



República Dominicana  
Secretariado Técnico de la Presidencia

Programa de Apoyo a la Reforma y Modernización  
del Poder Ejecutivo (Pro-Reforma)  
Unidad Ejecutora del programa BID 1176/OC-DR

## **Componente II**

### **Título consultoría Desarrollo de las áreas TICs**

#### **Informe 1**

Kian Abolfazlian  
**Código Contrato**  
C2-A3-09

“Queda establecido que las opiniones y recomendaciones de los Consultores no comprometen ni a la Entidad Contratante, ni a otras entidades locales, ni al Banco, los que se reservan el derecho de formular al respecto las observaciones o salvedades que consideren apropiadas”

<b>INTRODUCCIÓN.....</b>	<b>5</b>
<b>MISIÓN, VISIÓN, OBJETIVOS ESTRATÉGICOS Y LAS PRINCIPALES FUNCIONES.....</b>	<b>6</b>
MISIÓN.....	7
VISIÓN .....	10
OBJETIVOS ESTRATÉGICOS Y LAS PRINCIPALES FUNCIONES .....	12
<b>PROTOCOLOS DE SEGURIDAD .....</b>	<b>14</b>
1. SEGURIDAD FÍSICA .....	15
1.1 <i>Desastres Naturales, Incendios Accidentales, Tormentas e Inundaciones</i> .....	16
1.1.1 Incendios .....	16
1.1.2 Inundaciones .....	18
1.1.3 Instalaciones Eléctricas .....	19
1.1.4 Ergonomía .....	21
1.2 <i>Amenazas ocasionadas por el hombre</i> .....	22
1.3 <i>Disturbios, Sabotajes internos y externos deliberados</i> .....	23
1.3.1 Control de Acceso .....	23
2. SEGURIDAD LÓGICA.....	24
2.1 <i>Controles de Acceso</i> .....	25
2.1.1 Identificación y Autenticación.....	26
2.1.2 Roles .....	29
2.1.3 Transacciones .....	29
2.1.4 Limitaciones a los Servicios.....	29
2.1.5 Modalidades de Acceso.....	30
2.1.6 Ubicación y Horario .....	31
2.1.7 Control de Acceso Interno .....	32
2.1.8 Control de Acceso Externo .....	34
2.1.9 Administración .....	36
2.2 <i>Niveles de Seguridad Informática</i> .....	38
2.2.1 Nivel D .....	39
2.2.2 Nivel C1: Protección Discrecional.....	39
2.2.3 Nivel C2: Protección de Acceso Controlado .....	40
2.2.4 Nivel B1: Seguridad Etiquetada.....	41
2.2.5 Nivel B2: Protección Estructurada .....	41
2.2.6 Nivel B3: Dominios de Seguridad .....	42
2.2.7 Nivel A: Protección Verificada.....	42
3. LOS ESTÁNDARES.....	43
<b>PROTOCOLOS Y PROCEDIMIENTOS DE BACKUP .....</b>	<b>46</b>
<b>DISASTER RECOVERY PLANNING (PLAN DE CONTINGENCIA).....</b>	<b>65</b>
RESUMEN EJECUTIVO .....	66
INTRODUCCIÓN .....	66
<i>PROPOSITO</i> .....	67
<i>ALCANCE</i> .....	67
DESCRIPCION DE PLAN DE CONTINGENCIA.....	67
<i>PROVISIONES Y DIRECTIVOS APLICABLES</i> .....	67
<i>OBJETIVOS</i> .....	67
<i>ORGANIZACION</i> .....	68
<i>FASES DEL LABOR DE CONTINGENCIA</i> .....	69
FASE 1: RESPUESTA.....	69
FASE 2: RESUMIR EL TRABAJO .....	69
FASE 3: RECUPERACION .....	69
FASE 4: RESTAURACION.....	69
<i>ASUNCIONES</i> .....	70
<i>FACTORES CRITICOS DE EXITO</i> .....	70

<i>SISTEMAS/APLICACIONES/SERVICIOS CRITICOS Y DE ALTA IMPORTANCIA</i> .....	70
<i>AMENAZAS</i> .....	70
<i>AMENAZAS PROBABLES</i> .....	71
<i>DESCRIPCION DE SISTEMA</i> .....	71
<i>AMBIENTE FISICO</i> .....	71
<i>AMBIENTE TECNICO</i> .....	71
<i>PLAN</i> .....	71
<i>GESTION DEL PLAN</i> .....	71
GRUPOS DE TRABAJO PARA LA PLANEACION DEL PLAN DE CONTINGENCIA .....	71
COORDINADOR DEL PLAN DE CONTINGENCIA.....	72
COORDINADORES DE PLAN DE CONTINGENCIA PARA CADA SISTEMA.....	72
NOTIFICACION DE LOS INCIDENTES .....	72
NOTIFICACION INTERNA AL PERSONAL .....	72
NOTIFICACION A LOS CONTACTOS EXTERNOS .....	72
RUEDA DE PRENSA .....	72
SITIOS ALTERNATIVOS DE OPERACIONES .....	72
<i>EQUIPOS DE TRABAJO</i> .....	73
EQUIPO DE TRABAJO PARA EVALUACION DE LOS DAÑOS.....	73
EQUIPO DE OPERACIONES .....	73
EQUIPO DE COMUNICACION .....	73
EQUIPO DE DATA .....	73
OFF-SITE STORAGE.....	73
EQUIPO DE ADMINISTRACION.....	74
PROCUREMENT.....	74
EQUIPO DE CONFIGURACION .....	74
EQUIPO DE FACILIDADES DE RESPALDO.....	74
EQUIPO DE SOFTWARE Y APLICACIONES.....	74
EQUIPO DE AUDITORIA INTERNA.....	74
EQUIPO DE ASISTENCIA AL USUARIO .....	74
<i>COMUNICACIÓN DE DATA E INFORMACION</i> .....	74
<i>RESPALDOS</i> .....	75
<i>LOS EQUIPOS DE OFICINA Y SUMINISTRO</i> .....	75
<i>PROCEDIMIENTOS DE TESTING</i> .....	75
<i>ESTRATEGIAS</i> .....	75
<i>DEFINICIONES</i> .....	75
<i>APENDICE A – INFORMACION DE CONTACTOS PARA EL PLAN DE CONTINGENCIA</i> .....	76
<i>APENDICE B – PROCEDIMIENTOS DE EMERGENCIA</i> .....	78
<i>APENDICE C – EQUIPOS DE TRABAJO Y SUS FUNCIONES</i> .....	80
<i>APENDICE D – PROCEDIMIENTOS DE LOS SITIOS ALTERNATIVOS DE OPERACION Y RESPALDO</i> .....	82
<i>APENDICE E – LISTADO DE DOCUMENTOS</i> .....	84
<i>APENDICE F – INVENTARIO DE SOFTWARE Y APLICACIONES</i> .....	86
<i>APENDICE G – INVENTARIO DE HARDWARE</i> .....	88
<i>APENDICE H – REQUERIMIENTOS DE COMUNICACION</i> .....	90
<i>APENDICE I –LISTADO DE LOS PROVEEDORES Y TERCEROS</i> .....	92
<i>APENDICE J – ACUERDOS PARA EL SOPORTE EXTERNO EN CASO DE EMERGENCIA</i> .....	94
<i>APENDICE K – REQUERIMIENTOS Y PROCEDIMIENTOS DE CONTINGENCIA PARA EL CENTRO DE DATA Y OPERACIONES</i> .....	96
<i>APENDICE L – PROCEDIMIENTO DEL MANTENIMIENTO PARA EL PLAN DE CONTINGENCIA</i> .....	98
<i>APENDICE M - CONTINGENCY LOG</i> .....	100
<b>PROTOCOLOS DE LAS POLÍTICAS DEL DESARROLLO DE APLICACIONES</b> .....	<b>102</b>
INTRODUCCIÓN .....	103
<b>PROTOCOLOS DE LAS POLÍTICAS DE SUBCONTRATACIÓN DE SERVICIOS INFORMÁTICOS</b> .....	<b>110</b>
ANÁLISIS DEL ENTORNO Y DISEÑO DEL DOCUMENTO DE SOLICITUD DE PROPUESTA.....	111

EVALUACIÓN, SELECCIÓN Y CONTRATACIÓN DEL PROVEEDOR DE SERVICIO.....	112
ADMINISTRACIÓN Y MONITOREO DE LA IMPLEMENTACIÓN .....	114
<b>CONSULTORÍA JURÍDICA DEL PODER EJECUTIVO.....</b>	<b>115</b>
MISIÓN.....	116
VISIÓN .....	117
OBJETIVOS ESTRATÉGICOS Y LAS PRINCIPALES FUNCIONES .....	118

## **Introducción**

El informe 1 es el entregable para el Producto 1 de esta consultoría, y contiene la Misión, Visión, los Objetivos y las Principales funciones a desarrollar, los protocolos de políticas de seguridad, backup, DRP, estándares de Desarrollo de aplicaciones y subcontratación de servicios informáticos para los centros y departamentos de Informática de las Instituciones Públicas de la Republica Dominicana.

Las definiciones presentadas son genéricas y así son de base para el desarrollo propio en caso específico de cada institución. Esto significa que se puede/debe añadir a este base los detalles que con mejor exactitud identifica las realidades de cada institución. Es importante notar que este, bajo ninguna circunstancia, significa que se puede eliminar puntos de esta base, pero más bien añadir los detalles que identifican cada institución.

## **Misión, Visión, Objetivos Estratégicos y las principales funciones**

## **Misión**

Les recordamos que la Misión de una organización es:

- *“La razón de ser de la organización”. Es lo que define y justifica la existencia de la organización. Es una herramienta operacional y táctico, que dicta las funciones principales de la organización. No es dependiente de un periodo específico de tiempo. Cambiar la Misión es igual cambiar la organización.*

En el contexto de este trabajo proponemos el siguiente como la base para la Misión del departamento de Informática de cada institución:

- ***Proveemos el liderazgo y las mas avanzadas tanto como adecuadas soluciones tecnológicas que apoyan <<LA INSTITUCION>> en lograr su misión, visión y objetivos estratégicos. Supervisando y coordinando la capacitación de los empleados de la institución, tanto como el diseño, adquisición, mantenimiento y el uso de la información y las soluciones de Tecnología de Información de <<LA INSTITUCION>>, aseguramos su gestión efectiva, y la apoyamos en sus esfuerzos para la entrega de los mejores servicios a la ciudadanía.***

Es preciso detallar algunos puntos que puedan ayudar el mejor entendimiento de la misión propuesta en este trabajo.

### ***Proveer el liderazgo... que apoya <<La INSTITUCION>> en lograr su misión, visión y objetivos estratégicos***

Esto significa que el departamento de Informática de la institución se responsabiliza para liderar los esfuerzos que la institución conlleva para alcanzar su misión, visión y objetivos estratégicos, cuando hablando de las soluciones tecnológicas adecuadas ofrecidas en manera pro-activa a la alta dirección de la institución.

### ***Soluciones tecnológicas***

Una solución tecnológica es una o un conjunto de aplicaciones tecnológicas junto con sus procedimientos y protocolos de uso, mantenimiento y desarrollo continuo, aplicadas en un contexto de trabajo. Tal y como la palabra “solución” indica, la razón de ser de la aplicación (o conjunto de aplicaciones) implementado en el ámbito de trabajo, debe ser “el solucionar una (o un

conjunto) de tarea(s), que apoyan la institución lograr sus metas estratégicas y operacionales”.

### **... adecuada**

El adjetivo “adecuada” se utiliza para aclarar la alineación con las metas estratégicas y operacionales

- **Solución tecnológica adecuada:** Basado en la definición de una solución tecnológica, se ve claramente que la manera de solucionar la tarea (o el conjunto de tareas) que la solución tecnológica ofrece, debe estar alineada con las metas estratégicas y operacionales de la institución.

### ***Proveer... las mas avanzadas tanto como adecuadas soluciones tecnológicas que apoyan <<LA INSTITUCION>> en lograr su misión, visión y objetivos estratégicos***

Esto significa que el departamento de Informática se responsabiliza para ofrecer pro-activamente a la institución las soluciones más avanzadas y adecuadas que la apoya en alcanzar las metas propuestas en su misión, visión y objetivos estratégicos.

### ***Supervisando y coordinando la capacitación de los empleados de la institución, tanto como el diseño, adquisición, mantenimiento y el uso de la información y las soluciones de Tecnología de Información de <<LA INSTITUCION>>, aseguramos su gestión efectiva, y la apoyamos en sus esfuerzos para la entrega de los mejores servicios a la ciudadanía.***

Esto significa que el departamento de Informática de la institución trabaja pro-activamente para asegurar la efectiva gestión operacional de la institución y así logrando que la institución podrá ofrecer los mejores servicios a la ciudadanía, por vía de:

1. La detección de las necesidades, la coordinación y la supervisión de las capacitaciones que los profesionales de la institución requieren para poder desempeñar su mejor labor utilizando las soluciones avanzadas y adecuadas que el departamento de Informática ofrece a la institución

2. La pro-activa y adecuada gestión de diseño, adquisición, mantenimiento, y el uso de la información y las soluciones tecnológicas de la institución.

## **Visión**

Les recordamos que la Visión de una organización es:

- *“A donde queremos llegar dentro de un periodo específico de tiempo”, obviamente partiendo de la misión de la organización. Es una herramienta estratégica. Es muy dependiente de un periodo específico y se debe revisarse constantemente. Cambiar la Visión “NO” es igual cambiar la organización*

En el contexto de este trabajo proponemos el siguiente como la base para la Visión del departamento de Informática de cada institución:

- ***Ser el socio estratégico de <<TITULO DE SECRETARIO>> en materia de información y soluciones adecuadas de Tecnología de Información.***
- ***Apoyar <<LA INSTITUCION>> en la eficientización de su gestión y el mejoramiento de los servicios que brinda a la ciudadanía.***
- ***Convertir <<LA INSTITUCION>> en un parte integral y uno de los pilares de la solución de gobierno electrónico que la Presidencia de la Republica desea brindar a la ciudadanía.***

Es preciso detallar algunos puntos que puedan ayudar el mejor entendimiento de la visión propuesta en este trabajo.

### ***Ser el socio estratégico de <<TITULO DE SECRETARIO>> en materia de información y soluciones adecuadas de Tecnología de Información.***

Esto significa que el departamento de Informática de la institución se responsabiliza para ofrecer pro-activamente su apoyo al secretario de estado en cuando la formulación de las estrategias de la institución, relacionadas a la información y las soluciones adecuadas de Tecnología de Información. Esto incluye:

1. Desarrollar y ofrecer pro-activamente y en manera sistemática, las diferentes opciones de dichas estrategias institucionales

2. Tomando en cuenta la misión, la visión y los objetivos estratégicos de la institución, apoyar activamente al secretario de estado en el definir:
  - Que es una solución para institución?
  - Que significa “adecuada” en el contexto de la institución?

- **Objetivos Estratégicos y las Principales Funciones**

Les recordamos que los Objetivos Estratégicos se tratan de:

- *Para poder alcanzar, en manera sistemática tanto como operativamente, lo propuesto en la Misión y la Visión organizacional, se define un conjunto de Objetivos a lograr. Dichos objetivos se puede definir para sub-periodos dentro del tiempo en lo cual se define la Visión organizacional*

En el contexto de este trabajo proponemos el siguiente como la base para los Objetivos Estratégicos y las Principales Funciones del departamento de Informática de cada institución:

- 1. *Facilitación de la comunicación y el compartir la información en manera eficaz y eficiente utilizando la operabilidad y conectividad necesaria dentro de <<LA INSTITUCION>> tanto como entre la misma y demás instituciones de la administración pública. A este fin, identificamos los puntos necesarios de compatibilidad de la información y las soluciones de la Tecnología de Información de <<LA INSTITUCION>> para así desarrollar la adecuada estrategia de Tecnología de Información y la infraestructura tecnológica que habilita <<LA INSTITUCION>> promover el intercambio, el acceso y el uso de la información por los usuarios internos tanto como externos utilizando la Intranet, Extranet e Internet de <<LA INSTITUCION>>.***
- 2. *Administración de la captura y la validación de la información necesaria para la gestión eficaz y eficiente de <<LA INSTITUCION>>. Identificación e implementación de la estrategia de información que facilita <<LA INSTITUCION>> lograr sus metas estratégicas hacia la administración pública electrónica y disminuir el uso de la documentación física.***
- 3. *Identificación, promoción y facilitación de las capacitaciones adecuadas que habilitan el empleomanía de <<LA INSTITUCION>> tener el nivel y la experiencia necesaria para el efectivo y eficiente uso, mantenimiento y desarrollo de la información y las soluciones tecnológicas de <<LA INSTITUCION>>.***
- 4. *Identificación de los niveles adecuados y justos de la inversión en la Tecnología Información y aseguramiento de que esa inversión se convierte en los activos estratégicos de <<LA INSTITUCION>> que la***

*apoya en lograr sus metas estratégicas tanto como las puestas por la Presidencia de la República.*

- 5. Diseño e implementación de las políticas de seguridad y el uso adecuado de la información y las soluciones estratégicas de <<LA INSTITUCION>>. Administración y monitoreo de cumplimiento de dichas políticas.*
- 6. Planeación estratégica y presupuestaria adecuada de la Tecnología de Información de <<LA INSTITUCION>> en coordinación con la oficina de <<TITULO DE SECRETARIO>> y alineada con las metas estratégicas de <<LA INSTITUCION>>.*
- 7. Planeación de la estrategia de desarrollo de las soluciones de Tecnología de Información de <<LA INSTITUCION>>, incluyendo las políticas y criterios de decisión sobre el desarrollo interno tanto como externo, la identificación de alcance, adquisición de servicios, implementación de las soluciones y el sistema de monitoreo de los resultados, el uso y el mantenimiento de dichas soluciones.*

*Administración de los activos de las soluciones tecnológicas y la información de <<LA INSTITUCION>>, incluyendo el aseguramiento de la calidad e integridad de data e información crítica de <<LA INSTITUCION>>.*

# Protocolos de Seguridad

## **1. Seguridad Física**

Cada sistema es único y por lo tanto la política de seguridad a implementar no será única. Este concepto vale, también, para el edificio donde se ubica la infraestructura tecnológica. Es por ello que siempre se recomendarán pautas de aplicación general y no procedimientos específicos.

Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro.

Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.
  2. Amenazas ocasionadas por el hombre.
  3. Disturbios, sabotajes internos y externos deliberados.
- A continuación se analizan los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

## **1.1 Desastres Naturales, Incendios Accidentales, Tormentas e Inundaciones**

### **1.1.1 Incendios**

Los incendios son causados por el uso inadecuado de combustibles, fallas de instalaciones eléctricas defectuosas y el inadecuado almacenamiento y traslado de sustancias peligrosas.

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas.

Los diversos factores a contemplar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

- El área en la que se encuentran las computadoras debe estar en un local que no sea combustible o inflamable.
- El local no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.
- Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

### ***Seguridad del Equipamiento***

Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.

- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

### ***Recomendaciones***

- El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.
- Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.
- Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.
- Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.
- Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

Suministrar información, del Departamento Informática, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia. Hacer que este departamento esté consciente de las particularidades y vulnerabilidades del sistema, por excesivas cantidades de agua y la conveniencia de una salida para el humo, es importante. Además, ellos pueden ofrecer excelentes consejos como precauciones para prevenir incendios.

### **1.1.2 Inundaciones**

Se las define como la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Para evitar este inconveniente se pueden tomar las siguientes medidas:

Construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

### 1.1.3 Instalaciones Eléctricas

Trabajar con computadoras implica trabajar con electricidad. Por lo tanto esta una de las principales áreas a considerar en la seguridad física.

En la medida que los sistemas se vuelven más complicados se hace más necesaria aplicar las soluciones que estén de acuerdo con una norma de seguridad industrial.

#### ***Picos y Ruidos Electromagnéticos***

Las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios. También está el tema del ruido que interfiere en el funcionamiento de los componentes electrónicos. El ruido interfiere en los datos, además de favorecer la escucha electrónica.

#### ***Cableado***

Los cables que se suelen utilizar para construir las redes locales van del cable telefónico normal al cable coaxial o la fibra óptica. Algunos edificios de oficinas ya se construyen con los cables instalados para evitar el tiempo y el gasto posterior, y de forma que se minimice el riesgo de un corte, rozadura u otro daño accidental.

Los riesgos más comunes para el cableado se pueden resumir en los siguientes:

- *Interferencia*: estas modificaciones pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los cables de fibra óptica no sufren el problema de alteración (de los datos que viajan a través de él) por acción de campos eléctricos, que si sufren los cables metálicos.
- *Corte del cable*: la conexión establecida se rompe, lo que impide que el flujo de datos circule por el cable.
- *Daños en el cable*: los daños normales con el uso pueden dañar el apantallamiento que preserva la integridad de los datos transmitidos o dañar al propio cable, lo que hace que las comunicaciones dejen de ser fiables.

El cable de red ofrece también un nuevo frente de ataque para un determinado intruso que intentase acceder a los datos. Esto se puede hacer:

- *Desviando o estableciendo una conexión no autorizada en la red*: un sistema de administración y procedimiento de identificación de acceso adecuados hará difícil que se puedan obtener privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.

- Haciendo una escucha sin establecer conexión, los datos se pueden seguir y pueden verse comprometidos.

Luego, no hace falta penetrar en los cables físicamente para obtener los datos que transportan.

### ***Cableado de Alto Nivel de Seguridad***

Son cableados de redes que se recomiendan para instalaciones con grado de seguridad militar. El objetivo es impedir la posibilidad de infiltraciones y monitoreos de la información que circula por el cable. Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión y el cable. A lo largo de la tubería hay sensores conectados a una computadora. Si se detecta algún tipo de variación de presión se dispara un sistema de alarma.

### ***Pisos de Placas Extraíbles***

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con computadoras y equipos de procesamiento de datos pueden ser, en caso necesario, alojados en el espacio que, para tal fin se dispone en los pisos de placas extraíbles, debajo del mismo.

### ***Sistema de Aire Acondicionado***

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, es recomendable instalar redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

#### **1.1.4 Ergonomía**

Se debe cumplir con la legislación existente en el área de ergonomía en cuando trabajo con los equipos informáticos, incluyendo las direcciones pertinentes sobre Trastornos Óseos y/o Musculares, Trastornos Visuales, la iluminación del ambiente de trabajo, y el clima del medioambiente de trabajo.

## **1.2 Amenazas ocasionadas por el hombre**

Los componentes de la infraestructura tecnológica son posesiones valiosas de las instituciones y están expuestas, de la misma forma que lo están las piezas de stock e incluso el dinero.

Es frecuente que los operadores utilicen la computadora de la institución para realizar trabajos privados o para otras organizaciones y, de esta manera, robar tiempo de máquina.

La información importante o confidencial puede ser fácilmente copiada. Muchas empresas invierten millones de dólares en programas y archivos de información, a los que dan menor protección que la que otorgan a una máquina de escribir o una calculadora.

El software, es una propiedad muy fácilmente de sustraer y las cintas y discos son fácilmente copiados sin dejar ningún rastro.

### ***Recomendaciones***

- Todos los equipos que componen la infraestructura tecnológica de la institución deben estar instalados en manera no fácil de sustraer. Su posicionamiento y ubicación se debe registrar y auditar en manera frecuente.
- El uso que los empleados de la institución dan a los diferentes componentes de la infraestructura tecnológica de la institución debe estar registrado basado en las direcciones del secretario de estado al cargo y el gobierno de la República Dominicana. Este uso se debe auditar de manera frecuente en coordinación con los supervisores y encargados de los diferentes departamentos de la institución y el reporte se debe presentar, cuando requerido, a la alta dirección de la institución.
- Para la protección de la data y el software ver los capítulos acerca de dichos componentes.

## **1.3 Disturbios, Sabotajes internos y externos deliberados**

### **1.3.1 Control de Acceso**

A cualquier personal ajeno a la institución y/o Departamento de Informática se le solicitará completar un formulario de datos personales, los motivos de la visita, hora de ingreso y de egreso, etc.

El uso de credenciales de identificación es uno de los puntos más importantes del sistema de seguridad, a fin de poder efectuar un control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa.

En este caso la persona se identifica por algo que posee, por ejemplo una tarjeta de identificación. Cada una de ellas tiene un PIN (Personal Identificación Number) único, siendo este el que se almacena en una base de datos para su posterior seguimiento, si fuera necesario.

Estas credenciales se pueden clasificar de la siguiente manera:

- Normal o definitiva: para el personal permanente de planta.
- Temporaria: para personal recién ingresado.
- Contratistas: personas ajenas a la empresa, que por razones de servicio deben ingresar a la misma.
- Visitas.

### ***Detectores de Metal***

El detector de metal es un elemento sumamente práctico para la revisión de personas, ofreciendo grandes ventajas sobre el sistema de palpación manual.

La utilización de este tipo de detectores debe hacerse conocer a todo el personal. De este modo, actuará como elemento disuasivo.

### ***Soluciones Opcionales***

En caso necesario y basado en las decisiones institucionales se puede utilizar las soluciones adicionales basado en el uso de Sistemas Biométricos, Verificación Automática de Firmas, Protección con animales y Sistemas Electrónicos (ejemplos: Barreras Infrarrojas y de Micro-ondas, Detector Ultrasonico, Detectores pasivas sin Alimentación, Sonorización y Dispositivos Luminosos, Circuitos cerrados de televisión).

## **2. Seguridad Lógica**

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

El activo más importante que se posee la institución es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

En el siguiente tratamos dos puntos importantes de seguridad lógica informática:

1. Controles de Accesos
2. Niveles de Seguridad Informática

## 2.1 Controles de Acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Constituyen una importante ayuda para proteger al sistema operativo de la red, al sistema de aplicación y demás software de la utilización o modificaciones no autorizadas; para mantener la integridad de la información (restringiendo la cantidad de usuarios y procesos con acceso permitido) y para resguardar la información confidencial de accesos no autorizados.

Asimismo, es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. Al respecto, el **National Institute for Standards and Technology** (NIST) (<http://www.nist.gov>) ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:

- Identificación y Autenticación
- Roles
- Transacciones
- Limitaciones a los Servicios
- Modalidad de Acceso
- Ubicación y Horario
- Control de Acceso Interno
- Control de Acceso Externo
- Administración

### 2.1.1 Identificación y Autenticación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema; y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- *Algo que solamente el individuo conoce:* por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- *Algo que la persona posee:* por ejemplo una tarjeta magnética.
- *Algo que el individuo es y que lo identifica unívocamente:* por ejemplo las huellas digitales o la voz.
- *Algo que el individuo es capaz de hacer:* por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale mencionar sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede

tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios.
  - Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
- La identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.
  - Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
- Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
- Detección de actividades no autorizadas.
  - Además de realizar auditorías o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.

- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado.
  - Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no.
  - Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

### **2.1.2 Roles**

Se implementara controles al acceso a la información a través de la función o rol del usuario que requiere dicho acceso.

Algunos ejemplos de roles serían los siguientes: programador, líder de proyecto, gerente de un área usuaria, administrador del sistema, etc.

En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.

### **2.1.3 Transacciones**

Se implementara controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.

### **2.1.4 Limitaciones a los Servicios**

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

Un ejemplo podría ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para 2 personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un tercero usuario.

### 2.1.5 Modalidades de Acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- *Lectura*: el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.
- *Escritura*: este tipo de acceso permite agregar datos, modificar o borrar información.
- *Ejecución*: este acceso otorga al usuario el privilegio de ejecutar programas.
- *Borrado*: permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.
- *Todas las anteriores*.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- *Creación*: permite al usuario crear nuevos archivos, registros o campos.
- *Búsqueda*: permite listar los archivos de un directorio determinado.

### **2.1.6 Ubicación y Horario**

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas.

En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana.

De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

Se debe mencionar que estos dos tipos de controles siempre deben ir acompañados de alguno de los controles anteriormente mencionados.

## 2.1.7 Control de Acceso Interno

### ***Palabras Claves (Passwords)***

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se debe limitar la elección de passwords débiles.

- ***Sincronización de passwords***
  - Consiste en permitir que un usuario acceda con la misma password a diferentes sistemas interrelacionados y, su actualización automática en todos ellos en caso de ser modificada. Podría pensarse que esta es una característica negativa para la seguridad de un sistema, ya que una vez descubierta la clave de un usuario, se podría tener acceso a los múltiples sistemas a los que tiene acceso dicho usuario. Sin embargo, estudios hechos muestran que las personas normalmente suelen manejar una sola password para todos los sitios a los que tengan acceso, y que si se los fuerza a elegir diferentes passwords tienden a guardarlas escritas para no olvidarlas, lo cual significa un riesgo aún mayor. Para implementar la sincronización de passwords entre sistemas es necesario que todos ellos tengan un alto nivel de seguridad.
- ***Caducidad y Control***
  - Este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un período máximo que puede transcurrir para que éstas caduquen.
- ***Encriptación***
  - La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. Se debe elegir un sistema de encriptación adecuado para la institución.
- ***Listas de Control de Accesos***
  - Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado

recurso del sistema, así como la modalidad de acceso permitido. Este tipo de listas varían considerablemente en su capacidad y flexibilidad.

- ***Límites sobre la Interfase de Usuario***
  - Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario.
  
- ***Etiquetas de Seguridad***
  - Consiste en designaciones otorgadas a los recursos (como por ejemplo un archivo) que pueden utilizarse para varios propósitos como control de accesos, especificación de medidas de protección, etc. Estas etiquetas no son modificables

## 2.1.8 Control de Acceso Externo

- **Dispositivos de Control de Puertos**
  - Estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.
  
- **Firewalls o Puertas de Seguridad**
  - Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización. Los diferentes tipos de Firewalls son:
    - *Filtrado de Paquetes*
  
    - *Proxy-Gateways de Aplicaciones*
  
    - *Dual-Homed Host*
  
    - *Screened Host*
  
    - *Screened Subnet*
  
    - *Inspección de Paquetes:*
      - Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. Generalmente son instalados cuando se requiere seguridad sensible al contexto y en aplicaciones muy complejas.
  
    - *Firewalls Personales:*
      - Estos Firewalls son aplicaciones disponibles para usuarios finales que desean conectarse a una red externa insegura y mantener su computadora a salvo de ataques que puedan ocasionarle desde un simple "cuelgue" o infección de virus hasta la pérdida de toda su información almacenada.
  
- **Acceso de Personal Contratado o Consultores**
  - Debido a que este tipo de personal en general presta servicios temporarios, debe ponerse especial consideración en la política y administración de sus perfiles de acceso.

- **Accesos Públicos**
  - Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

### **2.1.9 Administración**

Una vez establecidos los controles de acceso sobre los sistemas y la aplicación, es necesario realizar una eficiente administración de estas medidas de seguridad lógica, lo que involucra la implementación, seguimientos, pruebas y modificaciones sobre los accesos de los usuarios de los sistemas.

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los datos, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones. Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Para la ejecución exitosa del programa de la administración de los usuarios informáticos, es imprescindible que exista una conciencia de la seguridad institucional por parte de todos los empleados. Esta conciencia de la seguridad puede alcanzarse mediante el ejemplo del personal directivo en el cumplimiento de las políticas y el establecimiento de compromisos firmados por el personal, donde se especifique la responsabilidad de cada uno.

Pero además de este compromiso debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la institución.

## ***Administración del Personal y Usuarios - Organización del Personal***

Este proceso lleva generalmente cuatro pasos:

- ***Definición de puestos***
  - Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
- ***Determinación de la sensibilidad del puesto***
  - Para esto es necesario determinar si la función requiere permisos riesgosos que le permitan alterar procesos, perpetrar fraudes o visualizar información confidencial.
- ***Elección de la persona para cada puesto***
  - Requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto. Asimismo, para los puestos definidos como críticos puede requerirse una verificación de los antecedentes personales
- ***Entrenamiento inicial y continuo del empleado***
  - Cuando la persona seleccionada ingresa a la institución, además de sus responsabilidades individuales para la ejecución de las tareas que se asignen, deben comunicárseles las políticas institucionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones institucionales, su responsabilidad en cuanto a la seguridad informática y lo que se espera de él.
  - Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).
  - Sólo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual. Para esto, el ejemplo de la gerencia constituye la base fundamental para que el entrenamiento sea efectivo: el personal debe sentir que la seguridad es un elemento prioritario dentro de la institución.

## 2.2 Niveles de Seguridad Informática

El estándar de niveles de seguridad mas utilizado internacionalmente es el **TCSEC Orange Book** (US Department of Defense, Library N° S225, 711. EEUU. 1985. <http://www.doe.gov>), desarrollado en 1983 de acuerdo a las normas de seguridad en computadoras del Departamento de Defensa de los Estados Unidos.

Los niveles describen diferentes tipos de seguridad del Sistema Operativo y se enumeran desde el mínimo grado de seguridad al máximo. Estos niveles han sido la base de desarrollo de estándares europeos (ITSEC/ITSEM) y luego internacionales (ISO/IEC).

Cabe aclarar que cada nivel requiere todos los niveles definidos anteriormente: así el sub-nivel B2 abarca los sub-nivel B1, C2, C1 y el D. Los niveles son:

- **Nivel D**
- **Nivel C1**: Protección Discrecional
- **Nivel C2**: Protección de Acceso Controlado
- **Nivel B1**: Seguridad Etiquetada
- **Nivel B2**: Protección Estructurada
- **Nivel B3**: Dominios de Seguridad
- **Nivel A**: Protección Verificada

### 2.2.1 Nivel D

Este nivel contiene sólo una división y está reservada para sistemas que han sido evaluados y no cumplen con ninguna especificación de seguridad.

Sin sistemas no confiables, no hay protección para el hardware, el sistema operativo es inestable y no hay autenticación con respecto a los usuarios y sus derechos en el acceso a la información. Los sistemas operativos que responden a este nivel son MS-DOS y System 7.0 de Macintosh.

### 2.2.2 Nivel C1: Protección Discrecional

Se requiere identificación de usuarios que permite el acceso a distinta información. Cada usuario puede manejar su información privada y se hace la distinción entre los usuarios y el administrador del sistema, quien tiene control total de acceso.

Muchas de las tareas diarias de administración del sistema sólo pueden ser realizadas por este "super usuario"; quien tiene gran responsabilidad en la seguridad del mismo. Con la actual descentralización de los sistemas de cómputos, no es raro que en una organización encontremos dos o tres personas cumpliendo este rol. Esto es un problema, pues no hay forma de distinguir entre los cambios que hizo cada usuario.

A continuación se enumeran los requerimientos mínimos que debe cumplir la clase C1:

- **Acceso de control discrecional**
  - Distinción entre usuarios y recursos. Se podrán definir grupos de usuarios (con los mismos privilegios) y grupos de objetos (archivos, directorios, disco) sobre los cuales podrán actuar usuarios o grupos de ellos.
  
- **Identificación y Autenticación**
  - Se requiere que un usuario se identifique antes de comenzar a ejecutar acciones sobre el sistema. El dato de un usuario no podrá ser accedido por un usuario sin autorización o identificación.

### **2.2.3 Nivel C2: Protección de Acceso Controlado**

Este sub-nivel fue diseñado para solucionar las debilidades del C1. Cuenta con características adicionales que crean un ambiente de acceso controlado. Se debe llevar una auditoria de accesos e intentos fallidos de acceso a objetos.

Tiene la capacidad de restringir aún más el que los usuarios ejecuten ciertos comandos o tengan acceso a ciertos archivos, permitir o denegar datos a usuarios en concreto, con base no sólo en los permisos, sino también en los niveles de autorización.

Requiere que se audite el sistema. Esta auditoria es utilizada para llevar registros de todas las acciones relacionadas con la seguridad, como las actividades efectuadas por el administrador del sistema y sus usuarios.

La auditoria requiere de autenticación adicional para estar seguros de que la persona que ejecuta el comando es quien dice ser. Su mayor desventaja reside en los recursos adicionales requeridos por el procesador y el subsistema de discos.

Los usuarios de un sistema C2 tienen la autorización para realizar algunas tareas de administración del sistema sin necesidad de ser administradores.

Permite llevar mejor cuenta de las tareas relacionadas con la administración del sistema, ya que es cada usuario quien ejecuta el trabajo y no el administrador del sistema.

#### **2.2.4 Nivel B1: Seguridad Etiquetada**

Este sub-nivel, es el primero de los tres con que cuenta el nivel B. Soporta seguridad multinivel, como la secreta y ultrasecreta. Se establece que el dueño del archivo no puede modificar los permisos de un objeto que está bajo control de acceso obligatorio.

A cada objeto del sistema (usuario, dato, etc.) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.) y con unas categorías (contabilidad, nóminas, ventas, etc.).

Cada usuario que accede a un objeto debe poseer un permiso expreso para hacerlo y viceversa. Es decir que cada usuario tiene sus objetos asociados.

También se establecen controles para limitar la propagación de derecho de accesos a los distintos objetos.

#### **2.2.5 Nivel B2: Protección Estructurada**

Requiere que se etiquete cada objeto de nivel superior por ser padre de un objeto inferior.

La Protección Estructurada es la primera que empieza a referirse al problema de un objeto a un nivel mas elevado de seguridad en comunicación con otro objeto a un nivel inferior.

Así, un disco rígido será etiquetado por almacenar archivos que son accedidos por distintos usuarios.

El sistema es capaz de alertar a los usuarios si sus condiciones de accesibilidad y seguridad son modificadas; y el administrador es el encargado de fijar los canales de almacenamiento y ancho de banda a utilizar por los demás usuarios.

### **2.2.6 Nivel B3: Dominios de Seguridad**

Refuerza a los dominios con la instalación de hardware: por ejemplo el hardware de administración de memoria se usa para proteger el dominio de seguridad de acceso no autorizado a la modificación de objetos de diferentes dominios de seguridad.

Existe un monitor de referencia que recibe las peticiones de acceso de cada usuario y las permite o las deniega según las políticas de acceso que se hayan definido.

Todas las estructuras de seguridad deben ser lo suficientemente pequeñas como para permitir análisis y tests ante posibles violaciones.

Este nivel requiere que la Terminal del usuario se conecte al sistema por medio de una conexión segura.

Además, cada usuario tiene asignado los lugares y objetos a los que puede acceder.

### **2.2.7 Nivel A: Protección Verificada**

Es el nivel más elevado, incluye un proceso de diseño, control y verificación, mediante métodos formales (matemáticos) para asegurar todos los procesos que realiza un usuario sobre el sistema.

Para llegar a este nivel de seguridad, todos los componentes de los niveles inferiores deben incluirse. El diseño requiere ser verificado de forma matemática y también se deben realizar análisis de canales encubiertos y de distribución confiable. El software y el hardware son protegidos para evitar infiltraciones ante traslados o movimientos del equipamiento.

### 3. Los Estándares

Componente	Estándares
Análisis de riesgos	ISO/IEC 17799 NIST SP 800-30, NIST SP 800-6
Análisis de requerimientos y establecimiento de políticas de seguridad informática	ISO/IEC 17799 CSC-STD-001-83 ISO 15408 NIST SP 800-55 NIST SP 800-42 NIST SP 800-26 NIST SP 800-18 NIST SP 800-16
Aseguramiento de Componentes de Datos	ISO/IEC 17799 IEEE P1363 NIST SP 800-36 NIST SP 800-21 NIST SP 800-14 NIST SP 800-12
Aseguramiento de Componentes de Software	ISO/IEC 17799 NIST FIPS 73 NIST SP 800-44 NIST SP 800-41 NIST SP 800-36 NIST SP 800-14 NIST SP 800-5
Aseguramiento de Componentes de Hardware	ISO/IEC 17799 NSA/CSS Manual 130-2 NACSIM 5000 NIST SP 800-36 NIST SP 800-14
Aseguramiento de Componente Humano	ISO/IEC 17799 NSA Security Guidelines Handbook NIST SP 800-50 NIST SP 800-36 NIST SP 800-16 NIST SP 800-14 NSTISSI 4011 NSTISSD 500 NSTISSI 4013

	<p>NSTISSI 4014  NSTISSI 4015  CSC-STD-002-85</p>
<p>Aseguramiento de Componentes de Interconectividad</p>	<p>ISO/IEC 17799  IEEE P1363  NIST SP 800-45  NIST SP 800-47  NIST SP 800-41  NIST SP 800-36  NIST SP 800-25  NIST SP 800-21  NIST SP 800-14  NIST SP 800-13</p>
<p>Aseguramiento de Infraestructura Física</p>	<p>ISO/IEC 17799  DoD 5220.22-M  NSA Security Guidelines Handbook  NSTISSI 7000  NIST SP 800-36  NIST SP 800-14  NIST SP 800-12</p>
<p>Administración de la seguridad informática</p>	<p>ISO/IEC 17799  ISO/IEC DTR 13335  ISO/IEC DIS 14980  NIST SP 800-64  NIST SP 800-61  NIST SP 800-50  NIST SP 800-55  NIST SP 800-42  NIST SP 800-40  NIST SP 800-36  NIST SP 800-35  NIST SP 800-34  NIST SP 800-18  NIST SP 800-16  NIST SP 800-6  NIST SP 800-5</p>

## Los Estándares mencionados son:

<b>CSC-STD-001-83</b>	<i>DoD Trusted Computer System Evaluation Criteria, 1983</i>
<b>CSC-STD-002-85</b>	<i>DoD Password Management Guidelines, 1985</i>
<b>DoD 5220.22-M</b>	<i>National Industrial Security Program Operating Manual, 1995</i>
<b>ISO/IEC 17799</b>	<i>Information Technology, Code of Practice for Information Security Management, February 2001</i>
<b>ISO/IEC DTR 13335-1</b>	<i>Information technology -- Guidelines for the management of IT security</i>
<b>ISO/IEC 15408</b>	<i>Common Criteria for Information Technology Security Evaluation, August 1999</i>
<b>ISO/IEC DIS 14980</b>	<i>Information technology -- Code of practice for information security management, NSA Security Guidelines Handbook</i>
<b>NSA/CSS Manual 130-2</b>	<i>Media Declassification and Destruction Manual</i>
<b>NACSIM 5000</b>	<i>TEMPEST Fundamentals</i>
<b>NSTISSI 7000</b>	<i>Tempest Countermeasures for Facilities, September 1993.</i>
<b>NSTISSI 4011</b>	<i>National Training Standard for Information Systems Professionals, June 1994.</i>
<b>NSTISSD 500</b>	<i>Information Systems Security Education, Training and Awareness, February 1993</i>
<b>NSTISSI 4013</b>	<i>National Training Standard for System Administration in Information Systems Security, August 1997</i>
<b>NSTISSI 4014</b>	<i>National Training Standard for Information Systems Security Officers (ISSO), August 1997</i>
<b>NSTISSI 4015</b>	<i>National Training Standard for Systems Certifiers, December 2000</i>
<b>IEEE P1363</b>	<i>Standard Specifications For Public-Key Cryptography, 2003</i>
<b>NIST FIPS 73</b>	<i>Guidelines for Security of Computer Applications, 1980</i>
<b>NIST SP 800-64</b>	<i>Security Considerations in the Information System Development Life Cycle, October 2003</i>
<b>NIST SP 800-61</b>	<i>Computer Security Incident Handling Guide</i>
<b>NIST SP 800-50</b>	<i>Building an Information Technology Security Awareness and Training Program, October 2003</i>
<b>NIST SP 800-55</b>	<i>Security Metrics Guide for Information Technology Systems, July 2003</i>
<b>NIST SP 800-47</b>	<i>Security Guide for Interconnecting Information Technology Systems, September 2002</i>
<b>NIST SP 800-45</b>	<i>Guidelines on Electronic Mail Security, September 2002</i>
<b>NIST SP 800-44</b>	<i>Guidelines on Securing Public Web Servers, September 2002</i>
<b>NIST SP 800-42</b>	<i>Guideline on Network Security Testing, October 2003</i>
<b>NIST SP 800-41</b>	<i>Guidelines on Firewalls and Firewall Policy, January 2002</i>
<b>NIST SP 800-40</b>	<i>Procedures for Handling Security Patches, September 2002</i>
<b>NIST SP 800-36</b>	<i>Guide to Selecting Information Security Products, October 2003</i>
<b>NIST SP 800-35</b>	<i>Guide to Information Technology Security Services, October 2003</i>
<b>NIST SP 800-34</b>	<i>Contingency Planning Guide for Information Technology Systems, June 2002</i>
<b>NIST SP 800-30</b>	<i>Risk Management Guide for Information Technology Systems, January 2002</i>
<b>NIST SP 800-26</b>	<i>Security Self-Assessment Guide for Information Technology Systems, November 2001</i>
<b>NIST SP 800-25</b>	<i>Federal Agency Use of Public Key Technology for Digital Signatures and Authentication, October 2000</i>
<b>NIST SP 800-21</b>	<i>Guideline for Implementing Cryptography in the Federal Government, November 1999</i>
<b>NIST SP 800-18</b>	<i>Guide for Developing Security Plans for Information Technology Systems, December 1998</i>
<b>NIST SP 800-16</b>	<i>Information Technology Security Training Requirements: A Role- and Performance-Based Model, April 1998</i>
<b>NIST SP 800-14</b>	<i>Generally Accepted Principles and Practices for Securing Information Technology Systems, September 1996</i>
<b>NIST SP 800-13</b>	<i>Telecommunications Security Guidelines for Telecommunications Management Network, October 1995</i>
<b>NIST SP 800-12</b>	<i>An Introduction to Computer Security: The NIST Handbook, October 1995</i>
<b>NIST SP 800-6</b>	<i>Automated Tools for Testing Computer System Vulnerability, December 1992</i>
<b>NIST SP 800-5</b>	<i>A Guide to the Selection of Anti-Virus Tools and Techniques, December 1992</i>

# Protocolos y procedimientos de Backup

## Introducción

El manejo de la información y su retención constituyen elementos claves en toda organización, y depende del establecimiento y puesta en práctica de adecuados controles y directrices que regulen a favor de minimizar cualquier riesgo asociado al inadecuado uso y retención de información o de los medios que lo contienen.

## Propósito y Alcance

Esta política establece las directrices generales para el manejo adecuado de discos, cintas y cualquier otro dispositivo de almacenamiento de propiedad del \_\_\_\_\_, de forma que minimicen riesgos asociados a pérdidas y robos de dichos dispositivos de almacenamiento o de su contenido, así como la exposición de material sensible a personal no autorizado.

Esta política aplica a todo dispositivo de almacenamiento que pertenezca al \_\_\_\_\_ y en el que se retenga cualquier información, ya sea para ambientes de producción, prueba, o desarrollo.

## Control de Dispositivos de Almacenamiento

1. Todo dispositivo de almacenamiento y su contenido que sean administrados y operados por el Departamento de Informática es propiedad del \_\_\_\_\_.
2. Deberá establecerse y mantenerse una biblioteca de dispositivos de almacenamiento, incluyendo los utilizados para producción como para prueba y desarrollo. El mantenimiento de la misma es responsabilidad del Departamento de Informática. Dicha biblioteca de dispositivos de almacenamiento deberá mantener adecuados registros de inventario.
3. Todo dispositivo de almacenamiento deberá estar adecuadamente rotulado o etiquetado con un número de identificación una vez éste sea utilizado para cualquier propósito, ya sea para retener información como para realizar cualquier prueba. El número de identificación deberá estar de acuerdo a un formato previamente establecido, en el que se identifique el uso que se está dando al dispositivo de almacenamiento, el responsable del mismo y si se trata de información proveniente del ambiente de producción o no.
4. El registro de inventario de dispositivos de almacenamiento deberá asociar el número de identificación de cada etiqueta con la respectiva información relacionada del medio. El registro deberá contener por lo menos la siguiente información:
  - Número de Identificación del dispositivo de almacenamiento
  - Descripción del contenido
  - Fecha y hora de la última actualización de la información

**Seguridad de  
Dispositivos de  
Almacenamiento**

- contenida
  - Plataforma de sistema (ya sea “Mainframe” o Cliente/Servidor)
  - Nombre de la División del Departamento dueña del dispositivo de almacenamiento
  - Identificará si el contenido es de producción, desarrollo o prueba
  - Identificará si se trata de información “confidencial”
5. Todo dispositivo de almacenamiento nuevo que se incorpore al proceso deberá ser revisado físicamente para detectar cualquier defecto y pueda ser descartado antes de su uso.
  6. Ningún dispositivo de almacenamiento en uso podrá ser mutilado, removido o dispuesto sin la previa autorización del Departamento de Informática, representado por el dueño del dispositivo de almacenamiento y el encargado de la biblioteca de dispositivos de almacenamiento.
  7. El tiempo de vida útil de todo dispositivo de almacenamiento deberá ser controlado y monitoreado de acuerdo a las recomendaciones del fabricante, con el propósito de evitar el riesgo de perder la información contenida en el dispositivo.
  8. La destrucción de cualquier dispositivo de almacenamiento, independiente al uso que haya tenido, deberá incluir previamente la eliminación por medio electrónico de cualquier información contenida en el mismo.
  9. Todo dispositivo de almacenamiento inventariado deberá estar localizado en un lugar cuyo acceso físico esté adecuadamente controlado y únicamente al alcance de personal autorizado.
  10. El lugar donde se localizarán los dispositivos de almacenamiento en uso o inventariados deberá ser a prueba de fuego o contar con un sistema adecuado de prevención de incendios. Además, deberá proveer las características ambientales recomendadas por los fabricantes de dichos dispositivos de almacenamiento.
  11. Toda información almacenada en medios electrónicos que se utilice como parte de las operaciones normales y de seguridad del \_\_\_\_\_, deberá ser duplicada periódicamente y guardada en bóvedas, tanto internas como externas.

## Introducción

Debido a la importancia y la sensibilidad de la información que se procesa el Computador Central ("Mainframe") del \_\_\_\_\_, deberá mantenerse copia de la información y los datos residentes en todas las bases de datos.

Dichas copias se prepararán diariamente, semanalmente, mensualmente, anualmente o según sean requeridos para casos especiales. Los períodos de retención de estas copias serán mantenidos, por lo menos según lo establecido en la tabla siguiente:

Tipo de respaldo	Período de retención	Cantidad de colecciones
Diario	15 Días	15 - (En duplicado)**
Semanal	1 Mes	4 - (En triplicado)***
Mensual	1 Año	12 - (En duplicado)**
Anual	10 Años	10 - (En triplicado)***
Especial*	Permanente	N/A - (En triplicado)***

Nota:

(\*) Se prepararán copias de respaldo Especiales cuando se realicen modificaciones mayores al sistema o a las aplicaciones.

(\*\*) En la Cantidad de colecciones, el duplicado significa, el original más una copia.

(\*\*\*) En la Cantidad de colecciones, el triplicado significa, el original más dos copias.

## Responsabilidad

## Acción

### Operador de Computadoras

1. Verifica la colección de cartuchos que utilizará, dependiendo del tipo de respaldo que va a realizarse. Con ayuda de la aplicación que se usa para la administración de respaldo determina cuáles y cuántos cartuchos serán utilizados.
2. Solicita al Técnico de Operaciones encargado del manejo, control y depósito de las copias de respaldo los cartuchos a utilizarse.

### Técnico de Operaciones

3. Entrega los cartuchos necesarios, debidamente identificados, para realizar la copia de respaldo.
  - Actualiza el registro de medios magnéticos
  - Etiqueta cualquier cartucho nuevo que se requiera incorporar en la colección o conjunto de cartuchos.
4. De ser necesario añadir una nueva definición de un cartucho, define los cartuchos que se desean incorporar en el sistema de acuerdo a las instrucciones de uso del sistema.

## Operador de Computadoras

5. Inserta los cartuchos para que se realice la copia de respaldo según haya sido programada.
  - En la medida que sea posible todo proceso de respaldo deberá realizarse fuera de horas laborables.
  - Toda copia de respaldo debe ser “full backup” y deberá realizarse por duplicado o triplicado, según el tipo de respaldo establecido previamente.
  - Si se trata de una copia permanente, la etiqueta deberá identificar claramente la siguiente información: tipo de respaldo, fecha y hora realizada, contenido y cantidad de cartuchos incluidos
  - El software deberá estar programado para que realice una verificación del “backup” generado contra todos los archivos originales, según aplica.
  - Toda copia de respaldo deberá poseer un conjunto o colección de cartuchos individual, por lo que no se deberá compartir en un mismo cartucho simultáneamente dos o más procesos de “backup”.
6. Una vez terminado el proceso de respaldo, verifica que el proceso haya culminado satisfactoriamente.
  - En caso de que ciertas porciones del respaldo no terminaran de forma satisfactoria, deberá evaluar su sensibilidad tomando en cuenta si se trata de porciones de aplicaciones, base de datos y/o servidores identificados como críticos en el Análisis de Impacto de Negocio (“Business Impact Analysis”); y en cuyo caso deberá forzar un nuevo proceso de respaldo de ser necesario.
7. Entrega al Técnico de Operaciones encargado del inventario de “backups” los dos (2) o tres (3) juegos de cartuchos, según el tipo de respaldo, identificando el período de retención correspondiente.

## Técnico de Operaciones

8. Recibe y revisa los cartuchos entregados por el Operador de Computadoras, verificando que la colección o juego de cartuchos esté completa y debidamente etiquetada.
9. Almacena una de las copias en la bóveda interna dentro del Centro de Cómputos y la otra copia la envía a la bóveda externa fuera de las instalaciones del \_\_\_\_\_. En el caso de los respaldos que requieren tres (3) copias, la tercera copia deberá ser enviada al Centro de Contingencia (“Hot

Site”) del \_\_\_\_\_.

- Procede a entregar al mensajero el “backup” destinado a la bóveda externa.
- Envía la tercera copia al Centro de Contingencia del \_\_\_\_\_ de acuerdo al contrato establecido.

10. Actualiza el registro de inventarios de copias de respaldo, tanto en el del inventario de la bóveda interna como en el de la bóveda externa.

## Instrucciones Especiales

### **Analista de Control de Calidad**

Con la colaboración del Operador de Computadoras restaura cada trimestre una copia de respaldo seleccionada al azar dentro de los últimos tres (3) meses, con el propósito de verificar que el proceso se esté realizando satisfactoriamente. La restauración deberá realizarse en un ambiente de prueba para su posterior remoción.

### **Operador de Computadoras:**

Deberá preparar diariamente un reporte dirigido al Supervisor de Operaciones Técnicas en donde se expliquen los procesos de respaldos realizados, problemas presentados durante su ejecución y cualquier comentario que entienda sea pertinente.

## Introducción

Debido a la importancia y la sensibilidad de la información que se procesa en la red de sistemas de información (“network”) del \_\_\_\_\_, deberá mantenerse copia de la información y los datos residentes en todas las bases de datos de producción de todos los servidores.

Dichas copias se prepararán diariamente, semanalmente, mensualmente, anualmente o según sean requeridos para casos especiales. Los períodos de retención de estas copias serán mantenidos según lo establecido en la tabla siguiente:

Tipo de respaldo	Período de retención	Cantidad de colecciones
Diario	1 Mes	30 - (En duplicado)**
Semanal	1 Mes	4 - (En triplicado)***
Mensual	1 Año	12 - (En duplicado)**
Anual	10 Años	10 - (En triplicado)***
Especial*	Permanente	N/A - (En triplicado)

Nota:

(\*) Se prepararán copias de respaldo Especiales cuando se realicen modificaciones mayores al sistema o a las aplicaciones.

(\*\*) En la Cantidad de colecciones, el duplicado significa, el original más una copia.

(\*\*\*) En la Cantidad de colecciones, el triplicado significa, el original más dos copias.

## Responsabilidad

## Acción

### Operador de Computadoras

1. Verifica la colección de cartuchos que utilizará, dependiendo del tipo de respaldo que va a realizarse. Con ayuda de la aplicación que se usa para la administración de respaldo determina cuáles y cuántos cartuchos serán utilizados.
2. Solicita al Técnico de Operaciones encargado del manejo, control y depósito de las copias de respaldo los cartuchos a utilizarse.

### Técnico de Operaciones

3. Entrega los cartuchos necesarios, debidamente identificados, para realizar la copia de respaldo.
  - Actualiza el registro de medios magnéticos
  - Etiqueta cualquier cartucho nuevo que se requiera incorporar en la colección o conjunto de cartuchos.
4. De ser necesario añadir una nueva definición de un cartucho, define los cartuchos que se desean incorporar en el sistema de acuerdo a las instrucciones de uso del sistema.

## Operador de Computadoras

5. Inserta los cartuchos para que se realice la copia de respaldo según haya sido programada.
  - En la medida que sea posible todo proceso de respaldo deberá realizarse fuera de horas laborables.
  - Toda copia de respaldo debe ser “full backup” y deberá realizarse por duplicado o triplicado, según el tipo de respaldo establecido.
  - Si se trata de una copia permanente, la etiqueta deberá identificar claramente la siguiente información: tipo de respaldo, fecha y hora realizada, contenido y cantidad de cartuchos incluidos
  - Toda copia de respaldo deberá poseer un conjunto o colección de cartuchos individual, por lo que no se deberá compartir en un mismo cartucho, no más de un día el proceso.
6. Una vez terminado el proceso de respaldo, verifica que el proceso haya culminado satisfactoriamente.
  - En caso de que ciertas porciones del respaldo no terminaran de forma satisfactoria, el Operador de Computadoras deberá consultar con el Especialista de Sistemas para evaluar su sensibilidad tomando en cuenta si se trata de porciones de aplicaciones, base de datos y/o servidores identificados como críticos en el Análisis de Impacto de Negocio (“Business Impact Analysis”); y en cuyo caso deberá forzar un nuevo proceso de respaldo de ser necesario.
7. Entrega al Técnico de Operaciones encargado del inventario de “backups” los dos (2) o tres (3) juegos de cartuchos, según el tipo de respaldo, identificando el período de retención correspondiente.

## Técnico de Operaciones

8. Recibe y revisa los cartuchos entregados por el Operador de Computadoras, verificando que la colección o juego de cartuchos esté completa y debidamente etiquetada.
9. Almacena una de las copias en la bóveda interna dentro del Centro de Cómputos y la otra copia la envía a la bóveda externa fuera de las instalaciones del \_\_\_\_\_. En el caso de los respaldos que requieren tres (3) copias, la tercera copia deberá ser enviada al Centro de Contingencia (“Hot Site”) del \_\_\_\_\_.
  - Procede a entregar al mensajero el “backup” destinado a la bóveda externa.

- Envía la tercera copia al Centro de Contingencia del \_\_\_\_\_ de acuerdo al contrato establecido.

10. Actualiza el registro de inventarios de copias de respaldo, tanto en el del inventario de la bóveda interna como en el de la bóveda externa.

## Instrucciones Especiales

### **Analista de Control de Calidad**

Con la colaboración del Operador de Computadoras restaura cada trimestre una copia de respaldo seleccionada al azar dentro de los últimos tres (3) meses, con el propósito de verificar que el proceso se esté realizando satisfactoriamente. La restauración deberá realizarse en un ambiente de prueba para su posterior remoción, en coordinación con las partes propuestas.

### **Operador de Computadoras**

Deberá generar diariamente un reporte dirigido al Supervisor de Operaciones Técnicas en donde se expliquen los procesos de respaldos realizados, problemas presentados durante su ejecución y cualquier comentario que entienda sea pertinente.

## Introducción

La importancia de realizar copias de respaldo (“backups”) de los sistemas de información se evidencia cuando surge la necesidad de utilizar dicha información.

La restauración de archivos constituye la actividad complementaria que se inicia con el proceso de respaldo (“backups”) y la posibilidad de restaurar información crítica es el objetivo fundamental de crear un plan adecuado de respaldo. Por tal razón, el establecimiento de un procedimiento con el objetivo de garantizar la adecuada restauración de información salvaguardada, es imprescindible en la continuidad de las operaciones normales del Departamento de Informática.

Independientemente de la razón que origine la restauración de las copias de respaldo, toda restauración deberá estar debidamente autorizada por escrito por el Gerente de la División de Operaciones Técnicas y deberá ser llevada a cabo en coordinación con el Analista de Control de Calidad.

## Responsabilidad

## Acción

**Especialista de Sistemas, Analista de Sistemas o Administrador de Datos**

1. Identifica o evalúa la necesidad de llevar a cabo la restauración de información contenida en una copia de respaldo. Dicha necesidad puede surgir también por petición de un usuario a través del “Help Desk”.
  - Verifica si se trata de una restauración parcial o total del sistema en el computador central.
  - Verifica si se trata de una restauración de prueba o si es una restauración en el ambiente de producción.
  - En el caso de que la restauración esté asociada al restablecimiento de las operaciones del \_\_\_\_\_ como consecuencia de la activación del Plan de Recuperación de Desastres, dicha restauración deberá realizarse de acuerdo al Plan de Recuperación de Desastres “DRP”.
2. Analiza el impacto de la restauración y las consecuencias potenciales de su ejecución.
  - El análisis del impacto deberá ser realizado según la complejidad de la restauración y tomando en cuenta los siguientes criterios:
    - Tipo de restauración: de prueba o de producción
    - Áreas del \_\_\_\_\_ impactadas por la restauración

- Aplicaciones involucradas en la restauración
- Fecha desde cuando se desea restaurar
- Disponibilidad de espacio en disco
- Usuarios afectados

3. Documenta en notificación dirigida al Gerente de la División de Operaciones Técnicas el impacto potencial que tendría la restauración de la información bajo estudio, su justificación y solicita autorización para realizar la restauración, si aplica.

- En la notificación deberá incluir una recomendación al respecto, que pudiese incluir desde una recomendación afirmativa al proceso de restauración, hasta una recomendación de realizar una evaluación más detallada con la participación de los usuarios.
- Dicha notificación deberá provenir aprobada por el Gerente de División correspondiente.

4. Recibe y revisa la notificación, evaluando la razón que origina la restauración del mismo y su impacto según se mencionó anteriormente.

- De acuerdo a la urgencia de la restauración, la evaluación podrá realizarse inmediatamente. En casos de emergencia y ante cualquier contingencia en las operaciones, se procederá de acuerdo al Plan de Recuperación de Desastres del \_\_\_\_\_.
- En caso de que la restauración de la información afecte áreas sensibles del \_\_\_\_\_ (según están establecidas en el “Análisis de Impacto de Negocio” realizado para el “Plan de Continuidad de Negocio”) deberá someter la aprobación del Director del Departamento de Informática.
- En caso de que se trate de una restauración para un ambiente de prueba verificará que no se trate de información sensible (ejemplo: información de nómina), en cuyo caso establecerá la confidencialidad de la información y con ayuda del dueño de dicha información se definirá la responsabilidad de su manejo entre las personas que la usarán.

5. Aprueba la restauración del (los) archivo(s) firmando o iniciando la notificación recibida y asigna a un Operador de Computadoras como responsable de ejecutar la restauración (“Restore”).

- Entrega al Operador de Computadoras copia de la notificación firmada, como prueba de su aprobación.

**Gerente de la  
División de  
Operaciones  
Técnicas**

**Operador de  
Computadoras**

**Técnico de  
Operaciones**

**Operador de  
Computadoras**

- En caso de que la restauración involucre el ambiente de producción, notificará al Analista de Control de Calidad para que participe del proceso de restauración.
6. En coordinación con el Analista de Control de Calidad, determina la copia de respaldo que contiene la información que se desea restaurar, identificándola por la fecha del respaldo.
  7. Solicita al Técnico de Operaciones que administra las copias de respaldo, el o los medios digitales que contienen los datos o la información.
    - Entrega copia de la notificación firmada por el Gerente de la División de Operaciones Técnicas.
  8. Ubica el medio digital que contiene la copia de respaldo de la información que se quiere restaurar.
    - Para la restauración, selecciona el medio digital que está guardado en la bóveda interna del \_\_\_\_\_. Sólo si no es posible restaurar desde esa copia, selecciona el medio digital guardado en la bóveda externa. Como última alternativa solicita el medio digital que es almacenado en el Centro de Contingencia (“Hot Site”) del \_\_\_\_\_, si aplica. Para la alternativa del Centro de Contingencia deberá mediar una aprobación por escrito del Director del Departamento de Informática.
    - Realizará cualquier gestión necesaria para obtener la copia de respaldo si ésta proviene de la bóveda externa o del Centro de Contingencia.
  9. Entrega al Operador de Computadoras el medio digital que contiene la copia de respaldo que fue requerida y solicita su firma en la copia de la notificación como prueba de la entrega.
  10. Recibe y verifica que los medios digitales entregados por el Técnico de Operaciones sean los que fueron solicitados.
    - De existir algún error lo notifica y solicita al Técnico de Operaciones los medios digitales correctos.
  11. Notifica a los usuarios que pudiesen ser afectados por la restauración, la fecha, hora y el tiempo estimado en que la misma será ejecutada.
  12. En coordinación con el Analista de Control de Calidad, ejecuta la restauración de la copia de respaldo tomando en cuenta el manual de instrucciones del equipo y el “software” que fue utilizado para generar el “Backup”.

- Deberá considerarse la versión y compatibilidad del “software” y equipo antes de ejecutar la restauración.
  - En caso de existir algún problema que impida la culminación de la restauración, notifica el problema al Gerente de la División de Operaciones Técnicas para llegar a una solución.
13. Devuelve al Técnico de Operaciones los medios digitales utilizados, solicitando su firma en la notificación del análisis de impacto, como evidencia de la devolución.
  14. Documenta la ejecución de la restauración de la copia de respaldo en un memorando dirigido al Gerente de la División de Operaciones Técnicas. En la notificación debe incluir cualquier comentario sobre problemas presentados durante la ejecución.
  15. En caso de que la restauración surgiese de una solicitud hecha al “Help Desk”, notifica al Representante de Servicio que la restauración fue completada para que proceda a cerrar el “ticket”.
  16. Guarda en la bóveda correspondiente el medio digital utilizado.

## Introducción

La importancia de realizar copias de respaldo (“backups”) de los sistemas de información, es evidenciada cuando surge la necesidad de restaurar dicha información.

La restauración de dichos archivos constituye la actividad final que se inicia con el proceso de respaldo. La posibilidad de poder realizar la restauración el objetivo fundamental de crear un plan adecuado de respaldo. Por tal razón, el establecimiento de un procedimiento con el objetivo de garantizar la adecuada restauración de la información resguardada es imprescindible en las operaciones normales del Departamento de Informática.

Independiente a la razón que origine la restauración de las copias de respaldo, toda restauración deberá estar debidamente autorizada por escrito por el Gerente de la División de Operaciones Técnicas y deberá ser llevada a cabo en coordinación con el Analista de Control de Calidad.

## Responsabilidad

## Acción

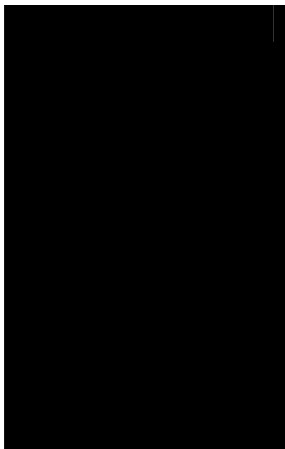
**Especialista de Sistemas, Analista de Sistemas o Administrador de Datos**

1. Identifica o evalúa la necesidad de llevar a cabo la restauración de información contenida en una copia de respaldo. Dicha necesidad puede surgir también por petición de un usuario a través del “Help Desk”.
  - Verifica si se trata de una restauración parcial o total del servidor o servidores involucrados.
  - Verifica si se trata de una restauración de prueba o si es una restauración en el ambiente de producción.
  - En el caso de que la restauración esté asociada al restablecimiento de las operaciones del \_\_\_\_\_ como consecuencia de la activación del Plan de Recuperación de Desastres, dicha restauración deberá realizarse de acuerdo al Plan de Recuperación de Desastres “DRP”.
2. Analiza el impacto de la restauración y las consecuencias potenciales de su ejecución.
  - El análisis del impacto deberá ser realizado según la complejidad de la restauración y tomando en cuenta los siguientes criterios:
    - Tipo de restauración: de prueba o de producción
    - Áreas del \_\_\_\_\_ involucradas en la restauración
    - Servidores involucrados en la restauración



- Fecha desde donde se desea restaurar
- Disponibilidad de espacio en disco
- Usuarios afectados
- Aplicaciones afectadas
- Base de datos afectadas

3. Documenta en una notificación dirigida al Gerente de la División de Operaciones Técnicas el impacto potencial que tendría la restauración de la



Información bajo estudio, la razón o motivo y pide su autorización para realizarlo.

- En la notificación deberá concluirse una recomendación al respecto, que pudiese incluir desde una recomendación afirmativa al proceso de restauración, hasta una recomendación de realizar una evaluación más detallada con la participación de los usuarios.
- Dicha notificación deberá provenir aprobado por el Gerente de División correspondiente.

**Gerente de la División de Operaciones Técnicas**

4. Recibe y revisa la notificación, evaluando la razón que origina la restauración del mismo y su impacto según se mencionó anteriormente.

- De acuerdo a la urgencia de la restauración, la evaluación podrá realizarse inmediatamente. En casos de emergencia y ante cualquier contingencia en las operaciones se procederá de acuerdo al Plan de Recuperación de Desastres del \_\_\_\_\_.
- En caso de que el impacto de la restauración de la información afecte áreas sensibles del \_\_\_\_\_ (según están establecidas en el "Análisis de Impacto de Negocio" realizado para el "Plan de Continuidad de Negocio") deberá someter la aprobación del Director del Departamento de Informática.
- En caso de una restauración para un ambiente de prueba verificará que no se trate de información sensible (ejemplo: información de nómina), en cuyo caso establecerá la confidencialidad de la información y con ayuda del dueño de dicha información se definirá la responsabilidad de su manejo entre las personas que la usarán.

5. Aprueba la restauración del (los) archivo(s) firmando o iniciando la notificación recibida y asigna a un Especialista de Sistemas como responsable de ejecutar la restauración

(“Restore”).

- En caso que la restauración involucre información contenida en bases de datos de aplicaciones, notifica y coordina la aprobación del Gerente de la División de Administración de Datos.
- En caso de que la restauración involucre el ambiente de producción, notificará al Analista de Control de Calidad para que participe del proceso de restauración.
- Entrega al Especialista de Sistemas copia de la notificación firmada, como prueba de su aprobación.

### **Operador de Computadora**

6. Determina la copia de respaldo que contiene la información que se desea restaurar, identificándola por el servidor y fecha del respaldo.

7. Solicita al Técnico de Operaciones que administra las copias de respaldo, el o los medios digitales que contienen la copia de respaldo que se desea restaurar.

- Entrega copia de la notificación firmada por el Gerente de la División de Apoyo Técnico o Especialista de Sistemas.

### **Técnico de Operaciones**

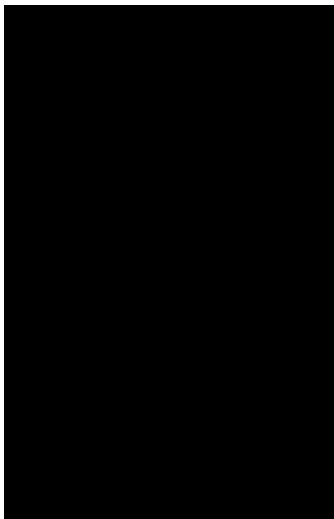
8. Ubica el medio digital que contiene la copia de respaldo de la información que se quiere restaurar.

- Para la restauración, selecciona el medio digital que está guardado en la bóveda interna del \_\_\_\_\_. Sólo si no es posible restaurar desde esa copia, selecciona el medio digital guardado en la bóveda externa. Como última alternativa solicita el medio digital que es almacenado en el Centro de Contingencia (“Hot Site”) del \_\_\_\_\_, si aplica. Para la alternativa del Centro de Contingencia deberá mediar una aprobación por escrito del Director del

**Operador de  
Computadoras o  
Especialista de  
Sistemas**

Departamento de Informática.

- Es responsable de realizar cualquier gestión necesaria para obtener la copia de respaldo si ésta proviene de la bóveda externa o del Centro de Contingencia.
9. Entrega al Especialista de Sistemas el medio digital que contiene la copia de respaldo que fue requerida y solicita su firma en la copia de la notificación como prueba de la entrega.
  10. Recibe y verifica que los medios digitales entregados por el Técnico de Operaciones sean los que fueron solicitados.
    - De existir algún error lo notifica y solicita al Técnico de Operaciones los medios digitales correctos.
  11. Notifica a los posibles usuarios afectados por la restauración, la fecha, hora y el tiempo estimado en que la misma será ejecutada.
  12. En coordinación con el Analista de Control de Calidad, ejecuta la restauración de la copia de respaldo tomando en cuenta el manual de instrucciones del equipo y el “software” que fue utilizado para generar el “Backup”.
    - Deberá considerarse la versión y compatibilidad del “software” y equipo antes de ejecutar la restauración.
    - Ejecuta la restauración en compañía del Especialista de Sistemas.
    - En caso de existir algún problema que impida la culminación de la restauración, notifica el problema al Gerente de la División de Apoyo Técnico para llegar a una solución.
  13. Devuelve al Técnico de Operaciones los medios digitales utilizados, solicitando su firma en la notificación del análisis de impacto, como



**Técnico de Operaciones**

evidencia de la devolución.

14. Documenta la ejecución de la restauración de la copia de respaldo en un memorando dirigido al Gerente de la División de Apoyo Técnico. En la notificación debe incluir cualquier comentario sobre problemas presentados durante la ejecución.
15. En caso de que la restauración surgiese de una solicitud hecha al "Help Desk", notifica al Representante de Servicio que la restauración fue completada para que proceda a cerrar el "ticket".
16. Guarda en la bóveda correspondiente el medio digital utilizado.

## **Disaster Recovery Planning (Plan de Contingencia)**

## **RESUMEN EJECUTIVO**

Se escribe después de la preparación del plan. Incluye los puntos más importantes del plan.

## **INTRODUCCIÓN**

*Este documento contiene el Plan de Contingencia Informática de <<LA INSTITUCION>>. Su propósito es el servir como el vehículo e instrumento principal que apoya a la alta dirección de la institución en su toma de decisión en caso de las situaciones donde los servicios y procesos de trabajo de la institución están interrumpidos en periodos mas largo de lo permitido por los directivos institucionales y especialmente donde los procedimientos operaciones normales del Departamento de Informática no puedan resolver los incidentes y la interrupción de trabajo.*

*Por su importancia como la herramienta principal y guía de trabajo en caso de emergencia, es imprescindible proteger su contenido y la confidencialidad de lo previsto en dicho documento. Solo personal autorizado por la alta dirección de <<LA INSTITUCION>> deben tener acceso a dicho documento y el cumplimiento con los niveles de seguridad institucional, relacionados a este Plan de Contingencia, se debe asegurar por vía de un documento tipo contrato entre por un parte, el equipo involucrado en la preparación, el mantenimiento y la ejecución del plan, y por otro parte <<LA INSTTUCION>>.*

*Un Plan de Contingencia no es un proyecto de trabajo con una fecha de inicio y terminación. Es un compromiso continuo entre la alta dirección de la institución, los departamentos y los profesionales involucrados y <<LA INSTITUCION>>. Se debe mantener y rediseñar el plan con frecuencias necesarias y las actividades planeados en dicho plan se deben ejecutar (de modo de entrenamiento) y el personal involucrado debe recibir entrenamiento continuo en el uso y la ejecución apropiada de dicho plan. Es imprescindible:*

- *Ejecutar todas las actividades necesarias para la preparación del plan*
- *Entrenamiento continuo de los empleados*
- *Desarrollo y revisión de las políticas y los procedimientos cada vez que el departamento y/o <<LA INSTITUCION>> cambia*
- *Reportes de seguimiento a la alta dirección de <<LA INSTITUCION>>*
- *Mejorar las políticas y los procedimientos en base de las mejores prácticas internacionales y la investigación continua*
- *Mantener el plan actualizado*

## **PROPOSITO**

*El propósito del plan es facilitar la operabilidad sostenible de la infraestructura tecnológica y las aplicaciones críticos y de alto valor de <<LA INSTITUCION>>, tanto como el acceso a su Data e Información de valor estratégico y táctico, en caso de emergencias y incidentes extraordinarios que impiden las operaciones de <<LA INSTITUCION>> en un periodo de tiempo mas largo de lo permitido por las políticas institucionales. El plan contiene todo los procedimientos y las políticas necesarios para asegurar el funcionamiento y la operabilidad continuo de <<LA INSTITUCION>>.*

## **ALCANCE**

*<<Inserta la información sobre los sistemas específicos, lugares, ambientes físicos y tecnológicos, que son incluidos en el plan>>.*

## **DESCRIPCION DE PLAN DE CONTINGENCIA**

### **PROVISIONES Y DIRECTIVOS APLICABLES**

*<<Inserta el marco legislativo, todas las políticas y decretos institucionales alrededor de dicho plan>>.*

## **OBJETIVOS**

*El enfoque principal del plan es la protección de los dos activos más importantes de <<LA INSTITUCION>>: Data/Información, y los profesionales/empleados. Enfoques adicionales son:*

- Minimizar la cantidad de las decisiones no previstas que se debe tomar durante una emergencia*
- Identificar los recursos necesarios para ejecutar a manera satisfactoria las acciones definidas en el plan*
- Identificar las actividades de los equipos de trabajo que se define en el plan*
- Identificar la Data e Información critica que se debe respaldar, proteger y restaurar durante la ejecución del plan*
- Definir los procesos de prueba, mantenimiento del plan y el entrenamiento continuo de los profesionales que son involucrados en la ejecución del mismo*

## ORGANIZACION

*En caso de emergencia, la organización de la institución se convierte en una organización de emergencia con sus diferentes integrantes y equipos de trabajo.*

*Las funciones primarias de la organización de emergencia son:*

- *Proteger los empleados y la Data/Información hasta que las operaciones han vuelto a su normalidad.*
- *Asegurar que existe una capacidad adecuada para responder a la emergencia.*
- *Gestionar y ejecutar todas las actividades previstos en el plan de contingencia.*
- *Brindar el apoyo y la comunicación continua a todo personal, los administradores del sistema, los gerentes y la alta dirección, y los oficiales de seguridad.*
- *Lograr restauración de todos los servicios, data e información, y las operaciones críticos de <<LA INSTIUCION>> en manera eficiente y en menor tiempo posible.*
- *Asegurar el cumplimiento con la legislación pertinente.*
- *Asegurar la comunicación continua y eficiente entre los actores del plan y la alta dirección.*

## **FASES DEL LABOR DE CONTINGENCIA**

<<LA INSTITUCION>> junto con la alta dirección del Departamento de Informática deciden los fases de trabajo y los equipos y personal involucrados en cada fase.

### **FASE 1: RESPUESTA**

- *Establecer presencia inmediata en el lugar de incidente y emergencia.*
- *Conducir una evaluación preliminar del impacto.*
- *Establecer y comunicar la fecha/hora de que el acceso al lugar de incidente y las operaciones serán re-establecidos.*
- *Proveer a la alta dirección la información necesaria para la toma de decisiones críticas.*

### **FASE 2: RESUMIR EL TRABAJO**

- *Establecer el sede de operaciones.*
- *Movilizar los equipos de trabajo establecidos en el plan..*
- *Notificar la evaluación y el progreso del plan a los responsables de las operaciones críticas y de alto valor de la institución.*
- *Informar a los contactos internos y externos a la situación.*

### **FASE 3: RECUPERACION**

- *Preparar y ejecutar los procedimientos necesarios para recuperar los procesos críticos y de alto valor de la institución.*
- *Coordinar el trabajo de recuperación con los contactos internos y externos.*

### **FASE 4: RESTAURACION**

- *Preparar y ejecutar los procedimientos necesarios para restaurar los procesos críticos y de alto valor de la institución, en el sitio alternativo decidido para resumir las operaciones.*
- *Implementar los procesos necesarios para migrar las operaciones y los departamentos críticos de la institución.*

- *Administrar la migración y informar el progreso de dicho trabajo a la alta dirección, los empleados afectados y los contactos externos.*

**ASUNCIONES**

*Incluye todas las asunciones basad en las cuales el plan de contingencia esta establecido.*

**FACTORES CRITICOS DE EXITO**

*<<Incluir todas los Factores Críticos de Éxito. Algunos ejemplos son:>>*

- *Compromiso absoluto de la alta dirección de <<LA INSTITUCION>>.*
- *Compromiso presupuestario para la implementación del plan.*
- *.....*

**SISTEMAS/APLICACIONES/SERVICIOS CRITICOS Y DE ALTA IMPORTANCIA**

NOMBRE	DESCRIPCION
<i>Exchange Mail</i>	<i>Microsoft E-mail system</i>

**Figure 3-2 Sistemas críticos y de alto valor**

**AMENAZAS**

*Es imprescindible preparar un listado de todas las amenazas posibles (aun los menos probables) para considerar en la preparación del plan de contingencia.*

## AMENAZAS PROBABLES

PROBABILIDAD DE AMENAZA ( <i>ejemplos</i> )			
AMENAZA	ALTO	MEDIO	BAJO
Problemas con el sistema de Aire-acondicionado	X		
Accidentes aéreos			X
Extorsiones		X	
Bombas		X	
Pedida de Comunicación	X		
Destrucción de Data	X		
Terremotos		X	
Incendio	XX		
Inundaciones	X		
Apagones	XXX		
Sabotaje / Terrorismo		X	
Huracanes	XXX		
Vandalismo			X

Figure 3-3 Ejemplo de Risk Analysis Matriz

### **DESCRIPCION DE SISTEMA**

#### **AMBIENTE FISICO**

<<Insertar la descripción del ambiente físico>>.

#### **AMBIENTE TECNICO**

<<Insertar la descripción del ambiente lógico/tecnológico>>.

### **PLAN**

#### **GESTION DEL PLAN**

#### **GRUPOS DE TRABAJO PARA LA PLANEACION DEL PLAN DE CONTINGENCIA**

*Para poder responder en manera adecuada y eficiente en las emergencias se ha pre-establecido grupos/equipos de trabajos específicos con sus funciones y enfoques necesarios que facilitan la ejecución exitosa del plan de contingencia.*

## **COORDINADOR DEL PLAN DE CONTINGENCIA**

*Se nombra un coordinador y sub-coordinador del plan cuya responsabilidad es administrar el diseño, la implementación y el mantenimiento del plan, tanto como supervisión de la ejecución del plan en caso de accidente. Además, el coordinador asegura el entrenamiento continuo de todo personal involucrado en la ejecución del plan. En caso de emergencia funcionara como el referente principal de la ejecución y mantendrá la comunicación continua con la alta dirección, los empleados y contactos externos.*

## **COORDINADORES DE PLAN DE CONTINGENCIA PARA CADA SISTEMA**

*Además del coordinador y subcoordinador del plan, cada sistema y aplicación (basado en su importancia se puede agrupar aplicaciones y sistemas) tendrá su referente en cuando la ejecución del plan de contingencia. Esta responsabilidad se debe reflejar en la descripción de puesto de dichos coordinadores después de nombramiento.*

## **NOTIFICACION DE LOS INCIDENTES**

*El responsable de los edificios/departamentos donde se encuentran los sistemas y las aplicaciones de alto valor de <<LA INSTITUCION>> deben tener números de contactos del coordinador del plan y los coordinadores de dichos sistemas/aplicaciones para poder reunir y asegurar la evaluación preliminar de la situación y los daños. La reunión será en la localidad de los sistemas/aplicaciones al menos que la situación no permite entrar dicha localidad.*

## **NOTIFICACION INTERNA AL PERSONAL**

*<<Insertar los procedimientos institucionales de la notificación interna a los empleados de LA INATITCION>>.*

## **NOTIFICACION A LOS CONTACTOS EXTERNOS**

*<<Insertar los procedimientos institucionales de la notificación externa a los proveedores de servicios de LA INATITCION>>.*

## **RUEDA DE PRENSA**

*<<Insertar los procedimientos y las políticas de LA INATITCION en cuando la entrega de información a los medios de comunicación >>*

## **SITIOS ALTERNATIVOS DE OPERACIONES**

*<<Inserta todas las localidades externos y/o alternativos de operaciones de LA INSTITUCION. Incluye todos los acuerdos con los proveedores y contactos externos de la institución con acuerdos contractuales para ofrecer este servicio en caso de emergencia>>.*

## **EQUIPOS DE TRABAJO**

### **EQUIPO DE TRABAJO PARA EVALUACION DE LOS DAÑOS**

*Un grupo de profesionales con alta capacidad y conocimiento profundo de los sistemas y las aplicaciones de <<LA INSTITUCION>>. Son profesionales con alto entendimiento de Software y Hardware, y proceso de procurement, quienes pueden hacer una evaluación preliminar de la situación, tomar decisiones en cuando restaurar y/o cambiar/reemplazar cualquier componente de la infraestructura tecnológica de la institución. El equipo de trabajo debe incluir los representantes de los proveedores externos de servicios y equipamientos a la institución.*

*Este equipo de trabajo entra en la localidad de accidente (después de haber recibido permiso del administrador de dicha localidad) para hacer la evaluación preliminar con enfoque principal sobre el estado del ambiente físico y lógico. El quipo hará recomendaciones para transportar los componentes del ambiente físico y lógico al sitio alternativo de las operaciones para poder establecer la viabilidad de restauración y/o cambio del componente.*

### **EQUIPO DE OPERACIONES**

*Son operadores de los sistemas y las aplicaciones que reemplazan los sistemas/aplicaciones críticos y de alto valor de la institución, en caso de emergencia. También incluye el personal responsable de restaurar y recuperar los micro-computadoras (PCs) en caso de emergencia.*

### **EQUIPO DE COMUNICACION**

*El equipo de Comunicación esta compuesto de los especialistas de restauración de la comunicación por voz, data y video, entre los usuarios finales y las computadoras (y la infraestructura tecnológica en su totalidad). Es importante involucrar el proveedor de los servicios de comunicaciones en al preparación del plan de contingencia y los procedimientos relacionados a la restauración de los servicios de comunicaciones.*

### **EQUIPO DE DATA**

*Son especialistas responsables de entrar la data recuperada y/o restaurada que cumple con los requerimientos de integridad y es de la mejor backup disponible.*

### **OFF-SITE STORAGE**

*Son responsables de recuperación de backup de copias de las aplicaciones del sistema operativo, aplicaciones de data, junto con el aseguramiento de la integridad de data, el sitio de backup y el sitio original de operaciones. Son especialistas con conocimiento profundo de los documentos y data de la institución.*

## **EQUIPO DE ADMINISTRACION**

*Es responsable de la ejecución satisfactoria del plan en su totalidad. Es también responsable de la supervisión de la recuperación y restauración de todos estándares, procedimientos, aplicaciones, y sistemas tal y como requerido por el procedimiento de backup y la interacción al sitio de backup. Coordinara la logística de transpone de los profesionales involucrados en la ejecución del plan entre las oficinas de <<LA INSTITUCION>> y el sitio de backup.*

## **PROCUREMENT**

*Este equipo consiste de los profesionales con alto nivel de entendimiento de los recursos de información necesaria, los inventarios, los aspectos presupuestarios, el procedimiento de adquisición de bienes y servicios, y que pueden tomar decisiones puntuales y acertadas para la compra de los recursos necesarios.*

## **EQUIPO DE CONFIGURACION**

*Este equipo esta compuesto de los especialistas de telecomunicación trabajando junto con el equipo de comunicación.*

## **EQUIPO DE FACILIDADES DE RESPALDO**

*Son responsables de las facilidades de Backup.*

## **EQUIPO DE SOFTWARE Y APLICACIONES**

*Los programadores de sistemas responsables de recuperación y restauración de los sistemas y aplicaciones críticos y de alto valor de la institución durante la emergencia.*

## **EQUIPO DE AUDITORIA INTERNA**

*Es responsable de la observación y supervisión de alta nivel (sin involucramiento directo) en la ejecución del plan de contingencia.*

## **EQUIPO DE ASISTENCIA AL USUARIO**

*Son profesionales con el conocimiento del uso de las aplicaciones y los sistemas. Esta compuesto de los gerentes de las áreas grandes de usuarios, gerentes de producciones, y los analistas seniors de aplicaciones, junto a los cuales facilitan la recuperación y la restauración de la data/información y los sistemas y las aplicaciones críticos de la institución.*

## **COMUNICACIÓN DE DATA E INFORMACION**

*Son especialistas de la infraestructura física que facilita la comunicación de data e información, tal y como el cableado.*

## **RESPALDOS**

*<<Ver el plan de Backup>>.*

## **LOS EQUIPOS DE OFICINA Y SUMINISTRO**

*<<Insertar el plan institucional de contingencia en cuando los activos físicos de LA INSTITUCION>>.*

## **PROCEDIMIENTOS DE TESTING**

*El objetivo principal de dichos procedimientos es el mejoramiento continuo de los procedimientos previstos en el plan para disminuir la posibilidad de fallos y errores.*

*Hay dos tipos de procedimientos de Testing: Coordinado y Aleatorio.*

*Diseño e implementación de los detalles de los testings, los procedimientos y el personal incluid, es la responsabilidad del coordinador del plan de contingencia.*

## **ESTRATEGIAS**

*Incluye las recomendaciones a la alta dirección y todo personal involucrado en el diseño, el mantenimiento y la ejecución del plan de contingencia.*

## **DEFINICIONES**

*<<Insertar la definición de todas las palabras, y los términos tecnológicos importantes para la ejecución del plan de contingencia>>.*

***APENDICE A – INFORMACION DE CONTACTOS PARA EL PLAN  
DE CONTINGENCIA***



## ***APENDICE B – PROCEDIMIENTOS DE EMERGENCIA***

Incluir los procedimientos de emergencias, incluyendo los escenarios diferentes (ejemplos: Huracán, Inundaciones) juntos con los planes de evacuaciones.

## ***APENDICE C – EQUIPOS DE TRABAJO Y SUS FUNCIONES***

Incluir todas las responsabilidades por el equipo de trabajo y cada uno de sus integrantes. Un ejemplo es:

<b>Rol</b>	<b>Nombre</b>
<i>Coordinador del Plan de Contingencia (Team Leader)</i>	
<i>Representantes técnicos</i>	

<b>Pre-emergencia</b>	
<i>Acción 1</i>	
<i>Acción 2</i>	
<b>Respuesta inmediata a la emergencia</b>	
<i>Acción 1</i>	
<i>Acción 2</i>	
<b>Post-emergencia</b>	
<i>Acción 1</i>	
<i>Acción 2</i>	

***APENDICE D – PROCEDIMIENTOS DE LOS SITIOS  
ALTERNATIVOS DE OPERACION Y RESPALDO***

Este apéndice debe incluir los procedimientos de set-up de dichos sites, los contactos (incluyendo toda la información para comunicación inmediata y de emergencia).

## ***APENDICE E – LISTADO DE DOCUMENTOS***



## ***APENDICE F – INVENTARIO DE SOFTWARE Y APLICACIONES***



## ***APENDICE G – INVENTARIO DE HARDWARE***



## ***APENDICE H – REQUERIMIENTOS DE COMUNICACION***

El listado complete de la plataforma de comunicación, incluyendo el inventario y la topología de los equipos de data y voz, los diagramas de la infraestructura de comunicación, Data WAN y circuitos de LAN, alternativos para el data network backup, y la especificación de voice network.

***APENDICE I –LISTADO DE LOS PROVEEDORES Y TERCEROS***



***APENDICE J – ACUERDOS PARA EL SOPORTE EXTERNO EN  
CASO DE EMERGENCIA***



***APENDICE K – REQUERIMIENTOS Y PROCEDIMIENTOS DE  
CONTINGENCIA PARA EL CENTRO DE DATA Y OPERACIONES***



***APENDICE L – PROCEDIMIENTO DEL MANTENIMIENTO PARA  
EL PLAN DE CONTINGENCIA***



***APENDICE M - CONTINGENCY LOG***



# **Protocolos de las políticas del Desarrollo de Aplicaciones**

## ***Introducción***

En este informe les presentamos los procesos importantes que cualquier proyecto de Desarrollo de aplicaciones debe utilizar como el punto principal para asegurar la ejecución exitosa del proyecto de desarrollo.

La fase más importante del proyecto de Desarrollo de aplicaciones, es decir la fase de Diseño esta explicado. Los métodos de programación específicos no están incluidos, pues dichos métodos son dependientes del tipo de las aplicaciones existentes y las plataformas y ambientes de desarrollo (ejemplo: .NET) sobre la cual la infraestructura tecnológica de la institución esta basada.

---

**Propósito**

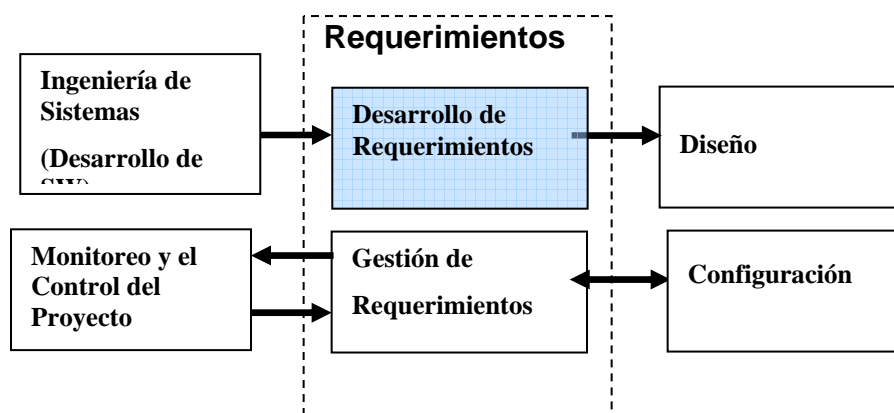
El propósito de este documento es el establecer una herramienta para poder lograr un entendimiento común (entre los desarrolladores y los usuarios/clientes internos) de las necesidades de los usuarios/clientes internos, el uso propuesto del producto, las capacidades necesarias del software, los recursos y las limitaciones del proyecto de desarrollo.

Este proceso describe las tareas y actividades necesarias para el levantamiento, definición y la documentación detallada de los requerimientos del software.

El resultado de este proceso es un listado organizado y detallado de los requerimientos para un proyecto de desarrollo de software, incluyendo:

- Las necesidades, objetivos y metas del usuario final/ cliente interno
- Un alcance definido y estructurado
- Mecanismos de monitoreo de los costos y recursos utilizados
- Identificación de los recursos necesarios y las limitaciones existentes
- Desarrollo de un base de datos sobre los requerimientos de software

---

**Diagramo del Proceso**

---

**Roles y Responsabilidades****Usuario / Cliente Interno**

- Proveer las necesidades, expectativas, limitaciones y recursos
- Proveer requerimientos del mas alto nivel
- Definir los interfaces externos
- Evaluar el listado de los requerimientos levantados y desarrollados

**Autor**

- Levantar e investigar los requerimientos del mas alto nivel del usuario final / Cliente Interno
- Traducir las necesidades y los requerimientos del alto nivel del usuario a un listado detallado de requerimientos del usuario y el producto
- Documentar los conceptos operacionales refinados
- Documentar los requerimientos y las especificaciones

- 
- Documentar los interfaces

*AYUDA: El Autor puede ser el Desarrollador Senior o un representante de el.*

#### **Desarrollador de Software**

- Proveer el Autor con conceptos y herramientas necesarias para el desarrollo del listado detallado de requerimientos
- Evaluar las soluciones comerciales (Commercial-off-the-shelf: COTS) y Gubernamentales (Government-off-the-shelf: GOTS) y proponer el uso de las soluciones existentes

*AYUDA: Normalmente se involucra mas de un solo desarrollador de software en el trabajo de desarrollo. En los proyectos de menor alcance, se puede cumplir el rol el mismo Desarrollador Senior.*

#### **Representante de los interfaces**

- Proveer un punto de contacto autorizado que compromete su recurso para proveer el soporte e información necesario para mejor entendimiento del funcionamiento de la interfase externo.

*AYUDA: Este rol se puede asumir tambien un gerente y/o un usuario de alto nivel.*

#### **Evaluador**

- Validar los requerimientos para asegurar la consistencia y cumplimiento con las necesidades y limitaciones.

*AYUDA: Este rol se puede asumir cualquier miembro del grupo de desarrollo.*

---

**¿Cuándo/donde debe utilizar este proceso?**

- Este proceso debe utilizar como el primer paso en el proyecto de desarrollo de software.

---

**Input**

- Los requerimientos de mas alto nivel
- Los Conceptos Operacionales del Sistema
- Las necesidades de usuarios final y/o clientes internos

*AYUDA: Los requerimientos de mas alto nivel consisten af:*

- *La documentación de los requerimientos de Sistema y los Subsistemas*
- *La documentación de los requerimientos de Software*
- *Los requerimientos de Interfase*

*Los requerimientos de mas alto nivel son provistos externamente o e puede desarrollar por vía de la ejecución de las actividades de proyecto. La documentación de los requerimientos que utiliza como input para la fase de planeación del proyecto puede ser en forma de borrador. La calidad de esta documentación directamente limita el alcance y los objetivos del proyecto de desarrollo, e indirectamente identifica los requerimientos de la interfase. Se debe registrar todos los documentos utilizados como input.*

	<p><i>Los Conceptos Operacionales son un conjunto de definiciones, situaciones, y funciones que el software desarrollado debe tener. Los escenarios operacionales serán desarrollados cuando la definición de los requerimientos, las necesidades de los usuarios, el flujo de trabajo donde el producto se integra, esta listo. Dichos escenarios se puede documentar por vía de descripciones utilizando el lenguaje normal y/o diagramas.</i></p> <p><i>Las necesidades de los usuarios son levantados por vía de las entrevistas personales o las intervenciones de Focus Group.</i></p>
<b>Criterio para iniciar</b>	<ul style="list-style-type: none"> <li>• Los requerimientos de mas alto nivel están listos</li> <li>○</li> <li>• Existe la documentación sobre las necesidades de los usuarios finales</li> </ul>
<b>Criterio para terminar</b>	<ul style="list-style-type: none"> <li>• La documentación de los requerimientos es validada, aprobada y estructuradas.</li> </ul>
<b>Output</b>	<ul style="list-style-type: none"> <li>• Los requerimientos validados y estructurados</li> </ul> <div data-bbox="472 921 1385 1081" style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><i>AYUDA: Debe incluir:</i></p> <ul style="list-style-type: none"> <li>• <i>El documento de estructura de los requerimientos</i></li> <li>• <i>Aceptación de los requerimientos por todos los partes interesados</i></li> <li>• <i>Relación de los requerimientos a nivel de software, recursos humanos, hardware, y los sub-sistemas</i></li> </ul> </div> <ul style="list-style-type: none"> <li>• Documentación de interfase</li> </ul> <div data-bbox="472 1228 1385 1388" style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><i>AYUDA: Dicha documentación:</i></p> <ul style="list-style-type: none"> <li>• <i>Identifica todas interfases externas</i></li> <li>• <i>Asignar una persona de contacto para cada interfase</i></li> <li>• <i>Describe la información que será transferida por vía de interfase</i></li> <li>• <i>Describe el plan de prueba incluyendo los equipos necesarios</i></li> </ul> </div> <ul style="list-style-type: none"> <li>• Planes de reutilización</li> </ul> <div data-bbox="472 1486 1385 1549" style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><i>AYUDA: Especificar los COTS y GOTS que se puede reutilizar, basado en un análisis de costo/beneficio.</i></p> </div> <ul style="list-style-type: none"> <li>• Matrice de relaciones</li> </ul> <div data-bbox="472 1648 1385 1711" style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><i>AYUDA: Proveer un matrice de relaciones que identifica la relación entre los diferentes requerimientos.</i></p> </div> <ul style="list-style-type: none"> <li>• Escenarios Operacionales</li> </ul> <div data-bbox="472 1810 1385 1873" style="background-color: #e0e0e0; padding: 5px; margin: 10px 0;"> <p><i>AYUDA: Este escenario visualiza la interacción entre el software, hardware, las interfases y los usuarios finales.</i></p> </div>

- 
- El historial

*AYUDA: Toda la documentación y los minutos de las reuniones se debe registrar e incluir en la documentación final del proyecto.*

---

### **Tareas Principales**

1. Analizar los requerimientos de mas alto nivel [Autor, Usuario final, Desarrollador de Software]
  2. Definir/Desarrollar el listado detallado de los requerimientos y las especificaciones [Autor, Representante de Interfase, Desarrollador de Software]
  3. Verificar los requerimientos y las especificaciones [Autor, Usuario final, Desarrollador de Software, Representante de Interfase, Evaluador]
  4. Validar los requerimientos y las especificaciones [Autor, Usuario final, Desarrollador de Software, Representante de Interfase, Evaluador, La alta Dirección]
  5. Obtener Aprobación [Autor, La alta Dirección]
- 

### **Tarea 1:**

**Analizar los requerimientos de más alto nivel.** [Autor, Usuario final, Desarrollador de Software]

- a) Examinar, discutir y entender los requerimientos de mas alto nivel y los Conceptos Operacionales.
  - b) Identificar el alcance de los requerimientos, el propósito del software y analizar cualquier limitación que puede afectar los requerimientos de software.
  - c) Alinear el alcance de los requerimientos dentro de las limitaciones existentes.
  - d) Desarrollar y documentar los escenarios operacionales.
  - e) Estudiar las opciones de COTS y GOTS y documentar los resultados.
  - f) Identificar y documentar las asunciones durante el desarrollo del análisis.
- 

### **Tarea 2:**

**Definir/Desarrollar el listado detallado de los requerimientos y las especificaciones** [Autor, Representante de Interfase, Desarrollador de Software]

- a) Mejorar los Conceptos y Escenarios Operacionales para asegurar que todas las funcionalidades son documentadas.
- b) Desarrollar el listado detallado de los requerimientos basado en los requerimientos de mas alto nivel.
- c) Definir los requerimientos externos de las interfases.
- d) Alocar el listado detallado de los requerimientos y las especificaciones a los sub-sistemas y los componentes de la infraestructura tecnológica.
- e) Analizar el listado de los requerimientos para asegurar que dichos requerimientos son dentro de las limitaciones existentes.
- f) Desarrollar el matrice relacional entre los requerimientos en el listado detallado, los requerimientos de mas alto nivel, y los sub-sistemas.
- g) Documentar el listado detallado de los requerimientos y las especificaciones.

**Tarea 3:**

**Verificar los requerimientos y las especificaciones** [Autor, Usuario final, Desarrollador de Software, Representante de Interfase, Evaluador]

- a) Implementar evaluaciones entre los stakeholders del mismo nivel para asegurar que existe un entendimiento y acuerdo sobre el propósito, el alcance y las limitaciones de dichos requerimientos y especificaciones. Es importante que como resultado de este trabajo, ningún requerimiento ambiguo existe.
- b) Determinar para cada requerimiento el alcance que se puede lograr utilizando las tecnologías existentes, al mismo tiempo que se queda claro todo riesgo de la metodología del desarrollo utilizado para cada requerimiento.
- c) Verificar la consistencia de los requerimientos documentado contra la documentación utilizada para la preparación y articulación del requerimiento.
- d) Cuando necesario, diseñar y implementar un prototipo para mejor entendimiento de los requerimientos.

**Tarea 4:**

**Validar los requerimientos y las especificaciones** [Autor, Usuario final, Desarrollador de Software, Representante de Interfase, Evaluador, La alta Dirección]

- a) Determinar y documentar el método de validación y evaluación para cada requerimiento.
- b) Presentar los requerimientos a todos los stakeholders y incorporar cualquier cambio al listado detallado de los requerimientos.

**Tarea 5:**

**Obtener Aprobación** [Autor, La alta Dirección]

- a) Obtener aprobación escrita para poder iniciar el proceso de implementación y desarrollo.
- b) Desarrollar un plan de trabajo detallado incluyendo el orden del desarrollo de los requerimientos y las especificaciones.
- c) Presentar este plan de trabajo a todos los stakeholders.

**Herramientas y Templates**

Nombre	Descripción
Contents of the Software Requirements Review	Checklist for Contents of the Software Requirements Review <a href="http://software/AssetsApproved/PA2.2.1.6.doc">http://software/AssetsApproved/PA2.2.1.6.doc</a>
CORE	Tool supporting model-based systems engineering and product design including requirements analysis <a href="http://www.vitechcorp.com/CORE/productline.html">http://www.vitechcorp.com/CORE/productline.html</a>
DOORS	Requirements tracing aid – <a href="http://www.telelogic.com/products/doorsers/doors/">http://www.telelogic.com/products/doorsers/doors/</a>
FSW Requirements Document Template	<a href="http://software/AssetsApproved/PA2.2.1.2.1.doc">http://software/AssetsApproved/PA2.2.1.2.1.doc</a>

**Herramientas y Templates**

Nombre	Descripción
FSW Requirements Review Standard	<a href="http://software/AssetsApproved/PA2.2.1.6.1.doc">http://software/AssetsApproved/PA2.2.1.6.1.doc</a>
Rational Rose	Requirements tracing aid - <a href="http://www.rationalrose.com/">http://www.rationalrose.com/</a>
SLATE	Requirements tracing aid <a href="http://www.sdrc.com/">http://www.sdrc.com/</a>

**Referencias**

- **ETVX Diagram:** A hyper-link to this diagram can be found in the Process Asset Library on-line version of this document.
- **Glossary:** <http://software.gsfc.nasa.gov/glossary.cfm>  
Defines common terms used in ISD processes
- **IEEE 830-1998: Recommended Practice for Software Requirements Specifications** (available through: <http://standards.nasa.gov/npts/login.taf> at <http://standards.ieee.org/catalog/olis/se.html>)
- **NPR: 7150.2: NASA Software Engineering Requirements**  
[http://software.nasa.gov/npr\\_7150\\_2/index.cfm](http://software.nasa.gov/npr_7150_2/index.cfm)
- **Process Asset Library:** <http://software.gsfc.nasa.gov/process.cfm>  
Library of all ISD process descriptions
- **In-House Development And Maintenance Of Software Products – GPG 8700.5**  
[http://gdms.gsfc.nasa.gov/gdmsnew/srv/GDMSNEWDatabaseObject?document\\_id=6152](http://gdms.gsfc.nasa.gov/gdmsnew/srv/GDMSNEWDatabaseObject?document_id=6152)
- **SQ Software Specification Review (SSR) Product Checklist** [http://sw-assurance.gsfc.nasa.gov/disciplines/quality/checklists/pdf/software\\_specification\\_review.pdf](http://sw-assurance.gsfc.nasa.gov/disciplines/quality/checklists/pdf/software_specification_review.pdf)
- **SQ Software Requirements Specification (SRS) Document Checklist**  
[http://sw-assurance.gsfc.nasa.gov/disciplines/quality/checklists/pdf/software\\_requirement\\_specification.pdf](http://sw-assurance.gsfc.nasa.gov/disciplines/quality/checklists/pdf/software_requirement_specification.pdf)
- **Systems Engineering – GPG 7120.5A –**  
[http://gdms.gsfc.nasa.gov/gdmsnew/srv/GDMSNEWDatabaseObject?document\\_id=6153](http://gdms.gsfc.nasa.gov/gdmsnew/srv/GDMSNEWDatabaseObject?document_id=6153)

## **Protocolos de las políticas de subcontratación de servicios informáticos**

El proceso de subcontratación de los servicios informáticos es parecido en su estructura a cualquier otro proceso de subcontratación de servicios en que el proceso contiene 3 fases principales:

1. Análisis del entorno y diseño del documento de solicitud de propuesta
2. Evaluación, selección y contratación del proveedor de servicio
3. Administración y monitoreo de la implementación del servicio

### ***Análisis del entorno y diseño del documento de solicitud de propuesta***

La fase de Análisis del entorno básicamente utiliza el proceso descrito en el documento de las políticas de desarrollo de aplicaciones, pues en la fase de análisis, la institución asegura tener el listado detallado de los requerimientos y las especificaciones del servicio a recibir. Es imprescindible que el trabajo aquí incluya todos los requerimientos de alto nivel, las especificaciones y el plan detallado de implementación de dichos requerimientos. Es imprescindible planear el trabajo en el sistema lógico que la institución aprecia como oportuno para si mismo, en vez de obedecer el plan de implementación que los diferentes proveedores desean ofrecer, pues dichos planes ofrecidos por los proveedores siempre están basado en las limitaciones de dichos proveedores y/o sus aplicaciones/servicios a ofrecer.

El resultado de dicho análisis será incorporado en el documento de solicitud de propuesta, que también incluirá todos los requisitos legales y económicos que las políticas de contratación del gobierno/estado han establecido.

Es importante que el documento de la solicitud de propuesta exige a los proveedores una propuesta donde el proveedor responde a cada requerimiento, y no solo presenta sus servicios. Es importante que el proveedor describa como sus servicio/aplicación satisface cada requerimiento y/o especificación indicada en el documento de la solicitud, y no es solamente una presentación general de sus servicios.

La preparación de este documento tanto como el análisis de los requerimientos es responsabilidad de un grupo focal compuesto de los representantes técnicos (normalmente miembros del departamento de informática), los representantes de los usuarios finales (normalmente los súper-usuarios conjunto con los gerentes/supervisores departamentales) y la representación de la alta dirección de la institución. Es imprescindible respetar la composición del dicho grupo y dedicar el tiempo necesario a su trabajo, pues las herramientas tecnológicas de

la institución componen una herramienta institucional que afecta el trabajo diario y el rendimiento institucional.

### ***Evaluación, selección y contratación del proveedor de servicio***

La fase segunda de proceso de subcontratación incluye:

- Publicación de la solicitud de propuesta
  - La solicitud de propuesta será publicado basado en los reglamentos institucionales y las políticas del estado.
  - Normalmente la institución ofrece a los solicitantes de proveer servicios, una (o más) sesiones de preguntas/respuestas donde se aclara los requerimientos, las especificaciones y cualquier duda que los proveedores puedan tener. Es importante asegurar que dichas sesiones se enfocan solamente en el responder las preguntas relacionadas al contenido de la solicitud de propuesta.
- Recepción y evaluación de las propuestas
  - La recepción de las propuestas de los proveedores obedece las políticas y reglamentos institucionales.
  - El grupo focal de la subcontratación es responsable de la evaluación de dichas propuestas.
  - En la evaluación de las propuestas es importante que el equipo se prepara un documento de evaluación donde se establece una métrica y criterio de evaluación para cada requerimiento y bloques de requerimientos, y así asegurando que la evaluación del proveedor será de manera equitativa para todos proveedores. También así se asegura que las limitaciones de las aplicaciones/servicios de los proveedores no impida la selección correcta y conveniente del proveedor correcto. Esto es porque las aplicaciones/servicios de los proveedores obedecen la lógica de trabajo y negocio de dichos proveedores y no necesariamente puede satisfacer los requerimientos de la institución en 100%. De hecho es importante que el grupo focal prioriza (basado en importancia relativa) los bloques de requerimientos tanto como cada requerimiento, y así asegura que el servicio y/ la aplicación del proveedor seleccionado satisface un porcentaje adecuado de los requerimientos de la institución.

- Es importante que el trabajo de evaluación de las propuestas es combinado en las presentación (en sitio) de dichas propuestas por el proveedor, y así asegurar que el proveedor pueda explicar los detalles de su propuesta en caso de que la descripción que contiene la propuesta física no esta adecuada.
- Es imprescindible que la priorización de los requerimientos (tal y como mencionada mas arriba) se queda confidencial. Ningún proveedor debe conocer el contenido de dicha priorización.
- Contratación de proveedor de servicio
  - Después de haber elegido el proveedor que satisface las condiciones del trabajo y los requerimientos priorizados, se debe trabajar con la contratación del servicio
  - Existe algunas mejores practicas para esta fase:
    - Siempre involucrar al director/gerente de proyecto asignado por el proveedor de servicio/aplicación en la fase de contratación. Es porque normalmente los representantes de ventas del proveedor participan en esta fase cuando el gerente de proyecto del proveedor estará encargado de la implementación del mismo. Los gerentes de proyecto del proveedor solo se relacionan al contenido del contrato y cualquier promesa verbal del representante de venta del proveedor será olvidado al momento de la implementación.
    - Siempre asegurar que el resultado de trabajo ofrecido por el proveedor (especialmente a nivel de aplicación) será propiedad de la institución. Esto se debe en que cualquiera actualización, parametrización y/o costumización del trabajo entregado por el proveedor tendrá las características de la institución y de hecho es un parte integral del conocimiento institucional, un activo que pertenece a la institución.
    - Los pagos para el servicio y/o la aplicación deben ser or entregables y no basado en el esquema de pago que conviene al proveedor.
    - Siempre asegurar que el pago de la contratación esta dividido en las fases de la implementación, incluyendo un pago final que asegura la satisfacción de los usuarios del servicio y/o la aplicación ofrecido. Esto se asegura por un pago (normalmente entre 10-20% del monto total) guardado para entrega al final de un periodo de prueba, donde la institución asegura que el servicio y/o la aplicación ofrecida esta a toda

satisfacción de todo el personal (y no solo los miembros del grupo focal). Acordamos que no todo el personal de la institución participa en el trabajo de subcontratación, mientras todo personal será afectado por el rendimiento del servicio y/o la aplicación ofrecida por el proveedor.

- Es importante que las garantías ofrecidas por el proveedor cubra todos los detalles del servicio y/o la aplicación. Recordamos que el servicio y/o la aplicación debe convertirse en una solución sostenible para la institución y de hecho no solo su implementación pero el mantenimiento del mismo es de importancia.
- Es importante que el contrato contiene los mecanismos de comunicación (monitoreo del progreso) que la institución entiende oportuno y no lo que el proveedor ofrece (basado en su manera de trabajo). Es importante que los procesos de comunicación esta alineada con el plan detallada de la implementación de los requerimientos (tal y como fue preparado en la fase de análisis) y no las fases de la implementación de servicio/aplicaron (que normalmente obedece la lógica interna del servicio/aplicación del proveedor).
- Es imprescindible exigir que los equipos de trabajo ofrecido por el proveedor tengan las capacidades necesarias (por vía de certificaciones presentadas), y que este equipo no se cambia en el periodo de implementación.

### ***Administración y monitoreo de la implementación***

Para la administración de la implementación se debe asignar un gerente de proyecto (normalmente el miembro técnico del grupo focal con mayor experiencia en la materia). Dicho gerente será responsable total del trabajo de la implementación. Su trabajo se debe monitorear el grupo focal.

## **Consultoría Jurídica del Poder Ejecutivo**

## **Misión**

Les recordamos que la Misión de una organización es:

- *“La razón de ser de la organización”. Es lo que define y justifica la existencia de la organización. Es una herramienta operacional y táctico, que dicta las funciones principales de la organización. No es dependiente de un periodo específico de tiempo. Cambiar la Misión es igual cambiar la organización.*

En el contexto de este trabajo proponemos el siguiente como la base para la Misión del departamento de Informática de cada institución:

- ***Proveemos el liderazgo y las más avanzadas tanto como adecuadas soluciones tecnológicas que apoyan la Consultoría Jurídica del Poder Ejecutivo en lograr su misión, visión y objetivos estratégicos.***
- ***Supervisando y coordinando la capacitación de los empleados de la institución, tanto como el diseño, adquisición, mantenimiento y el uso de la información y las soluciones de Tecnología de Información de la Consultoría Jurídica del Poder Ejecutivo, aseguramos su gestión efectiva, y la apoyamos en sus esfuerzos para la entrega de los mejores servicios a la ciudadanía.***

## **Visión**

Les recordamos que la Visión de una organización es:

- *“A donde queremos llegar dentro de un periodo específico de tiempo”, obviamente partiendo de la misión de la organización. Es una herramienta estratégica. Es muy dependiente de un periodo específico y se debe revisarse constantemente. Cambiar la Visión “NO” es igual cambiar la organización*

En el contexto de este trabajo proponemos el siguiente como la base para la Visión del departamento de Informática de cada institución:

- ***Ser el apoyo estratégico del Consultor Jurídico del Poder Ejecutivo en materia de información y soluciones adecuadas de Tecnología de Información.***
- ***Apoyar la Consultoría Jurídica del Poder Ejecutivo en la eficientización de su gestión y el mejoramiento de los servicios que brinda a la ciudadanía.***
- ***Convertir la Consultoría Jurídica del Poder Ejecutivo en un parte integral y uno de los pilares de la solución de gobierno electrónico que la Presidencia de la Republica desea brindar a la ciudadanía.***

## **Objetivos Estratégicos y las Principales Funciones**

Les recordamos que los Objetivos Estratégicos se tratan de:

- *Para poder alcanzar, en manera sistemática tanto como operativamente, lo propuesto en la Misión y la Visión organizacional, se define un conjunto de Objetivos a lograr. Dichos objetivos se puede definir para sub-periodos dentro del tiempo en lo cual se define la Visión organizacional*

En el contexto de este trabajo proponemos el siguiente como la base para los Objetivos Estratégicos y las Principales Funciones del departamento de Informática de cada institución:

- 8. Facilitación de la comunicación y el compartir la información en manera eficaz y eficiente utilizando la operabilidad y conectividad necesaria dentro de la Consultoría Jurídica del Poder Ejecutivo tanto como entre la misma y demás instituciones de la administración pública. A este fin, identificamos los puntos necesarios de compatibilidad de la información y las soluciones de la Tecnología de Información de la Consultoría Jurídica del Poder Ejecutivo para así desarrollar la adecuada estrategia de Tecnología de Información y la infraestructura tecnológica que habilita la Consultoría Jurídica del Poder Ejecutivo promover el intercambio, el acceso y el uso de la información por los usuarios internos tanto como externos utilizando la Intranet, Extranet e Internet de la Consultoría Jurídica del Poder Ejecutivo.***
- 9. Administración de la captura y la validación de la información necesaria para la gestión eficaz y eficiente de la Consultoría Jurídica del Poder Ejecutivo. Identificación e implementación de la estrategia de información que facilita la Consultoría Jurídica del Poder Ejecutivo lograr sus metas estratégicas hacia la administración pública electrónica y disminuir el uso de la documentación física.***
- 10. Identificación, promoción y facilitación de las capacitaciones adecuadas que habilitan el empleomanía de la Consultoría Jurídica del Poder Ejecutivo tener el nivel y la experiencia necesaria para el efectivo y eficiente uso, mantenimiento y desarrollo de la información y las soluciones tecnológicas de la Consultoría Jurídica del Poder Ejecutivo.***
- 11. Identificación de los niveles adecuados y justos de la inversión en la Tecnología Información y aseguramiento de que esa inversión se***

**convierte en los activos estratégicos de la Consultoría Jurídica del Poder Ejecutivo que la apoya en lograr sus metas estratégicas tanto como las puestas por la Presidencia de la República.**

- 12. Diseño e implementación de las políticas de seguridad y el uso adecuado de la información y las soluciones estratégicas de la Consultoría Jurídica del Poder Ejecutivo. Administración y monitoreo de cumplimiento de dichas políticas.**
- 13. Planeación estratégica y presupuestaria adecuada de la Tecnología de Información de la Consultoría Jurídica del Poder Ejecutivo en coordinación con la oficina del Consultor Jurídico del Poder Ejecutivo y alineada con las metas estratégicas de la Consultoría Jurídica del Poder Ejecutivo.**
- 14. Planeación de la estrategia de desarrollo de las soluciones de Tecnología de Información de la Consultoría Jurídica del Poder Ejecutivo, incluyendo las políticas y criterios de decisión sobre el desarrollo interno tanto como externo, la identificación de alcance, adquisición de servicios, implementación de las soluciones y el sistema de monitoreo de los resultados, el uso y el mantenimiento de dichas soluciones.**
- 15. Administración de los activos de las soluciones tecnológicas y la información de la Consultoría Jurídica del Poder Ejecutivo, incluyendo el aseguramiento de la calidad e integridad de data e información crítica de la Consultoría Jurídica del Poder Ejecutivo.**