ARICA Y PARINACOTA

APRUEBA MANUAL DE POLITICAS TI, GOBIERNO REGIONAL DE ARICA Y PARINACOTA

RESOLUCION EXENTA N° 2320

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** Manual de Políticas Ti, para el Gobierno Regional de Arica y Parinacota.

2. En cumplimiento de lo señalado en el Artículo 6 de la Resolución N° 1600 de 2008, de la Contraloría General De La República, se insertan la Política de Seguridad, que por medio de este acto se aprueban, cuyo texto, es el siguiente:

Gobierno Regional Arica y Parinacota: Manual de Políticas TI

ÍNDICE

1. INTRODUCCIÓN

Este documento recoge las Políticas de los Sistemas Tecnológicos (Políticas TI) del Gobierno Regional de Arica y Parinacota como complemento a los siguientes documentos:

- Política de Seguridad de la Información.
- Normas de uso aceptable de la Seguridad de la Información.
- Manual de Procedimientos de Seguridad de la Información 2011-2012 del Gobierno Regional de Arica y Parinacota.
- Manual de Procedimientos TI del Gobierno Regional de Arica y Parinacota.

2. OBJETIVOS

El objetivo de las Políticas presentadas en este documento es lograr establecer las mejores prácticas en la gestión TI en general, incluyendo los aspectos de seguridad y solventar las posibles brechas en la gestión informática.

3. ÁMBITO DE APLICACIÓN

El ámbito de aplicación de las políticas aquí definidas es el mismo que el mencionado Manual de Procedimientos de Seguridad de la Información 2011-2012 del Gobierno Regional de Arica y Parinacota en su apartado *"ÁMBITO DE APLICACIÓN"*.

4. ASPECTOS LEGALES

La legislación aplicable es la contenida en el mencionado Manual de Procedimientos Seguridad de la Información 2011-2012 del Gobierno Regional de Arica y Parinacota en su apartado *"ASPECTOS LEGALES"*.

5. POLITICA – OPERACIÓN Y MANTENIMIENTO POR TERCEROS

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Política de Intercambio de Información. • Manual de Procedimientos de Seguridad de la Información. Apartado 2.1 "Identificación de Riesgos".

5.1. Objetivo

- Garantizar la correcta operación, administración y funcionamiento de los sistemas de procesado de la información en caso de que dependan parcial o totalmente de terceros.

5.2. Identificación de Riesgos del Acceso de Terceras Partes

Previamente a proporcionar acceso a terceras partes a la información del Gobierno Regional, el Encargado de Seguridad y el Responsable del Sistema afectado llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta:

- Tipo de acceso requerido (físico, lógico, y a qué recurso).
- Período de acceso.
- Motivos que solicitan el acceso.
- El valor de la información accedida.
- Controles de seguridad empleados por el tercero.
- Posibles incidencias de este acceso en la seguridad del Servicio.

En todos los contratos cuyo objeto sea la prestación de servicios bajo cualquier modalidad jurídica que deban desarrollarse dentro del Gobierno Regional se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se proporcionará acceso a terceros a la información, a las instalaciones de procesado (Centro de Proceso de Datos o CPD) u otras áreas de servicios críticos, hasta que se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso a los mismos.

5.3. Términos de la contratación

Siempre que se lleve a cabo la contratación de obras o servicios con empresas o terceras personas que supongan el acceso a la información del Gobierno Regional, se llevarán a cabo previamente las siguientes acciones:

- Comprobación de las referencias y experiencias indicadas por la empresa oferente en cuanto a otras obras y servicios similares en otros clientes
- Investigar posibles antecedentes de la empresa en cuanto a incumplimientos o irregularidades anteriores
- Incluir, salvo que no procedan en cada caso concreto, cláusulas específicas de seguridad en el contrato, tales como:
    - De Confidencialidad, en la que se indique el deber de guardar secreto profesional sobre cualquier información a la que tenga acceso, incluso tras la finalización de la relación laboral, esto deberá exigirse además en la contratación de su personal interno o posibles subcontrataciones.
    - La obligación del cumplimiento de las políticas, normas y procedimientos de seguridad establecidas en el Gobierno Regional.
    - Procedimiento para determinar si ha ocurrido algún evento de seguridad así como la obligación de comunicar las incidencias de seguridad detectadas que comprometan los bienes del Gobierno Regional.
    - La protección del equipamiento, soportes e información en las dependencias de terceros y/o en su traslado.
    - En el caso de existir tratamiento de datos de carácter personal se incluirán en el contrato las cláusulas estipuladas para dar cumplimiento a la legislación correspondiente.

- Se incluirá acuerdos de nivel de servicios con los niveles de servicio mínimos a obtener, definiéndose además los controles de seguridad aplicables y las políticas, normas y procedimientos de operación y seguridad a cumplir.
- Derecho a auditar responsabilidades contractuales o surgidas del contrato
- La devolución, a la finalización de la relación laboral, de toda la información y equipamiento del Gobierno Regional en su poder.
- Restricciones a la copia y divulgación de toda información perteneciente y concerniente al Gobierno Regional, así como lo relativo a los derechos de Propiedad Intelectual.
- Responsabilidades relativas a la instalación y mantenimiento de hardware y software

- Incluir, según necesidad, los siguientes controles
  - Acuerdos de control de acceso que contemplen:
    - Métodos de acceso permitidos
    - Proceso de autorización de acceso y privilegios de usuario
    - Requerimientos para mantener actualizada una lista de usuarios autorizados a utilizar los servicios a implementar y sus derechos y privilegios con respecto a dicho uso
  - Procedimiento claro y detallado de la gestión y administración de cambios
  - Métodos y procedimientos de formación a usuarios y administradores en materia de Seguridad de la Información.
  - Controles que garanticen la protección contra software malicioso
  - Métodos empleados para mantener la disponibilidad de los servicios ante la ocurrencia de desastres.

5.4. Outsourcing

En caso de *outsourcing* se deberá tener en cuenta además:

- La planificación de la transmisión de la información y conocimientos necesarios durante el proceso
- Establecimiento de controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Gobierno Regional
- Prever y acordar los pasos necesarios para la recuperación de la información a la finalización del contrato
- Derechos a auditar por parte del Gobierno Regional de forma directa o a través de un tercero subcontratado por el organismo.

5.5. Responsabilidad

Cualquiera que sea el grado de externalización del servicio u operaciones, se nombrará uno o varios responsables de los servicios externalizados en el GORE como responsable de monitorizar y velar por el cumplimiento de los niveles de servicio y seguridad acordados.

5.6. Confidencialidad de la Información

El personal externo que tenga acceso a información del GORE deberá considerar que dicha información, por defecto, tiene el carácter de confidencial.

- Se evitará la revelación, modificación, destrucción o mal uso de la información cualquiera que sea el soporte en que se encuentre contenida.

- Se guardará por tiempo indefinido la máxima reserva y no se emitirá al exterior, información confidencial, salvo que esté debidamente autorizado.

- Se minimizará el número de informes en formato papel que contengan información confidencial y se mantendrán los mismos en lugar seguro y fuera del alcance de terceros.

- Ningún colaborador en proyectos, trabajos puntuales, etc., deberá poseer, para usos no propios de su responsabilidad, ningún material o información propia o confiada al GORE.

- En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado de la empresa proveedora de servicios entre en posesión de información confidencial contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le confiera derecho alguno de posesión, titularidad o copia sobre dicha información. Asimismo, el empleado deberá devolver el o los soportes mencionados, inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación con el GORE.

- Todas estas obligaciones continuarán vigentes tras la finalización de las actividades que el personal externo desarrolle para el GORE.

- La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en los que esté ubicada dicha información, únicamente podrá ser autorizada por el responsable del fichero.

5.7. Intercambio de información

- Ninguna persona debe ocultar o manipular su identidad bajo ninguna circunstancia.

- La distribución de información ya sea en formato digital o papel se realizará mediante los recursos determinados en el contrato de provisión de servicios para tal cometido y para la finalidad exclusiva de facilitar las funciones asociadas a dicho contrato.

- Si el tratamiento de datos de carácter personal se llevase a cabo fuera de los locales donde está ubicado el fichero, dicho tratamiento deberá ser autorizado expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

- La transmisión de datos de carácter personal de nivel alto, a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

5.8. ANEXO – Normas de seguridad en subcontrataciones

5.8.1. Prestación de Servicios al Gobierno Regional

- Los proveedores sólo podrán desarrollar para el Gobierno Regional aquellas actividades cubiertas bajo el correspondiente contrato de provisión de servicios.

- La empresa proveedora informará puntualmente al Gobierno Regional de cualquier cambio (alta, baja, sustitución o cambio de funciones o responsabilidades) que se produzca en las personas que presten los servicios.

- En caso de incumplimiento de cualquiera de las políticas aquí definidas, el Gobierno Regional se reserva el derecho de veto sobre el personal que haya cometido la infracción, así como la adopción de las medidas sancionadoras que se consideren pertinentes en relación a la empresa contratada, y que pueden llegar a la resolución de los contratos que tenga vigentes con dicha empresa.

- Cualquier tipo de intercambio de información que se produzca entre el Gobierno Regional y las empresas proveedoras se entenderá que ha sido realizado dentro del marco establecido por el contrato de provisión de servicios correspondiente, de modo que dicha información no podrá ser utilizada en ningún caso fuera de dicho marco, ni para fines diferentes a los asociados a dicho contrato.

- De forma genérica, los activos incluyen toda forma de información, además de las personas y la tecnología que soportan los procesos de información.

5.8.2. Acceso a los sistemas

- El personal externo que necesite acceder a los sistemas del Gobierno Regional, deberá solicitar credenciales temporales a su contacto o persona que será responsable de la visita dentro del Gobierno Regional. Dicha persona del Gobierno Regional, deberá solicitar las credenciales a la Unidad Informática a través de los cauces oficiales.

- La persona responsable dentro del Gobierno Regional deberá especificar las tareas concretas que realizará la visita y el ámbito de acción, así como la fecha e inicio de los trabajos.

- Queda prohibido comunicar a otra persona el identificador y contraseña que se les haya entregado para acceder a los sistemas del Gobierno Regional así como tenerlo apuntado en sitio visible. En caso de hacerlo, el usuario será responsable de los actos que haya realizado la persona que utilice de forma no autorizada dichas credenciales.

- El usuario está obligado a utilizar al intranet del Gobierno Regional y sus datos sin incurrir en actividades que puedan ser ilegales o ilícitas, que infrinja los derechos del Gobierno Regional o a terceros.

- Está prohibido intentar descifrar claves de otros usuarios.

- Por defecto, está prohibido el acceso de personal externo a sistemas en entornos de producción. Para ello, necesitará una autorización especial por parte del responsable del servicio en cuestión y del responsable de la Unidad Informática del Gobierno Regional.

5.8.3. Soporte y material informático

- Queda prohibido trasladar fuera de las instalaciones del Gobierno Regional soportes o material informático de cualquier tipo sin la expresa autorización del responsable de la visita dentro del Gobierno Regional.

- Está prohibido destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos del Gobierno Regional o de terceros.

5.8.4. Seguridad durante el desarrollo

Todos los proveedores de servicios que impliquen el acceso a los sistemas de información del Gobierno Regional y que realicen actividades de desarrollo de aplicativos deberán garantizar que se cumplen, al menos, las siguientes políticas de seguridad en dicha actividad:

- Se incorporan mecanismos de identificación, autentificación, control de acceso, auditoría e integridad en todo el ciclo de vida de diseño, desarrollo, implementación y operación de los aplicativos.

- Las especificaciones de los aplicativos deberán contener expresamente los requisitos de seguridad a cubrir en cada caso.

- Las aplicaciones que se desarrollen deberán incorporar validaciones de los datos de entrada que verifiquen que los datos son correctos y apropiados y que eviten la introducción de código ejecutable.

- Los procesos internos desarrollados por las aplicaciones deberán incorporar todas las validaciones necesarias para garantizar que no se producen corrupciones de la información.

- Siempre que sea necesario se deberán incorporar funciones de autenticación y control de integridad en las comunicaciones entre los diferentes componentes de las aplicaciones.

- El acceso al código fuente de los aplicativos deberá estar limitado al personal del servicio.

- Durante las pruebas de los aplicativos se verificará que no existen canales de fuga de información no controlados, y que por los canales establecidos sólo se ofrece la información prevista.

- Sólo se transferirán al entorno de producción aquellos aplicativos que hayan sido expresamente aprobados.

6. POLITICA – INTERCAMBIO DE INFORMACIÓN

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Política de Gestión de Soportes. • Política de Operación y Mantenimiento por Terceros. • Manual de Procedimientos de Seguridad de la Información. Apartado 3.2. Clasificación de los recursos informáticos.

6.1. Objetivo

Establecer los criterios para el correcto tratamiento de la información cuando es intercambiada, con el fin de minimizar el riesgo por daños de pérdida, revelación o apropiación indebida. Dentro de la información se incluye también el software.

6.2. Política general de intercambio

La información relacionada con el Gobierno Regional clasificada como *Pública* puede ser conocida y utilizada sin autorización por cualquier persona, pertenezca o no al Gobierno Regional.

La información relacionada con el Gobierno Regional clasificada como de *Uso Interno* puede circular libremente dentro de las instalaciones del Gobierno Regional; fuera de éste sólo para personal autorizado.

La información marcada como *Reservada Secreta* podrá circular libremente por el Gobierno Regional para el personal autorizado, debiendo incluir, antes de mostrar la información propiamente dicha, un listado de las personas autorizadas a acceder a la misma. Las copias que se realicen de este tipo de información deberán estar expresamente autorizadas por el Propietario de la misma y la conformidad del Comité de Seguridad.

6.3. Transporte de la información a través de la red

Toda la información no *Pública*, cuando se transmita por redes inalámbricas deberá ser cifrada. El cifrado debe ser fuerte, al menos cuando la información transmitida sea *Reservada Secreta*.

Toda la información clasificada como *Reservada Secreta* deberá circular cifrada tanto en la red interna como en redes externas o públicas. En cualquier caso, la información *Reservada Secreta* se cifrará cuando circule por redes públicas.

Deberá evitarse la utilización de correo electrónico para transmitir información clasificada como *Reservada Secreta*. En caso de que fuera necesario, se tomarán las medidas de cifrado conforme a lo anterior. Para la información *Reservada Secreta* se habilitarán métodos para confirmar la identidad del destinatario y del remitente del mensaje de correo.

El personal autorizado a tratar información *Reservada Secreta* no podrá transmitirlos ni comunicarlos fuera del Gobierno Regional, en modo alguno (correo electrónico, transferencia de ficheros, soportes magnéticos, teléfono, fax, etc.) a menos que cuente con la autorización del Propietario o Responsable de la Información.

6.4. Acuerdos de Intercambio de Información

Cuando se realicen acuerdos entre el Gobierno Regional y otra entidad, pública o privada, para el intercambio de información se especificará su clasificación, siguiendo los criterios de clasificación de la información recogidos en el *Manual de Procedimientos de Seguridad de la Información* (apartado 3.2) y en cada caso se tendrán en cuenta los siguientes aspectos:

- Establecer un procedimiento para notificación de información, tanto al enviar como al recibir.
- Normas técnicas sobre cómo empaquetar y transmitir.
- Responsabilidades y pérdidas en caso de pérdidas de información.

6.5. Borrado de la Información

El borrado o destrucción de la información clasificada deberá realizarse conforme a lo establecido en la *Política de Gestión de Soportes*.

6.6. Consideraciones legales. Datos de Carácter Personal

Además de lo expuesto en los apartados anteriores, se debe considerar que los ficheros que contengan datos de carácter personal están regulados por la Ley 19.629 sobre la protección de la vida privada o protección de datos de carácter personal, de modo que es obligatoria la aplicación de las correspondientes medidas de seguridad sobre estos datos.

El personal del Gobierno Regional que por razones del desarrollo de su actividad laboral tengan acceso a dicha información, deben estar informados del contenido de dicha Ley y de sus obligaciones al respecto.

6.7. Tratamiento de la información por terceros

El personal externo subcontratado que trabaje para el Gobierno Regional, así como el perteneciente a empresas terceras y demás profesionales, sólo podrá tratar aquella información imprescindible para el desarrollo de sus funciones en la relación laboral que mantenga con el Gobierno Regional, durante el tiempo que esta perdure. Para información clasificada como de *Uso Interno* o superior estará sometido a las condiciones de confidencialidad estipuladas (*Política de operación y mantenimiento por terceros*).

Sin perjuicio de lo anterior, y en general, podrán tratar la información clasificada con nivel igual o inferior a de *Uso Interno*. Para clasificación superior, o datos de carácter personal, deberán estar expresamente autorizados por el Propietario de la Información. Se exigirá en el contrato con terceros que a la finalización de la relación laboral, se haga entrega de toda información de clasificación superior a Uso Público del GORE en su poder, y la eliminación de toda copia de la que pudiesen disponer.

6.8. Información en soportes en tránsito

En general, los soportes informáticos se almacenarán y transportarán de manera segura para garantizar la confidencialidad, disponibilidad e integridad de la información contenida en los mismos, conforme a la *Política de Gestión de Soportes*.

Toda información clasificada con nivel igual o superior a *Reservada Secreta*, incluidos los datos de carácter personal, que sea copiada a soportes de información, incluyendo las estaciones de trabajo del personal o cualquier otro soporte sin las medidas de seguridad adecuadas, deberá ser cifrada, al menos cuando estos vayan a salir de las dependencias del Gobierno Regional.

6.9. Fotocopias, impresión y uso del fax

Deberá evitarse el envío de información *Reservada Secreta* por fax. No obstante, cuando se deba enviar, y excepto para información de Uso Público, será necesario ponerse en contacto con el receptor para quedar a una hora concreta para el envío, de manera que lo recoja inmediatamente en destino. Lo mismo será aplicable cuando se envíe a una impresora en red.

Siempre que se use fax, fotocopiadora o impresoras se debe asegurar que éstas no retienen copia en memoria, de forma que se permita de nuevo su envío, copia o impresión.

7. POLITICA – GESTION DE SOPORTES

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Procedimiento de Etiquetado y Clasificación de Activos • Política de Seguridad Física de los Equipos • Política de Copias de Seguridad • Procedimiento de Gestión de Soportes • Procedimiento de Salida de Información y Entrada/Salida y Traslado de Soportes/Equipos. • Manual de Procedimientos de Seguridad de la Información. Apartado 3.3. Procedimientos Específicos - Rotulado de la Información e Inventario de Activos.

7.1. Objetivo

Medidas necesarias para la correcta manipulación y gestión de los soportes de información, incluido papel, minimizando el riesgo de daños de pérdida, revelación o apropiación indebida de la información contenida en ellos.

7.2. Tipo de soportes

Los soportes empleados para las copias de seguridad deben ser estándares en cada momento, de modo que se facilite la recuperación de la información contenida en los mismos en otros sistemas, si no es posible disponer del sistema original.

7.3. Etiquetado (Rotulado)

Los soportes de copias de seguridad serán etiquetados e inventariados conforme a las directrices del Procedimiento de Rotulado de la Información e Inventario de Activos del Manual de Procedimientos de Seguridad de la Información. En concreto, serán etiquetados e inventariados mediante la propia herramienta automatizada de copia de seguridad que tenga el Gobierno Regional, la cual incluiría toda la información necesaria para su correcta identificación, localización y gestión.

Aquellos soportes que contengan ficheros con datos de carácter personal deberán informar de ello en la etiqueta.

7.4. Almacenamiento

Para los soportes que estén almacenados por largos periodos de tiempo, antes de su utilización y periódicamente se debe comprobar el tiempo medio de vida del soporte, de manera que se deseche cuando se estime que puede estar cerca de alcanzarse.

Deberán estar adecuadamente protegidos conforme a la *Política de Seguridad Física del Equipamiento* y contra acceso físico no autorizado.

Se mantendrán soportes de copias de seguridad en dos lugares distintos y a ser posible no sometidos a los mismos riesgos de seguridad, con copias de la información iguales o al menos, realizadas en turnos alternos, en cada uno de ellos.

Cuando se trate de información Reservada Secreta en papel, incluidos los datos de carácter personal, esta debe almacenarse en un armario o similar, con llave o medidas de protección contra apertura.

7.5. Traslado

Para el traslado de los soportes de las copias de respaldo fuera de las instalaciones del Gobierno Regional deben contemplarse las medidas de transporte adecuadas según la *Política de Seguridad Física del*

Equipamiento. Será condición indispensable que el lugar de destino de los soportes disponga de condiciones de seguridad físicas similares al de origen. Cualquier salida de soportes de las instalaciones, con información no pública, deberá ser autorizada por el Propietario de la Información contenida en ellos y registrado utilizando siempre un medio de transporte o servicio de mensajería confiables en el caso de información física.

7.6. Baja

Se eliminará la información de los soportes que vayan a ser reutilizados conforme al procedimiento asociado. Los soportes que sean desechados definitivamente serán destruidos físicamente.

Toda documentación impresa, cuya información sea confidencial o contenga datos de carácter personal, debe ser destruida empleando un sistema que impida la recuperación de su contenido.

Para la destrucción de documentación en formato electrónico/magnético, con información Reservada Secreta o que contenga datos de carácter personal, será necesario realizar un borrado físico y seguro de los datos, de modo que no pueda recuperarse la información.

Los soportes con información del GORE, incluidos documentos en papel, que puedan poseer colaboradores o terceras empresas, como consecuencia de una relación laboral, serán devueltos en su totalidad a la finalización de esta, para que el GORE proceda a su almacenamiento o destrucción según convenga. En el caso de que existan soportes informáticos propiedad de aquéllos, deberán realizarse un borrado físico seguro de toda la información. Esto será aplicable a toda la información "no pública".

8. POLITICA – SEGURIDAD FISICA

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Normativa de Uso y Acceso Físico al CPD • Procedimiento Control de Acceso Físico al CPD • Manual de Procedimientos de Seguridad de la Información. Apartado 5.1. Tipos de Seguridad y 5.2. Procedimientos Específicos.

8.1. Objetivo

- Proteger adecuadamente los lugares físicos donde residen los elementos que mantienen y procesan la información crítica o sensible contra incidentes o ataques intencionados.
- Prevenir e impedir el acceso no autorizado y/o daños físicos a las sedes e instalaciones del Gobierno Regional.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que almacena la información del Gobierno Regional.
- Implementar medidas para proteger la información utilizada por el personal en sus funciones habituales.

8.2. Alcance

Esta Política se aplica a todos los recursos físicos relacionados con los sistemas de información del GORE.

8.3. Responsabilidades

El Encargado de la Unidad Informática junto con el Encargado de Seguridad y los Responsables de los Sistemas definirán las medidas de seguridad física para proteger los activos críticos.

El Encargado de la Unidad Informática junto con el Encargado de Seguridad definirán además, las medidas de seguridad física de las áreas protegidas (CPD y ubicaciones de elementos de comunicaciones, principalmente) y coordinará su implementación.

Se tendrán en cuenta las mejores prácticas internacionales reconocidas en seguridad de la información (ISO 27002, BS2599).

8.4. Seguridad de las áreas críticas del GORE

Los sistemas de información del Gobierno Regional deberán estar situados en áreas o salas protegidas con las adecuadas medidas de protección: acceso, desastres naturales, alteraciones del entorno, ataques, robo, etc.

El Gobierno Regional utilizará los llamados perímetros de seguridad para proteger las áreas de procesamiento de información críticas, de suministro eléctrico, de aire acondicionado y cualquier otra área necesaria para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad queda limitado por una barrera, por una pared, una puerta de acceso controlada, un mostrador de recepción, etc.

Se tendrán en consideración y se implementarán los siguientes controles, según corresponda:

- Las áreas deberán tener asignado un responsable claramente identificado
- Las salidas de emergencia deben tener alarmas, audibles y monitorizadas, preferiblemente funcionando con alimentación de energía ininterrumpida y los incidentes de alarma deben ser investigados en todos los casos. Periódicamente debe realizarse y documentarse una verificación de que las alarmas de salida de emergencia están funcionando correctamente
- Habilitar algún sistema de detección de intrusos: detección de apertura de puertas y ventanas no autorizadas, cámaras de video-vigilancia, detectores de movimiento, etc.
- Las salas deberán estar alejadas de pasos de agua, gas, materiales inflamables, ruidos y vibraciones.
- Las ventanas, al igual que las puertas deberán estar construidas con materiales adecuados y resistentes a vandalismo.
- Se deberá contar con sistemas de climatización adecuado que controle las medidas de humedad y temperatura, adecuadamente revisado y mantenido
- Ante riesgos de daños por agua, se deben implementar las medidas compensatorias adecuadas, como detectores de humedad o fugas de agua en los lugares adecuados (techo, suelo, paredes, etc.), techo impermeable, falso suelo para elevación de los equipos, disponer de bombas de extracción, etc.
- Cumplir las normativas y legislación aplicable contra incendios: disponer de mecanismos de extinción, respetar las normas de seguridad de las personas, construcciones con materiales incombustibles, extintores con sus normas de uso, etc. Todo el sistema deberá estar certificado y periódicamente revisado.
- Las salas no deben tener identificación alguna visible desde el exterior de su contenido o cometido.
- Se prohibirá al personal comer o beber dentro de las salas, así como, salvo autorización, el uso de dispositivos fotográficos o de grabación de video.
- No estará permitido el almacenamiento de material dentro de la sala (excepto el imprescindible), como papel, equipos obsoletos o de reserva, cableado, etc.

El Encargado de Seguridad llevará un registro actualizado de los sitios protegidos, indicando al menos:

- Identificación del Edificio y Área
- Mapa de ubicación

- Principales elementos a proteger
- Medidas de protección física implantadas

8.5. Acceso físico al CPD

Las salas en las que se encuentran los sistemas de información del Gobierno Regional, estarán considerados como zonas críticas de acceso controlado y restringido exclusivamente a personal autorizado, teniendo en cuenta los siguientes controles:

- El personal sólo podrá acceder a ellas con la finalidad de efectuar las actividades propias de administración, operación y mantenimiento de los equipos que contienen. Así mismo, estará permitido el acceso para realizar tareas de mantenimiento y limpieza de salas, pero siempre supervisado.
- El acceso deberá estar controlado con un mecanismo físico (tarjeta de acceso, control biométrico, botonera, etc.) que permita su identificación unívoca. El acceso debe quedar registrado, ya sea concedido o denegado (Ver el *Procedimiento Control de Acceso Físico al CPD*)
- En caso de que el mecanismo anterior no sea posible se utilizará una llave la cual deberá permanecer vigilada en todo momento y conocer el número de copias existentes y quién es el propietario o responsable de las mismas.
- Las personas que no dispongan de autorización permanente de acceso a dichas zonas, incluido el personal esporádico de mantenimiento y limpieza de la sala y que necesite entrar temporalmente por causa justificada, deberá obtener una autorización temporal previa y ser acompañada durante toda su estancia por personal con acceso autorizado que supervisará en todo momento el trabajo del anterior.
- El acceso a las salas sólo será posible desde las áreas del edificio a las cuales el público en general no tiene acceso.
- Revisar y actualizar cada 6 meses (máx.) los derechos de acceso a las áreas protegidas.
- Revisar periódicamente los registros de acceso a las salas y áreas protegidas.

9. POLITICA – SEGURIDAD FISICA DE LOS EQUIPOS

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Política de Seguridad Física • Política de Gestión de Soportes • Procedimiento de Baja de Equipos/Soportes y destrucción de su información • Procedimiento de salida de información y entrada/salida y traslado de soportes/equipos • Manual de Procedimientos de Seguridad de la Información. Apartado 5.1. Tipos de Seguridad y 5.2. Procedimientos Específicos.

9.1. Objetivo

- Protección física adecuada del equipamiento para evitar su pérdida, deterioro o cualquier daño físico que pueda afectar a la disponibilidad y correcto rendimiento.

9.2. Ubicación y protección de los equipos

Los equipos críticos serán ubicados y protegidos de manera que se reduzcan los riesgos debidos a amenazas y a peligros ambientales. Para ello:

- Los equipos se ubicarán en lugares donde se minimice el acceso innecesario existiendo un control de acceso adecuado.
- Adoptar los controles adecuados para minimizar los riesgos de amenazas potenciales tales como: robo o hurto, explosivos, incendios, polvo, etc.
- Revisar periódicamente las condiciones ambientales para verificar que las mismas no afecten de manera adversa el funcionamiento de las instalaciones.

9.3. Suministros de Energía

Los equipos deberán estar protegidos ante fallos en el suministro de energía u otras anomalías eléctricas. El suministro de energía seguirá en todo momento las especificaciones del fabricante o proveedor de cada uno de los equipos contemplándose las siguientes medidas de control:

- Ubicar interruptores de emergencia cerca de las salidas de las salas donde se encuentran los equipos a fin de facilitar un corte rápido de suministro eléctrico en caso de producirse una situación crítica.
- Proveer de iluminación de emergencia en caso de producirse un fallo en el suministro principal de energía.
- Utilizar UPS para asegurar el apagado regulado y sistemático, o bien asegurar la ejecución continua de los equipos, sobre todo de aquellos que realizan tareas críticas.
- Revisar y probar periódicamente los UPS para asegurar que funcionan correctamente y que tienen las autonomías necesarias
- Los UPS deberán contar con alarmas sonoras de estado y ser revisados periódicamente por el personal encargado de este tipo de elemento
- Si se detectaran fallos continuos y prolongados del suministro eléctrico, se instalará un generador de respaldo o grupo electrógeno con el correspondiente suministro de combustible para garantizar que dicho generador pueda funcionar por un periodo amplio. Si el encendido del generador no fuera automático, se asegurará que el tiempo de funcionamiento de los UPS permita el encendido manual del mismo.
- Revisar y probar periódicamente los generadores para asegurar que funcionan correctamente.

9.4. Seguridad del cableado

Todas las instalaciones de cableado de datos deberán realizarse por empresas y personal debidamente certificado. Tras la instalación deberán realizarse mediciones y entregarse un certificado como prueba de que se cumplen todos los requisitos para su correcto funcionamiento.

Antes de realizar la instalación de cableado se realizará un estudio previo de trazado. Las canalizaciones de datos deben realizarse independientes de las de cableado de corriente eléctrica y lejos de las zonas con posibles interferencias electromagnéticas. Así mismo, debe evitarse, que estén a la vista o fácilmente accesible a personal no autorizado.

Los armarios de cableado y comunicaciones deben estar en zonas protegidas con acceso controlado y cerrados con llave.

9.5. Mantenimiento y manipulación de equipos

Se realizará un mantenimiento de los equipos de tipo medio para asegurar su disponibilidad e integridad permanente. De este modo:

- Se someterá al equipamiento a tareas de mantenimiento preventivo, conforme a los intervalos de servicio y especificaciones recomendadas por el proveedor y con la autorización formal del Encargado de la Unidad Informática.

- Aquellos equipos cuyo coste o necesidad de disponibilidad lo justifiquen deberán estar protegidos con un contrato de mantenimiento, reparación y/o sustitución en un tiempo máximo determinado con el proveedor o fabricante de los mismos.

- Se recomienda el establecimiento de un sistema de renovación o actualización periódica con el proveedor o fabricante.

- Sólo el personal autorizado, o bien de mantenimiento del proveedor, podrá manipular físicamente los equipos

- Deberá registrarse toda salida de equipamiento fuera de las instalaciones del Gobierno Regional para su mantenimiento. Se eliminará toda información confidencial que pueda contener el equipo, haciendo copia de seguridad si es necesario, previamente a la salida de las instalaciones del Gobierno Regional.

9.6. Seguridad del equipo fuera de las instalaciones

El uso de equipamiento para la realización de tratamiento de información fuera del ámbito del Gobierno Regional deberá quedar autorizado por el Jefe del trabajador que lo requiera, informando éste además al Encargado de Seguridad. En cualquier caso, la seguridad a aplicar deberá ser equivalente a la proporcionada dentro del Gobierno Regional para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera del mismo.

9.7. Baja de equipos

Se habilitarán los métodos adecuados para eliminar, de forma no recuperable, toda la información sensible o crítica de los equipos o soportes que causen baja y vayan a ser desechados o destinados a otra finalidad. Se eliminarán tanto software como datos o posibles configuraciones lógicas existentes de acuerdo al *Procedimiento de Baja de Equipos/Soportes y destrucción de su información*.

9.8. Traslado de equipos

Ni los equipos, ni la información, ni el software serán retirados de las correspondientes sedes del Gobierno Regional sin autorización formal.

Antes de realizar el traslado de equipos se tomarán las adecuadas medidas de protección contra golpes, utilizando para ello embalajes con protección, identificación exterior de "muy frágil", transporte adecuado, etc.

Se tomarán medidas contra robo utilizando contenedores con apertura protegido y/o personal especializado presente durante todo el traslado.

Se respetarán en todo momento las instrucciones del fabricante respecto del cuidado del equipo, así como se mantendrá una adecuada cobertura de seguro para proteger el equipamiento fuera del ámbito del Gobierno Regional cuando sea conveniente.

Los dispositivos portátiles, cuando estén fuera de las instalaciones del Gobierno Regional o en lugares de acceso libre no se abandonarán en ningún momento. En cualquier caso, la salida de este tipo de equipos deberá estar autorizada y registrada, y en el caso de que el equipo almacenara información clasificada deberá ser aprobado por el propietario de la información.

Cuando la salida de los equipos sea por motivos de mantenimiento, se eliminará previamente toda su información almacenada.

En el *Procedimiento de salida de información y entrada/salida y traslado de soportes/equipos* se presentan los detalles para el traslado del equipamiento.

9.9. Política de Escritorios y Pantallas Limpias

Se debe adoptar una política de escritorios limpios para proteger los documentos en papel y los dispositivos que almacenen información temporal, así como una política de pantallas limpias en las instalaciones del Gobierno Regional con el objetivo de reducir los riesgos de acceso no autorizado, pérdida de la información, durante y fuera del horario laboral.

Se instaurarán los siguientes controles:

- Los documentos en papel y los portátiles se almacenarán bajo llave sobre todo fuera de horario laboral
- Se guardará bajo llave la documentación sensible o crítica del Gobierno Regional, preferiblemente en caja fuerte o armario ignífugo, cuando no esté en uso.
- Se apagarán completamente los ordenadores asignados a funciones críticos cuando estén desatendidos por un periodo de tiempo largo, en caso contrario y ante la ausencia del trabajador, deberá bloquearse automáticamente la pantalla.
- Se protegerán los puntos de recepción y envío de correo postal y las máquinas de fax no atendidas continuamente.
- La información sensible o confidencial se retirará inmediatamente una vez impresa.

10. POLITICA – ACEPTACION DE NUEVOS PRODUCTOS Y SISTEMAS

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Procedimiento de Aceptación de Nuevos Sistemas y Productos.

10.1. Objetivo

- Asegurar que el producto o servicio entregado al Gobierno Regional cubre los requisitos de negocio que propiciaron su creación, ya sea el producto o servicio adquiridos o desarrollados internamente.

10.2. Introducción

Cuando se pongan en marcha los proyectos para el desarrollo e implantación de nuevos sistemas, o ampliación/mejora de los ya existentes, además de las actividades tradicionales de cada una de las fases de éstos, se llevarán a cabo igualmente, al inicio y durante el desarrollo, las actividades para determinar e implementar los requerimientos necesarios.

Cuando se vaya a adquirir un producto, se establecerán igualmente, los requerimientos que debe cumplir, y se revisará dicho cumplimiento antes de su compra asegurando que están alineados con el negocio del Gobierno Regional.

10.3. Desarrollo de nuevos sistemas. Análisis y especificación de Requerimientos.

Se determinarán los requerimientos que se van a requerir por el servicio a prestar, dependiendo de la naturaleza del sistema a desarrollar. Se establecerán teniendo en cuenta las necesidades reales del servicio teniendo en cuenta las componentes de funcionalidad, seguridad, usabilidad y accesibilidad.

Se realizará un catálogo de requisitos que contendrá todos los servicios del sistema a desarrollar o adquirir.

En la fase de diseño se introducirán las pruebas a someter al producto final para su validación. Esta actividad es primordial en esta fase del proyecto, ya que el coste de re-trabajo debido a errores en el código, se reduce considerablemente cuando las pruebas del sistema (trazadas con los requisitos) se tienen en cuenta en la fase de diseño. Se llevará a cabo la definición de la arquitectura de seguridad a utilizar en el sistema.

Tras la implementación del sistema, se llevarán a cabo pruebas de validación del sistema desarrollado. Dichas pruebas deben cubrir el 100% de los requisitos definidos.

10.4. Adquisición de nuevos sistemas/productos

Se determinarán los requerimientos que debe cumplir el producto, dependiendo de su naturaleza. Se establecerán teniendo en cuenta los objetivos de negocio que afecta al servicio para el que va a ser desarrollado.

Se llevarán a cabo pruebas sobre el producto para comprobar que se cumplen todos los requerimientos antes identificados, los casos de pruebas cubrirán el 100% de los requisitos.

Se realizará un informe en el que se incluyan las pruebas realizadas y el resultado de los mismos.

Cuando el producto no cumpla los requerimientos, sólo se adquirirá cuando se haya aceptado el riesgo (por parte de su Propietario) o se hayan definido los controles compensatorios que se pueden implementar (y la conveniencia de ello) para mitigarlo.

10.5. Aprobación del sistema o aplicación

Una vez finalizadas las pruebas, y antes de la compra en su caso, y de la puesta en marcha del sistema, el Propietario o Responsable deberá aprobarla, teniendo en cuenta los riesgos residuales que hayan resultado.

10.6. Responsabilidades

Del Responsable del servicio a desarrollar, a adquirir..:

- Establecer los requerimientos del sistema o producto.
- Aprobar, junto con el Propietario, las pruebas a ser ejecutadas sobre los nuevos sistemas.

Del Propietario del sistema:

- Aprobar, junto con el Responsable del servicio, las pruebas para los nuevos sistemas.
- Responsable último de la funcionalidad del sistema obtenido.

11. POLITICA – COMUNICACIÓN Y GESTION DE INCIDENTES

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Manual de Procedimientos de Seguridad de la Información: o Apartado 6.1. "Procedimientos y Responsabilidades Operativas-Procedimientos de Manejo de Incidentes." o Apartado 7.2. "Monitoreo del acceso y uso de los sistemas". o Capítulo IX. "Dominio de Incidentes en la Seguridad de la Información". • Procedimiento de Comunicación, Gestión y Respuesta ante Incidentes.

11.1. Objetivo

- Asegurar que los incidentes y debilidades detectadas en los sistemas de información son gestionados y comunicados adecuadamente, de forma que se puedan tomar a tiempo las acciones correctivas adecuadas, evitando así, posibles daños.

11.2. Detección y deber de comunicación

Todos los incidentes y vulnerabilidades de seguridad detectados por el personal deben ser comunicados lo más rápidamente posible y por los canales adecuados. Esta es una obligación de todos, tanto personal interno, como externo o contratas.

Se establecerá en los contratos con terceros la obligación y los medios para la comunicación y gestión de las incidencias de seguridad.

Adicionalmente a los incidentes y vulnerabilidades que el personal pueda detectar de forma manual, deberán establecerse siempre que sea posible, los mecanismos y herramientas para su detección automática o ayudar en su detección manual, especialmente en entornos de sistemas críticos. El objetivo de estas herramientas será la detección temprana de incidentes de seguridad mediante la recolección y análisis de todos los eventos que ocurren en los sistemas.

Se definirán los procedimientos a seguir para la comunicación y gestión de incidencias, incidentes y vulnerabilidades, garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad

Los procedimientos de comunicación serán distribuidos a todos los empleados del Gobierno Regional, trabajadores externos y terceras partes en el ámbito de esta política. Deberá ser bien conocido por todos ellos, estableciendo programas de formación y concienciación en caso de ser necesario.

Así mismo, los procedimientos de gestión serán distribuidos a todo el personal implicado en dicha gestión, según sus funciones y el tipo de incidente a tratar, y serán igualmente, bien conocidos por todos ellos.

11.3. Comunicación

Los procedimientos de comunicación establecerán y detallarán entre otros aspectos:

- Los métodos y canales a utilizar para la comunicación, incluyendo las confirmaciones necesarias para asegurar que la comunicación ha sido efectiva.

- Personas de contacto (cada persona deberá conocer el "punto de contacto" asignado para la comunicación).

11.4. Gestión de incidencias

Los procedimientos de gestión deberán contener los posibles tipos de incidencias/incidentes y las acciones a llevar a cabo para cada uno de ellos. Entre estas, deberán encontrarse las siguientes:

- Identificación y análisis de la causa de incidente.
- Recolección de evidencias con calidad suficiente, y mantenimiento y protección de éstas, especialmente cuando el incidente pueda conllevar acciones legales. En este caso, se deberán mantener de forma que resulten admisibles en posibles procesos posteriores, de acuerdo con la ley.
- Contención del incidente.
- Si fuese necesario, planificación e implementación de las acciones correctivas para evitar que se repita.
- Escalado a seguir (persona o grupo de gestión de siguiente nivel) cuando sea necesario.
- Puesta en conocimiento de las autoridades pertinentes, en su caso.

Cuando la naturaleza del incidente o de los daños causados adquiera relevancia, se pondrá en conocimiento del Comité de Seguridad, quien decidirá las siguientes acciones a realizar, así como la naturaleza y destinos de las comunicaciones que se llevarán a cabo sobre el mismo.

11.4.1. Cierre

Cuando se finalice la gestión de un incidente se dará a conocer su cierre de forma retroactiva a todos los participantes en su gestión, en sus distintos niveles de escalado y hasta al origen de la comunicación, así como a las personas afectadas por ella. Sólo cuando se estime oportuno, se comunicará también el resultado y acciones llevadas a cabo.

11.4.2. Registro

Todas las acciones y cambios llevados a cabo en el tratamiento de los incidentes y vulnerabilidades deberán registrarse y revisarse posteriormente, de forma que sirvan como modo de aprendizaje y se pueda evitar que ocurran de nuevo.

11.4.3. Indicadores

Se establecerán los indicadores necesarios para conocer y medir el volumen, tipo, origen, destino y coste de los incidentes de seguridad, de forma que ayude en la toma de decisiones y a efectos de establecer la necesidad de mejora o agregar controles para limitar la frecuencia, daño y costes.

12. POLITICA – COPIAS DE SEGURIDAD

Responsable

Responsable	Encargado de la Unidad Informática

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Documentos	
Políticas, Procedimientos, Normas	• Manual de Procedimientos de Seguridad de la Información o Apartado 6.2. "Mantenimiento-Resguardo de la Información". o Apartado 3.2. "Clasificación de los recursos informáticos".

	• Política de Gestión de Soportes. • Política de Comunicación y Gestión de Incidencias. • Procedimiento de Copias de Seguridad (BackUp) y de Restaurado de la Información.

12.1. Objetivo

- Evitar la pérdida, ante incidentes, de la información de que se dispone de, así como tener la posibilidad de recuperarla y ponerla de nuevo disponible para los sistemas de procesamiento o las personas.

12.2. Introducción

En esta política deben incluirse todos los sistemas involucrados en el GORE. Dependiendo de la arquitectura de cada sistema y las funciones que desempeñe, deben adaptarse los procedimientos empleados: *Procedimiento de Copias de Seguridad (backup) y Procedimiento de Restaurado de Información* para llevar a cabo las copias de respaldo así como la recuperación de la información.

12.3. Planificación

Atendiendo a la importancia de la información contenida en cada sistema, a su criticidad y a las características de aquéllos, se elaborará una planificación de copias de seguridad donde deben incluirse todos los sistemas existentes en el momento y permitir una fácil escalabilidad para contemplar la incorporación de sistemas futuros.

La periodicidad máxima de realización de copias de seguridad será de **una semana** excepto cuando la información no cambie, sin perjuicio de disminuir dicha periodicidad cuando la criticidad de la información lo requiera.

Las copias de seguridad serán planificadas para ser ejecutadas en horas en las que interfiera lo menos posible con los servicios ofrecidos. Siempre que sea viable, la copia se realizará sin detener el servicio.

Para aquellos sistemas que por sus peculiaridades no puedan ser incorporados en la planificación de copias de seguridad común establecida (por ejemplo, sistemas operativos no contemplados por las herramientas de copias de seguridad generalizadas), deben disponer de un sistema de copias de seguridad alternativo que garantice su recuperación.

Adicionalmente a la información en sí, se deberá guardar copia de seguridad de todo aquel software activo en los sistemas completo en caso de desastre.

12.4. Revisiones

Se revisará, de acuerdo con la frecuencia de ejecución y lo antes posible tras su finalización, los registros de las copias de seguridad realizadas e intentos fallidos. Aquellas que hayan fallado deben ser planificadas para ser ejecutadas cuanto antes, sin que interfieran con el resto de la planificación definida de copias a ejecutar.

Es recomendable mantener un historial de incidencias de copias de seguridad y ser revisado periódicamente, de modo que se facilite la identificación de errores ya existentes y se optimice el tiempo de resolución de los mismos.

Deberán tomarse las medidas necesarias para mantener actualizada la planificación de copias de seguridad, de modos que se contemple la inclusión de nuevos ficheros o modificaciones en los sistemas relacionados.

12.5. Restaurado

Se realizarán pruebas de restaurado de copias de seguridad de modo que se compruebe periódicamente la validez de los datos y la posibilidad de recuperarlos.

El restaurado de la información, cuando sea debido a una pérdida de la misma, no a una prueba, deberá estar autorizada por el propietario de la información. El hecho debe registrarse como una incidencia de seguridad, siguiendo para ello el *Procedimiento de Gestión de incidencias*.

12.6. Almacenamiento

Las copias de seguridad realizadas se almacenarán en un recinto ignífugo y resistente a agentes corrosivos externos. Adicionalmente, se mantendrán soportes con la información en dos emplazamientos distintos con las adecuadas medidas de protección. La gestión de estos soportes, así como su transporte, se regula en la *Política de gestión de soportes*.

12.7. Herramienta de realización de copias de seguridad

El sistema o herramientas seleccionadas para realizar las copias de seguridad deben permitir la realización de copias de seguridad para los sistemas operativos involucrados en los servicios del Gobierno Regional.

Se mantendrá un contrato de mantenimiento con el proveedor o fabricante, o sistema de copia auxiliar, que asegure su disponibilidad en un tiempo máximo determinado.

Se debe guardar registro de copias realizadas con éxito, registrando la fecha y hora de la misma.

Se debe guardar registro asimismo de intentos de copias fallidos, registrando la fecha y hora de los mismos y el mensaje de error por el que no se ha procedido a realizar la misma, o bien no se ha concluido con éxito.

ANÓTESE Y COMUNÍQUESE.

GOBIERNO DE CHILE
INTENDENTE
REGION ARICA Y PARINACOTA

PATRICIO LÓPEZ 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