los administradores del sistema 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.

### 4.7 Responsabilidades

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.

Si algún usuario 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.

### 4.8 Compromisos mínimos de los usuarios

Todo usuario de los sistemas de información se compromete 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.
- Asegurarse de que su cuenta sea cerrada al final de cada sesión.
- La cuenta y contraseña son personales e intransferibles, por tal razón para todos los efectos, su uso se presume que proviene del usuario registrado.
- Mantener en el escritorio de la computadora o portátil la mínima información de manera que esta no pueda ser visualizada por personal ajeno o no autorizado.

## 5. NORMATIVA DE USO DE LAS INFRAESTRUCTURAS DEL SERVICIO

**Responsables y Personal:**

| | |
|---|---|
| **Responsable** | Encargo de Seguridad |

### 5.1 Objeto

Establecer las reglas de uso de la Infraestructura perteneciente al Gobierno Regional, por parte del personal Administración de Sistemas y Comunicaciones a fin de evitar el impacto que pudiese derivarse de su falta de regulación y uso inadecuado.

### 5.2 Introducción

La infraestructura tecnológica del Gobierno Regional está formada principalmente por una red de comunicaciones que interconecta a un conjunto de equipos que están, cada uno de ellos, dedicados en exclusiva a la prestación de uno o varios servicios concretos, servicios orientados al ciudadano o bien servicios al propio Gobierno Regional. Por lo tanto los equipos deben ser exclusivamente utilizados para realizar las operaciones necesarias para la consecución y el buen funcionamiento del servicio al que han sido encomendados.

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.

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.

### 5.3 Servidores y Redes de Comunicaciones

#### *5.3.1 Uso general*

En general, los servidores no deben ser utilizados, ni deben ser instalados en ellos aplicaciones que permitan llevar a cabo actividades propias que se pueden realizar en un puesto de trabajo del usuario, en concreto:

- Uso de herramientas ofimáticas para la elaboración de documentación.
- Almacenamiento de cualquier tipo de archivos no relacionados con los servicios prestados: documentación, software, etc.
- Uso de Internet, entendiendo como tal cualquier acceso externo a páginas Web, Chat, IRC, Telnet, FTP, Videoconferencia, mensajería electrónica, etc. no autorizados
- La descarga de Internet de cualquier tipo de archivos.

Estas actividades se deben realizar por tanto, en el puesto de trabajo habitual del que dispone el empleado a tal efecto.

*5.3.2 Uso aceptable*

- Se utilizará la infraestructura de red y los servidores para la generación e intercambio de información, cuyo contenido esté relacionado con el desempeño de sus funciones: administración, operación, desarrollo de los servicios y actividades del Gobierno Regional y de la infraestructura que los soporta.

- Se deberá utilizar eficientemente con el fin de evitar en la medida de los posible la congestión de los mismos

*5.3.3 Uso no aceptable*

No está permitido, el uso de los servidores y demás equipamiento que mantiene los servicios del Gobierno Regional para:

- La instalación y uso de los servidores, o de software de cualquier otro propósito, que no esté relacionado con el servicio prestado, o que pueda causar mal funcionamiento o degradación en cualquier elemento.

- Con fines privados o no estrictamente profesionales.

- La creación o transmisión de material que cause congestión en la red o en los servidores, mediante programas concebidos a tal fin.

- La conexión a los servidores o a la red de cualquier equipo o elemento propio sin aprobación del Encargado de Seguridad.

- El cambio de ubicación o configuración de cualquier elemento de la red o los servidores no contemplada, sin autorización del Encargado de Seguridad

- Realizar escuchas del tráfico que se transmite por la red

- Realizar cualquier tipo de ataque tanto a elementos internos como externos, intentar ganar acceso a facilidades o información para los que no ha sido autorizado y, en general, sobrepasar o anular las protecciones de seguridad establecidas.

- Destrucción o modificación malintencionada de la información de otros empleados o de los servicios.

- Violación de privacidad e intimidad de otros empleados o deterioro de su trabajo

- Provocar daños físicos a equipos o infraestructura de cableado y comunicaciones

Los servidores del Servicio no tendrán permitida la conexión a Internet, a fin de evitar su uso, salvo que sea estrictamente necesario y requerido para el buen funcionamiento del servicio ofrecido, en cuyo caso, se permitirá el acceso exclusivamente hacia o desde aquellos sitios y para aquellos puertos concretos que sean necesarios.

### 5.4 Responsabilidades

Los administradores de sistemas, personal de soporte, CAU, desarrolladores externos e internos, y demás personal con acceso a la información e infraestructura de redes y servidores, son los únicos responsables de los usos que de ellos realicen.

Sólo 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.

## 6. NORMATIVA DE USO DE ORDENADORES PORTÁTILES

**Responsables y Personal:**

| | |
|---|---|
| **Responsable** | Encargo de Seguridad |

### 6.1 Objeto

Establecer las reglas de uso de los ordenadores portátiles, PDA, teléfonos, y cualquier otro dispositivo móvil o portátil de almacenamiento y tratamiento de la información por el personal del Servicio tanto en sus instalaciones e infraestructuras como para la protección de la información almacenada en ellos

### 6.2 Requerimientos generales

- No se podrán tener instaladas y configuradas herramientas destinadas al análisis y/o ataques a la red, a los recursos y a la información que contienen (herramientas de intrusión, escaneado de puertos, ataques de denegación de servicio, análisis de tráfico, etc.)

- No se podrán tener instalados y configurados servicios de red que puedan interferir en alguna forma, directa o indirectamente con los existentes en la red interna del Servicio (servidores de correo electrónico, servidores de direcciones IP (DHCP), servidores DNS, IDS, Proxy, etc.)

- Se usará TCP/IP como único protocolo de comunicaciones, no estando permitido en ningún caso cambiar la configuración de red asignada, en especial la dirección IP del equipo.

### 6.3 Información contenida en los portátiles

Toda la información del Gobierno Regional residente en el portátil que necesite cifrado, estará copiada bajo una misma carpeta que será cifrada al completo, bien haciendo uso del cifrado del sistema operativo o bien utilizando una herramienta específica a tal efecto.

### 6.4 Trabajo en redes externa de comunicaciones

Cuando el equipo portátil tenga que ser conectado a otras redes ajenas y externas a la red de comunicaciones del Servicio (internet en casa, por ejemplo) y contuviera éste información no clasificada como de tipo Pública, será eliminada previamente conforme a la *Normativa de Uso de Discos Extraíbles*, salvo que tenga autorización expresa del propietario de la información.

### 6.5 Medidas de seguridad mínimas en los portátiles

Los equipos portátiles deberán contar con al menos las siguientes medidas de seguridad:

- Cortafuegos personal, adecuadamente configurado para evitar la entrada no autorizada al equipo.

- Antivirus actualizado periódicamente (al menos 1 vez a la semana), tanto motor como el fichero de firmas. Realizar y programar el chequeo periódico de la información del disco.

- Software anti-espía, actualizado periódicamente (al menos 1 vez por semana).
- Inicio de sesión protegido, al menos con usuario y contraseña.
- Configuración de acceso a carpetas y archivos de información del Gobierno Regional sólo a personal debidamente autorizado por el Encargado de Seguridad.
- Sistema operativo y demás software actualizado en cuanto a "parches" de seguridad, siendo recomendable su configuración para actualizarse periódicamente.
- En caso de tener que viajar con el portátil, nunca se facturará con el equipaje

### 6.6 Portátiles de propiedad del Gobierno Regional para uso personal

- Cada ordenador portátil estará asociado a una persona que aceptará conocer las normas de uso normativa de seguridad, siendo responsable de los incidentes que pudieran originarse por una mala práctica.
- No se instalará en el portátil o se ejecutará ningún software que no esté autorizado por la Unidad Informática.
- No se modificará la configuración (hardware o software) del portátil sin autorización del Encargado de Seguridad.
- El portátil es una herramienta personal e intransferible, no debiendo por tanto, permitir el acceso al mismo a otras personas no autorizadas expresamente.
- El usuario vigilará su portátil para que no sea sustraído, no abandonándolo en lugares no protegidos
- En caso de pérdida o sustracción se pondrá inmediatamente en conocimiento del Encargado de Seguridad.
- Se realizarán revisiones periódicas de los equipos con el objeto de examinar las aplicaciones instaladas y registro del sistema operativo, así como comprobaciones del estado del antivirus.

### 6.7 Conexión de equipos portátiles propios a la red del Gobierno Regional

En general, queda prohibida la conexión de equipos propios del usuario a la red del Servicio. Sólo se podrá conectar cuando así lo requiera para el desarrollo de las funciones del personal interno o externo y se obtenga la adecuada autorización y visto bueno del Encargado de Seguridad.

Una vez conectado estará sometido a las mismas medidas y requerimientos de seguridad, monitorización, etc. que el resto de equipos internos, pudiendo ser requerido en cualquier momento por el personal de la Unidad Informática para su revisión.

El personal que no cumpla con estas normas, se le podrá denegar la conexión en cualquier momento y será el único responsable de aquellas infracciones o daños de cualquier tipo originados de forma intencionada, en su equipo.

No se permitirá la conexión de portátiles propios cuando no cumplan con las medidas de seguridad impuestas por el Servicio, cumpliendo al menos las indicadas en la presente normativa y debiendo ser implementadas por el usuario.

## 7. NORMATIVA DE USO Y ACCESO FISICO AL CPD

**Responsables y Personal:**

| | |
|---|---|
| **Responsable** | Responsable de Seguridad |

### 7.1 Objeto

Establecer las reglas de acceso al Centro de Proceso de Datos (CPD) por parte del personal del Gobierno Regional, así como por parte del personal externo.

### 7.2 Introducción

El Centro de Proceso de Datos (CPD) constituye una estancia muy importante y sensible dentro del Gobierno Regional es por ello que deben garantizarse determinadas medidas de seguridad y cerciorarse que sean seguidas por cualquier persona que intente acceder físicamente a ella.

### 7.3 Uso general

- El acceso al CPD debe estar debidamente autorizado por el Encargado de Seguridad el cuál suministrará una llave, personal e intransferible.
- La pérdida de la llave deberá comunicarse inmediatamente al Encargado de Seguridad y proceder a modificar la cerradura con una nueva llave.
- El acceso al CPD por personal ajeno al Servicio o no autorizado deberá ser siempre acompañado por personal autorizado a acceder a la estancia.
- Los armarios de equipamiento permanecerán cerrados con llave.
- El CPD debe mantenerse tan limpio como sea posible. Toda persona que acceda es responsable de dejarlo en las mismas condiciones de limpieza que cuando entró.
- Todo material debe ser desembalado fuera del CPD.

### 7.4 Uso no aceptable

Queda terminantemente prohibido:

- Dejar la llave de acceso al CPD a terceras personas.
- El uso de dispositivos de audio y/o video dentro del CPD, incluido los Smartphone, sin autorización expresa.
- La entrada de comida o bebida al interior del CPD.

## 8. ANEXOS

### 8.1 Uso del Correo Electrónico del Gobierno Regional

La Unidad de Informática entrega dos herramientas de correo electrónico para que los usuarios puedan trabajar tanto 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.
- MS Outlook (trabajo interno o local).

#### *8.1.1 Correo Vía Web*

Es la manera de leer los correos que están llegando al servidor de correos desde fuera de la estación de trabajo asignada en las instalaciones del Servicio. 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.gorearicayparinacota.cl**".

#### *8.1.2 Correo vía Equipos de Escritorio*

La Unidad de Informática sólo admite la instalación del software de lectura de correo MS OUTLOOK de su versión 2007 o superior, lo que significa que cualquier otra herramienta de este tipo no será aprobado por la Unidad y tampoco se le dará soporte

La Unidad de Informática configura 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 MS OOTLOOK es muy sencillo de utilizar. Para acceder a los correo de forma local, se debe hacer doble click sobro el ícono que se encuentra en el escritorio y que como se mencionó anteriormente se encuentra configurado para acceder a la cuenta del usuario.

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

#### *8.1.3 Manejo de archivos adjuntos 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.

### *8.1.4 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 MS OUTLOOK, 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.

### *8.1.5 Listas de Correo*

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.

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, cuanta 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.

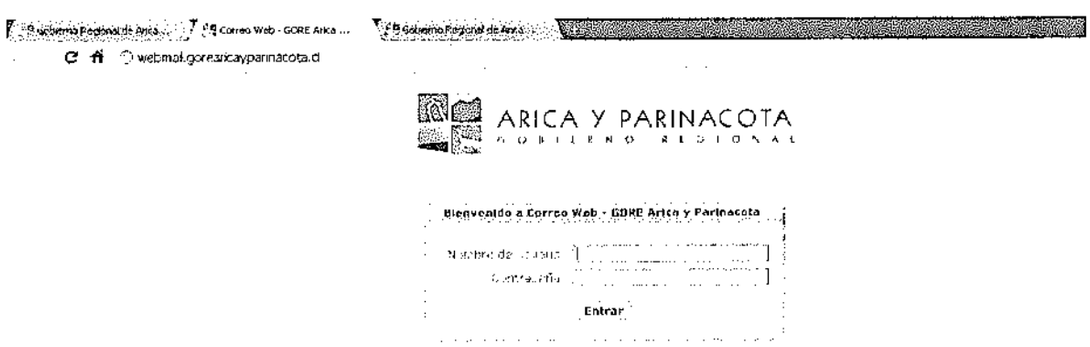
El correo electrónico de esta lista es: funcionarios@gorearicayparinacota.gov.cl

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.

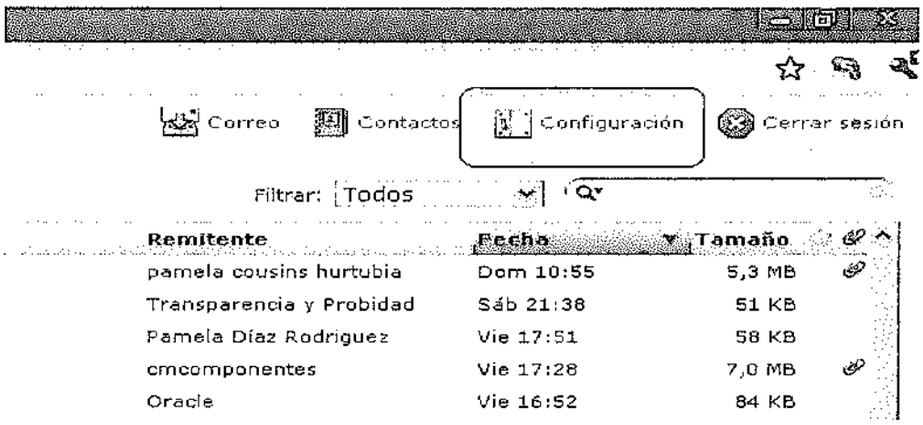
### *8.1.6 Cambio de password del correo*

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.

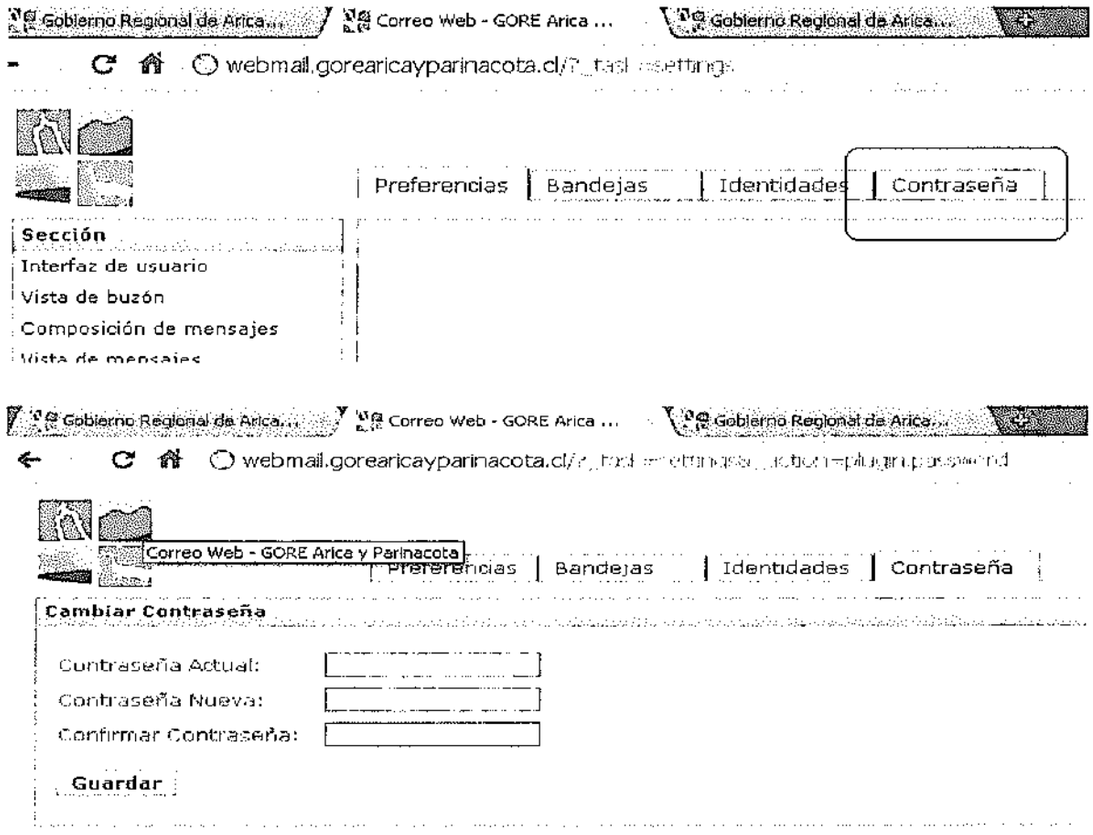
Este cambio se realiza a través del Sitio del Gobierno Regional en el ícono de CORRE WEB. Al pinchar se abre una ventana (ver figura)



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.....




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.



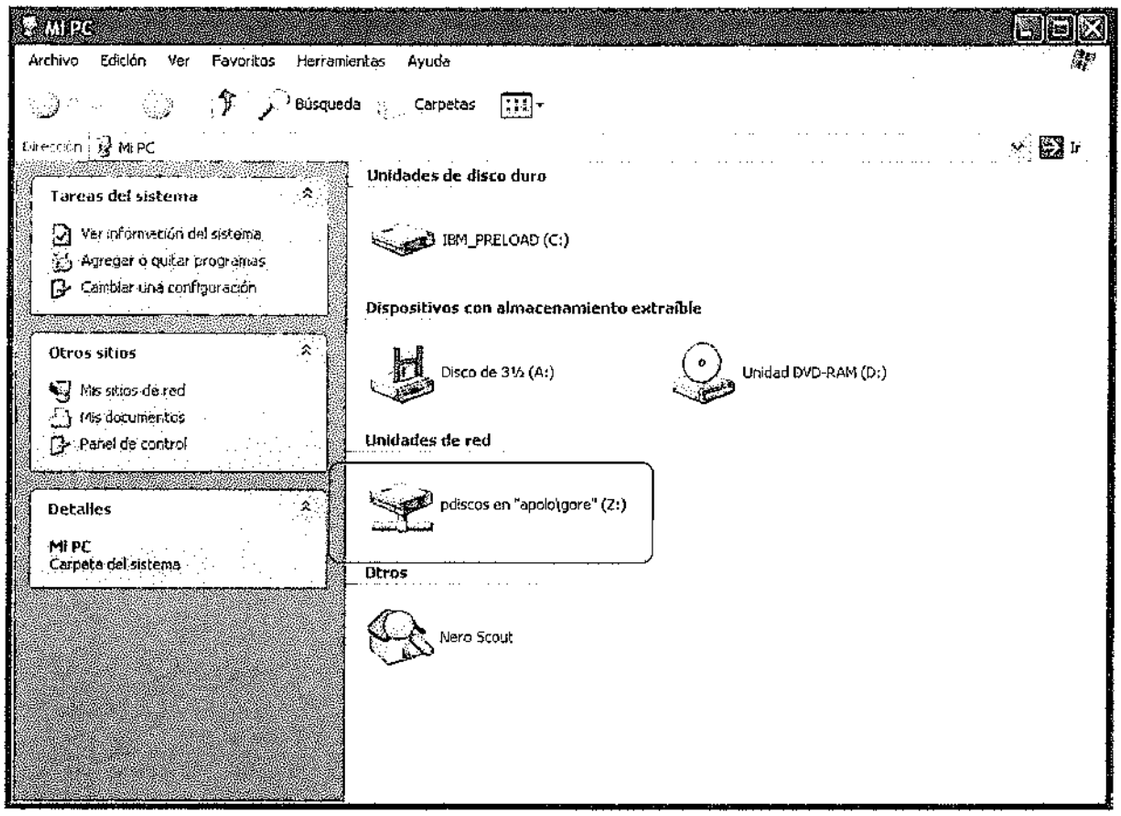

Se debe ingresar la clave actual y luego la nueva clave y confirmarla. Realizado este paso la clave ha sido cambiada y será su responsabilidad mantenerla secreta. Se recuerda a los funcionarios que en caso de olvido de la clave, la Unidad de Informática sólo podrá generar la clave genérica y el usuario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

### 8.2 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 (MP3 u otro formato), fotos y videos.

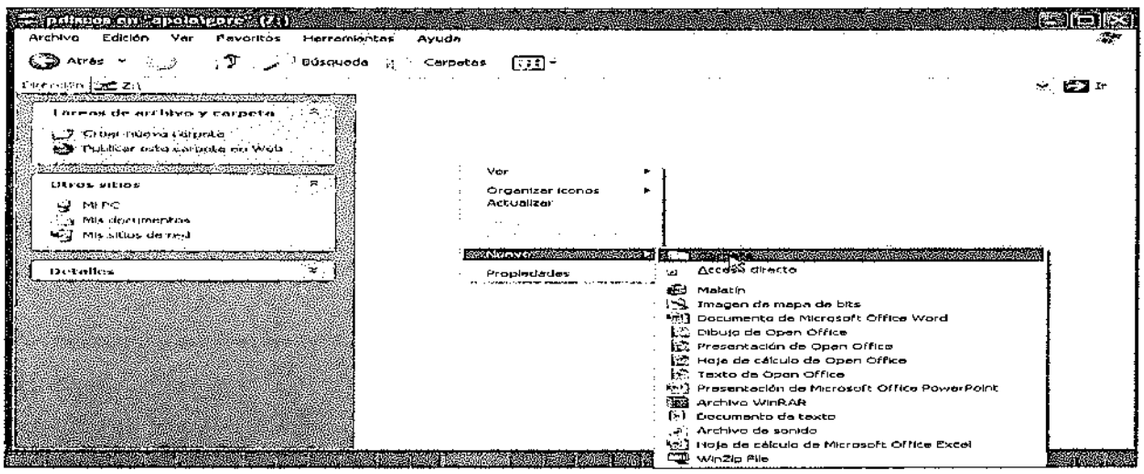
La siguiente pantalla muestra la ventana cuando hacemos doble click sobre el ícono Mi Pc.

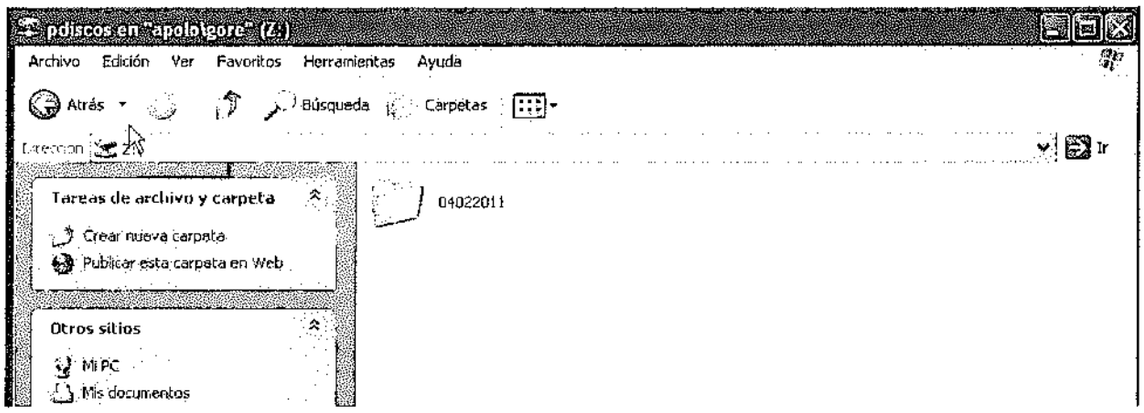



En esta ventana se observa un volumen Z: Esta es la carpeta del servidor donde el funcionario deberá respaldar su información a lo menos **una vez a la semana**.

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)




### 8.3 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, Win 7 Pro.
- Browser de navegación: Mozilla Firefox, Internet Explorer, Google Chrome.

- Software de ofimática: Office 2007 o superior, OpenOffice .
- Lectura de Correo: MS Outlook.
- Manejo de archivos compacatados: WINRAR, WINZIP.
- Lectura de archivos PDF: Adobe Acrobat Reader.
- Grabación de archivos: Nero Smart Suite.

**ANÓTESE Y COMUNÍQUESE.**

GOBIERNO DE CHILE
INTENDENTE
REGION ARICA Y PARINACOTA

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

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