



ARICA Y PARINACOTA
GOBIERNO REGIONAL

**APRUEBA INSTRUCCIONES E IMPLEMENTA
PROCEDIMIENTOS DE SEGURIDAD DE LA
INFORMACIÓN DEL GOBIERNO REGIONAL DE ARICA
Y PARINACOTA.**

RESOLUCIÓN EXENTA Nº 2332/2011

ARICA, 30 DIC 2011

VISTO: La Resolución Exenta Nº233 de fecha 21 de febrero de 2011 que designa funcionarios responsables del Programa de Mejoramiento de Gestión año 2011; La Resolución Exenta Nº 427 de fecha 28 de marzo de 2011 que aprueba Políticas de Seguridad de la Información; Las leyes Números 19.553, 19.882 y 20.212; el Decreto Supremo Número 475 del 6 de mayo de 1998, del Ministerio de Hacienda; el Decreto con Fuerza de Ley Nº29, de 2004, que fija el texto refundido, coordinado y sistematizado de la Ley Nº18.834, sobre Estatuto Administrativo; el Decreto con Fuerza de Ley Nº1, de 2005, que fija el texto refundido, coordinado y sistematizado de la Ley Nº18.757, Orgánica Constitucional de Bases Generales de Administración del Estado; el Decreto con Fuerza de Ley Nº1, de 2005, que fija el texto refundido, coordinado, sistematizado y actualizado de la Ley Nº19.175, Orgánica Constitucional sobre Gobierno y Administración Regional; el Decreto Ley Nº573, de 1974, sobre Estatuto de Gobierno y Administración Interiores del Estado; Ley Nº20.175, que crea la Región XV de Arica y Parinacota y Provincia del Tamarugal, en la Región de Tarapacá; la Ley Nº19.880 que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado; el Decreto Supremo Nº258, del 11 de Marzo de 2010, del Presidente de la República, sobre nombramiento de Intendente Titular en la Región de Arica y Parinacota; lo dispuesto en la Resolución Nº1600, de 2008, que fija el texto refundido, coordinado y sistematizado de la Resolución Nº55, de 992, de la Contraloría General de la República, que establece normas sobre exención de trámite de toma de razón; Ley Nº20.481, de 2010, que establece los Presupuestos del Sector Público del año 2011; y las facultades que envisto como Intendente del Gobierno Regional de Arica y Parinacota.

CONSIDERANDO: La necesidad de establecer procedimientos de control interno en el Servicio que permitan definir límites de seguridad, resguardar los activos entre ellos la información y contribuir al logro de los objetivos estratégicos del Gobierno Regional de Arica y Parinacota

RESUELVO:

APRUEBASE Procedimientos de Seguridad de los bienes y de la información del Servicio Administrativo del Gobierno Regional de Arica y Parinacota que a continuación se indican:

Artículo PRIMERO: pantallas y escritorios limpios

- a) Se deben mantener permanentemente las pantallas limpias de archivos, textos, planillas electrónicos a la vista durante y fuera de la Jornada de trabajo. En la pantalla debe quedar sólo los accesos programas y sistemas autorizados.
- b) Todos los terminales y estaciones de trabajo dispondrán de control de acceso mediante usuario y contraseña, y mecanismos de bloqueo automático tras un período de inactividad del sistema.
- c) Cuando el usuario se ausente de su puesto de trabajo, bloqueará su terminal mediante Control+Alt+Supr, o bien lo apagará directamente la pantalla o el computador.
- d) Los buzones de correo convencional, dispositivos de fax y fotocopiadoras nunca deben quedar desconectados si no poseen algún tipo de protección.
- e) La información impresa será recogida inmediatamente de las impresoras, una vez haya sido enviada a las mismas.
- f) Al terminar la jornada laboral, el empleado recopilará y asegurará el material confidencial, cerrará con llave cajones y oficinas, y desconectará todos los dispositivos y terminales que no vayan a ser utilizados.
- g) Los escritorios o estaciones de trabajo, una vez terminada la jornada, deben quedar libres de documentos, archivos otro con información sensible.
- h) Con carácter general, nunca deben quedar a la vista: nombres de usuario, contraseñas, direcciones IP, directorios, contratos, números de cuenta, listas de clientes, datos de empleados, etc.

Artículo SEGUNDO: Control de registro y perfiles

- 1) El encargado de informática deberá mantener un registro con los sistemas que maneja el Servicio, especialmente aquellos sistemas que se accedan a través de internet.
- 2) Para mantener actualizado este archivo, todos los funcionarios del servicio están obligados a informar a su jefatura directa y al encargado de informática, cuando haya solicitado una pass word en algún sistema nacional o internacional, para gestionar acciones a nombre del GORE.
- 3) Es caso de desvinculación de funcionarios del servicio, el dpto. de RRHH informará por correo institucional al Encarado de Informática, de bloquear la clave del correo y la cuenta del usuario.

Artículo TERCERO: Intranet

A contar del 19 de Diciembre del 2011 con la Resolución exenta N° 2141, entró en uso el sistema documental y control de materiales con los subsistemas de Bienes fungibles y Bienes no financieros. En marcha blanca durante la 2º quincena de diciembre del 2011 y en forma obligatoria a partir del 1º de enero del 2012.

Artículo CUARTO: Control equipos portátiles

- 1º. Los PC's y equipos portátiles que el Servicio pone a disposición de los funcionarios y consejeros, sólo deben ser utilizados para desarrollar las actividades propias de la gestión del Gobierno Regional de Arica y Parinacota.
- 2º. La petición de los equipos informáticos deberá ser formalizada desde la Jefatura requirente por sistema documental a través de Memorándum al Jefe División de Administración y Finanzas. En el caso de los Consejeros Regionales, esta solicitud debe ser realizada por el Secretario Ejecutivo del CORE, el mismo medio.
- 3º. La formalización de la entrega debe ser a través de acta firmada por el Jefe DAF y el usuario del equipo.
- 4º. El uso de cualquier equipo por personal externo al Servicio, debe ser autorizado por escrito del Jefe División.
- 5º. Cada usuario dispondrá de una cuenta personalizada, dotada de los accesos y aplicaciones exclusivamente necesarios para el correcto desarrollo de sus labores profesionales.
- 6º. El usuario no deberá modificar ni vulnerar los permisos procurados por el GORE, especialmente con intención de instalar aplicaciones no relacionadas con el trabajo. En caso de que el usuario estime oportuna la extensión de sus permisos o la instalación de una aplicación específica para llevar a cabo su labor, deberá consultarlo con el Encargado de Informática, quien será responsable de dicho acceso.
- 7º. No se aprobará la instalación de software sin que mediere su correspondiente licencia.
- 8º. El usuario deberá velar por la seguridad y confidencialidad de la información contenida en sus equipos, especialmente cuando se encuentre fuera de las dependencias de la organización. Para ello, cada usuario:
 - a) Debe sustituir las contraseñas que le han sido asignadas por defecto por contraseñas difíciles de adivinar y, en la medida de lo posible, de acuerdo con los criterios de robustez recomendados por la política de contraseñas la organización.

- b) No debe revelar sus contraseñas ni hacer uso de cuentas ajenas, ni siquiera con el permiso expreso del propietario de la cuenta. Las cuentas de usuario y sus contraseñas son personales e intransferibles.
- c) Debe bloquear su equipo cuando vaya a ausentarse de su puesto de trabajo. Se aconseja mantener activado un salvapantallas protegido con contraseña.
- d) Aunque no es recomendable almacenar en el equipo información confidencial o relevante para la organización, dado el caso, deberá asegurarse de que se realizan copias de seguridad de la misma.
- e) La información sensible y confidencial que se encuentre almacenada en los ordenadores portátiles debe ser protegida mediante herramientas de cifrado.
- f) En caso de tener que viajar con el equipo, se debe portar en la mano y guardar en cabina, nunca con el equipaje.
- g) Nunca se debe dejar el portátil desatendido y a la vista del público, especialmente en situaciones que puedan aumentar el riesgo de robo.
- h) En los hoteles, el portátil deberá guardarse en un espacio cerrado bajo llave o en una caja fuerte.
- i) La pérdida del dispositivo informático portátil debe ser notificada inmediatamente a Carabineros e informar al servicio formalmente al Jefe DAF.
- j) Antes de introducir/descargar información en los equipos desde cualquier dispositivo móvil de almacenamiento, éste debe ser examinado por las herramientas antivirus.
- k) Para verificar el cumplimiento de estas obligaciones, así como el correcto funcionamiento de los equipos y el buen uso de los mismos, El Servicio podrá realizar inspecciones y mantenencias periódicas.
- l) Estas revisiones se realizarán tantas veces se estime oportuno. Una vez examinado el equipo del usuario, el contenido no autorizado será eliminado, aplicando en su caso las medidas oportunas consecuentes de no respetar las directrices.
- m) Los equipos deberán ser entregados al usuario en perfecto estado y funcionamiento. Así mismo deberá ser devuelto en buenas condiciones de uso.
- n) En caso de mal funcionamiento, defecto, contenido inapropiado el usuario al recibir el equipo, deberá poner inmediatamente en conocimiento Encargado de Informática, con el fin de solucionar el incidente y que el usuario quede exonerado de toda responsabilidad.

Artículo QUINTO: Supervisión del Instructivo

Este instructivo le corresponderá ser supervisado por el Encargado de Seguridad, quien deberá informar al Sr. Intendente Regional de su cumplimiento.

Artículo SEXTO: Sanciones y responsabilidad administrativa

El incumplimiento de las normas establecidas en el presente instructivo, dará lugar a responsabilidad administrativa y la posterior sanción que deberá establecerse según dicta la normativa vigente.

**Título II
Artículos Transitorios**

Artículo Transitorio Primero: Autorizaciones

Por el solo ministerio de este instructivo, se considerará autorizado a todo aquel sistema de procesamiento que se encuentre instalado en los sistemas computacionales del Gobierno Regional de Arica y Parinacota.

Estos sistemas de procesamiento, serán listados y comunicados a todos los funcionarios del Gobierno Regional, durante el mes de diciembre del 2011.

ANÓTESE Y COMUNÍQUESE



**JOSÉ DURANA SEMIR
INTENDENTE
GOBIERNO REGIONAL DE ARICA Y PARINACOTA**

MPS/CCCH/ASL/asl
Distribucion:
Funcionarios
Encargado SSI - GORE