ARICA Y PARINACOTA

APRUEBA MANUAL DE PROCEDIMIENTOS BUENAS PRACTICAS EN TI, GOBIERNO REGIONAL DE ARICA Y PARINACOTA

RESOLUCION EXENTA N° 2318

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 Procedimientos Buenas Practicas en TI, 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 Procedimientos
Buenas Prácticas en TI

ÍNDICE

1. INTRODUCCION

Este documento recoge los Procedimientos de los Sistemas de Información del Gobierno Regional de Arica y Parinacota como complemento a los siguientes documentos:

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

2. OBJETIVOS

El objetivo de los Procedimientos presentados en este documento es lograr establecer las mejores prácticas en los procedimientos 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 los procedimientos aquí definidos 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. PROCEDIMIENTO DE ETIQUETADO Y CLASIFICACION DE ACTIVOS

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	
Personal de Operación	

5.1. Objetivo

- Establecer los métodos de etiquetado de los activos conforme a la clasificación asignada según la información que contienen.

5.2. Procedimiento

Sólo será necesario etiquetar los activos con la clasificación correspondiente cuando sea distinta a *Reservada Secreta*. Toda información no etiquetada, se entenderá que tiene clasificación *Reservada Secreta*.

5.3. Documentos

La persona que cree o modifique el documento tiene la responsabilidad de establecer su clasificación y ámbito según las instrucciones de su Propietario.

5.3.1. *Documentos electrónicos*

1. Cuando se vaya a crear un documento por medios electrónicos (ordenador), se utilizará una plantilla en la que, bien en la primera página, o bien la cabecera de cada una de ellas, aparezca la clasificación del documento.

2. Existirán plantillas con la marca correspondiente para cada tipo de documento, de acuerdo al *Anexo A. Marcas de clasificación de los activos.*

3. Cuando se trate de información *Reservada Secreta*, incluidos datos de carácter personal, la plantilla contendrá igualmente una página inicial o anexa al final, donde se relacione el listado de personas o grupos de ellas con acceso autorizado al documento.

4. Si un documento se modifica incluyendo o eliminando información de forma que de lugar a una nueva clasificación, se deberá cambiar a la plantilla correspondiente, o la marca de la misma.

5. Al imprimir un documento, la marca anterior deberá aparecer impresa, igualmente.

5.3.2. *Documentos escritos a mano en papel*

De la misma forma, se deberá poner la etiqueta que corresponda al generar un documento escrito directamente en papel. Se etiquetará igualmente en la primera página o en la parte superior o pie de cada página del documento. Si la información es *Reservada Secreta*, incluidos los datos de carácter personal, se añadirá una página inicial o anexa al final, donde se relaciones el listado de personas o grupos de ellas con acceso autorizado al documento.

5.3.3. *Servidores, estaciones de trabajo y soportes*

Se etiquetarán las estaciones de trabajo que contengan información cuando ésta resida en ellos con carácter permanente o de forma habitual, no siendo necesario entonces el etiquetado de los activos con información temporal.

En el caso de los servidores, el etiquetado se recomienda mediante la aparición de un mensaje al conectarse a él, cuando sea posible y sobre todo, si la información que contiene es Reservada Secreta.

Se etiquetará físicamente, en un lugar visible, y si es posible también de forma lógica.

En los soportes, es la persona encargada de la realización de copias en él quién deberá ponerle una marca de clasificación. Cuando las copias se realicen mediante herramientas mecanizadas, el etiquetado será el realizado por ellas (o no será necesario, ya que los soportes se gestionan y controlan de manera automática). El etiquetado de los soportes se realizará de acuerdo al *Procedimiento de Gestión de Soportes*.

Cuando se haya establecido el nivel de clasificación a un equipo, no se podrá copiar información en él de una clasificación superior sin autorización del Propietario o Responsable del equipo. El responsable deberá informar sobre esto a los usuarios del equipo con permisos para grabar o modificar información.

5.3.4. *Aplicaciones, Sistemas y Bases de Datos*

El responsable de la aplicación, base de datos o sistema tiene la responsabilidad de establecer su clasificación según la información que contenga y que será igual a la más alta de ésta.

En el caso particular de aplicaciones asociadas a la Web Corporativa, sólo se podrá publicar aquella información de uso público, a menos que su acceso esté protegido mediante algún mecanismo de control de acceso (contraseña, por ejemplo). Por tanto, la información de uso interno o reservada secreta no podrá ser publicada a través del portal corporativo y, en caso de que se publicase en la intranet, se deberá asegurar

que ésta sólo sea accesible por el personal interno, controlando adecuadamente que no existan accesos desde redes abiertas (Internet).

Siempre que sea posible, cuando se trabaje con este tipo de activos de manera electrónica, se mostrará un mensaje al usuario acerca del nivel de clasificación al comenzar a trabajar con ellos. Dicho mensaje informará de que no se podrá grabar información con clasificación superior sin autorización del Responsable o Propietario del sistema.

5.4. Anexo A – Marcas de Clasificación de los Activos

Las posibles marcas de clasificación de los activos son: *Público*, *Uso Interno*, *Reservada* Secreta. Cuando se trate de datos de carácter personal se añadirá a la marca *D.P.*

Ejemplo:

Marca: *Reservada Secreta – D.P.*

6. PROCEDIMIENTO DE GESTION DE CAMBIOS Y VERSIONES

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	
Personal de Operación	

6.1. Objetivo

- Establecer las actividades necesarias para llevar a cabo los cambios y actualizaciones en los sistemas los cambios de una manera eficiente, minimizando el impacto y las incidencias que se puedan producir debido a ellos.

6.2. Alcance

La gestión de cambios y versiones es aplicable a cualquier alta, baja o modificación de cualquier elemento de la infraestructura, servicios o actividades del Gobierno Regional, en concreto los activos y recursos:

- Hardware
- Software
- Equipos y software de comunicaciones
- Software de sistemas
- Aplicaciones de sistemas
- Toda la documentación de soporte y mantenimiento asociada a los sistemas
- Políticas, normas o procedimientos

6.3. El Responsable de Gestión de Cambios y Versiones

El Responsable de Gestión de Cambios podrá ser el Encargado de la Unidad de Informática o aquellas personas en las que ellos deleguen y velen por la seguridad de los mismos.

6.4. Prioridades de los cambios

La prioridad del cambio indica el orden de ejecución en el tiempo, o con respecto a otras tareas a realizar en el sistema, según el impacto sobre ellos, de no ser llevado a cabo en tiempo y forma.

Inmediata: El cambio debe ser aprobado y llevado a cabo de forma inmediata y urgente. Son cambios que afectan a aspectos como: pérdida total del servicio, problemas de uso a una gran cantidad de usuarios, mal funcionamiento de sistemas críticos.

Alta: afecta de forma grave a un grupo de usuarios o de forma moderada a un gran número de usuarios. El cambio debe comenzar cuanto antes, a ser posible, en el mismo día o al siguiente.

Media: No tiene gran impacto pero no puede esperar al siguiente cambio de versión o actualización. El cambio debería realizarse a lo largo de los cinco días siguientes.
Baja: No tiene apenas impacto y por lo tanto puede esperar a realizarse junto con el siguiente cambio planificado.

6.5. Clasificación de los cambios

La clasificación del cambio indica el impacto que tendrá dicho cambio en términos de recursos necesarios para llevarlo a cabo.
Mayores: Tienen un gran impacto en recursos y en tiempos de preparación (generalmente, más de 20 jornadas), así como de ejecución. Suelen afectar directamente varias áreas tecnológicas: sistemas, aplicaciones o servicios, así como también a varias áreas de los departamentos.
En general este tipo de cambios suelen ser tratados como nuevos proyectos, o vienen dados a través del ciclo de vida de éstos, teniendo planes de implantación y de marcha atrás bien definidos.

Necesitan la aprobación del Responsable Gestor del Cambio, así como contar con la aprobación previa del Propietario o Responsable del Sistema.

Medios: Tienen un impacto significativo, tanto en recursos y en tiempos de preparación (hasta 20 jornadas), así como de ejecución. Suelen afectar directa o indirectamente a varias áreas tecnológicas: sistemas, aplicaciones o servicios. Tendrán un plan de implantación y marcha atrás definido.

Necesitan la aprobación del Responsable Gestor del Cambio, así como contar con la aprobación previa del Propietario o Responsable del Sistema.

Planificado: Son cambios que se realizan bajo una planificación en el tiempo.

Cada sistema tendrá asignado una "ventana de tiempo" para realizar tareas de actualización, mejora o mantenimiento. Esta ventana será en horarios donde el posible impacto sobre el sistema tenga la menor repercusión sobre los usuarios y sobre otros sistemas que hagan uso de ellos. Los cambios planificados serán llevados a cabo, siempre que sea posible, en la ventana de tiempo asignada al sistema, evitando así que éste se vea afectado en horarios donde su disponibilidad es importante.

Los cambios de tipo Mayor y Medio serán normalmente planificados, así como muchos menores. A los cambios Planificados se les puede asignar las prioridades Alta, Baja y Media.

No Planificado (Urgente): Cambios producidos normalmente debido a una incidencia de prioridad Grave (o con prioridad de tratamiento Alta conforme al *Procedimiento de Comunicación y Gestión de Incidencias*).

Siempre se valorará la adecuación o no de esperar a la ventana de tiempo cuando ésta no esté muy distante en el tiempo, del momento en que surge la necesidad del cambio.

6.6. Gestión de Versiones

Cuando surge la necesidad de realizar varios cambios sobre un sistema, estos se agruparán en un *Versión*.

Todos los cambios que componen la nueva versión se probarán y validarán previamente, de forma conjunta para detectar cualquier irregularidad en el sistema total modificado. Una vez validados se instalarán en el sistema en cuestión conjuntamente como si se tratara de un solo cambio utilizando el proceso de gestión de cambios.

Cada una de las versiones construidas estará documentada de forma detallada, describiendo cada uno de los cambios que la componen, llevando un registro de todas las versiones instaladas en cada sistema.

6.7. Procedimiento

6.7.1. *Comunicación de cambios*

Los cambios *Mayores* y cuando se considere necesario los Medios, serán comunicados por parte del Responsable del Sistema, a aquel personal afectado, incluyendo funcionarios técnicos y no técnicos del Gobierno Regional.

Una vez diseñado el plan detallado del cambio, se enviará por correo electrónico interno a todos los afectados para que pueda ser revisado.

Una vez revisado, podrán enviar sus comentarios para que sean tenidos en cuenta.

Cuando la magnitud del cambio así lo requiera, se dará formación a dicho personal.

En este caso la documentación generada se almacenará en lugar con acceso permanente al personal implicado (SGDOC).

El Responsable de Gestión de Cambios llevará un registro de los cambios aprobados del sistema que efectivamente van a llevarse a cabo y la fecha prevista de implantación. A este registro podrá tener acceso todo el personal implicado.

6.7.2. *Solicitud/Petición de Cambio*

La solicitud de un cambio puede venir por varios motivos:

- Resolución de un incidente o problema
- Descontento de un usuario con determinado servicio o aplicación
- Modificaciones en las configuraciones de los sistemas
- Actualización de componentes en la infraestructura
- Nuevos servicios
- Nuevas normativas legales o cambios en las existentes
- Cambios en los productos o servicios de proveedores o fabricantes
- Otros.

Autorización para solicitar cambio

El Responsable de Gestión del Cambio decidirá/autorizará quiénes pueden solicitar cambios de manera habitual, debiendo mantener una lista actualizada de las personas autorizadas para ello.

Comunicación del cambio

Previamente a la solicitud del cambio, se deberá haber comunicado mediante correo interno al personal afectado, haber tenido en cuenta los comentarios recibidos y, si fuese necesario, haber impartido la formación necesaria

Solicitud del cambio

1. INICIO: Se solicitará mediante la herramienta software para la gestión de los cambios:
   - Cuando el cambio sea debido a una incidencia o problemas, se deberá indicar la referencia/ticket de la incidencia o problema.
   - Se incluirá el plan detallado para ejecutar el cambio así como la vuelta atrás para deshacerlos.
2. Si el cambio es Mayor, o Medio si se considera necesario, una vez aprobado, el solicitante lo comunicará al personal implicado mediante correo electrónico interno, indicando la fecha y hora en la que estará operativo el cambio

3. FIN del procedimiento

6.7.3. *Tratamiento del cambio por parte del Responsable de Gestión del Cambio*

Una vez recibida la solicitud, el Responsable de Gestión del Cambio, o en quien delegue realizará los siguientes pasos:

1. INICIO: Asignará al cambio un número de identificación, en orden secuencial, que será utilizado en todas las comunicaciones posteriores con todos los implicados. Comprobará que el solicitante está en la lista de autorizados, en caso contrario ir al paso RECHAZADO

2. REVISION: Revisará que todos los datos necesarios para el cambio están y son correctos. Si no es así, ir al paso RETENIDO

3. EVALUACIÓN: Evaluará el cambio. Se revisarán todos los datos aportados por el solicitante, y se evaluará su viabilidad y adecuación, teniendo en cuenta el impacto y los riesgos que pudiera provoca. Se revisará especialmente la fecha y hora propuesta de implementación, el plan detallado, el plan de marcha atrás, el impacto y la formación a los usuarios según sea necesario.

    - Si el cambio no es viable, ir al paso RECHAZADO

    - En caso contrario, pedir autorización al Responsable del Sistema, Servicio, poniendo el cambio en estado APROBADO y lo incluirá en el registro de cambios aprobados.

4. EJECUCIÓN: Enviará el cambio al grupo o persona asignado para su implementación. El cambio será devuelto en estado RECHAZADO o FINALIZADO al Responsable de Gestión de Cambio, quien lo revisará:

    - En caso de que el estado sea RECHAZADO, ir al paso RECHAZADO

    - En caso de que el estado sea FINALIZADO:

        - Si la revisión es satisfactoria, lo pasará al estado CERRADO, y comunicará el resultado al solicitando. Ir al paso FIN.

        - Si la revisión no es satisfactoria el Responsable de Gestión del Cambio tomará las decisiones oportunas sobre los pasos a seguir:

            - Volver a EJECUCIÓN,

            - Rechazarlo en caso de no haber cumplido los objetivos y requerir que se deshagan los pasos efectuados

            - Volver a realizar una nueva solicitud planteando modificaciones, etc.

5. RECHAZADO: Poner el cambio en estado RECHAZADO y comunicarlo por correo electrónico interno al solicitante, indicando la razón de éste. El solicitante podrá realizar comentarios sobre la razón del rechazo y enviarlos al Responsable de Gestión del Cambio. Ir al paso FIN

6. RETENIDO: Poner el cambio en estado RETENIDO. Comunicar al solicitante que el cambio está retenido y la razón y la forma de subsanar el problema que causó dicha retención para poder continuar con el cambio. El solicitante enviará los datos necesarios al Responsable de Gestión del Cambio. Ir al paso REVISION

7. FIN del procedimiento.

El Responsable de Gestión del Cambio deberá mantener un registro de todas las acciones llevadas a cabo con el cambio.

6.7.4. *Cambios Urgentes*

Se consideran cambios urgentes aquellos con prioridad Inmediata y algunos con prioridad Alta.

Los cambios urgentes se pueden realizar saltando algunas de las fases del procedimiento descrito en el apartado anterior. En general, se podrán saltar aquellas fases que se consideren que su tiempo de preparación es demasiado amplio y retrasaría la implementación del cambio. Los cambios saltados serán completados y documentados posteriormente.

Todo cambio urgente debe ser igualmente documentado y registrado.

6.8. Anexo A – Información necesaria para la Solicitud/Petición del Cambio

- Prioridad, Categoría, Planificado, No Planificado
- Incidencia asociada (en su caso)
- Sistemas y elementos asociados
- Resumen del Cambio
- Plan detallado y Plan de Marcha Atrás
- Efectos de la no implementación
- Razón del cambio
- Fecha y hora propuestas para la realización/implantación
- Duración estimada
- Impacto en el/los sistemas
- Persona/Grupo que debe implementarlo
- Grupos implicados
- Comunicación a los implicados (realizada, no realizada, no necesaria)
- Formación a los implicados (realizada, no realizada, no necesaria)

7. PROCEDIMIENTO DE CONTROL DE ACCESO FÍSICO A LOS SISTEMAS DE INFORMACIÓN

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Manual de Procedimientos de Seguridad 2011-2012: Apartado 5.2 Procedimientos Específicos "Controles de Acceso Físico".
Políticas, Procedimientos, Normas	Normativas de Uso y Acceso al CPD.

7.1. Objeto

- Establecer el método de acceso a la sala de servidores

7.2. Procedimiento

Los servidores de los Servicios Centrales del Gobierno Regional se encuentran ubicados en una sala cerrada e independiente (Centro de Proceso de Datos o CPD), a la que se puede acceder tecleando un código numérico de acceso/tarjeta de aproximación, o bien en caso de fallo, se utiliza una llave. Dicha sala siempre se encuentra cerrada.

El personal sólo podrá acceder a dicha sala con la finalidad de efectuar las actividades propias de administración, operación y mantenimiento de los equipos y servicios que contienen.

Todo el personal que necesite la entrada habitual a la sala de servidores, deberá obtener autorización del Encargado de Seguridad, el cuál solicitará un código de acceso/tarjeta temporal.

El personal autorizado para acceder a la sala de servidores deberá quedar registrado en el listado del Anexo A.

Cada persona será responsable de custodiar su código de acceso y/o su llave, debiendo informar de inmediato al Encargado de Seguridad, en caso de pérdida u otra incidencia con ella para que ésta sea renovada.

El Encargado de Seguridad revisará periódicamente los accesos al CPD en busca de posibles anomalías (accesos a deshoras, bloqueo de código de acceso, acceso frente a bajas o vacaciones del personal, etc.)

El personal de limpieza, o aquel que fuera a realizar labores de mantenimiento de los equipos procedente de una empresa externa, estará autorizado a entrar en la sala de servidores para el fin exclusivo de prestación de sus servicios. Este personal será acompañado por una de las personas autorizadas para acceder a la sala de servidores, que le abrirá la puerta y, cuando acabe su trabajo avisará para que vuelva a cerrar la puerta. Se recomienda que, en la medida de lo posible, estas personas no se encuentren absolutamente solas en la sala de servidores sin vigilancia alguna.

Las empresas terceras con acceso al CPD se deberán registrar en el listado del Anexo B.

7.3. Anexo A - Personal con autorización para acceder a la sala de servidores

NOMBRE Y APELLIDOS

7.4. Anexo B - Empresas con acceso temporal al CPD

EMPRESA	PERSONA RESPONSABLE	HORARIO DE ACCESO PERMITIDO

8. PROCEDIMIENTO DE EMISION Y CONTROL DE PASES DE VISITA

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Manual de Procedimientos de Seguridad 2011-2012: Apartado 5.2 Procedimientos Específicos "Controles de Acceso Físico".
Políticas, Procedimientos, Normas	

8.1. Objeto

- Establecer un plan de control de las visitas a las instalaciones del Gobierno Regional que proteja el acceso físico no autorizado a los locales donde se ubican los sistemas de información.

En el momento de redacción de este procedimiento no se realiza ningún registro acerca de las visitas que se llevan a cabo en las instalaciones del Gobierno Regional.

8.2. Procedimiento

El diseño de cualquier sistema está basado en la posibilidad de acceso de personal ajeno a la organización, es decir, acceso público (visitantes, vendedores, mensajería, correo, entregas comerciales, clientes, ciudadanos, etc.) por ello y para asegurar el control de acceso en las instalaciones del Gobierno Regional, se deberán llevar a cabo una serie de medidas de seguridad que impidan el acceso físico no autorizado a las dependencias de la organización tales como:

- El establecimiento de un perímetro físico de seguridad que proteja la información de la organización es vital para prevenir incidencias. El perímetro físico es la primera barrera de protección del sistema de información que garantiza en gran medida el funcionamiento del resto de medidas.

- El acceso al edificio, mediante vías de acceso autorizadas y controladas, barreras arquitectónicas como paredes o ventanas, elementos adicionales como áreas de descarga controladas, deberán ser gestionadas para proteger las zonas que contienen instalaciones informáticas o permiten el acceso a las mismas.

- Validar las medidas de seguridad físicas de acceso al perímetro de seguridad compuestas por puertas, cerraduras, alarmas, vigilancia, etc. y formalizarlas en instrucciones de acceso a las estancias, locales que deberán ser comunicarlas a todo el personal.

8.3. Acceso a las instalaciones

La recepción deberá estar aislada del resto de estancias por una barrera, torno, puerta de seguridad, de manera que los usuarios que accedan al edificio deban pasar por recepción y obtener la identificación de acceso (pase), que les permita circular y acceder a la dependencia o dependencias autorizadas.

Los pases a entregar a los visitantes deberán mostrar tal propósito (indicando V, VISITA o VISITANTE). Se recomienda que además, en la medida de lo posible se recoja, además de los datos básicos de identificación del visitante (nombre, apellidos, número de identificación) otro tipo de información como por ejemplo: fecha, hora de la visita, persona a la que se desea visitar, las dependencias, el tiempo de validez, etc. En el *Anexo A* se muestra un ejemplo de registro de visitas.

El pase de visita deberá estar visible en todo momento, así como deberá ser devuelto a la salida o fin de la misma

8.4. Anexo A – Campos del registro de visita

- Fecha:
- Hora:
- Nombre/Apellidos
- Empresa visitante:
- Persona a la que se desea ver:

9. PROCEDIMIENTO DE COMUNICACIÓN, GESTION Y RESPUESTA ANTE INCIDENTES

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Comunicación y Gestión de Incidentes
Políticas, Procedimientos, Normas	Manual de Procedimientos de Seguridad de la Información. Apartado IX. "Dominio de incidentes en la seguridad de la información".

9.1. Objetivo

- Establecer los flujos de comunicación, y los pasos para contener, tratar y reparar las incidencias de Seguridad y de los Sistemas de Información de la organización.

9.2. Conceptos

Evento: Cualquier ocurrencia instantánea, no perteneciente a las operaciones estándares, que pueden afectar al estado (cambiar) global en la seguridad de un sistema. Puede ser persistente o temporal.

Incidencia: Cualquier evento o conjunto de eventos que afecta o puede afectar al correcto funcionamiento, rendimiento o seguridad (confidencialidad, integridad y disponibilidad) de un sistema y que hace necesario llevar a cabo alguna acción determinada.

Incidente: Incidencia o conjunto de incidencias que causan un impacto real sobre la seguridad del sistema.

A efectos del presente procedimiento se considerarán igualmente incidentes e incidencias, y se referirá siempre como incidencias.

9.3. Introducción

Siempre que el personal de la organización detecte una posible incidencia de seguridad, deberán comunicarlo lo antes posible.

Se deberán reportar al CAU (Centro de Atención a usuarios) o, en su defecto, a la Jefatura por el medio más al alcance del comunicante y más adecuado, según su naturaleza y urgencia (en la medida de lo posible por correo electrónico o memorándum, con copia al Encargado de Seguridad o quien lo supla y al Jefe de la Unidad Informática).

En caso de eventos de fuerza mayor tales como desastres naturales, accidentes de cualquier tipo, intervenciones de personas no autorizados en las zonas de seguridad, robo o sustracción de bienes, atentados terroristas, incendios, tsunamis, terremotos, etc. se debe considerar la intervención de las autoridades (organismos de seguridad y emergencia) tales como Carabineros, Policía de investigaciones, bomberos, ambulancias, etc.

Se mantendrá un *"Registro de Incidencias"*, donde se almacenarán todas las resoluciones efectuadas a las incidencias ocurridas, de forma que pueda ser consultado posteriormente para facilitar y agilizar la resolución de futuras incidencias similares.

9.4. Minimización del número de incidencias y su gravedad

La mejor manera de gestionar las incidencias de seguridad es evitarlas, aunque esto no siempre es posible. Las acciones que en general se deben llevar a cabo para minimizar el número de incidencias y su repercusión sobre los activos están recogidas en las políticas, normas y procedimientos de seguridad. Cabe destacar las siguientes:

- Poner en práctica todas las políticas, normativas y procedimientos.
- Evaluar de forma regular las vulnerabilidades de los sistemas y servicios. Las evaluaciones deben ser realizadas por un experto en seguridad.
- Comprobar con regularidad todos los sistemas y servicios para garantizar que tienen instalados los parches de seguridad más recientes.
- Establecer programas de formación sobre la seguridad tanto para el personal de TI como para los usuarios finales.
- Enviar notificaciones o trípticos de seguridad que recuerden a los usuarios sus responsabilidades y restricciones.
- Garantizar el cumplimiento de los procedimientos asociados a la gestión de cuentas de usuario (incluyen una política de contraseñas seguras).
- Utilizar herramientas automáticas para analizar con regularidad el tráfico de red y el rendimiento de los sistemas y supervisarlo.
- Comprobar periódicamente todos los registros de eventos del sistema operativo, de aplicaciones, servicios, Cortafuegos, etc.
- Llevar a cabo revisiones de los procedimientos de copia de seguridad y restauración que se implementen.
- Categorizar y documentar las acciones emprendidas a raíz de los incidentes de seguridad, para poder realizar revisiones y consultas posteriores. Estos pueden ayudar a resolver nuevos incidentes futuros similares y a implementar las medidas de seguridad más adecuadas.
- Realizar auditorías y pruebas de penetración periódicamente.
- Estar al día sobre las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.
- Investigar acerca de nuevas revisiones de software.

9.5. Categorías de las Incidencias

Establecer la categorización de todas las incidencias de seguridad que ocurren ayudará a asignarles la prioridad con la que deben ser tratadas y hará posible el establecimiento de indicadores (cuadro de mando) que muestre posteriormente el estado del tratamiento de éstas y los puntos necesarios a reforzar.

A continuación se exponen los principales grupos de incidencias de seguridad que se pueden producir. Se pueden categorizar, según distintos conceptos:

- De origen: Interno / Externo, Humano / Físico / Lógico.
- Intento de ataque / Ataque consumado / No intencionado (error).
- Provoca pérdida de: Confidencialidad / Integridad / Disponibilidad / Imagen
- De carácter Legal: Ley 19.629 sobre la protección de la vida privada o protección de datos de carácter personal / Otros

Una incidencia podrá pertenecer a uno o varios, de los anteriores grupos y categorías.

9.6. Prioridad del tratamiento

La prioridad del tratamiento y resolución de la incidencia indica el orden de ejecución en el tiempo (o con respecto a otras tareas a realizar en el sistema) según el impacto sobre los sistemas de no ser llevado a cabo en tiempo y forma.

- **Alta**: Tienen un gran impacto. Son incidencias que afectan a temas tales como pérdida total del servicio, problemas de uso a una gran cantidad de usuarios, mal funcionamiento en sistemas críticos, etc. Debe ser tratada y resuelta de forma prioritaria.
- **Media**: No tienen un gran impacto. No obstante, deben ser tratadas cuanto antes para evitar que derive en daños mayores..

9.7. Grupos de Comunicación y/o gestión de incidencias. Datos de contacto

Nombre	Teléfono / Extensión	Correo Electrónico	Responsable
Centro de Atención al Usuario (CAU) (*)	<Teléfono del CAU> En su defecto de un responsable de la Unidad de Informática		

(*) El CAU se encargará de redirigir y derivar las incidencias a los responsables asignados:

- Técnico de la Unidad Informática.
- Otros terceros/proveedores
- Autoridades

9.8. Datos necesarios en la comunicación de incidencias

En general, el personal a quién se realiza la comunicación de la incidencia recabará del usuario toda la información posible acerca de la incidencia:

- Persona que ha comunicado la incidencia.
- Fecha/hora de la incidencia.
- Descripción detallada de la incidencia.
- Descripción del impacto.

Los grupos de comunicación y/o de gestión de incidencias establecerán:

- Prioridad de la incidencia y,

- Categoría de la incidencia

Una vez resuelta se completará la siguiente información:

- Fecha/hora de resolución.
- Acciones y medidas aplicadas para su resolución

A cada incidencia se le asignará un número de identificación único.

9.9. Procedimiento de comunicación y gestión de incidencias

9.9.1. *Incidencias relativas a los sistemas de información*

1. COMUNICACIÓN DE LA INCIDENCIA: Cualquier usuario final comunicará las incidencias detectadas llamando al CAU (o Unidad Informática). En el caso de que se trate de una incidencia detectada en la propia Unidad de Informática los pasos 1 y 2 se omitirán pasándose directamente al paso 3.

2. REVISIÓN: La persona que atiende la llamada, recopilará los datos mínimos necesarios para proceder a su resolución (Persona que llama, Teléfono de Contacto, Activo de Información o Recurso afectado, etc.).

3. PRIORIDAD: Dependiendo de la criticidad de la incidencia se le asignará una prioridad de resolución (alta o media).

4. APERTURA: Se dará de alta la incidencia (si se dispone de aplicación específica y, sino, en la herramienta que se haya contemplado a tal fin para realizar su seguimiento y registro.

5. RESOLUCIÓN: En el caso de que la incidencia no pueda ser resuelta por el receptor de la llamada, será el responsable de asignación de incidencias quien la escalará al grupo de resolución correspondiente:

6. La resolución de la incidencia se llevará a cabo, siempre que sea posible teniendo en cuenta el procedimiento de "Resolución de Incidencias", que se muestra en el punto 9.1010.

7. COMUNICACIÓN DE LA RESOLUCIÓN: Una vez resuelta la incidencia, la persona o grupo que recibió la comunicación informará de dicha resolución al comunicante y/o personas afectadas.

8. REGISTRO DE ACCIONES: Se registrarán en la herramienta en la que se haya cursado el alta las acciones y medidas llevadas a cabo para la resolución de la incidencia, la fecha y la hora de la resolución.

9. CIERRE: La incidencia se cerrará.

10. BÚSQUEDA DE TENDENCIAS: Periódicamente, al menos trimestralmente, se revisará el registro de incidencias para comprobar el estado y descubrir posibles tendencias.

9.10. Procedimiento de Resolución de Incidencias

En general, las fases que se deben seguir en la resolución de una incidencia de Seguridad son las siguientes:

1. Identificación y análisis de la causa. Ante una incidencia es preciso determinar la causa que la está provocando e identificar el origen de la misma. Establecer o modificar la categoría y prioridad de la incidencia. Para ello se intentará aclarar los siguientes puntos sobre la incidencia

   - la naturaleza (podría ser diferente a la determinada en la evaluación inicial)
   - el origen
   - la intención (si es aleatorio o muestra indicios de estar planificado y dirigido a algo concreto)
   - los sistemas y servicios exactos a los que ha afectado
   - efecto producido (la información a la que se ha tenido acceso y su grado de confidencialidad, activos perdidos o deteriorados, servicios interrumpidos o degradados, etc.)

2. Informar a las partes interesadas acerca de los sucesos ocurridos y como proceder hasta que se resuelva la incidencia.

3. Recolección de evidencias con calidad suficiente y mantenimiento y protección de las mismas, especialmente cuando la incidencia ha provocado daños importantes y pueda conllevar acciones legales. La recolección de evidencias se realizará lo antes posible, teniendo en cuenta el punto siguiente y se almacenarán en lugar seguro, se tendrán en consideración tanto las evidencias electrónicas como las evidencias en papel.
4. Contención del incidente. Detener los efectos que pueda estar causando en los sistemas y servicios.
5. A la hora de la contención del incidente se establecerán una serie de prioridades que podrán variar en función del mismo, pero que en general debería ser:
   - Proteger la vida humana
   - Proteger la información Reservada Secreta
   - Proteger el hardware y el software contra el ataque, la pérdida o la modificación de los archivos de sistema y contra daños físicos al hardware.
6. Restablecer los sistemas/servicios afectados a su estado normal de funcionamiento. Para ello, se debe investigar todo lo que ha sido afectado o comprometido en el sistema y reponerlo. En caso de que sea necesario se restaurará el sistema afectado por completo.
7. Evitar que se repita la incidencia, eliminando los motivos que la han provocado y/o implementando los controles correctivos necesarios en los sistemas/servicios.
8. Aprendizaje de la incidencia, de los motivos que la han provocado y de las acciones para su corrección. Estudiando periódicamente los tipos de incidencias más frecuentes, los costes, controles a reforzar, etc.
9. Revisar y mejorar los procedimientos implicados si procede.

Los primeros pasos, del 1 al 4, no siempre tienen que darse necesariamente en ese orden, ya que dependerá de las circunstancias y tipo de incidencia en cada caso.

9.11. Acciones especiales

Se recogen a continuación acciones especiales a llevar a cabo por los Administradores, durante el proceso de resolución de las incidencias, según la categoría de ésta:

- **De origen humano por un empleado**
  - Comunicar al responsable del empleado, al Encargado de Seguridad y si se estima oportuno, al departamento de Administración y Recursos Humanos.
- **De origen Físico o Robo / Destrucción / Manipulación del Equipamiento:**
  - Informar al Encargado de Seguridad.
- **De origen natural:**
  - Notificar al Comité de Seguridad, que decidirá sobre la notificación a las autoridades y organismos públicos pertinentes.
- **De Origen en la Operación (cambios)**
  - Si la aplicación es externa o soportada por un tercero, se le avisará.
  - Si no se puede resolver la incidencia, se volverá a la versión o configuración anterior.
  - Se instruirá al personal implicado para que se lleven a cabo los cambios de forma correcta según el *Procedimiento de Cambios y Versiones*.
- **Ingeniería Social y Suplantación de Identidad**
  - Dar aviso a los empleados. Instruirles sobre las medidas de seguridad que deben tomar al respecto.
  - Forzar el cambio de contraseña.
- **Ataque consumado con pérdida de Confidencialidad/Integridad/Disponibilidad sobre datos confidenciales o superiores, incluidos los datos de carácter personal**
  - En caso de intrusión:

- Como medida Urgente, si el Administrador de sistemas percibe que la gravedad de la intrusión lo aconseja, debe desconectar el sistema afectado de la red, antes que poner en peligro información confidencial. Siempre que sea posible, esta acción debe ser respaldada por el Comité de Seguridad.
    - Si es Administrador del Sistema estima que el sistema afectado puede tener múltiples daños y no es posible su recuperación tal como estaba antes de la intrusión (limpio de virus, troyanos, programa de hacking ocultos, etc.) debe restaurar el sistema desde cero. Siempre que sea posible, esta acción debe ser respaldada por el Comité de Seguridad.
- En caso de Escucha de Tráfico, si es detectado en tiempo real, se dejará de transmitir y se forzará el cambio de contraseña.
- Realizar las acciones indicadas para el Intento de Intrusión y Ataque.
- Informar al Comité de Seguridad, quién decidirá las acciones adicionales a llevar a cabo.

- **Intento de intrusión o ataque (intentos de intrusión aprovechando una vulnerabilidad, sin llegar a ser consumida)**
    - Impedir que el intruso continúe, siempre que se pueda detectar en tiempo real, bloqueando el paso a su dirección IP.
    - Corregir lo antes posible la vulnerabilidad que se está aprovechando para ello.
    - Si se realiza a través de un puerto no necesario, éste se cerrará.
    - Si el Administrador percibe que es potencialmente peligroso se debe obtener información exhaustiva, dentro de lo posible:
        - Fecha y hora de cada intento de ataque.
        - Dirección IP con resolución inversa de DNS, identificando el dominio.
        - Vulnerabilidad encontrada y tipo de exploit o programa que se está usando para el ataque.
        - Informe de la estrategia de ataque seguida por el atacante.
        - Servicios que se han visto afectados por el atacante.
        - Historia anterior de ataques procedentes del mismo lugar (misma dirección IP).
- **Legal:**
    - Notificar al Comité de Seguridad, que decidirá sobre las comunicaciones o denuncias a las autoridades pertinentes
    - En caso de datos de carácter personal notificar al Encargado de Seguridad y al Propietario de la Información.
- **De Origen Interno y destino externo.** Este tipo de incidencias suele detectarse por aviso del destino atacado
    - Reconocimiento: cuando el atacante está buscando información y posibles vulnerabilidades, pero sin realizar aún ninguna acción de ataque que aproveche dichas vulnerabilidades:
        - No se enviará respuesta alguna al dominio atacado. Si en algún caso particular se considera necesario emitir una respuesta, se evitará explícitamente dar cualquier información acerca de las infraestructuras de seguridad del Gobierno Regional, servicios, políticas, procedimientos, o en general, cualquier detalle más allá de una mera respuesta de cortesía.
        - Intento:
            - El Administrador de sistemas informará al Comité de Seguridad que decidirá si se responde a la notificación del dominio atacado, en cuyo caso se tendrán en consideración lo anteriormente mencionado respecto a la divulgación de información sensible del Gobierno Regional.
        - Consumado:
            - Se informará al Comité de Seguridad.

- Se obtendrá información exhaustiva del incidente.
- Se impedirá la salida a Internet del sistema atacante
- A criterio del Comité de Seguridad, se cooperará con el dominio atacado para esclarecer los hechos.
- El Comité de Seguridad informará al Intendente.

A criterio del Intendente se informará del incidente a otras organizaciones que pudieran verse afectados por el mismo.

10. PROCEDIMIENTO DE ALTA, BAJA Y MODIFICACION DE CUENTAS DE USUARIO

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

10.1. Objeto

- Desarrollar las actividades necesarias a llevar a cabo para el Alta, Baja y Modificación de cuentas de usuario
- Describir el proceso a seguir en el flujo de Autorización de Acceso a la información y aplicaciones y sistemas

10.2. Procedimiento de Alta de cuenta de usuario

En el contexto del Gobierno Regional se pueden dar dos tipos de cuentas:

- De Administrador: aquellos que tienen la facultad de modificar programas, accesos, claves, y privilegios de acceso de los usuarios
- De Usuario: todas las personas, empleados, usuarios autorizados o colaboradores que tengan acceso a la información contenida en las aplicaciones y sistemas de información para el desarrollo de sus funciones, sin capacidad de modificar sus privilegios de acceso. Cada persona tiene un perfil de usuario, estando el acceso regulado por medio del usuario y la contraseña que lo hacen unívoco y personal, o bien a través del uso de certificado digital para determinadas aplicaciones.

El procedimiento de alta de usuario es el siguiente:

1. El departamento de Personal comunica mediante correo electrónico al Encargado de la Unidad de Informática la necesidad de acceso a la red de un nuevo empleado, enviándole cumplimentado los datos del *Anexo A.*
   En caso de externalización de servicios o de usuarios ajenos al Gobierno Regional, será el Responsable del Servicio que afecta el acceso por parte de personal externo quien comunique al Encargado de Seguridad y al Encargado de la Unidad Informática la necesidad de habilitar acceso a la red a dicho tercero.
2. El Jefe del Servicio o de la Unidad en el que entre a trabajar el nuevo empleado comunicará al Encargado de la Unidad Informática los permisos de acceso que requiera, enviándole por correo electrónico los datos del Anexo B.
3. El usuario o tercero solicitante de la cuenta firma por duplicado las Cláusulas del Anexo D entregándose una copia al Encargado de Seguridad.
4. La Unidad Informática procederá a dar de alta al usuario.
5. Fin del Procedimiento.

Se puede solicitar el alta en grupos de usuario con un mismo Jefe, a través de una sola petición para varios usuarios.

En la medida de lo posible se añadirá una fecha de Baja de cuenta a cumplimentar por el Jefe del Usuario o Responsable del Servicio en caso de que se trate de un servicio externalizado.

10.2.1. *Administradores y Desarrolladores*

Para los usuarios con perfil de Administrador y/o Desarrollador, cada usuario tendrá una cuenta diferenciada, a fin de que se puedan identificar los accesos al realizar auditorías de los sistemas.

Las cuentas de este tipo de usuarios deben disponer de al menos 8 caracteres de longitud, ser alfanuméricos y de mayor complejidad (caracteres especiales).

10.3. Procedimiento de Modificación de cuenta de usuario

El Jefe del empleado o Responsable del Servicio que afecta el acceso por parte de personal externo cumplimentará la solicitud de Alta o Modificación en los Sistemas de Información (Anexo B), y la enviará a la Unidad de Informática para que proceda a modificar la cuenta.

10.4. Procedimiento de Baja o Bloqueo de cuenta de usuario

10.4.1. *Solicitud de la baja o bloqueo de cuenta*

El Jefe del usuario o Responsables del Servicio que afecta al acceso del personal externo debe solicitar la baja de una cuenta siempre que el uso de la misma no sea necesario por más tiempo, ocurra un uso fraudulento de ella o haya sospecha de que ha sido comprometida.

1. El Jefe de Usuario solicita la baja o bloqueo de la cuenta de usuario, por correo interno, a la Unidad Informática y con copia al departamento de personal si se trata de un empleado del Gobierno Regional, cumplimentando los datos del Anexo C.

2. La Unidad Informática, procederá a la baja o bloqueo de la cuenta. En caso de bloqueo, se realizará por el tiempo indicado por el Jefe del usuario.

3. Fin del procedimiento.

10.5. Registro y revisiones

El departamento de Personal, así como la Unidad Informática, junto con los Responsable de los Sistemas afectados por las diversas actuaciones en materia de cuentas de usuario, deberán guardar registro de todas las solicitudes cursadas.

El Encargado de la Unidad Informática, o aquella persona en quien delegue esta tarea, revisará cada 6 meses el listado de cuentas de usuario y privilegios en los sistemas, aplicaciones o servicios de su responsabilidad, con objeto de identificar posibles usuarios cuyos privilegios no estuvieran actualizados.

10.6. Anexos

10.6.1. *Anexo A – Datos para la Solicitud de Alta de cuenta de Usuario*

- Fecha de Solicitud
- Fecha de Alta efectiva
- Fecha de Fin de contrato
- Servicio al que se destina
- Datos de usuario a dar de Alta
  - Nombre, Apellidos, Número Identificativo, Tipo (Interno, Externo)
- Pertenece a: (Unidad/Servicio/Área, Empresa Externa)

10.6.2. *Anexo B – Datos para la Solicitud de Alta o Modificación en los Sistemas de Información*

- Fecha de Solicitud
- Fecha de asignación de permisos efectiva
- Fecha de fin de asignación de permisos
- Sistema, Aplicación o Servicio
- Datos de usuario:
  - Nombre, Apellidos
- Derechos de acceso:
- Acceso Remoto (si/no)
- Método de Acceso Remoto
  - Módulo / Carpeta / Aplicación / --- Derechos (Lectura, Escritura, Borrado)

(Repetir para cada elemento que requiera acceso)

10.6.3. *Anexo C – Datos para la Solicitud de Baja/Bloqueo de cuenta de Usuario*

- Fecha de Solicitud
- Fecha de Baja/Bloqueo efectiva
- Datos de usuario:
  - Nombre, Apellidos
  - Cuenta de usuario
- Baja o bloqueo --- Duración
- Motivo:

10.6.4. *Anexo D – Cláusulas de Confidencialidad*
Acuerdo de confidencialidad

- _____ *se compromete a guardar estricta confidencialidad de la información que con motivo de su autorización de acceso al equipamiento informático del Gobierno Regional para el desarrollo de sus funciones pudiera.*
- _____ *guardará secreto profesional sobre todas las información, documentos y asuntos a los que tenga acceso estando obligado a no hacerlo público o transmitir cuantos datos conozca como consecuencia o con ocasión de su ejecución, incluso después de finalizar el plazo o la duración del acceso.*
- *Finalizadas las tareas y previa a la desconexión de los equipos informáticos se borrará toda información utilizada o que se derive de la ejecución del acceso.*
- _____ *reconoce que cualquier difusión, divulgación pública o cualquier otro tipo de transferencia de información confidencial por quien tiene obligación contractual de guardar reserva sobre la misma constituye un delito previsto en el derecho internacional y las leyes chilenas y que tales actos serían procesados de acuerdo a la ley aplicable.*
- *La información necesaria para el acceso (identificador de usuario, contraseñas, parámetros de configuración, direcciones IP internas, etc.) no podrá ser divulgada bajo ningún concepto a terceras personas, ajenas o no al Gobierno Regional.*
- *La información necesaria para el acceso (identificador de usuario, contraseñas, parámetros de configuración, direcciones IP internas, etc.) no podrá ser utilizada con posterioridad a la finalización de la autorización de acceso, y durante la misma, en equipamiento diferente al utilizado.*

Firmado: _____ *(Solicitante de acceso)*
Firmado: _____ *(Encargado de la Unidad Informática)*

11. PROCEDIMIENTO DE ANALISIS Y GESTION DE RIESGOS

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Seguridad de la Información
Políticas, Procedimientos, Normas	Manual de Procedimientos de Seguridad 2011-212 PMG-SSI

11.1. Objetivo

- Describir el proceso de análisis y gestión de riesgos de acuerdo a las normas ISO/IEC 27001 e ISO/IEC 27002.

11.2. Definiciones

Activo: cualquier bien que tiene valor para el Gobierno Regional de Arica y Parinacota.

Disponibilidad: garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con Gobierno Regional cada vez que lo requieran

Integridad: salvaguarda de la exactitud y totalidad de la información y los métodos de procesado

Seguridad de la Información: preservación de la confidencialidad, la integridad y la disponibilidad de la información, pudiendo abarcar otras propiedades como autenticidad, fiabilidad y el no repudio

Incidente de Seguridad de la Información: evento o eventos de seguridad de la información, inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del Gobierno Regional y de amenazar la seguridad de la información

Riesgo Residual: riesgo remanente que existe después de que se hayan tomado las medidas de seguridad

Aceptación del riesgo: decisión de aceptar un riesgo

Análisis de Riesgos: utilización sistemática de la información disponible para identificar peligros y estimar los riesgos

Evaluación de Riesgos: proceso general de análisis y estimación de los riesgos

Gestión de Riesgos: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos

Tratamiento de Riesgos: proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.

11.3. Requisitos

- **Niveles de aceptación del riesgo.** Es necesario establecer como criterio previo el disminuir aquellos riesgos que valgan o estén por encima de un determinado valor, si bien podría aceptarse un riesgo residual de dicho valor siempre y cuando se tenga un plan de acción (a corto, medio o largo plazo) para reducirlo.

- **Debe definirse una Política de Seguridad** que recoja las normas en las que basarse la seguridad de la información, debiendo estar apoyada y respaldada por la Dirección del Gobierno Regional.

- **Debe existir un inventario de activos de información.**

11.4. Procedimiento

1. METODOLOGÍA DE EVALUACIÓN DE RIESGOS. Es necesario definir una metodología de evaluación de riesgos en materia de seguridad de la información.

2. IDENTIFICAR LOS RIESGOS, para ello:

    - Se identificarán los activos y los propietarios (personas responsables de los activos en términos de su administración, desarrollo, mantenimiento, uso, seguridad, etc.) bajo el alcance del análisis de riesgos.

    - Se identificarán las amenazas por cada activo y las vulnerabilidades bajos las que podrían actuar dichas amenazas. El Anexo A – Catálogo de Amenazas, recoge un listado de las amenazas más comunes.

- Se identificará el impacto de las amenazas sobre los activos de información en términos de la confidencialidad, integridad y disponibilidad.

3. ANÁLISIS Y VALORACION DE RIESGOS

   - Se evaluarán los efectos en la actividad del Gobierno Regional que pudiesen derivarse de la materialización de los fallos de seguridad en términos de pérdida de confidencialidad, integridad o disponibilidad.

   - Se evaluará la probabilidad de fallos de seguridad considerando las amenazas identificadas, las vulnerabilidades, los impactos y los controles implementados (basados en la ISO 27002, por ejemplo) sobre los activos.

   - Se estimarán los niveles de riesgos, y se determinarán si los riesgos obtenidos son aceptables o necesitan tratamiento de acuerdo a los criterios de aceptación.

   Como resultado de estas etapas se dispondrá del llamado *Informe de Análisis y Gestión de riesgos* que cuantifica el riesgo al que están sometidos los activos identificados y se indicará el riesgo residual, en vías de mejora a través de la siguiente etapa (Gestión de Riesgos).

4. GESTION DE RIESGOS. Realizado el Análisis de Riesgos y comparando los resultados con los niveles de aceptación definidos, el siguiente paso consiste en identificar un plan para alcanzar tales niveles de aceptación y llegar a un nuevo mapa de riesgos, para ello se seguirán los siguientes pasos.

   - Identificación de las opciones para el tratamiento de riesgos tales como:

     - Aplicación de controles.

     - Asumir los riesgos conforme a los criterios de aceptación

     - Evitarlos

     - Transferirlos a otras partes (compañías aseguradoras, proveedores, terceros,etc.)

   - En el caso de aplicar controles (caso más usual), se seleccionarán aquellos que se emplearán para disminuir el riesgo en etapas o periodos sucesivos.

   Como resultado de las actividades anteriores se ampliará el *Informe de Análisis y Gestión de Riesgos* que mostrará el nivel de cumplimiento actual de cada uno de los controles y el nivel de cumplimiento planificado. Este informe definirá las líneas de acción necesarias para conseguir un aumento del grado de cumplimiento de la norma ISO 27002 y el mapa de riesgo resultante (riesgo residual tras implantar los controles).

5. PLAN DE TRATAMIENTO DE RIESGOS. Se definirán las líneas de acción previstas para disminuir los niveles de riesgo a los nuevos niveles residuales.

6. IMPLEMENTACION DEL PLAN DE TRATAMIENTO DE RIESGOS. Las líneas de acción se describirán a modo de proyectos y actuaciones concretas quedando identificadas con un código.

11.5. Anexo

11.5.1. *Catálogo de amenazas*

TIPO DE AMENAZA	SUBTIPOS
[N] Desastres naturales: sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta	[N.1] Fuego. [N.2] Daños por agua.

TIPO DE AMENAZA	SUBTIPOS
	[N.*] Otros desastres naturales que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc.
[I] De origen industrial: sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada	[I.1] Fuego. [I.2] Daños por agua. [I.3] Contaminación mecánica. [I.4] Contaminación electromagnética. [I.5] Avería de origen físico o lógico. [I.6] Corte del suministro eléctrico. [I.7] Condiciones inadecuadas de temperatura y/o humedad. [I.8] Fallo de servicios de comunicaciones. [I.9] Interrupción de otros servicios y suministros esenciales. [I.10] Degradación de los soportes de almacenamiento de la información [I.*] Otros desastres industriales debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc.
[E] Errores y fallos no intencionados: fallos no intencionales causados por las personas. La numeración no es consecutiva, sino que está alineada con los ataques deliberados ([A]), muchas veces de naturaleza similar a los errores no intencionados, difiriendo únicamente en el propósito del sujeto.	[E.1] Errores de los usuarios. [E.2] Errores del administrador. [E.3] Errores de monitorización (log). [E.4] Errores de configuración. [E.7] Deficiencias en la organización. [E.8] Difusión de software dañino. [E.9] Errores de [re-]encaminamiento. [E.10] Errores de secuencia. [E.14] Escapes de información. [E.15] Alteración de la información. [E.16] Introducción de información incorrecta. [E.17] Degradación de la información. [E.18] Destrucción de la información. [E.19] Divulgación de información. [E.20] Vulnerabilidades de los programas (software). [E.21] Errores de mantenimiento / actualización de programas (software). [E.23] Errores de mantenimiento / actualización de equipos (hardware). [E.24] Caída del sistema por agotamiento de recursos. [E.28] Indisponibilidad del personal.
[A] Ataques intencionados: fallos deliberados causados por las personas. La numeración tampoco es consecutiva en este caso, para coordinarla con los errores no intencionados ([E]), muchas veces de naturaleza similar a los ataques deliberados, difiriendo únicamente en el propósito del sujeto.	[A.4] Manipulación de la configuración. [A.5] Suplantación de la identidad del usuario. [A.6] Abuso de privilegios de acceso. [A.7] Uso no previsto. [A.8] Difusión de software dañino. [A.9] [Re-]encaminamiento de mensajes. [A.10] Alteración de secuencia. [A.11] Acceso no autorizado. [A.12] Análisis de tráfico. [A.13] Repudio. [A.14] Intercepción de información (escucha). [A.15] Modificación de la información. [A.16] Introducción de falsa información. [A.17] Corrupción de la información. [A.18] Destrucción de la información. [A.19] Divulgación de información. [A.22] Manipulación de programas. [A.24] Denegación de servicio. [A.25] Robo. [A.26] Ataque destructivo. [A.27] Ocupación enemiga.

TIPO DE AMENAZA	SUBTIPOS
	[A.28] Indisponibilidad del personal. [A.29] Extorsión. [A.30] Ingeniería social.

12. PROCEDIMIENTO DE SALIDA DE INFORMACIÓN Y ENTRADA/SALIDA/TRASLADO DE SOPORTES Y EQUIPOS

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias
Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Gestión de Soportes Política de Seguridad Física del Equipamiento
Políticas, Procedimientos, Normas	Política de Intercambio de Información Procedimiento de Gestión de Soportes

12.1. Objeto

- Desarrollar las actividades necesarias para llevar a cabo la autorización de salida de información y entrada/salida de soportes o equipamiento.
- Implantar las medidas de seguridad adecuadas durante el transporte de los soportes.

12.2. Procedimiento

Este procedimiento **no será de aplicación** cuando:

- La información que contenga el soporte o equipo sea Pública en su totalidad. En este caso, solamente será necesario el paso para la protección física en el transporte.
- Cuando se trate de entrada/salida de un equipo por motivos de mantenimiento o restauración, en cuyo caso se eliminará previamente al traslado la información.

Los pasos a llevar a cabo cuando la información contenida en el soporte/equipo no sea de carácter Público son los siguientes:

7. Notificar, si procede, el movimiento del equipo/soporte a la División de Administración y Finanzas para su registro y gestión interna adecuada.
8. El usuario solicitará autorización para la salida de la información (contenida en un equipo o soporte o a través de la red o correo electrónico), a su responsable o Responsable de su Unidad, cumplimentando la información que aparece en el *Anexo A - Datos para la autorización de salida de información al exterior*.
9. Cuando se trate de entrada/salidas periódicas, se hará constar así en la solicitud indicando su periodicidad, y sólo será necesaria dicha solicitud y autorización la primera vez que se realice.
10. Se establecerán al menos, la siguientes medidas de seguridad física para protegerlos en su transporte:
    - Embalaje con protección contra golpes (si procede).
    - Etiqueta exterior indicando *Muy Frágil* (si procede).
    - Estará acompañado en todo momento por personal, no abandonando el vehículo de transporte o el equipo/soporte en sí durante el trayecto.

- Si la información contenida está clasificada como *Reservada Secreta,* o se trate de datos de carácter personal, se dotará de un embalaje resistente a robo y cerrado con llave o cerradura de seguridad o estará acompañado en todo momento por personal de seguridad especializado.

11. La Entrada/Salida de Soportes/Equipos deberá ser controlada y registrada por el Encargado de Seguridad de la Información, o en quién se delegue para esta acción. Los datos a incluir en el registro y formulario se muestran en el *Anexo B- Registro de Entrada de Soportes/Equipos*.

12. Cuando se envíe información a otras personas, bien en soportes o por cualquier otro medio, se incluirán indicaciones para que los destinatarios realicen la confirmación de la recepción al emisor. Para ello se adjuntarán los datos de contacto de este último, según el medio más conveniente a utilizar para dicha confirmación (nombre, dirección, teléfono, dirección de correo electrónico, etc.).

13. Fin del Procedimiento

12.3. Anexos

12.3.1. *Anexo A – Autorización de salida de información al exterior*

Datos a incluir:

- Fecha de Solicitud
- Nombre de solicitante y departamento
- Información contenida en el soporte/equipo/documento (con indicación de su clasificación)
- Tipo de soporte: Cinta, PC, PDA, Disco Duro, Documento...
- Nombre del destinatario
- Dirección completa de destino
- Forma de envío. Medidas de protección en el transporte
- Fecha de envío o en su caso, periodicidad

AUTORIZACIÓN DE SALIDA DE INFORMACIÓN AL EXTERIOR	
Fecha y Hora de Salida del soporte	
SOPORTE	
Tipo de soporte y número	
Contenido	
Ficheros de donde proceden los datos	
Clasificación y nivel de protección de los datos	
Fecha de creación	
FINALIDAD Y DESTINO	
Finalidad	
Dirección completa de destino	
Nombre del destinatario	
FORMA DE ENVÍO	
Medio de envío	
Nombre del remitente	
Medidas de protección para el transporte	
Fecha de envío	
AUTORIZACIÓN	

AUTORIZACIÓN DE SALIDA DE INFORMACIÓN AL EXTERIOR	
Persona responsable de la entrega	
Persona que autoriza	
Cargo / Puesto	
Observaciones	
Firma	

12.3.2. *Anexo B – Registro de Entrada/Salida de Soportes/Equipos*

Datos a incluir:

- Persona que realiza el envío/recepción
- Información contenida en el soporte/equipo/documento con indicación de su clasificación y, en caso de datos de carácter personal, de su nivel: alto, medio o básico
- Tipo: Cinta, PC, PDA, CD, documento, etc.
- Nombre del origen/destinatario
- Dirección completa de origen/destino
- Forma de envío. Medidas de protección en el transporte
- Fecha de envío o en su caso, periodicidad
-

REGISTRO DE ENTRADA/SALIDA DE SOPORTES/EQUIPOS						
E/S	FECHA Y HORA	EMISOR	RECEPTOR	NÚMERO DE SOPORTES/EQUIPOS	TIPO DE INFORMACIÓN CONTENIDA	MODO DE ENVÍO

13. PROCEDIMIENTO DE GESTION DE SOPORTES

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Gestión de Soportes
Políticas, Procedimientos, Normas	Política de Intercambio de Información Procedimiento de Etiquetado de Clasificación de los Activos e Información Procedimiento de Entrada/Salida de Soportes/Equipos

13.1. Objetivo

- Desarrollar las actividades necesarias para llevar a cabo la autorización de entrada/salida de soportes o equipamiento

- Implantar las adecuadas medidas de seguridad durante el transporte conforme a la *Política de Gestión de Soportes y la Política de Seguridad Física del Equipamiento.*

13.2. Procedimiento

13.2.1. *Soportes de información*

Están autorizados como soportes de almacenamiento de datos los siguientes tipos de soporte: Servidores, estaciones de trabajo, ordenadores portátiles, CD y DVD, cintas de backup, correo electrónico, PDA, memorias externas, documentos en papel, así como material fotográfico.

13.2.2. *Soportes gestionados por sistemas robotizados o automáticos (Cintas de BackUp)*

Los soportes de copias de seguridad se almacenan en las matrices de almacenamiento del equipo. A estos soportes sólo se puede acceder mediante sus correspondientes herramientas software que gestionan su funcionamiento, por lo que no es necesario su etiquetado. El inventario de los soportes es llevado a cabo por las propias herramientas.

Estos soportes no salen del armario robotizado salvo en caso de defectos de funcionamiento, o de que venza el tiempo de vida estipulado.

Como medida de seguridad adicional para recuperación ante desastres se realizará periódicamente una segunda copia del contenido de estas cintas que se traslada a otras dependencias, almacenándose en una caja fuerte. A estas copias, convenientemente etiquetadas con la información indicada en el *Anexo A – Etiquetado de Soportes*, sólo tiene acceso el personal autorizado por el Comité de Seguridad (*Anexo C – Personal con acceso autorizado a los soportes de copias de seguridad*).

13.2.3. *Copias de Seguridad en dependencias externas al CPD*

Las copias de seguridad en dependencias ajenas al CPD (otras sedes) se realizan a través de un disco duro externo. Estas copias de seguridad se etiquetarán con la información del *Anexo A – Etiquetado de Soportes*, así como también se actualizará el inventario según el *Anexo B – Inventario de Soportes*. El personal detallado en el *Anexo C – Personal con acceso autorizado a los soportes de copias de seguridad y discos duros externos* será el único con acceso a estos elementos de copias de seguridad.

13.2.4. *Acceso a los soportes de copias de seguridad*

Las personas con acceso a los soportes de copias de seguridad se relacionan en el *Anexo C – Personal con acceso autorizado a los soportes de copias de seguridad y discos duros externos.*

13.2.5. *Almacenamiento de documentos en papel*

Todos los documentos en papel con clasificación *Reservada Secreta* o con datos de carácter personal, son almacenados en armarios/cajoneras bajo llave, teniendo acceso a ellos exclusivamente el personal autorizado del mismo.

13.2.6. *Traslado*

El traslado de los soportes se realizará conforme al Procedimiento de Entrada/Salida de Soportes/Equipos y bajo los términos de un contrato en el que se reflejen las condiciones adecuadas de confidencialidad y protección de los soportes en el traslado en caso de utilizarse una empresa externa para ejecutar dicha actuación.

13.2.7. *Baja y reutilización de soportes*

En caso de reutilización de los soportes, se procederá a su borrado previo mediante una herramienta o método que permita hacerlo de forma segura.

Los soportes que no vayan a ser utilizados más, debido fundamentalmente a su deterioro, serán completamente destruidos antes de ser desechados.

La destrucción física de los soportes magnéticos se realizará sacando completamente la cinta y asegurándose de que queda completamente destrozada (pueden usarse elementos mecánicos de destrucción, como, por ejemplo, una sierra radial).

Para la información que pudiera estar en soporte óptico, se romperá físicamente el soporte.

13.2.8. *Documentos en papel*

En el caso del papel, se romperá lo suficiente para que su información no pueda ser recuperada. Cuando contenga información clasificada como Reservada-Secreta y no deba ser retenida, se utilizará una destructora de documentos.

13.3. Anexos

13.3.1. *Anexo A – Etiquetado de Soportes*

Los soportes externos deberán llevar una etiqueta identificativa de su contenido, cuyo formato es el siguiente:

Nº	Clasificación	Sistema
Fecha	Tipo Copia	

13.3.2. *Anexo B – Inventario de Soportes*

El inventario de soportes se encuentra en la Unidad de Informática.

13.3.3. *Anexo C – Personal con acceso autorizado a los soportes de copias de seguridad y discos duros externos*

PERSONAL CON ACCESO A SOPORTES DE COPIAS DE SEGURIDAD

14. PROCEDIMIENTO DE DESARROLLO DE APLICACIONES INFORMATICAS

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de la Unidad Informática
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política - Operación y mantenimientos por terceros Política - Aceptación de Nuevos Productos y Sistemas
Políticas, Procedimientos, Normas	Procedimiento de Gestión de Cambios y Versiones Procedimiento de Comunicación, Gestión y Respuesta ante Incidentes Procedimiento de Aceptación de Nuevos Sistemas y Productos Procedimiento de Puesta en Producción de Sistemas de Información Procedimiento de Etiquetado y Clasificación de Activos

14.1. Objetivo

- El objetivo de este procedimiento es el de establecer las actividades, herramientas y personal implicado en el desarrollo de aplicaciones informáticas

14.2. Procedimiento

14.2.1. *Estudio de Viabilidad del sistema*

La primera actividad a desarrollar antes de plantearse la creación de un nuevo sistema software es la de estudiar la viabilidad del sistema.

Para ellos, el responsable del servicio al que dará soporte dicha aplicación debe definir los objetivos de negocio que debe soportar ese software.

A posteriori, el responsable de la unidad informática debe extraer los requisitos técnicos que deberá cumplir ese software en base a los requisitos de negocio. En ese momento, hay que realizar un análisis de si es viable o no, en términos presupuestarios, de esfuerzo y medios, el desarrollar la aplicación informática.

Como producto de esta fase tendremos un informe que contendrá el análisis realizado y la decisión de la viabilidad del proyecto.

14.2.2. *Estimación del esfuerzo*

Una vez, el estudio de viabilidad da paso a comenzar esta fase, es necesario realizar una estimación del esfuerzo (horas) que cuesta desarrollar el sistema informático. Para ellos se pueden utilizar una de las siguientes técnicas:

1. Estimación con UCP (puntos de casos de uso).
2. Estimación puntos de función.
3. Estimación Delphi (opinión de experto).

Bien es cierto que una versión en borrador de la estimación, ha debido surgir de la actividad anterior.

La utilidad de esta actividad es ayudar a la hora de decidir si el desarrollo se puede acometer *in-house* o debería ser subcontratado y a su vez, tener una estimación en tiempo y económica aproximada para publicar el concurso público o cualquier otro medio que el Gobierno Regional utilice para subcontratar trabajo.

Como producto de esta fase tendremos un documento que contiene la valoración aproximada en horas del coste del proyecto.

14.2.3. *Decisión de desarrollo interno o externalización*

Como se ha dicho en la actividad anterior, el responsable del servicio y de la unidad informática deben decidir si asumen el coste del desarrollo o es mejor subcontratarlo.

Para ello se debe hacer un análisis de las jornadas disponibles por funcionarios técnicos del Gobierno Regional, conocimientos técnicos necesarios y el plazo necesario para la ejecución (en base a los objetivos de negocio).

Bien es cierto que el Gobierno Regional puede decidir subcontratar todo o parte del proyecto. Esta decisión también debe tomarse en esta fase.

Como producto de esta fase tendremos un informe que contiene la decisión de si el desarrollo se hace *in-house* o se externaliza, incluyendo las razones que han llevado a esa conclusión.

14.2.4. *Planificación del desarrollo*

Asumiendo que el desarrollo se hiciese *in-house* por funcionarios del Gobierno Regional, en este caso procedería comenzar con una planificación del trabajo, para ello, lo primero que hay que hacer es descomponer el proyecto en módulo o bloques, también llamados *Work Breakdown Structure (WBS)*. Dichos bloques permiten una gestión del proyecto más eficiente. Cada bloque debe tener finalizar en un entregable ya sea documental o de código.

La planificación debe tener en cuenta las variables:

- Estimación del esfuerzo
- Recursos disponibles
- Calendario laboral
- Plazos de los objetivos del negocio

14.2.4.1.1 Planificación de los WBS

De la planificación del proyecto, se debe extraer un diagrama de *Gantt* que no es más que una foto del proyecto por tareas a lo largo del tiempo. Para ello se empleará la herramienta estándar de la unidad informática para planificar proyectos de índole tecnológica.

La planificación resultante deberá ser volcada en la herramienta software del Gobierno Regional destinada a la gestión de proyectos de índole técnica.

14.2.4.1.2 Planificación de las Pruebas

Es muy importante tener en cuenta que la fase de Pruebas del software no atañe únicamente al código fuente sino también a los entregables documentales (Catálogo de Requisitos, Análisis Funcional, etc...) y que la fase de pruebas nace y muere con el proyecto, esto debe estar reflejado en la planificación del proyecto incluyendo el Plan de Pruebas del proyecto.

Como producto de esta fase tendremos el Plan de Proyecto.

14.2.5. *Desarrollo de Requisitos*

Lo primero a realizar antes del desarrollo es la definición del Catálogo de Requisitos. En las actividades previas a esta, ya se han esbozado los requisitos de negocio y técnicos del proyecto.

En esta fase, cada requisito debe quedar completamente definido e identificado (identificadores únicos) de manera que no sean ambiguos y que sean suficientemente claros como para que un técnico pueda realizar un análisis/diseño funcional del sistema en base a los requisitos.
Como producto de esta fase tendremos el Catálogo de Requisitos.

14.2.5.1 Validación del Catálogo de Requisitos

El Catálogo de Requisitos debe ser validado tanto por la parte responsable del servicio y unidad informática como por el responsable del desarrollo del software de manera que todos tengan conocimiento de los mismos requisitos y los comprendan de la misma manera.
Por otro lado, hay que validar que los requisitos son:

- Claros.
- Completos.
- Son consistentes los unos con los otros y los objetivos de negocio.
- No ambigüedad.
- Viables en su implementación.
- Verificables (testeables).
- Trazables.

14.2.5.2 Trazabilidad

La trazabilidad consiste en que todos los requisitos deben ser trazables con su caso de uso (diseño) y sus pruebas en ambas dirección:
Requisitos <<->> caso de uso <<->> caso de prueba
De esta manera aseguramos que todos los requisitos serán diseñados e implementados y que han podido ser probados.

14.2.6. *Diseño de arquitectura*

En esta tarea se diseña la arquitectura de la solución en una estructura de módulos y capas en los que se definen los elementos estructurales y los mecanismos de coordinación necesarios para satisfacer los requisitos de la aplicación.
Toda la definición de arquitectura se realizará utilizando una herramienta CASE estándar en la cual se tendrá el modelado completo del proyecto. Las tareas a realizar serán:

- Definición de la Arquitectura
- Lista de componentes a comprar/reutilizar
- Definición de la Arquitectura. Modelo lógico
- Definición de la Arquitectura. Modelo de desarrollo
- Definición de la Arquitectura. Modelo de procesos
- Definición de la Arquitectura. Modelo físico
- Validación de la Arquitectura
- Definición de las notas globales de la Arquitectura
- Aplicación base

14.2.7. *Análisis Funcional*

En esta tarea se analiza el Catálogo de Requisitos que el sistema requiere, con objeto de obtener una documentación detallada de las distintas funcionalidades que debe implementar la aplicación, así como de las clases del dominio de la aplicación y del interfaz de usuario, de modo que sirvan de entrada para la fase de diseño técnico.

Toda la definición de análisis funcional se realizará la herramienta CASE estándar en la cual se tendrá el modelado completo del proyecto. Las tareas a llevar a cabo son:

- Definición de los casos de uso
- Definición de los escenarios de pruebas

- Definición del modelo de dominio
- Definición de la interfaz de usuario
- Definición del modelo de datos
- Análisis funcionales
- Validación funcional
- Confección de la Matriz de trazabilidad requisitos-casos de uso
-

14.2.8. *Diseño Técnico*

En esta tarea se especifica el "cómo" llevar a cabo las funcionalidades indicadas en los análisis funcionales bajo la arquitectura del proyecto, con objeto de obtener una documentación técnica detallada de las codificaciones que el programador debe realizar en cada una de las capas definidas en la arquitectura de forma que no tenga dudas sobre lo que tiene que hacer.

Toda la definición de diseño técnico se realizará en la plantilla EA estándar en la cuál se tendrá el modelado completo del proyecto. Las tareas a llevar a cabo son:

- Definición del diagrama de clases
- Definición del diagrama de secuencias
- Definición del modelo de datos

- Definición de las pruebas unitarias

14.2.9. *Codificación*

Una vez se tiene realizado el diseño técnico, se entra en la fase de la codificación del proyecto utilizando el entorno tecnológico correspondiente a la tecnología a utilizar.

Se deberá utilizar un sistema de control de versiones para controlar el código fuente que se va generando.

14.2.10. *Pruebas*

Las pruebas a ejecutar sobre el código fuente deben ser:

- Unitarias: Una vez finalizado el desarrollo de cada clase o componente.
- Integración: Una vez diferentes módulos que interactuarán entre ellos mediante interfaces han sido desarrollados, estos deben ser probados en un entorno de integración. Comprobando cada interfaz y sus posibles respuestas.
- Sistema: Pruebas en las que se certifica que el software desarrollado funciona, interactuando con terceros sistemas y en ele entorno hardware y software definitivo.
- Carga y estrés: Pruebas que miden el rendimiento del sistema.

14.2.11. *Empaquetado y entrega*

Una vez se ha finalizado y probado el desarrollo, debe ser empaquetado para el despliegue en su entorno final. Hay que tener en cuenta que en el paquete debe estar:

- Código fuente compilado
- Scripts de base de datos
- Ficheros de configuración
- Manual de despliegue
- Manual de usuario
- Manual de administración

El compilado y empaquetado del código fuente debe ser una tarea automatizable mediante alguna herramienta disponible para la tecnología utilizada.

Cada entrega validada deberá ser etiquetada dentro del sistema de control de versiones como línea base del proyecto.

15. PROCEDIMIENTO DE ADQUISICIÓN, ACEPTACION O AUTORIZACION DE NUEVOS SISTEMAS Y PRODUCTOS

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de la Unidad Informática
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Aceptación de Nuevos Productos y Sistemas
Políticas, Procedimientos, Normas	Procedimiento de Gestión de Cambios y Versiones Procedimiento de Desarrollo de Aplicaciones Informáticas

15.1. Objetivo

- El objetivo de este procedimiento es el de establecer las actividades, herramientas y personal implicado en las tareas para la adquisición, aceptación o autorización de sistemas informáticos.

15.2. Procedimiento

15.2.1. *Identificación de necesidades*

En esta actividad se trata de identificar las distintas soluciones que pueden encajar con el proyecto según los requisitos indicados ya sean soluciones basadas en elementos reutilizables propios o bien COTS, evaluarlas y definir unos criterios de selección para poder realizar una selección final.
A la hora de tomar una decisión sobre qué solución aplicar, puede ser necesario ejecutar una técnica de toma de decisiones en la que un grupo de entendidos sobre la materia deciden la solución a implementar.

15.2.2. *Solicitud de adquisición*

Una vez se tiene claro qué es lo que se necesita, es necesario realizar una solicitud interna de adquisición del hardware o software necesario. Para ellos, el responsable de la unidad de informática deberá pedir presupuesto a aquellos proveedores habituales de los elementos en cuestión.
También será necesario evaluar a los propios proveedores para tomar una decisión final.
Finalmente, la solicitud debe estar ingresada en el sistema de gestión de cambios ya que ya sea una compra o modificación de un activo nuevo, deber estar gestionado mediante el proceso de Control de Cambios.

15.2.3. *Solicitar respuestas de proveedores*

En el proceso de oferta se eligen y desarrollan los documentos para tratar de comunicar las necesidades de la empresa que emite la oferta a los proveedores y el nivel de detalle de la solución que espera recibir.
Los principales métodos para obtener información de los proveedores son:

- RFI (*Request for information*) – Solicitud de información.
- RFP (*Request for proposal*) – Solicitud de propuesta.
- RFQ (*Request for quotation*) – Solicitud de presupuesto.
- IFB (*Invitation for Bid*) - Solicitud para ofertar.

15.2.4. *Aceptación*

Finalmente, una vez el producto está listo para ser recepcionado, el responsable de la unidad informática debe comprobar y validar que la entrega cumple con los requisitos que dieron lugar a la compra del mismo.
Para ello, deberá testear la entrega en base a un plan de pruebas o criterios de aceptación de la adquisición.

De esta fase debe liberarse un documento firmado por el responsable de la unidad informática en la que explícitamente, acepta la entrega recepcionada, asumiendo que esta cumple con los requisitos esperados.

15.2.5. *Autorización*

El responsable de la unidad informática también puede autorizar a otros funcionarios sobre los que el delegue, la compra y recepción de material TI (hardware y Software) para el Gobierno Regional.

Para ello, dicho responsable debe enviar un correo electrónico a la persona sobre la que delegue, especificando claramente el ámbito de la delegación y los objetivos que se persiguen, así las causas por las que éste delega dichas tareas.

16. PROCEDIMIENTO DE COPIAS DE SEGURIDAD (BACKUP)

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de la Unidad Informática
Personal de Operación	

Referencias
Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Copias de Seguridad
Políticas, Procedimientos, Normas	Procedimiento de Gestión de Cambios y Versiones Procedimiento de Comunicación, Gestión y Respuesta ante Incidentes Procedimiento de Administración de la Continuidad Procedimiento de Restaurado de la Información

16.1. Objetivo

- El objetivo de este procedimiento es el de establecer las actividades, herramientas y personal implicado en las tareas para la realización de las copias de seguridad o respaldo de los sistemas de información del Gobierno Regional.

16.2. Procedimiento

16.2.1. *Datos a incluir*

Lo primero que hay que establecer, es qué información es de la que se debe hacer copia de seguridad. El criterio en este caso es la criticidad de dichos sistemas para el correcto funcionamiento del Gobierno Regional.

Como resultado de esta fase, se debe generar un documento en el que se especifique la información y sistemas de los que hay que hacer backup así como de su ubicación, en definitiva, establecer el Plan de backups del Gobierno Regional. Los apartados a tener en cuenta en dicho plan son:

- Sistemas y/o ficheros de los que hacer copia
- Ubicación de las fuentes de la información.
- Periodicidad de las copias
- Destino de las copias

Para la catalogación de la criticidad de los sistemas de información, se seguirá el siguiente criterio:

- Alta: Los sistemas /ficheros son fundamentales para el funcionamiento del Gobierno Regional.
- Media: Los sistemas/ficheros son importantes para el funcionamiento de algún área del Gobierno Regional.
- Baja: Los sistemas/ficheros son útiles para personas dentro de los departamentos del Gobierno Regional.

16.2.2. *Frecuencia de las copias*

Se establece que la frecuencia de las copias debe realizarse:

- Diariamente: para los sistemas/ficheros catalogados con criticidad Alta.
- Semanales: para los sistemas/ficheros catalogados con criticidad Media.
- Mensual: para los sistemas/ficheros catalogados con criticidad Baja.

Dichas copias, serán realizadas por el sistema de backup disponible en el Gobierno Regional que se basará, en esta fase en discos duros físicos del servidor de copias de seguridad.

Por otro lado, se deberá realizar copias a cinta trimestrales. Dichas cintas deberán ser guardadas en lugar seguro y por un periodo mínimo de cinco años. Una vez cumplido dicho plazo, las cintas pueden ser utilizadas de nuevo.

16.2.3. *Generaciones de datos*
El número de generaciones de datos que se deben conservar va en función de la criticidad, para:

- Información de criticidad Alta: Se conservarán las últimas siete generaciones en disco.
- Información de criticidad Media: Se conservarán las últimas tres generaciones en disco.
- Información de criticidad Baja: Se conservarán las últimas dos generaciones en disco.

16.2.4. *Lugares utilizados*
Los lugares utilizados para realizar las copias de seguridad serán:

- Copias a disco: Sistemas de backup disponible en el Gobierno Regional. Dicho sistema debe disponer por un lado de un software capaz de realizar la copia de manera automatizada de los sistemas necesarios así como un hardware de respaldo con espacio en disco suficiente para la información a tener guardada así como de todas sus generaciones.

  Es decir, la capacidad del sistema de backup deberá estar dimensionada acorde a las necesidades del Gobierno Regional.

- Copias a cinta: Las copias a cinta se realizarán dentro del sistema de backup por otra unidad diferente a la de copias a disco. Dicho sistema deberá ser capaz de rotar las cintas de manera mecánica.

  Las cintas trimestrales serán almacenadas en cajones ignífugos dentro de las dependencias del Gobierno Regional.

16.2.5. *Comprobación de los backups*
Se debe realizar una comprobación de consistencia y validez de los backups una vez cada dos meses para comprobar que el sistema de backup es efectivo.

Para ello, el responsable de la unidad informática debe realizar un simulacro de pérdida de un sistema y restaurar una copia de cualquier sistema de información almacenado en el sistema de backup, tanto a disco como a cinta, en un entorno dedicado a dicha prueba, es decir, no sobre el entorno real del que se hizo copia.

La persona responsable de la información con la que se ha hecho la prueba, debe verificar que el sistema ha sido restaurado con éxito.

17. PROCEDIMIENTO DE RESTAURADO DE LA INFORMACIÓN

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de la Unidad Informática
Personal de Operación	

Referencias
Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Copias de Seguridad
Políticas, Procedimientos, Normas	Procedimiento de Gestión de Cambios y Versiones Procedimiento de Comunicación, Gestión y Respuesta ante Incidentes Procedimiento de Administración de la Continuidad Procedimiento de Copias de Seguridad

17.1. Objetivo

- El objetivo de este procedimiento es el de establecer las actividades, herramientas y personal implicado en las tareas para la realización de la restauración de información importante perdida o dañada en los sistemas del Gobierno Regional.

17.2. Procedimiento

Si se ha perdido el acceso a una información almacenada, dicha pérdida puede no ser definitiva si existen medios para restaurar la disponibilidad de acceso, en cuyo caso se puede plantear la recuperación de la información. El acceso a la información se puede perder por varios motivos, como son:

- Porque el dispositivo tiene dañado algún componente físico necesario para su funcionamiento.
- Porque, aún funcionando correctamente, la "lista de archivos" se ha corrompido impidiendo conocer la ubicación de los archivos almacenados.
- Porque los datos almacenados han sido remplazados por nuevos datos a través de la sobre-escritura.

En los dos primeros casos se puede intentar un proceso de recuperación, en el tercero no puede realizarse ya que esos datos ya no existen y por tanto no pueden recuperarse.

17.2.1. *Solicitud de restauración*

La solicitud para la restauración de una copia de disco o cinta deberá realizarse mediante el uso de la herramienta de atención al usuario o, en su defecto mediante correo electrónico al responsable de la unidad de informática del Gobierno Regional, indicando la información concreta (sistema o fichero) así como las razones para dicha restauración y la urgencia de la misma.

Una vez dicha solicitud llegue al responsable de la unidad informática, valorará la urgencia de la situación, viabilidad de la restauración y éste planificará la restauración, haciéndoselo saber al solicitante.

17.2.2. *Recuperación*

Una vez se va a abordar la recuperación de la información, en base a su causa, ésta puede realizarse de dos maneras

- Recuperación física: Se da en los casos en los que los dispositivos de almacenamiento de origen están dañados. En esos casos, antes de la restauración de la información, se deberá proceder a decidir si se puede reparar el dispositivo o aplica su sustitución.

  Esta decisión es exclusiva del responsable de la unidad de informática o persona sobre la que éste delegue.

- Recuperación lógica: Se da en los casos en las que los dispositivos de almacenamiento originales están en perfectas condiciones y es solo la información la que está corrupta. En estos casos, basta con restaurar la última copia que esté almacenada en los discos duros del sistema de backup para esa fuente de información que, dependiendo de su criticidad tendrá x días de antigüedad.

  El software del sistema de backups debe incluir la opción de restaurar las copias que tiene definidas realizar mediante un interfaz software.

17.2.3. *Verificación de la recuperación*

Una vez haya sido restaurada la copia, el responsable de la unidad de informática deberá informar al solicitante para su comprobación. El solicitante deberá comprobar que la restauración de la información ha concluido con éxito.

Éste hecho debe ser comunicado bien mediante el ticket abierto en la herramienta de atención al usuario o mediante correo electrónico, por el solicitante, al responsable de la unidad de informática.

18. PROCEDIMIENTO DE PUESTA EN PRODUCCION DE SISTEMAS DE INFORMACIÓN

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Política de Aceptación de Nuevos Productos y Sistemas
Políticas, Procedimientos, Normas	Procedimiento de Aceptación de Nuevos Sistemas y Productos

18.1. Objetivo

- Establecer y describir las tareas a desarrollar para efectuar la puesta en producción de los proyectos y nuevos sistemas de información, a fin de minimizar el riesgo de alteración de los sistemas productivos. Se aplicará tanto para los casos de que los desarrollos se ejecuten en las instalaciones del proveedor como en el caso de que se desarrolle en las propias instalaciones (aunque sea por parte de un tercero en modalidad "outsourcing").

18.2. Definiciones

- **Entorno de desarrollo**: Conjunto de normas, procesos y controles que rigen desde la presentación formal de una modificación/creación de un sistema informático por parte de la autoridad solicitante, hasta su entrega por parte de los desarrolladores.

- **Entorno de pruebas:** Conjunto de normas, procesos y controles que rigen desde la entrega del sistema informático por parte de los desarrolladores para su testeo, hasta la aceptación por parte de la autoridad solicitante. Incluye todas las pruebas necesarias del sistema para comprobar su buen funcionamiento y fiabilidad.

- **Entorno de Producción:** Programas informáticos puestos al alcance de los usuarios finales con sus respectivos permisos de acceso. Incluye además las tareas de realización de copias de seguridad de los datos y de las versiones anteriores de los sistemas.

- **Código Fuente:** conjunto de instrucciones que componen un programa o aplicación informática.

- **Código Ejecutable:** es un archivo binario cuyo contenido se interpreta por el ordenador como un programa.

18.3. Responsabilidades

Dentro del circuito de puesta en producción de un sistema existen diferentes roles según las acciones a realizar:

- **Responsable de la solicitud:** Persona con autoridad máxima para solicitar modificaciones a un sistema o la implementación de un nuevo sistema. Asimismo será el responsable de dar la aceptación formal de las pruebas, garantizando que cumple con los requerimientos solicitados.

- **Responsable Entorno de Pruebas**: Persona responsable de supervisar el cumplimiento del actual procedimiento sobre las aplicaciones soportadas.

- **Responsable del Desarrollo de la aplicación:** Persona responsable del cumplimiento del actual procedimiento para una aplicación en concreto, particularmente sobre las tareas relacionadas con el entorno de desarrollo y el proceso de backup de las aplicaciones soportadas.

- **Desarrollador o Proveedor del sistema:** Persona responsable de la construcción del código, efectuar las pruebas en el entorno de desarrollo y dejar listo el código fuente para que el administrador de versiones de continuidad al circuito. Asimismo es responsable de desarrollar o actualizar la documentación del sistema técnico y de usuario.

18.4. Procedimiento

El procedimiento general sigue las siguientes etapas:

Entorno de Desarrollo (según disponibilidad del entorno)

1. El Responsable de la Solicitud presenta el *Formulario 1 Pedido de Software o Modificación de Software*, según sea el caso, mediante el cual solicita la creación/modificación de un sistema.
2. El Responsable del Desarrollo de la aplicación determina si el requerimiento es válido o no. En el caso de que sea válido, asigna el trabajo a un grupo de desarrollo, de lo contrario devuelve el requerimiento al solicitante para q la corrija.

Entorno de Pruebas (según disponibilidad del entorno)

1. En caso que el requerimiento sea de modificación de un sistema ya existente, el desarrollador copia los programas fuentes al Entorno de Pruebas informando al Responsable de Desarrollo (notificación vía mail).
2. Actualización de bibliotecas de programas fuente y distribución de programas fuente a los programadores, con la autorización del Responsable asignado para el desarrollo de la aplicación pertinente.
3. Recibidos los archivos fuente del Desarrollador, el personal del Entorno de Pruebas pide modificación de los accesos a la Unidad de Informática para poder almacenarlos en un directorio de su entorno.
4. Posteriormente se compila y se permite que el desarrollador y el Responsable de la Solicitud (o en quién delegue) prueben en el Entorno de Pruebas el sistema. Si el Responsable de la Solicitud está de acuerdo con el desarrollo, firma el *Formulario 3 de Aceptación Final de Sistema.*
5. El Responsable del Desarrollo de la aplicación autoriza mediante el *Formulario 4 de Paso del Sistema a Producción*, el paso del Sistema desde el Entorno de Pruebas al Entorno de Producción. En esta etapa el desarrollador entrega al personal de Entorno de Pruebas toda la documentación del Sistema para su almacenamiento

Entorno de Producción

1. Una vez que el Responsable del Desarrollo de la aplicación autoriza el traspaso del sistema al Entorno de Producción, desde la Unidad de Informática se habilitarán los accesos necesarios para poder copiar el nuevo Sistema y se almacenar la versión que funciona en la actualidad a la carpeta o herramienta que albergue el histórico de versiones.
2. FIN PROCEDIMIENTO

18.5. Controles de Seguridad

Los controles mínimos que se contemplan en el **Entorno de Desarrollo** son:

- La tarea del desarrollador comienza solamente después de presentado el pedido formal firmado por la autoridad máxima solicitante.
- Ante la implementación de un sistema nuevo o cambios sobre sistemas ya existentes, el personal de desarrollo efectúa la construcción del código y las pruebas correspondientes, dejando listo el código fuente en un directorio del Entorno de Pruebas para dar continuidad al circuito.
- En caso de modificación de un sistema existente, la actualización de bibliotecas de programas fuentes y la distribución de programas fuentes a los programadores, sólo debe ser llevada a cabo por el personal del Entorno de Pruebas.

Los controles mínimos que se contemplan en el **Entorno de Pruebas** son:

- El personal de Pruebas debe copiar el código fuente del directorio de desarrollo (donde previamente había sido almacenado por los desarrolladores) y copiarlo al directorio de pruebas, para ser compilado por personal del mismo departamento.
- Una vez compilado, debe comenzar el testeo a cargo del solicitante del requerimiento.
- La actualización de las bibliotecas de programas de producción sólo debe ser realizada una vez autorizada adecuadamente por el responsable de la solicitud del requerimiento.
- El código ejecutable no debe ser implementado en un sistema de producción hasta que no se obtenga evidencia del éxito de las pruebas y se hayan actualizado las correspondientes bibliotecas de programas fuente.
- Garantizar que el usuario autorizado acepte los cambios antes de cualquier implementación según *Formulario 3 de Aceptación Final de Sistema.*

Los controles mínimos que se contemplan en el **Entorno de Producción** son:

- Una vez que el Responsable de la Solicitud acepta los cambios, se mueve el programa compilado desde el directorio del Entorno de Pruebas al directorio correspondiente del Entorno de Producción.
- Las versiones anteriores de los programas fuente deben ser archivadas con una clara indicación de las fechas y horas precisas en las cuales estaban en producción, junto con todo el software de soporte, el control de tareas, las definiciones de datos y los procedimientos.
- Se debe evitar el acceso a los servidores de producción por parte de los proveedores de sistemas. Solo debe otorgarse acceso lógico o físico a los proveedores con fines de soporte y si resulta necesario, y previa aprobación del Responsable del Desarrollo de la aplicación y del Responsable del

Entorno de Producción. Las actividades del proveedor deben ser monitoreadas a través de *logs* de auditoría de las tareas realizadas.

- Actualizar la documentación del nuevo sistema, archivando la documentación anterior.

18.6. Pruebas con datos reales o en producción

Se debe evitar el uso de bases de datos con datos de producción que contengan información personal real. Si se utiliza información de esta índole, esta debe ser despersonalizada o disociada antes del uso:

- Se debe llevar a cabo una autorización por separado (firmado por el Responsable del Desarrollo de la aplicación) según *formulario Copia de Base de Datos de Producción a Desarrollo*, cada vez que se copia información de producción a un sistema de pruebas a fin de suministrar una pista de auditoría.
- Se debe borrar la información de producción de un sistema de prueba inmediatamente después de completada la misma.

18.7. Registro

Cualquier actividad realizada a la hora de efectuar un paso al Entorno de Producción desde el Entorno de Desarrollo pasando por el Entorno de pruebas debe quedar registrada para ello se mantiene:

- Un registro de todas las solicitudes de cambios.
- Un registro de auditoría de todos los accesos a las bibliotecas de programa fuente.
- Un registro de todas las actualizaciones a las bibliotecas de programas de producción.

18.8. Formulario 1: Pedido de Software

Formulario: Pedido de Software
Nº Formulario:

_____, _____ *de*_____*de 20*__

Por la presente solicito a la Unidad de Informática _____ *el desarrollo de un Software para* _____ *con el fin de poder informatizar los trabajos que a continuación se detallan:*

1. _____
2. _____
3. _____
4. _____
5. _____

Características especiales:

_____

_____

Firma y Cargo:

_____

18.9. Formulario 2: Modificación de Software

Formulario: Modificación de Software.
Nº Formulario:

_____, _____ *de* _____*de 20*__

Por la presente solicito a la Unidad de Informática los cambios en el Software de _____ *con el fin de poder adaptar el mencionado software a las necesidades de nuestros trabajos administrativos, a continuación dejamos un detalle de las modificaciones pedidas.*

Modificaciones:

1. _____
2. _____
3. _____
4. _____
5. _____

Características especiales:

_____

_____

Firma y Cargo:

_____

18.10. Formulario 3: Aceptación final de Sistema

Formulario: Aceptación final de Sistema

_____, _____ de_____de 20__

Por la presente acepto en total conformidad la creación / modificación del sistema solicitado en el Formulario nº_____ presentado con fecha _____, después de haber realizado las pruebas y testeos de funcionamiento correspondientes.

_____ _____

Firma y Cargo:

_____

18.11. Formulario 4: Paso del Sistemas a Producción

Formulario: Paso del Sistema a Producción

_____, _____ de_____de 20__

Por la presente autorizo el paso del sistema solicitado en el Formulario nº _____ presentado con fecha _____, desde el Entorno de Pruebas al Entorno de Producción.

Firma y Cargo:

_____

18.12. Formulario 5: Copias de Base de Datos de Producción a Desarrollo

Formulario: Copia de Base de Datos de Producción a Desarrollo.

Nº Formulario:

_____, _____ de_____de 20__

Por el siguiente formulario autorizo la copia de las siguientes bases del Entorno de Producción al Entorno de Desarrollo:

a. _____

b. _____

c. _____

d. _____

Firma y cargo

_____

19. PROCEDIMIENTO DE PUESTA EN PRODUCCION Y EXPLOTACION DE EQUIPOS DE COMUNICACIONES Y SEGURIDAD DE RED

Ver documento "Manual de Procedimientos de Puesta en Producción y Explotación de Equipos de Comunicaciones y Seguridad de Red".

20. PROCEDIMIENTO DE AUDITORIA Y REGISTRO (LOGS) DE SISTEMAS

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Manual de Procedimientos de Seguridad de la Información. Apartado 11.1. "PROCEDIMIENTO- Protección de los Registros del Servicio". (es un complemento al mismo)
Políticas, Procedimientos, Normas	Procedimiento de Comunicación, Gestión y Respuesta ante Incidencias

20.1. Objetivo

- Conseguir la correcta recolección, almacenamiento y mantenimiento de los eventos de seguridad relevantes en los sistemas de información.

20.2. Procedimiento

Se activará la auditoría y se registrarán los sucesos correspondientes, ocurridos en los sistemas.

20.2.1. *Configuración de Auditorías de los Sistemas*

Para cada uno de los sistemas se realizarán las siguientes tareas:

1. RESPONSABILIDADES: Nombrar a una persona o grupo como Responsable del Registro, que realizará las operaciones necesarias para la correcta configuración de la auditoría y la revisión de los registros de sucesos. Siempre que sea posible esta persona será distinta del Administrador del Sistema. El Anexo A. detalla los responsables de registro de los sistemas, aplicaciones o servicios

2. PLAN DE REGISTRO AUDITORIA: crear un Plan de Registro de Auditoría tanto para el sistema operativo como para los servicios (ejemplo, servidor de páginas Web) y aplicaciones instaladas en el sistema. En este plan se definirán los tipos de sucesos concretos que se van a registrar, que se seleccionarán teniendo en cuenta que los registros de auditoría:

   - Ocupan espacio en disco y otros recursos del sistema (CPU, memoria...)
   - Ocupan tiempo para su revisión
   - Deben ser suficientes y no excesivos para alcanzar el objetivo: detectar intentos de intrusión, detectar errores, operaciones que realizan los usuarios, etc.

   Se registrarán como mínimo los siguientes sucesos, además de aquellos que por la naturaleza del sistema concreto se consideren de interés:

   - Activación y desactivación del proceso del registro
   - Cambios en la configuración de la auditoría
   - Cambios en las configuraciones en el sistema, aplicación o servicio en sí.
   - Cambios en las políticas de los cortafuegos
   - Inicios de sesión con éxito. Los intentos fallidos de sesión se activaran únicamente cuando sea estrictamente necesario para la detección de intrusos, ya que podrían dar lugar a una denegación de servicio.
   - Intentos fallidos de acceso a recursos u objetos concretos (archivos, carpetas, puertos, servicios, etc.) debido a permisos insuficientes. Activar esta auditoría indiscriminadamente puede consumir gran cantidad de recursos
   - Cambios exitosos en la administración de cuentas de usuario
   - Cambios en los privilegios de usuario
   - Acciones que realicen los usuarios privilegiados, como el arranque y parada de servicios o del sistema.
   - Activación/desactivación o modificación de los controles de seguridad instalados en los sistemas
   - Fallos o errores del sistema, aplicaciones y servicios

   Para cada evento se almacenarán al menos, los siguientes datos:

   - Identificación del usuario
   - Fecha, hora
   - Tipo y descripción del evento
   - Origen del evento

- Recurso sobre el que se ha realizado o ha actuado el evento

3. ACTIVACION: activación de la auditoría, muchos de los sistemas la tienen desactivada por defecto, y configurarla según el Plan de Registro de Auditoría
4. CONFIGURACION TAMAÑO DE LOS ARCHIVOS: configurar el tamaño máximo de los archivos de registros de eventos. Deberá ser un compromiso entre la capacidad de los discos del sistema, el número de sucesos generados, por unidad de tiempo y el periodo de revisión de estos por el personal.
5. SISTEMA RECOLECTOR DE EVENTOS: Cuando exista un sistema central de recolección de eventos, configurarlo para que, en tiempo real, envíe una copia de los sucesos. Se sincronizarán automáticamente su hora y fecha con el resto de sistemas.
6. LEGALIDAD: estudiar los requisitos legales que pueden exigir el almacenamiento de registros por un periodo de tiempo determinado (periodo de retención).
7. ALERTAS: Si el sistema lo permite se deberá configurar una alarma para que alerte o envíe un correo electrónico interno al grupo responsable de revisión de los registros en caso de que el espacio de almacenamiento de registros no sea suficiente.
8. ACCESO RESTRINGIDO: proteger los archivos de registro y las herramientas para su configuración y tratamiento contra los accesos no autorizados. Las copias de seguridad de dichos registros estén sujetas al mismo nivel de protección que los propios registros. Sólo tendrá acceso el Responsable de Registro. A los archivos sólo se podrá acceder en modo lectura para evitar su manipulación. Si el sistema lo permite, restringir el acceso incluso a los administradores.
9. REVISION DIARIA: Un vez configurado los sistemas, se deberá revisar diariamente el volumen y tipo de información registrado y ajustar la configuración en base a ello, hasta asegurar que los parámetros fijados son correctos.

10. FIN DEL PROCEDIMIENTO

    En el caso de que exista un sistema central de recolección de eventos, centralización de logs, etc. se aplicaría este mismo procedimiento.

20.2.2. *Revisión de los eventos generados*

La activación de la auditoría de eventos no tiene sentido si no se establece un plan de revisión de los eventos generados.

Cuando no se disponga de herramienta de recolección de eventos, gestión y correlación de eventos (herramienta SIEM), la revisión deberá hacerse de forma manual o con ayuda de herramientas semiautomáticas.
La revisión será llevada a cabo por el Responsable de Registro nombrado para cada sistema.
Cualquier incidencia relevante deberá ser comunicada mediante el *Procedimiento de Gestión y Respuesta ante Incidencias*.
La revisión se realizará con periodicidad no superior a una semana para sistemas no críticos y de tres días para los críticos. Se revisará:

- Eventos registrados
- Tamaño y número actual de los archivos de registro y capacidad restante del disco
- Fecha y hora de sistema y correcto funcionamiento de la sincronización
- El correcto envío de copia de los eventos al sistema central, en su caso, y recepción por parte de éste

20.3. Anexos A – Relación de Responsables de Registro

RELACION DE RESPONSABLE DE REGISTRO PARA LOS SISTEMAS, SERVICIOS O APLICACIONES	
Responsable del Registro	**Sistema, Aplicación o Servicios**

21. PROCEDIMIENTO DE ADMINISTRACION DE LA CONTINUIDAD

Ver procedimiento recogido en el Manual de Procedimientos de Seguridad de la Información. Apartado 10.1. "PROCEDIMIENTO DE LA GESTIÓN DE LA CONTINUIDAD- Proceso de la Administración de la Continuidad".

Se añade a dicho procedimiento que cualquier plan de continuidad de la organización deba estar alineado con las directrices descritas en el mismo.

22. PROCEDIMIENTO PARA LA GESTION DE CONTROLES CONTRA CODIGO MALICIOSO

Ver procedimiento recogido en el Manual de Procedimientos de Seguridad de la Información. Apartado 6.1. "Procedimientos y Responsabilidades Operativas- Controles contra software malicioso".

Se añade el procedimiento para verificar la información relativa a software malicioso que se publique (listas de correo, consultas a páginas web, etc.) garantizando que los boletines de alerta sean exactos.

23. PROCEDIMIENTO DE ETIQUETADO DEL CABLEADO

Responsable

Responsable	Encargado de la Unidad Informática
Responsable de Cumplimiento	Encargado de Seguridad de la Información
Personal de Operación	

Referencias

Listado de documentos, políticas directamente relacionadas y procedimientos derivados:

Deriva de	Manual de Procedimientos de Seguridad de la Información. Apartado 5.2. "Seguridad del Cableado". (es un complemento al mismo)
Políticas, Procedimientos, Normas	

23.1. Objetivo

- Normaliza la documentación relativa al etiquetado del cableado, tanto los utilizados en los puestos de usuario como los existentes en los armarios de comunicaciones y equipos medios de la red local del Gobierno Regional con el objeto de facilitar la labor de mantenimiento que realizan los técnicos responsables de los sistemas informáticos.

23.2. Procedimiento

Aplicando y respetando la norma TIA/EIA-606-A "Especificación sobre rotulado de los cables", se deberá añadir un identificador exclusivo para cada terminación de hardware, tanto en el Panel de Conexiones (Patch Panel) como en cada toma de red. Asimismo, se deberá rotular cada uno de los tendidos de cableado horizontal.
Todos los rótulos, ya sean adhesivos o insertables, deben cumplir los requisitos de legibilidad, protección contra el deterioro y adhesión especificados en el estándar UL969.

De acuerdo con lo anterior, se identificarán los cables UTP en ambos extremos del cableado horizontal, las tomas de red de los puestos de usuario y los paneles de conexión.

Los pasos a seguir son los siguientes:

1. **Identificación de los Racks:**

   Cada RACK se identificará con 3 caracteres: X Y Z donde:

   X [1..9]: Nº de Sala

   Y [1..9]: Nº de Fila o Columna dentro de la Sala X (utilizando 1 dígito)

   Z [1..9]: Nº de Rack en la Fila Y (utilizando 3 dígitos).

   El orden de numeración de las filas/columnas de racks será comenzando en 1 para la fila menos alejada de la puerta de acceso al CPD. En caso de que la puerta estuviera en el centro de la Sala, se numerarán de derecha a izquierda.

   El orden de numeración del rack será desde el más al menos alejado de la puerta de acceso al CPD.

   Recomendación: Tipo de letra Arial, Negrita, Tamaño 42.

2. Identificación de los Patch Panel

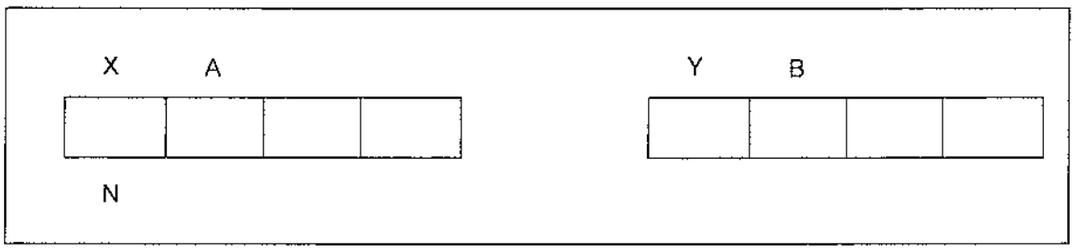
Cada Patch Panel se identificará con la siguiente nomenclatura: X A donde:

X [1..9]: Nº de Rack (utilizando 3 dígitos)

A: Nº Posición del Patch Panel dentro del Rack (utilizando 2 dígitos)

La posición del Patch Panel dentro del Rack se comienza a numerar desde la posición superior, o de más arriba, a la inferior.

3. Identificación en los Patch Panel



X [1..9]: Nº del Rack origen del cableado (utilizando 2 dígitos)

Y [1..9]: Nº del Rack destino del cableado (utilizando 2 dígitos)

A [1..9]: Nº de Patch Panel en el Rack origen (utilizando 2 dígitos)

B [1..9]: Nº de Patch Panel en el Rack destino (utilizando 2 dígitos)

N [1..9]: Nº de puerto del Patch Panel (utilizando 2 dígitos)

4. Identificación en los extremos del cable

Los identificadores de los cables se asocian con la identificación efectuada en el Patch Panel y la Caja/Roseta.

5. Identificación de las Cajas/Rosetas de Conexión

El identificador de las rosetas se asocia con el extremo del cable que se conecta con el Patch Panel de manera que el código de identificación sea el mismo.

6. Realizar plano del edificio

El plano debe mostrar la ubicación de los Cuadros de Distribución de Planta y la ubicación de las Cajas/Rosetas dentro de las mismas.

ANOTESE Y COMUNIQUESE.

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 Informática
3. Oficina de partes.
4. Dpto. Jurídico.