USAID/G/EGAD/EM
Support for Economic Growth and Institutional Reform (SEGIR)
Contract No. PCE-I-07-99-00009-00

Task Order 809

Economic Opportunities Strategic Team, RFS
CTO: Gabriela Salazar

Manuales para la Administración de Tecnologías de Información y Comunicación

Raúl Tapia
Richard Zegarra
Gabor Simon

Cuaderno No. 12

Noviembre, 2003

SOW-016/03
Development Alternatives, Inc./ Proyecto SEFIR
USAID/Bolivia

Teléfono 212-5974, 244-1266
www.microfinancebolivia.com
Heriberto Gutiérrez No. 2460, La Paz

Los autores son consultores del Proyecto SEFIR de USAID/Bolivia y las opiniones expresadas en este documento, así como los errores y omisiones, son de responsabilidad exclusiva de ellos y no necesariamente reflejan la posición oficial de USAID o de DAI.

PRESENTACIÓN

Entre los problemas más críticos que afectan el crecimiento y desarrollo de las entidades de micro finanzas en América Latina en general, y en Bolivia en particular, se cuenta la falta de apoyo real y eficaz de los servicios de tecnología en sus operaciones. Las instituciones de microfinanzas (IMF) hacen poco y mal uso de la tecnología en sus entidades, principalmente debido al desconocimiento y la poca importancia que le da la gerencia a las posibilidades de la tecnología, por una parte, y a la falta de orientación de los responsables de la unidad de tecnología, por otra. El resultado es generalmente una pobre e informal infraestructura tecnológica, muchas veces el feudo de una sola persona, que en muchos casos se convierte en un freno al desarrollo en lugar de promoverlo. No es raro encontrar entidades de micro finanzas para las cuales el sistema de información es una especie de regente que dicta qué servicios y en qué condiciones los debe prestar la entidad a sus clientes. Las IMF deben tomar conciencia de que el servicio de tecnología de la información y comunicaciones es precisamente eso, un servicio y como tal debe ser encarado seria y formalmente para lograr que sea una herramienta que está alineada con los objetivos y misión de la entidad.

SEFIR ha desarrollado tres manuales de tecnología de la información y comunicaciones que hacen a la formalidad y seriedad con que deben ser ejecutados ambos servicios en las entidades microfinancieras. Los manuales enfocan los tres temas principales del servicio, a saber: "Estructura, Organización y Funciones de la Unidad de Tecnología de la Información y Comunicaciones", "Seguridad de la Información y Contingencias", y "Metodología para el Desarrollo e Implementación de Sistemas de Información". En suma: cómo debe estructurarse la unidad de tecnología y cuáles deben ser sus funciones y responsabilidades; cómo y con qué herramientas debe protegerse la información y cómo se debe actuar en casos de contingencia; y, finalmente, cómo debe encararse el tema de la implantación de un sistema de información en la entidad.

Si bien los manuales están dirigidos a las unidades de tecnología de la información de las IMF, su aplicación personalizada en cada entidad depende en gran medida del compromiso que tome la gerencia general con los servicios de tecnología en su propia entidad. Se recomienda, en consecuencia, que sea la alta gerencia quien estudie o revise en principio estos manuales para luego buscar la mejor forma de apropiarlos y personalizarlos a la cultura institucional. Es claro que si no se toma una acción clara y decidida para formalizar los servicios de tecnología en las IMF, éstas seguirán enfrentando los problemas señalados en condiciones de desventaja. Por ello, se reta a las entidades a considerar la posibilidad de tomar ventaja del buen uso de los servicios de tecnología de información y comunicaciones en sus propias entidades.

MANUAL DE ESTANDARES

UNIDAD DE TECNOLOGIA DE INFORMACION Y COMUNICACIONES (Unidad TIC)

METODOLOGIA PARA DESARROLLO DE SISTEMAS

DAI/SEFIR/R.Zegarra/R.Tapia
Enero, 2003

RZV/RTG

METODOLOGÍA PARA DESARROLLO DE SISTEMAS

INDICE

I. Introducción

El presente manual es la guía del desarrollo de sistemas para todos los integrantes de la Unidad de Informática, el cual debe ser seguido estrictamente, con el objeto de mantener los estándares apropiados que aseguren la continuidad, buen funcionamiento y mantenimiento de los sistemas.

Asimismo, es importante mencionar que este manual puede ser modificado de acuerdo a las mejoras y propuestas que se deriven del dinamismo de las actividades inherentes a la tecnologia y de los negocios.

Las metodologías expuestas en este manual, son un compendio de metodologías internacionales que permiten la utilización dinámica de éstas en el objetivo de alcanzar estándares en los sistemas y documentación, apropiadas para todos los sistemas que se desarrollen en la Unidad de Informática. Se consideran de aplicación las metodologías estructuradas conocidas, en particular las de James Martin o Chen para el diseño de datos, Gane & Sarson o Yourdon para el diseño de procesos, y en el desarrollo se aplicarán las metodologías de desarrollo estructurado y orientado a objetos, de acuerdo a las que apliquen las herramientas automatizadas que se usen.

Estas metodologías de diseño y desarrollo de sistemas aportan con:

- El uso de reglas sencillas, claras y precisas.
- La definición de tareas concretas.
- Entendimiento real de los requerimientos antes de hacer el código.
- Desarrollo de soluciones a partir del conocimiento general de los problemas y la sucesiva descomposición en problemas/soluciones más pequeños y concretos, modelamiento y generación de prototipos, es decir análisis estructurado.
- Empleo de un lenguaje gráfico y simple de comunicación con los usuarios.
- Codificación estructurada y modular.
- Reusabilidad del código y los módulos.
- Estandarización en la forma de operación de los sistemas.

II. Definiciones generales

2.1 Ciclo de vida de los sistemas.

Análisis.

En esta fase se definen los requerimientos del usuario en materia de información y procesamiento, para realizar con éxito las funciones bajo su responsabilidad, se organizan en modelos lógicos los datos, procesos y el ambiente tecnológico.

Diseño.

En esta fase se traducen las necesidades de información (requerimientos) del usuario en modelos físicos de datos, se detallan los procesos hasta niveles de especificación funcional, es decir, se especifica la arquitectura del sistema dentro de las posibilidades tecnológicas a utilizar.

Construcción.

En esta fase se construye el sistema, en todos sus componentes automatizados: menús, ventanas, ventanas de datos, funciones, librerías, etcétera. Se crean o actualizan físicamente las estructuras de las bases de datos.

Pruebas.
Se prueban individual e integralmente los programas y módulos del sistema.

Implantación.

En esta fase se hace operativo el sistema, es decir, se capacita a los usuarios y se pone en producción el sistema.

2.2 Comité de Usuarios o Comité de Informática.

El Comité de usuarios o de informática será el organismo responsable de coordinar y orientar los desarrollos tecnológicos de la institución y de controlar todo trabajo relacionado con el desarrollo e incorporación de tecnología, entre ellos, el desarrollo de sistemas.

Sesionará regularmente una vez al mes y excepcionalmente cuando las condiciones lo exijan. Cada sesión será preparada con anticipación en una agenda de trabajo que incluya todos los temas a tratar, los objetivos centrales de las sesiones serán coordinar los trabajos futuros y evaluar el desarrollo de los trabajos en curso.

El Comité estará compuesto por los funcionarios de más alto nivel de la institución e incluirá al Jefe de la Unidad de Sistemas, el Jefe Administrativo y el Auditor Interno; estará presidido por el Máximo Ejecutivo de la entidad.

2.3 Proyectos de desarrollo.

Todo trabajo de desarrollo de sistemas será ejecutado en la modalidad de “Proyecto”, será asignado como responsable informático un único Analista/Programador de la Unidad de Sistemas como Jefe de Proyecto, quien será el responsable material del éxito de cada proyecto. El Comité de Informática asignará a un funcionario de contraparte del área usuaria, corresponderá a un área o unidad directamente involucrada en el sistema.

Cada proyecto de desarrollo estará apoyado por personal adicional de informática, de acuerdo a las necesidades y complejidad del proyecto, también contará con el concurso y trabajo de los funcionarios de las principales áreas involucradas o afectadas.

2.4 Roles informáticos.

Los roles informáticos corresponden a las tareas técnicas de desarrollo del sistema, comprenden a: la elaboración de modelos y diseños, construcción de programas, elaboración de manuales (personal de Organización y Métodos) de Usuarios y documentación técnica de los sistemas.

2.5 Roles de usuario.

Los roles de usuario corresponden a las tareas específicas de definir requerimientos, proporcionar detalles de las funciones comprendidas en el sistema (automatizables o no), revisar los modelos y diseños y aprobarlos, probar los productos automatizados y aprobar la documentación de los sistemas.

2.6 Terminología empleada.

Aún cuando la terminología informática es conocida, conviene aclarar el entendimiento común de los principales términos empleados por la institución en el desarrollo de sus sistemas y tecnología. A continuación se describen los términos más comunes, esta lista será enriquecida por el propio ejercicio de la institución.

Plan Integral de Sistemas: Guía de desarrollo tecnológico institucional.

Sistema: Conjunto de funciones automatizadas y no automatizadas con las que interactúan los usuarios o funcionarios, para procesar y obtener información útil a sus labores específicas.

Aplicación: Entiéndase como sistema.

Módulo: Conjunto de programas o funciones que son parte de un sistema o aplicación y sirven a un propósito más específico dentro del mismo.

Programa o función: Alguna operación automatizada que es parte de un módulo.

Modelo de datos: Representación esquemática y gráfica de la información en los sistemas.

Diagrama Entidad Relación (ERD): Entiéndase como Modelo de datos.

Modelo de procesos: Representación esquemática y gráfica de los procesos o

funciones en los sistemas.

Diagrama de Flujo de Datos (DFD): Entiéndase como Modelo de Procesos.

Diagrama de Transición de Estado (STD): Representación esquemática y gráfica de las transformaciones que ocurren en entidades de datos, durante el ciclo de proceso del sistema.

Tecnología: Describe los componentes físicos (hardware) y lógicos (programas de computadora o software), que se requieren y/o aplican en la institución.

Usuario: Funcionarios que no son desarrolladores del sistema, pueden ser de la institución o externos a ella, que tienen que ver o son afectados por el sistema. Tienen la responsabilidad de la definición de los requerimientos del sistema hasta en su último detalle.

Proyecto: Definición estructurada de un conjunto de actividades que deben ser realizadas por personas empleando recursos, en un plazo determinado para lograr una meta u objetivo.

Fases: Conjunto de actividades agrupadas por lógica secuencial de ejecución y asignación de recursos en un proyecto, para su efectiva realización y control de su ejecución.

Actividades: Tareas específicas agrupadas en una fase.

III. Análisis.

3.1 Objetivos y alcances del sistema.

En esta tarea se obtiene un conocimiento ordenado y documentado de: las funciones que la entidad realiza, quienes participan y son responsables de estas funciones, con que insumos trabajan y que productos generan o crean en su trabajo. La documentación alcanza a las funciones actuales y principalmente a las mejoras que la entidad cree posibles o requiere de introducir. Posteriormente, esta documentación se constituye en la base para determinar las funciones que se pretenden automatizar, así como los alcances específicos del sistema. Para este estudio y documentación de las funciones de la institución y de los productos de información que soportan o requieren estas funciones, pueden utilizarse los formularios TIC.DS.01, TIC.DS.02 y TIC.DS.03.

Los formularios deben ser llenados por los usuarios funcionales y no por el personal de informática, se recomienda organizar talleres por área funcional o globales para realizar esta labor.

El formulario TIC.DS.01 “Matriz de relación área – funcionario / procesos”, permite documentar los procesos, su secuencia, los responsables y participantes de los mismos. El formulario es una tabla de dos entradas, en las columnas se identifican los procesos y sus tareas y en las filas las áreas y funciones responsables y participantes. Debe incluirse en las áreas y funciones también a entes o personas externas, esto es natural ya que sin interactuar con el exterior la entidad no tiene razón de ser. Los entes externos pueden ser proveedores, clientes, etcétera.

MATRIZ DE RELACION AREA - FUNCIONARIO / PROCESOS

Form: TIC.DS.01 **Título :** Nombre del Modulo o función principal (ejemplo: Control de inventario de bienes) Hoja: ___ de ___

	Nombre del proceso 1						**Nombre del proceso 2**																							
Procesos																														
Area Funcionario (Función)	Tarea 1	Tarea 2			Tarea n																									
Area 1																														
Función 1																														
.....																														
Función n																														
.....																														
Area n																														

Registre en este formulario todas las funciones que realiza (sean estas automatizados o no) y todas las que necesita y no las realiza.
Marque: **X** si es reponsable de la tarea, **O** si participa de la tarea y ***** Si participa indirectamente de la tarea.
Reemplace las palabras **"Función"** y **"Tarea"** por el nombre apropiado de ambas en su entidad. Incluya tantas columnas de función y tarea sean necesarias. Utilice el número de páginas que sean necesarias.

Es recomendable que se especifique un solo responsable, el de mayor experticia, por tarea y es normal o común que de una tarea participen diferentes funciones e incluso áreas. Dependiendo del nivel de participación, se especificará una “O” o un “*”.

El formulario TIC.DS.02 “Matriz de relación área – funcionario / Productos”, permite documentar los productos que se utilizan o crean en los procesos, la frecuencia con que se generan o crean, y principalmente quienes los crean y/o utilizan.

MATRIZ DE RELACION AREA - FUNCIONARIO / PRODUCTOS

Form: TIC.DS.02 **Título:** Nombre del Modulo o función principal (ejemplo: Control de inventario de bienes) Hoja: ___ de ___

	Nombre del proceso 1						Nombre del proceso 2																							
Productos / **Area Funcionario**	Producto 1	Producto 2	....	Producto n																										
Area 1																														
Función 1																														
.....																														
Función n																														
.....																														
Area n																														
Frecuencia de elaboración																														

Registre en este formulario todos los productos que utiliza (sean automatizados o no) y todos los que necesita y no los tiene.

Marque: **G** si genera el producto, **U** si utiliza el producto y **A** Si lo modifica o actualiza.

Marque: **M** si es mensual, **S** si es semanal, **D** si es diario, **R** si es a requerimiento.

Remplace las palabras **"Función"** y **"producto"** por el nombre apropiado de ambas en su entidad. Incluya tantas columnas de función y producto como sean necesarias. Utilice el número de páginas que sean necesarias.

Es recomendable mantener el mismo orden de especificación de procesos y áreas o funciones utilizado en el formulario 01. También es recomendable especificar un único origen de un producto, asímismo, todo producto debe ser usado en al menos una tarea, finalmente, un producto generado en una tarea puede ser utilizado en otras otras tareas.

El formulario TIC.DS.03 “Detalles de información de productos”, permite documentar el contenido de los productos, es decir los datos, atributos y forma de los mismos, de la forma en que los requiere el usuario para apoyar efectivamente sus funciones o procesos operativos.

Form: TIC.DS.03 Hoja:___/___

DETALLES DE INFORMACION DE PRODUCTOS

Area: Función o Proceso:

Identificación del Producto: Nombre del producto (ejemplo: Factura)

Descripción General del Producto / Cambios solicitados:

Nro	Dato o variable	N	R	I	Fuente posible	Descripción del dato o variable

N: Marque una **"X"** si el dato es nuevo, no existe en el producto actual
R: Marque una **"X"** si el dato se repite en el producto, por ejemplo lineas de una factura o celdas de un tabulado de dos entradas.
I: Marque una **"X"** si el dato es imprescindible en el producto

Es recomendable identificar el producto con la referencia del área y proceso en el que se genera, esto ayuda a convocar a los responsables cuando se requieran aclaraciones y/o modificaciones. Debe intentarse especificar incluso los textos o gráficos que dan valor al producto, por ejemplo el Logotipo de la entidad, porque de una manera básica autentifica la validez del producto.

Finalmente, es recomendable trabajar los formularios en archivos electrónicos, al menos como hojas excel, ya que esto facilitará su mantenimiento y actualización futuras.

Una vez concluida la documentación, se debe determinar los alcances de la automatización, identificando en estas funciones cuales son: Automatizables o no, de las automatizables, cuales son posibles y cuales no y establecer prioridades para la automatización. Esta función es de responsabilidad del personal de informática, sin embargo las decisiones finales sobre que automatizar y que no, corresponden en exclusiva a la más alta dirección de la entidad.

3.2 Revisión y análisis del sistema existente.

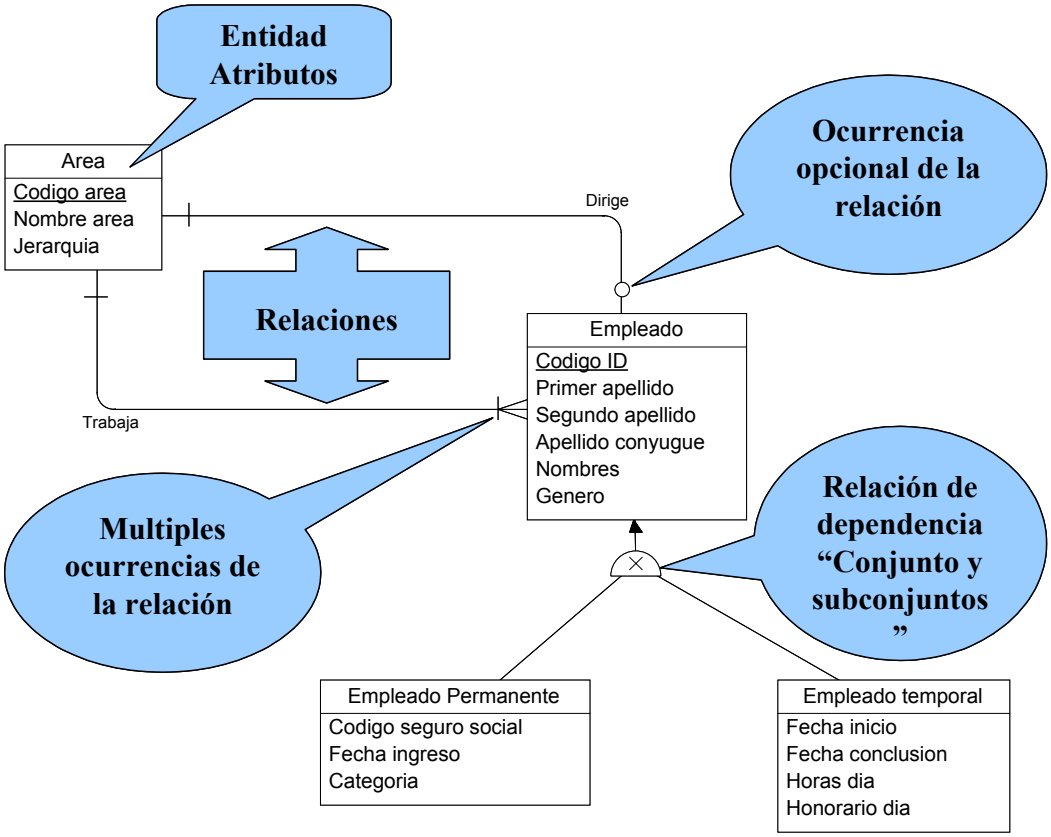
Si está disponible, se revisará y analizará el sistema existente, para identificar los componentes (datos y funciones), mejorables y reemplazables, en base a la identificación de requerimientos y funciones obtenida en los formularios TIC.DS.01,

02 y 03.

3.3 Definición conceptual de los datos.

Es la elaboración del modelo conceptual de datos, a partir de la identificación de la información requerida para el sistema, documentada en los productos y detalles de los productos. El modelo debe representar las entidades y las relaciones entre éstas, que sean de utilidad al sistema, aplicando herramientas de modelado de datos (ERD).

El siguiente ejemplo ilustra un modelo de datos típico y explica los componentes básicos de éste utilizando la metodología estructurada “Modelo de Datos Entidad – Relación (ERD)”.



Algunas reglas básicas del modelo indican:

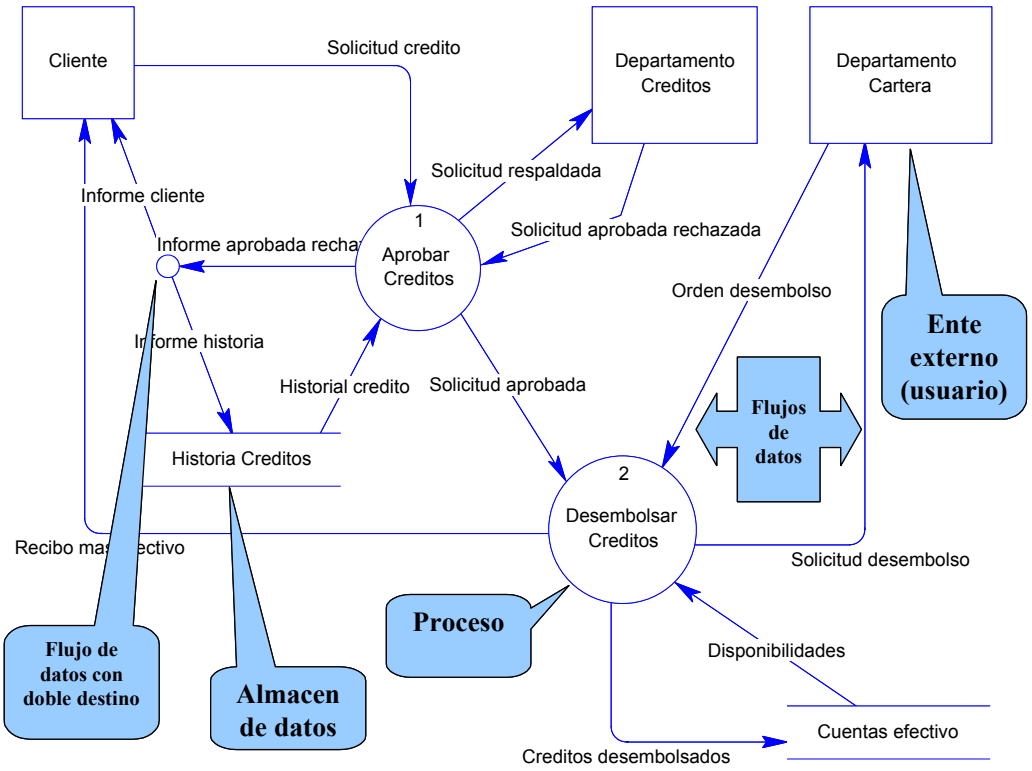
- No puede existir una entidad que no esté relacionada de algún modo al resto del modelo.
- No existe una entidad sin atributos.
- En una relación de dependencia, una ocurrencia de la entidad conjunto o "padre". no puede tomar simultáneamente la forma de más de un subconjunto o "hijo".

En general, estas reglas son simplemente las mismas que se dan en las empresas y el comportamiento de sus componentes e instrumentos en su operación regular diaria. En el ejemplo: Un área no puede tener más de un Jefe y no todos los empleados son jefes de área; Un área no tiene sentido si no cuenta con más de un empleado trabajando en ella, al menos uno y no es normal que un empleado trabaje simultáneamente para más de un área.

El modelamiento de datos se hace sencillo, particularmente si se emplea una herramienta automatizada de las muchas que existen en el mercado. Se ha usado en el ejemplo "Data Architect" de "Power Designor" que es un producto de Sybase. Este producto aplica las metodologías más reconocidas en el mercado, entre ellas: James Martin y Chen.

3.3 Definición de los procesos o funciones principales.

Es la elaboración del modelo de procesos o funciones del sistema, delimitando claramente los alcances de automatización del sistema. Deben incluirse los procesos o funciones seleccionados de los existentes, si corresponde, y las funciones mejoradas y nuevas. El modelo debe representar los entes (usuarios) que interactuarán con el sistema, los procesos del sistema, los flujos de información principales y los almacenes de datos requeridos, el trabajo de modelar procesos debe comenzar con el "Diagrama de contexto". Aplicando herramientas de modelado de procesos (DFD).



Los componentes básicos del modelo de procesos “Diagrama de Flujo de Datos (DFD)”, son simples e incluyen: Entes (usuarios) que interactuan con el sistema, Cliente, Departamento Créditos y Departamento Cartera, en el ejemplo; Procesos, Aprobar Créditos y Desembolsar Créditos, en el ejemplo; Almacenes de datos (vistas de una base de datos física), Historia Créditos y Cuentas efectivo, en el ejemplo; Finalmente Flujos de datos, Solicitud crédito, Créditos desembolsados, son algunos en el ejemplo.

De manera similar a los ERDs, los DFDs tienen ciertas reglas básicas:

- Si no existe al menos un flujo de datos desde y hacia un ente externo, el proceso

no tiene razon de ser.

- Ningún flujo de datos puede relacionarse directo entre dos almacenes de datos, ni entre dos entes externos, ni entre un almacen de datos y un ente externo. Un flujo de datos debe relacionarse siempre atravez de un proceso.
- Todo proceso debe ser descompuesto en procesos más pequeños, hasta que se constituyen en unidades "programables" en algún lenguaje de computadora.
- Todo proceso descompuesto (hijo) debe tener exactamente el mismo número de flujos de datos de entrada y salida, que los del proceso al que pertenece (padre).

En general, las herramientas de modelado de procesos, incorporan estas reglas y las mismas corresponde a metodologías populares como las de Chen, Gane & Sarson y otras.

Igual que en el ejemplo de ERD, en éste se ha empleado la herramienta "Proccess Analyst" de "S-Designor".

3.4 Identificación de los elementos tecnológicos.

Deben especificarse todos los elementos tecnológicos necesarios para la ejecución o proceso del sistema, hardware de servidores, estaciones de trabajo, equipos especiales, software, componentes de red, etcétera.

Los elementos tecnológicos definidos en esta etapa deberán ser claramente expuestos en el cronograma de adquisiciones que corresponda con el proyecto de sistematización.

3.5 Impacto del sistema en la institución y en entidades supervisadas.

Debe elaborarse una lista de los beneficios esperados para la institución desde el punto de vista de la parte económica, así como del mejor aprovechamiento del recurso humano, debe especificarse el impacto que tendrá el sistema considerando: niveles operativos de eficiencia, oportunidad de la información, mejoramientos en la toma de decisiones, calidad de la información y la comparación con el sistema actual. En la medida posible aplicar el criterio del ROI (retorno de la inversión).

3.6 Resultados del sistema.

Deben especificarse todos los resultados o productos que abarcará el sistema, clasificados en:

- Ingreso / modificación de datos
- Consultas
- Procesos y reportes

Estos, por lo general corresponderan con los productos identificados en la tarea 3.1

3.7 Areas afectadas, flujo de procesos operativos.

Debe especificarse el área principal afectada y todas las que de alguna forma se enlazan o vinculan con el sistema.

Debe comprender la especificación de qué datos están siendo procesados en la misma área y cuáles sirven para alimentar a las demás, así como el diagrama de flujo de procesos y actividades que se desarrollan en cada área afectada. En esta actividad se complementa la documementación obtenida en la tarea 3.1.

Alcances del análisis de sistemas

Las tareas y documentación de esta fase debieran comprender a todos los sistemas de la institución, aún en situaciones en las que se revise un sistema existente dentro del conjunto de sistemas automatizados de la institución, para estos casos se deberá como mínimo analizar el impacto que causará el sistema que se revisa en los otros sistemas de la institución. En el primer caso, el trabajo se enmarca en lo que se denomina "Planificación Integral de Sistemas", durante la cual se realiza el análisis inicial y diseño general de los sistemas, a partir del cual se desarrolla el trabajo de análisis detallado.

Responsabilidades en el análisis de sistemas

3.1	Objetivos y alcances del sistema:	Responsable informático Responsable usuario
3.2	Revisión y análisis del sistema existente:	Responsable informático Responsable usuario
3.3	Definición conceptual de los datos	Responsable informático
3.4	Definición procesos o funciones principales:	Responsable informático Responsable usuario
3.5	Identificación de elementos tecnológicos:	Responsable informático
3.6	Impacto del sistema en la institución	Responsable informático Responsable usuario
3.7	Resultados del sistema	Responsable informático Responsable usuario
3.8	Areas afectadas, ...	Responsable informático Responsable usuario

Productos del análisis de sistemas.

a. Documento de definición y descripción clara de los alcances del sistema.
b. Relación de elementos reemplazables y mejorables del sistema actual, si corresponde.
c. Modelo conceptual de datos (CDM o ERD).
d. Modelo de procesos (DFD) y formularios TIC.DS.01.

e. Especificación general de los elementos tecnológicos.
f. Relación y definición de resultados del sistema, formularios TIC.DS.02 y TIC.DS.03.
g. Diagrama de áreas afectadas y flujos de procesos operativos.

IV. Diseño y documentación

4.1 Diagrama de entidades relaciones (ERD).

Debe "refinarse" o detallar el modelo de Entidades y Relaciones siguiendo la metodología de diseño estructurado aplicada, deben incorporarse definiciones detalladas de atributos (tipos, dominios, reglas de validación, formatos de edición y de salida) y generarse el modelo físico de la estructura de datos.

4.2 Diagrama de flujo de datos (DFD).

Debe detallarse el Diagrama de Flujos de Datos “DFD”, siguiendo la metodología de diseño estructurado aplicada, hasta niveles de función "primitiva" o traducible a programa o función de computadora.

4.3 Diagrama de transición de estado (STD)

Si fuese necesario, deberán elaborarse los diagramas de transición de estado (STD) para aquellas entidades del modelo de datos, cuyos cambios de estado representen o involucren funciones específicas complejas, utilizando la metodología aplicada.

4.4 Diccionario de datos.

Debe detallarse el diccionario de datos que se ha especificado para el sistema, considerando lo siguiente:

- Tabla/Entidad

- Campos de Datos
  Descripción de los campos de datos
  Dominios y valores

- Relaciones

- Llaves o índices
  Primario
  Foráneos, alternativos

Este proceso se realiza a partir de los formularios TIC.DS.03 “Detalles de información de productos”

4.5 Prototipos de productos.

Se elaborarán los prototipos de productos y procesos del sistema, estos deben incluir forma y contenido de ventanas o pantallas, menús y procesos generales.

4.6 Tabla de resultados.

Debe especificarse una matriz con los resultados principales al detalle que emitirán los sistemas, de acuerdo al siguiente formato:

- Tipo de información: Descripción genérica que clasifica el tipo de reporte que se necesita emitir.

- Descripción: Descripción del reporte o consulta producto del sistema.

- Tipo de resultado: Especificar si es Reporte/Pantalla.

- Frecuencia: Especificar la frecuencia rutinaria o eventual del resultado.

- Usuarios principales: Especificar los usuarios que utilizan esta información emitida por el sistema.
- Area: Especificar el área a la que pertenecen los usuarios de la información.

- Formato: Especificar en qué tipo de formato se requiere la información, sólo en el caso de que existiera un formato diferente a pantalla o reporte.

- Prioridad: Especificar las prioridades en rangos de 1 a 5, donde 1 es el más urgente.

4.7 Matriz de resultados del sistema vs diccionario de datos.

Debe especificarse una matriz que incluya lo siguiente:

Nombre del reporte/Consulta,

Datos que entran en el reporte en base al diccionario de datos, detallando si es un campo de datos producto de un ingreso de datos interactivo, si es de cálculo o si es un campo de salida.

4.8 Especificación de programas.

Los programas, módulos o rutinas, identificados como procesos primitivos en el DFD, deberán especificarse con el siguiente detalle:

Objetivos: Es una descripción de los objetivos del programa, módulo o rutina.

Entradas: Deben especificarse las entradas del programa, módulo o rutina.

Salidas: Debes especificarse las salidas producto del programa, módulo o rutina.

Procesos y cálculos: Deben especificarse todos los procesos que se deben realizar y los cálculos que están considerados dentro del programa, módulo o rutina.

Alcances del diseño y documentación de sistemas

Las tareas y documentación de esta fase se realizan para cada sistema trabajado.

Responsabilidades en diseño y documentación de sistemas

4.1	Diagrama de entidades relaciones (ERD)	Responsable informático
4.2	Diagrama de flujo de datos (DFD)	Responsable informático
4.3	Diagrama de transición de estado (STD)	Responsable informático
4.4	Diccionario de datos	Responsable informático
4.5	Prototipos de productos	Responsable informático Responsable usuario
4.6	Tabla de resultados	Responsable informático Responsable usuario
4.7	Matriz de resultados del sistema	Responsable informático Responsable usuario
4.8	Especificación de programas	Responsable informático

La responsabilidad principal del usuario en esta fase se centra en la revisión exhaustiva de los productos y la aprobación formal del diseño.

Productos del diseño y documentación de sistemas.

a. Diseño de datos.
   - Modelo lógico (CDM) o Diagrama de entidades relaciones (ERD)
   - Modelo físico (PDM)
   - Diccionario de datos

b. Diseño de procesos.
   - Diagrama de flujo de datos (DFD)
   - Especificación de programas

c. Diagrama de transición de estado (STD).
d. Prototipos de productos del sistema.
e. Tabla de resultados.
f. Matriz de resultados del sistema.
g. Plan de desarrollo.

V. Construcción de los sistemas.

5.1 Generación de base de datos y programas.

Aplicando las herramientas de diseño automatizadas, se generará la base de datos (estructura) y se incluirán definiciones de espacios, áreas de datos, usuarios y esquemas de seguridad.

También aplicando las herramientas de desarrollo automatizadas (ambiente de desarrollo automatizado), se generarán los módulos y programas del sistema. En general los objetos del sistema consistirán de: Menús, Ventanas, Ventanas de datos y las funciones asociadas a éstos. Se aplicarán las técnicas de creación de "plantillas", "herencia" y "triggers". Todos los objetos de los sistemas serán almacenados en "librerías". Los conceptos de "objetos padre" y "herencia" se aplicarán dentro de cada proyecto y también a nivel institucional.

5.2 Programación de funciones especiales.

Se programarán todas las funciones especiales requeridas que no se generen en la herramienta de desarrollo automatizado que se use, funciones como: validaciones especiales, cargas masivas de datos y otras. Cada una de estas funciones será incorporada de forma modular en el sistema, es decir, asociada al objeto que corresponda, cuidando la posibilidad de "reusar" la función en otros objetos del sistema o de otros sistemas.

5.3 Pruebas individuales del sistema.

Se probarán todos los módulos y funciones del sistema en forma individual, para ello el grupo de desarrollo preparará una lista de opciones o funciones críticas que deben ser probadas en el módulo, las que deberan ser elaboradas por los usuarios involucrados en el proyecto, de manera que se disponga de la información de entrada y los resultados esperados, para que en la etapa de pruebas se valide si el sistema responde exactamente a lo requerido.

5.4 Pruebas integrales del sistema.

Se realizarán las pruebas integrales del sistema, para lo cual se elaborará un Plan de Pruebas general. Las pruebas estarán a cargo de funcionarios que preferiblemente no participaron en el diseño y desarrollo del sistema y se probará el sistema en todos sus módulos y componentes. Para estas pruebas los usuarios deberán preparar información para las pruebas en base a las preparadas para las pruebas individuales (punto 5.3) y realizar la comparación de los resultados que emite el sistema con los calculados por los usuarios.

5.5 Manuales de usuario y procedimientos o normas.

Se elaborarán los manuales de usuario, operación y administración del sistema, éstos deben ser descriptivos funcionales y no mecánicos. Los manuales se editarán por separado en lo que corresponde al usuario de lo que corresponde a operación y administración.

Se redactarán y editarán los documentos de procedimientos funcionales o normas de funciones nuevas y/o modificadas en la Institución, como producto del sistema automatizado.

5.6 Plan de Implantación.

Consiste en la elaboración de un Plan que considere la secuencia de actividades que permita implementar el sistema en las áreas de la Institución relacionadas con el sistema a instalarse. Debe considerar fechas previstas de instalación, el personal involucrado en cada una de las actividades (técnico y usuario) y los responsables de cada tarea.

Por otro lado, si es necesario realizar la carga de datos de otro sistema existente o de formularios, será necesario también considerar estas actividades.

Asimismo, es necesario considerar etapas de capacitación y entrenamiento para los usuarios encargados de la operación o utilización del sistema.

En caso de que la implementación de sistema involucre adquisición de hardware o software adicional, será necesario que este Plan de Implantación sea concordante con las fechas previstas para la incorporación de dichos componentes.

Alcances de la construcción de los sistemas.

Las tareas y documentación de esta fase se realizan para cada sistema diseñado.

Responsabilidades en la construcción de los sistemas.

5.1	Generación de programas	Responsable informático
5.2	Programación funciones especiales	Responsable informático
5.3	Pruebas individuales del sistema	Responsable informático Responsable usuario
5.4	Pruebas integrales del sistema	Equipo de pruebas Responsable usuario
5.5	Manuales de usuario y proced.....	Equipo de pruebas Responsable usuario
5.6	Plan de implantación	Responsable informático Responsable usuario

La responsabilidad principal del usuario en esta fase se centra en la prueba exhaustiva de los productos y la aprobación formal del sistema como producto terminado.

Productos de la construcción de sistemas.

a. Sistema probado y listo para operación.
b. Objetos, módulos y funciones del sistema en versión fuente.
c. Manuales de usuario, operación y administración.
d. Reglamentos de funciones o normas modificadas o nuevas.
e. Plan de implantación.

VI. Implantación de sistemas.

6.1 Programa de cursos de capacitación.

Definir los contenidos, calendario horarios y auditorio para cada curso a impartir al usuario acerca del sistema, es probable que los perfiles de usuario sean diferentes por lo que sería necesario programar capacitación personalizada a cada perfil, es decir, usuarios de contabilidad, usuarios de gerencia, etcétera.

Capacitar a los usuarios, empleando los recursos tecnológicos requeridos. La implantación de tecnología, se realizará de acuerdo a los Planes de implantación propios de la institución.

6.2 Plan de conversión y carga de datos.

Esta actividad se realizará cuando exista información disponible para ser cargada al inicio de operación del sistema, por ejemplo de otro sistema. Se elaborará el plan de conversión y carga de datos (migración), así como también las rutinas especiales o funciones de conversión y carga si fueran necesarios. Luego se realizará el proceso de conversión y carga.

6.3 Programa de operación y administración.

Se transfiere el sistema del ambiente de desarrollo y pruebas al ambiente de explotación, se habilitan los accesos de los usuarios reales del sistema, se complementa el manual de operación y administración del sistema con los calendarios de procesos regulares y masivos.

6.4 Definición de los niveles de perfiles y de seguridad

Definir los niveles de acceso que tendrán los usuarios y los perfiles para los mismos, indicando que módulos y/o sistemas pueden tener acceso y que tipo de operación pueden ejecutar (lectura solo, cambio de datos, etc.). Así

mismo definir los parámetros de seguridad de acceso indicando equipos, horarios, etc.

Alcances de la implantación de sistemas

Estas actividades se realizan para el sistema construido y con las áreas involucradas o afectadas por el sistema.

Responsabilidades en la implantación de sistemas.

6.1	Programa de cursos de capacitación	Equipo de pruebas: Responsable informático Responsable usuario
6.2	Plan de conversión y carga de datos	Equipo de pruebas
6.3	Programa de operación y administración	Equipo de pruebas

Productos de la implantación de sistemas.

a. Programa de cursos realizados.
b. Usuarios capacitados en uso del sistema.
c. Planes de implantación, conversión y carga de datos.
d. Sistema en funcionamiento.
e. Documentación final del sistema.
   - Documentos del diseño
   - Manuales de usuario, operación y administración

VII. Adecuaciones de la metodología.

7.1 Condiciones del problema.

La presente metodología de desarrollo de sistemas podrá ser revisada y adecuada a la institución en la etapa inicial del desarrollo de sistemas, por una de las siguientes razones:

- Cuando el alcance del proyecto requiera sólo de la aplicación de ciertas fases del proceso.

- El proyecto es pequeño y no todas las actividades aplican dentro de cada fase.

- Las herramientas automatizadas utilizadas, condicionan el enfoque empleado.

- Situaciones únicas del mercado que garanticen un cambio de enfoque hacia un nuevo estándar del propio mercado.

7.2 Apoyo de herramientas tipo RAD.

Las herramientas CASE y de desarrollo automatizado, apoyan el concepto RAD (Rapid Aplication Development) e incorporan las metodologías de diseño y desarrollo estructurado, así como también de diseño y desarrollo orientado a objetos. La estandarización de la documentación y los componentes de los sistemas deberá seguir las directrices implícitas en estas herramientas, utilizando la definida por la institución.

7.3 Ciclo Análisis-Diseño-Construcción (Prototipos).

Los procesos de análisis, diseño y construcción de "prototipos", apoyados por herramientas CASE y/o RAD, permiten transitar del análisis a la construcción muy rápidamente, permitiendo que el usuario aprecie en vivo y en forma material el prototipo de "su sistema". Así mismo, el feed-back agregado en el proceso de ida y vuelta entre al análisis y la construcción, permite enriquecer el proceso en todas sus fases. Lo cual no libera al proyecto de la responsabilidad de aprobar formalmente los productos derivados de cada fase.

VIII. Estructura de proyectos de desarrollo de sistemas.

El lugar y horario de trabajo del personal de proyectos de sistemas, será similar al usual en la institución.

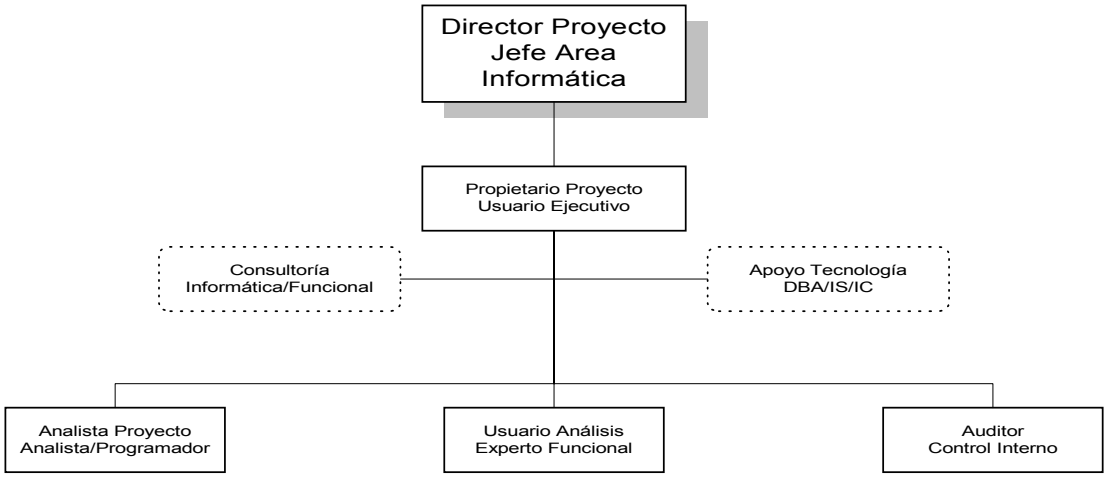
Los funcionarios informáticos asignados al proyecto trabajarán en él a tiempo completo y con dedicación exclusiva.

El personal usuario, será asignado al proyecto con **tiempo a requerimiento del mismo proyecto**, deberá preverse la atención de consultas del proyecto en al menos una hora diaria en el horario a convenir para cada proyecto.

Las sesiones de presentación, revisión y aprobación de productos se programarán con una duración de 2 a 3 horas como máximo, se asentarán en un acta los aspectos más importantes de cada sesión y la aprobación de los productos. Las sesiones se programarán con una anticipación no menor a 48 horas y se convocará al personal que el proyecto juzgue conveniente.

En general, los proyectos de desarrollo se guiarán por la siguiente estructura, roles y agenda de trabajo:

8.1 Estructura del proyecto.



8.2 Roles del proyecto.

a. Director del Proyecto: Jefe de Unidad de Informática

Funciones: Coordinar, supervisar, evaluar y orientar los trabajos del proyecto.

b. Propietario Proyecto: Usuario ejecutivo del área afectada por el sistema

Funciones: Liderar las actividades del proyecto, será responsabilidad de éste, que el proyecto culmine con éxito en los plazos establecidos. Principalmente es responsable de realizar la tareas de definición de los requerimientos, objetivos y alcances del sistema, controlar y evaluar el análisis, diseño, desarrollo, documentación, prueba e implantación del sistema, desde el punto de vista del usuario.

c. Analista proyecto: Analista Líder o Responsable.

Funciones: Dirigir y ejecutar las tareas de análisis, diseño y documentación,

construcción e implantación del sistema.

d. Analista proyecto: Analista Apoyo

Funciones: Ejecutar tareas de análisis, diseño y documentación, construcción e implantación del sistema, apoyando al Analista Responsable.

e. Usuario de análisis: Supervisor del área afectada por el sistema.

Funciones: Apoyar al Usuario Propietario e las tareas de definición de los requerimientos, objetivos y alcances del sistema, evaluar el análisis, diseño, desarrollo, documentación, prueba e implantación del sistema.

f. Auditor: Auditor especialista en control interno o auditoría externa, que no esté en el rol de usuario propietario ni de análisis.

Funciones: Participar del diseño verificando que los procesos a mecanizar no contemplen ineficiencias funcionales; que se incluyan puntos de seguridad y control en el sistema y evaluando estos puntos de control en su implantación.

g. Apoyo en tecnología: DBA (Administrador de la Base de Datos)

Funciones: Apoyar y orientar el análisis, diseño e implantación de la base de datos de los sistemas.

h. Apoyo en tecnología: Ingeniero de Sistemas (IS)
Funciones: Administrar y desarrollar el repositorio de diseño, construcción y documentación de los sistemas: librerías; triggers de eventos, rutinas comunes y funciones de usuario; rutinas especiales y objetos.

i. Apoyo en tecnología: Ingeniero de comunicaciones (IC)

Funciones: Apoyar en el análisis, diseño e implantación de los recursos y procedimientos tecnológicos de comunicaciones en los sistemas.

j. Consultoría Externa: Experto funcional, en el negocio de la entidad (opcional).

Funciones: Orientar y apoyar al Usuario en la definición de los requerimientos, objetivos y alcances del sistema.

d. Consultoría Externa: Experto en Informática

Funciones: Participar en la definición de los requerimientos, objetivos y alcances

del sistema, en el análisis y diseño del sistema. Supervisar, orientar y evaluar el trabajo de desarrollo, documentación, prueba e implantación del sistema.

8.3 Agenda de trabajo.

El Equipo de Proyecto definirá al inicio del mismo, la agenda de trabajo y las funciones específicas de cada participante, deberán realizarse regularmente reuniones de seguimiento al proyecto una vez por semana. Las sesiones de trabajo conjunto serán definidas y controladas de acuerdo a las necesidades del proyecto, estas podrán ser diarias y a tiempo completo si así lo requiere el proyecto entre una sesión de seguimiento y otra.

Cada sesión de seguimiento estará preparada con anticipación en una agenda de trabajo, la que se dará a conocer por escrito a cada participante al menos el día anterior al fijado para la sesión. Se informará en Acta, todos los aspectos importantes tratados, que afecten al desarrollo del proyecto.

8.4 Etapas y productos del proyecto.

Toda etapa del proyecto debe concluir con la presentación y aprobación de los productos específicamente señalados para ésta.

La aprobación se dará en dos instancias:

a. El equipo de proyecto aprobará en una sesión de seguimiento regular los productos que se hayan alcanzado hasta esa fecha, para luego ser sometidos a aprobación del Comité de Informática.

b. El Comité de Informática, en una sesión de seguimiento a proyectos, aprobará los productos presentados por el Equipo de Proyecto.

8.5 Herramientas a emplear en el proyecto.

a. Area de trabajo del proyecto.

Toda la documentación generada y usada por el proyecto deberá estar almacenada en un área común (directorio del proyecto), los nombres de directorios serán creados respetando los estándares de nombres de directorios y áreas de trabajo; el área común será compartido por todos los miembros del equipo del proyecto, en él se incluirán sub_áreas (Sub_directorios) de trabajo para almacenar archivos por tipo y fuente o destino, se incluirán como mínimo los siguientes:

/Proy/ Directorio en el que se almacenan todos los archivos del

proyecto, ejemplo: /Cartera, /Contabilidad, etc.

/Proy/Diseño/ Para almacenar todos los archivos generados por el proyecto y que tienen directa relación con el diseño.

/Proy/Docs/ Para almacenar toda la documentación de administración y seguimiento del proyecto.

b. Herramientas de administración y documentación del proyecto y del sistema.

Administración:	MS_Project
Agenda:	MS_Schedule+
Documentación:	MS_Word
Presentación:	MS_Power Point
Comunicación:	Lotus Notes / MS_Exchange

Las herramientas indicadas arriba son una referencia, la entidad puede utilizar herramientas similares que ella juzgue las más convenientes.

c. Herramientas de análisis y diseño y construcción.

Análisis y diseño:	S-Designor/System Architect.
Construcción de sistemas:	VBasic/Power Builder/Java/etc.
Base de datos:	Sybase/Oracle/Sql Server/etc.
Base documental:	Lotus Notes/MS Exchange/etc

Las herramientas indicadas arriba son una referencia, la entidad puede utilizar herramientas similares que ella juzgue las más convenientes.

Toda la información del proyecto deberá estar almacenada en el área del mismo, cada archivo estará protegido contra escritura para todos los miembros del equipo que no tengan atribución de modificación del archivo. Todos los miembros del equipo tendrán acceso de consulta sin restricciones a todos los archivos del proyecto.

La Paz, Enero de 2003.

RTG/RZV

MANUAL DE ESTANDARES

UNIDAD DE TECNOLOGIA DE INFORMACION Y COMUNICACIONES (Unidad TIC)

MANUAL DE SEGURIDAD Y CONTINGENCIAS

DAI/SEFIR/ R.Tapia
Abril, 2003

RTG

MANUAL DE SEGURIDAD Y CONTINGENCIAS

TABLA DE CONTENIDOS

MANUAL DE SEGURIDAD Y CONTINGENCIAS

INTRODUCCION

Actualmente la seguridad informática ha adquirido gran auge, dadas las cambiantes condiciones y nuevas plataformas de computación disponibles, situación que desemboca asimismo en la aparición de nuevas amenazas en los sistemas informáticos.

Esto ha llevado a que muchas organizaciones hayan desarrollado documentos y directrices que orientan en el uso adecuado de estas tecnologías para obtener el mayor provecho de las ventajas que brindan. De esta manera las políticas de seguridad informática surgen como una herramienta para concienciar a los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Las políticas de seguridad informática fijan los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen. Éstas políticas deben diseñarse "a medida" para así recoger las características propias de cada organización. No son una descripción técnica de mecanismos de seguridad, ni una expresión legal que involucre sanciones a conductas de los empleados, son más bien una descripción de lo que se desea proteger y el por qué de ello.

De acuerdo con lo anterior, el implementar políticas de seguridad requiere un alto compromiso con la organización, agudeza, destreza y experiencia técnica para detectar fallas y debilidades; y constancia para renovar y actualizar dichas políticas en función del dinámico ambiente que rodea las organizaciones modernas.

Para la generación de las políticas mencionadas, resulta conveniente realizar previamente la ejecución de una auditoría de seguridad informática. Esta es una disciplina que, a través de personas independientes de la operación auditada y mediante el empleo de técnicas y procedimientos adecuados, evalúa el cumplimiento de los objetivos institucionales con respecto a la seguridad de la información y emite recomendaciones que contribuyen a mejorar su nivel de cumplimiento.
Desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y, en última instancia, en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información y el conocimiento.

Riesgos a considerar en el servicio informático de la Entidad

Los riesgos a los que está expuesto el servicio informático son amplios y muy variados, sin embargo, pueden ser agrupados o categorizados en las siguientes categorías:

1. Suspensión del servicio informático. Es cuando a causa de una contingencia, el servicio informático es suspendido parcial o totalmente, por tiempos también variables, minutos, horas, días, etcétera.
2. Pérdida de la información. Es cuando datos valiosos para la entidad se han perdido por la ocurrencia de una contingencia y afectan al normal funcionamiento de la entidad.
3. Uso de información errónea. Ocurre cuando a causa de una contingencia, los niveles operativos y ejecutivos están haciendo uso de información errónea para sus tareas y toma de decisiones. Normalmente la ocurrencia de estos hechos es muy difícil de detectar.
4. Uso indebido de la información. Ocurre cuando la contingencia permite que personal de la entidad o personas externas hacen uso de la información de la entidad para usos ajenos a las funciones de la misma.
5. Uso indebido de los recursos informáticos. Ocurre cuando personal de la entidad o personas externas hacen uso de los equipos de la entidad para usos ajenos a los de la propia entidad.
6. Pérdida o daño en los equipos informáticos. Ocurre cuando la contigencia provoca daños físicos en los equipos e infraestructura informática de la entidad, dejándolos fuera de servicio parcial o totalmente durante periodos de tiempo variables.
7. Pérdida o daño en las instalaciones informáticas. Ocurre cuando las instalaciones físicas, edificaciones y ambientes de trabajo, sufren daños parciales o totales, que impiden el desarrollo de las actividades del servicio informático.

Causas posibles que ocasionan la ocurrencia de los hechos de riesgo

De manera similar a los riesgos, las causas posibles son múltiples y variadas. También de igual manera, pueden ser agrupadas en dos categorías:

1. Acciones negativas voluntarias. Son las acciones premeditadas para ocasionar daños en el servicio informático con el objeto de obtener alguna ventaja o ganancia ilícita del hecho. Puede provenir de fuentes externas y también de fuentes internas.
2. Accidentes involuntarios. Son acciones que se dan por falta de conocimiento o negligencia en las tareas habituales.

Niveles de tolerancia a la ocurrencia de contingencias

El punto crítico en el tema de contigencias y cómo enfrentarlas, es saber determinar el balance adecuado entre los niveles de riesgo tolerables y/o manejables. Esta ecuación implica tres factores concretos: Costos de operación del servicio informático; Costos de prevención de contingencias y Costos de solución de problemas ocasionados por las contingencias.

Para aclarar el punto anterior podemos señalar que un sistema de prevención y corrección ante contingencias no debe ser tan sofisticado y costoso que impida a la entidad lograr satisfactoriamente sus metas económicas. Tampoco debe ser tan simple o relajado que la ocurrencia de la más mínima contingencia provoque daños económicos que afecten de manera similar a lo anterior. El Plan de contigencia debe contemplar planes de contingencia, de recuperación de desastres y de reducción de riesgos, adecuados a la entidad.

Alcance del manual de contingencias

De acuerdo con los tres puntos anteriores, el presente documento pretende ser apenas una referencia básica de: Que riesgos concretos existen en el servicio informático; Que medidas preventivas pueden ser aplicadas para evitar la ocurrencia de contingencia; y Que medidas correctivas pueden ser aplicadas una vez que ocurren las contingencias.

El proponer y utilizar políticas de seguridad requiere un alto compromiso de la institución, agudeza técnica para establecer fallas y deficiencias, y constancia para renovar y actualizar dicha política en función de un ambiente dinámico.

Cada entidad debe seleccionar y aplicar estas medidas preventivas y correctivas de acuerdo al nivel de riesgo tolerable para ella buscando el balance apropiado entre los tres factores señalados.

Utilización del Manual

El presente Manual está orientado a todos los integrantes de la Unidad de Tecnología de Información y Comunicaciones (Unidad TIC) de las Entidades Financieras y tiene por objeto desarrollar los temas principales a implementar para lograr una adecuada seguridad de los sistemas, datos y equipamiento de la Institución.

Es de obligatorio conocimiento y aplicación por parte del personal. Su cumplimiento maximiza las garantías de seguridad en la información. Su actualización debe de ser constante, ya sea por algún cambio en las necesidades de la Unidad TIC o la revisión de algún procedimiento por conducir a situaciones de riesgo en la seguridad de la información.

Debe, como lineamiento principal mantenerse la información segura, libre de todo riesgo y disponible, en el momento que se requiera y a costos razonables. Así, el presente manual está sujeto a modificaciones y se debe mantener una copia en medio magnético en alguna gaveta de fácil alcance.

El manual está estructurado en dos partes que explican los temas principales a implementar para una adecuada seguridad y manejo de contingencias en los sistemas, datos y equipamiento de la Entidad.

MANUAL DE SEGURIDAD Y CONTINGENCIAS

PARTE I: GUIA DE REFERENCIA

1. ESTRUCTURA ORGANIZATIVA DE LA UNIDAD TIC

Utilización : Unidad TIC
Descripción : Procedimientos de seguridad en la estructura organizativa de la Unidad TIC.

La Unidad TIC tendrá un responsable y tres Departamentos o Sub-Unidades a su cargo: Departamento de Desarrollo de Sistemas, Departamento de Soporte Técnico y Departamento de Operaciones. Todas las actividades del personal de la Unidad TIC estarán regidas por los estándares aprobados por la Institución y por los Manuales de Estructura, Organización y Funciones.

El Departamento de Desarrollo de Sistemas tendrá asignadas las tareas exclusivas de desarrollo y mantenimiento de sistemas. El de Soporte Técnico, será el responsable de proveer los servicios de asistencia técnica. El de Operaciones será responsable de procesar la información, administrar y resguardar de forma directa la información y los recursos tecnológicos de la Institución.

En general las asignaciones de responsabilidades en la Unidad TIC deberán tener en cuenta los siguientes aspectos mínimos:

- División de funciones. Las funciones de diseño y desarrollo, administración de datos y las de operación o producción, deben estar completamente separadas, los analistas y programadores no deben tener acceso a los programas y datos en producción y los operadores no deben tener acceso a la información de los proyectos de desarrollo.

- Asignación de tareas. En el caso del personal de Soporte, este debe responder a las solicitudes de los usuarios evaluando la importancia e implicancia de las solicitudes para con la Unidad y la institución. Básicamente, cada uno de los servicios del Departamento de Soporte Técnico, debe ser realizado por diferentes personas, las que deberán estar dedicadas exclusivamente a ello.

- Rotación de personal. Es aconsejable una rotación trimestral del personal que realiza las tareas de producción. El Jefe del Departamento de Operaciones será el que promueva estas rotaciones.

- Asignación de activos fijos. Los activos fijos del sector deben estar distribuidos entre todos los integrantes de la Unidad, respondiendo a las necesidades y uso que haga cada persona de ellos. Por tratarse de equipos costosos, deben mantenerse en lugares bien definidos, para facilitar los procesos de inspección.

- Fin de la relación laboral de personal de la Unidad TIC. Cuando un integrante de la Unidad deja la institución, deben cumplirse los siguientes pasos:

- Transferencia de activos fijos. Todos deben ser revisados, que estén en buen funcionamiento y completos.
- Devolución de material y manuales prestados, según los registros.
- Devolución de Software prestado.
- Cancelación de cuentas y permisos de acceso a los sistemas, aplicaciones y equipos. No deben quedar espacios vulnerables en la seguridad.

Si se cumplen satisfactoriamente los anteriores puntos, se da por finalizada la relación laboral y se ejecutan los procesos administrativos pertinentes.

2. SEGURIDAD EN LOS PROCESOS DE PRODUCCIÓN Y EL CENTRO DE CÓMPUTOS

2.1 Seguridad en los procesos de producción

Utilización: Departamento de Operaciones
Descripción: Describe los procesos de producción que se realizan en el Departamento de Operaciones.

Para cualquier operación o proceso que se realiza en el área de producción, se deben describir todos los pasos a seguir y los procesos al detalle para la ejecución de un trabajo. Los cuales estarán detallados en las instrucciones del respectivo Manual de Operaciones de cada sistema o en el Manual de operaciones general de la Unidad TIC.

Para cada proceso se debe estructurar una o varias tarjetas de registro, las cuales norman los mismos y la forma en que se deben ejecutar. Cada tarjeta contiene básicamente:

- Nombre del proceso general
- Nombre del proceso de detalle
- Instrucciones del proceso, incluyendo instrucciones en caso de error
- Tiempo de duración de cada proceso en horas y minutos
- Procedimientos utilizados
- Responsables
- Fecha de ejecución
- Periodo de procesos
- Usuarios que reciben el resultado

Los manuales de operación de los sistemas o aplicaciones, así como de las funciones del área de operaciones deben estar actualizados. Incluyendo todos los pasos a seguir para el encendido y puesta en marcha de la red y los servidores de la red, para la resolución de problemas, y también para la "bajada" y "subida" de los servidores y la red.

La programación y carga de trabajo en los equipos debe guiarse por instructivos que permitan un equilibrio entre las necesidades de los usuarios y las capacidades de los equipos y sistemas. Así, los procesos largos en lotes (batch) deben programarse en horarios que no perjudiquen las actividades de los usuarios con los sistemas.

2.2 Seguridad del Centro de cómputos

Utilización : Departamento de Operaciones
Descripción : Normas generales de seguridad del centro de cómputos.

El centro de cómputos siempre debe estar en perfecto orden y limpio para permitir una cómoda operación. Debe organizarse el conjunto de manuales, herramientas y hardware de modo que estén cerca de las áreas de necesidad. También deben ser fácilmente accesibles.

El centro de cómputos debe contar con servicio de aire acondicionado, equipos de suministro de energia alternativa (UPS y/o Planta propia de energía), extinguidores apropiados para equipos, detectores de humo que en caso de incendio accionen sirenas.

Se debe realizar mantenimiento periódico de los equipos de emergencia, instalados en el centro de cómputos: ventiladores, luces de emergencia, UPS, líneas de comunicación de emergencia, etc. Todo servicio de mantenimiento se registrará en el Log del Sistema identificando fecha, equipo, falla, solución o servicio realizado. También deben realizarse inspecciones de los equipos extinguidores, ventiladores, detectores de humo, etc.

Toda la información almacenada en el centro de cómputos y archivo magnético debe ser guardada bajo llave. Se deben designar responsables de la información.

En el procedimiento de inspección periódica del centro de cómputos se debe realizar la revisión de todos los equipos una vez al mes. En cada inspección, también debe contarse con la revisión de otras probables causas de riesgo.

2.3 Seguridad en el acceso al Centro de cómputos

Utilización : Departamento de Operaciones
Descripción : Normas generales de acceso al centro de cómputos.

El Centro de cómputos debe ser una oficina a la cual tengan acceso únicamente los integrantes de las área de operaciones y producción. Debe estar prohibido el ingreso de otro tipo de personal.

El centro de cómputos debe contar con una cerradura electrónica cuya clave pueda ser cambiada fácilmente. El responsable del centro de cómputos debe tener, además, una llave que habilite el acceso a todos los operadores, para cerrar la oficina en los horarios fuera de trabajo.

Unicamente se pueden atender los pedidos a través de la puerta y personalmente, pues toda información que sale debe ser registrada con la firma del usuario. La puerta también tendrá una llave en poder del Jefe de Operaciones y otra del área de Administración general de la Institución. El jefe de la Unidad TIC es el único que podrá otorgar acceso en horarios fuera de trabajo al personal que no es del área de operaciones o producción.

2.4 Seguridad de los servidores de datos

Utilización : Departamento de Soporte Técnico.
Descripción : Normas generales sobre la seguridad de los servidores de datos.

Los servidores de datos deben estar en perfecto estado de funcionamiento. Cualquier falla debe reportarse inmediatamente al servicio técnico. También los operadores y el Administrador del sistema, deben monitorear constantemente el estado de los equipos, mediante los utilitarios con los que cuenta.

Se debe hacer una revisión diaria de los discos, directorios o "file systems" y chequeo del estado de las bases de datos. También es aconsejable hacer un chequeo de virus y del buen orden de datos.

Debe contratarse un servicio de mantenimiento para los servidores, para observar su buen funcionamiento.

Debe realizarse una limpieza de cabezales de los tape drives y disk drives, limpieza externa, revisión de cableado y pruebas del equipo.

Los passwords de administración deben estar anotados siempre en el Log de passwords con llave en la gaveta de passwords.

Es recomendable además contar con un servidor de respaldo que pueda ser utilizado ante una eventual caída del servidor principal de datos. Por ello, será necesario realizar pruebas cada cierto periodo de tiempo de los mecanismos de respaldo de los servidores como medida de prevención y certeza del funcionamiento del procedimiento, ya que puede ocurrir que estos mecanismos no funcionen correctamente o que los responsables del centro de cómputos no desempeñen sus funciones correctamente por falta de práctica.

Se debe considerar asimismo la posibilidad de que los dos servidores de la empresa no se encuentran en la misma habitación física, ya que ante una emergencia, ambos equipos quedarían inutilizados. Podría ser útil que alguno de los dos servidores, cuyas características son idénticas, se ubique en otra habitación o en otro edificio de la empresa.

2.5 Seguridad de las estaciones de trabajo de los usuarios

Utilización : Usuarios en general y Departamento de Soporte Técnico
Descripción : Normas generales de seguridad de los PC de usuarios

Aún cuando los equipos PC´s de usuarios están fuera del espacio del Centro de Cómputos, estos deben ser atendidos por el personal del Departamento de Soporte Técnico, quienes velaran por que los usuarios usen sus equipos cumpliendo con las siguientes normas:

- Leer detalladamente los mensajes de los antivirus. Periódicamente se deben instalar las últimas versiones en los computadores de los usuarios.

- Grabar los datos en el disco duro (C:, D:, etc). Los diskettes y CDs son medios secundarios de mantenimiento de información y se deben utilizar para el traslado de la información y para almacenar copias de la misma. Pero no se ha de grabar la copia única de un trabajo en un diskette o CD. Si necesariamente se trabaja en un diskette, debe mantenerse un backup del archivo en el disco duro.

- Guardar todos los archivos del usuario en directorios específicos. Nunca se debe grabar, por ejemplo, un trabajo dentro de directorios de programas como EXCEL, WORD o cualquier otra aplicación. Este aspecto apunta a evitar problemas de migraciones de datos, fallas en el disco duro, problemas de configuración o compresión de datos, renovación de aplicaciones, etc. Además, se acelera la forma de trabajo y mejora la organización de los archivos.

- Grabar el trabajo que se hace luego de cualquier avance, o cada 10 minutos. Muchas aplicaciones hacen esta operación de manera automática, mas, es mejor realizarla uno mismo. Así se protege de cortes de luz, olvidos o una detención excepcional del sistema.

- Solicitar el cambio de los passwords cada periodo prudente, ya sean del computador o del acceso a los sistemas de red. Una alternativa viable puede ser el cambio automático de password cada cierto tiempo. Debe evitarse, también, que otros usuarios los conozcan. Todo acceso a los sistemas de red debe quedar registrado, así como el tipo de operación que realice el usuario, por lo cual debe evitarse el "préstamo" de passwords.

- Terminar cada sesión de red con los procedimientos establecidos y no apagando el computador simplemente, o dejando de cumplir algún paso. La mayoría de retardos del sistema son causados por los mismos usuarios, ocupando sesiones ociosas.

- Encargarse de la limpieza externa del monitor y el teclado. Se debe tener extremo cuidado con los teclados, y evitar que adentro caigan líquidos, polvo, migajas o cualquier otro objeto.

- Periódicamente se deben dictar cursos de capacitación en el uso de sistemas operativos y del software de uso personal, en los cuales se instruya además sobre la forma y materiales que deben utilizarse para realizar un mantenimiento básico.

- Cubrir al final de cada día los monitores, teclados e impresoras con cobertores plásticos; de no tenerlos, la Unidad TIC debe procurar adquirirlos y tenerlos disponibles en almacén.

- No realizar conexiones o traslado de computadores sin contar con la ayuda de un funcionario de la Unidad TIC.

- Registrar todo error detalladamente en las bitácoras de área proporcionadas por la Unidad TIC. Estos registros serán de gran ayuda para resolver cualquier problema del computador o sus periféricos.

- Proteger los computadores del polvo, humedad y humo del cigarrillo.

- Utilizar únicamente el software de usuario aprobado por la institución, no cargar en los equipos software no autorizado, esto es fuente de problemas por ingreso de virus o por licencias de uso.

Deberán existir **estándares de configuración** de los puestos de trabajo. En base al estándar se deberá generar un **procedimiento** donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario.

3. SEGURIDAD DE LOS DATOS Y EN LOS ACCESOS A LOS DATOS

3.1 Seguridad en la organización de programas y datos

Utilización: Unidad TIC
Descripción: Normas generales de organización y protección de datos y programas.

Los datos de la Institución son el bien más valioso que recae en custodia de la Unidad TIC, por lo que la tarea más importante es velar por su seguridad y disponibilidad. En tal sentido, se definen las siguientes normas de protección de datos y programas:

- La información contenida en los equipos debe contar con reglas de seguridad que permitan el acceso a los usuarios autorizados únicamente, y no a personal de otras áreas, aún de la propia Unidad TIC. En lo posible, los supervisores de las áreas que utilicen la información deben ser quienes otorguen y cancelen accesos. Los passwords de administración de los equipos deben estar únicamente en poder del Administrador del Sistema del Departamento de Soporte Técnico. Los passwords de los equipos de los usuarios deben estar en poder de ellos mismos. La administración del Departamento de Soporte Técnico debe tener acceso a claves de administración de estos equipos, de manera que puedan garantizar el acceso de funcionarios superiores, sin dañar la información del usuario propietario del equipo.

- Se debe almacenar la información que es reportada por otras instituciones a la entidad, en un lugar seguro y fuera del alcance de cualquier persona. Toda entrega de información se registra; sólo se entregan copias de información a los usuarios autorizados, bajo plena responsabilidad del Administrador de Datos.

- Debe estar en vigencia y en absoluto cumplimiento el ciclo de copias de respaldo sugerido en el presente Manual de Seguridad y Contingencias. Todos los esquemas de respaldo de datos deben estar detallados en las bitácoras (Logs) de Operación.

- Los analistas y programadores de la Unidad TIC no deben tener acceso a los datos ni a las bibliotecas de programas que se utilizan para producción. Los operadores no pueden efectuar cambios a los programas o datos.

- Los sistemas de información deben ser desarrollados siguiendo estándares y una metodología definida y aprobada por la Entidad, los estándares deben cubrir todos los aspectos del análisis, diseño, desarrollo e implantación, de modo de garantizar que los mismos sean fáciles de mantener y actualizar aún cuando los autores de éstos no estén disponibles para realizar los cambios en los sistemas. Asimismo, todo mantenimiento de un sistema debe actualizar la documentación de diseño y desarrollo.

- Todo sistema que se ponga en producción, deberá contar con los manuales correspondientes: Manual de usuario, Manual de operaciones, digramas del flujo de información y procesos, y los manuales de administración, respaldo y recuperación; en todos los casos se deberán incluir instrucciones claras para resolver problemas y errores normales de operación de los sistemas.

- El procedimiento de puesta en producción de un sistema debe garantizar que los datos serán accesados únicamente por los programas ejecutables en producción. Asimismo, debe garantizar que los programas que están en producción no serán alterados. Debe guardarse una copia de todos los programas y componentes a partir de los cuales se han generado los programas que están en producción.

3.2 Seguridad de los datos

Utilización: Departamento de Operaciones
Descripción: Normas generales de seguridad de los datos

Es norma de la Institución mantener la información segura ante cualquier eventualidad. Seguidamente se listan algunos puntos importantes que hay que tener en cuenta para proteger la información.

- Toda la información recibida debe ser revisada antes de ser procesada y almacenada. Los medios magnéticos que la contengan deben estar sin fallas físicas, lógicas o virus. Los procedimientos de entrega y recepción de datos deben estar definidos entre todas las áreas. Se deben proteger los medios magnéticos de cualquier riesgo de sufrir daños físicos. La información no debe ser modificada bajo ninguna circunstancia.

- Si, por ejemplo un archivo llega con virus desde una entidad externa, éste no debe ser removido, se debe imprimir el tipo de virus encontrado y devolverlo a la entidad que envió el archivo.

- No puede añadirse ni eliminarse ninguna información en los medios de la fuente (diskettes u otros), sea un dato o un archivo. Por esta razón es obligatorio tener la información guardada en el Archivo Magnético y proporcionar cualquier información en copia, jamás en original.

- Deben habilitarse todos los procedimientos de control y verificación automáticos de los sistemas, para evitar fallas físicas y lógicas. Los backups realizados deben ser chequeados antes de almacenarse. La información irrelevante debe enviarse a los depósitos de la Institución. Deben hacerse controles de consistencia de la información según los procedimientos definidos para cada sistema.

- Toda información recibida de entidades externas debe ser almacenada en copias de respaldo tal como se recibe de la entidad.

- En todos los **equipos** de la empresa debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización.

- La **actualización** de los antivirus de todos los equipos de la empresa deberá realizarse a través de un procedimiento formal y si es posible, automático, a cargo de un empleado del centro de cómputos designado por el administrador.

- Deberá existir un **procedimiento formal** a seguir en caso que se detecte un virus en algún equipo del sistema.

3.3 Seguridad en el acceso general a los datos

Utilización: Unidad TIC y usuarios
Descripción: Normas generales de acceso a la información.

Las normas de seguridad para el acceso a la información vienen regidas por passwords. Es obligatorio mantener a los usuarios informados acerca del uso correcto de los passwords. Debe, generalmente, instruírseles acerca de:

- Evitar préstamos de passwords o darlos a conocer a otras personas.
- Cambiarlos dentro del período de uno o dos meses de vigencia.
- No se deben utilizar palabras fácilmente detectables como passwords, tampoco se debe usar un password único para todos los accesos de un mismo usuario.
- Los passwords deben tener un largo mínimo de 8 caracteres, los cuales deben incluir símbolos especiales, letras y números.
- El usuario debe solicitar la cancelación de su password en caso de no necesitarlo más.

Los sistemas desarrollados dentro de la entidad deben tener su propio sistema de claves de acceso, adicionalmente a los passwords de acceso a la red o servidor. Deben ser exhaustivamente probados para evitar fallas. Este es otro nivel de seguridad en la información que proveerá el Sistema.

Adicionalmente, se debe asignar passwords con permisos específicos a los objetos de la base de datos y directorios de la red.

Los accesos a la información por parte de usuarios externos vía intranet e internet deben ser controlados por equipo y software especializado del tipo "firewall".

La información que fluye entre la Entidad y entidades externas, debe incluir mecanismos de seguridad que garanticen que ésta no sea modificada. Uno de los mecanismos más efectivos es emplear técnicas de cifrado y decifrado con clave de emisor y receptor, así se garantiza que la información llegue tal como se la envía y que le llegue a quien corresponde.

Se debe capacitar períodicamente a los usuarios en los apectos de seguridad de acceso y uso de passwords.

3.4 Seguridad en el acceso a los datos por los usuarios

Utilización: Unidad TIC, usuarios en general
Descripción: Normas generales de acceso a la información por los usuarios de la Institución.

Los passwords y claves de los sistemas multiusuarios deben definirse en un esquema que permita al administrador cambiarlos únicamente cuando el usuario lo solicite y en forma rutinaria al menos cada uno o dos meses. Así se logrará que solamente el usuario conozca su password, y sepa si es que no ha sido cambiado. Si lo fue, debe informarlo a sus superiores. Además, los passwords de todos los usuarios de la Institución deberán estar registrados en la Unidad TIC, empleando mecanismos de seguridad que eviten que alguien más conozca estos. Para lo cual llenarán un registro en un sobre cerrado y lo entregarán al jefe de la Unidad TIC.

Esta medida debe ser implementada con el objeto de que exista un control centralizado de los passwords y para que, ante la ausencia de alguno de los funcionarios, se pueda accesar a las estaciones de trabajo en caso de emergencia.

Los accesos a los sistemas se otorgan y cancelan con la presentación de un volante interno del Supervisor de área encargado de la información. Debe exigirse a los supervisores que soliciten la cancelación de todas las cuentas de un usuario cuando éste abandona la Institución. En el Log de Operación debe haber un registro de todas las autorizaciones de acceso para cada usuario firmado por el Administrador de Datos.

Las entregas de información se realizan de manera personal, contra la firma de un comprobante de entrega. Cuando el acceso es por medios informáticos, cada sistema debe realizar un registro de los ingresos y de la información consultada. Mensualmente se entregará a los supervisores un listado de toda la información consultada. No hay distinciones en el tipo de información consultada, por ejemplo, si fuera en papel o por pantalla, por un instante o por el terminal de otro usuario. Toda información entregada debe ser registrada.

El sistema operativo, por su parte, debe registrar los accesos e intentos de violación de claves.

3.5 Seguridad en el acceso a los datos por el personal de la Unidad TIC

Utilización: Unidad TIC
Descripción: Acceso a los datos por la Unidad TIC, Servidores de Datos y Archivo Magnético.

El personal de informática, que por lo general tiene control sobre los servidores de datos, debe respetar las siguientes normas básicas de acceso a la información:

- El Administrador de la base de datos es responsable absoluto de la información contenida en los sistemas. Es su obligación, crear una estructura de accesos a la información de producción. También es su obligación proveer lotes de información aleatoria en áreas de prueba y los esquemas de seguridad requeridos por ellos.

- El personal del Departamento de Desarrollo de Sistemas no debe tener acceso a los sistemas en producción ni a sus datos. El personal de los Departamentos de Soporte Técnico y Operaciones, no deben tener acceso a las áreas de desarrollo de proyectos, exceptuando al responsable de la Administración de la Base de Datos.

- El Administrador de la base de datos es el único responsable de actualizar las reglas de integridad y excepciones a estas, usuarios, permisos, logins y paswwords, para el acceso de los usuarios a las bases de datos. Es también el único responsable de actualizar las estructura de las bases de datos.

4. RESPALDO Y RECUPERACIÓN

4.1 Procedimiento de respaldo y recuperación

Utilización: Departamento de Soporte Técnico
Descripción: Normas generales de Respaldo y Recuperación de la información.

4.1.1 Respaldo

El respaldo debe garantizar que los procesos continuarán a partir de la recuperación de información y software desde una copia de respaldo. Los procedimientos de respaldo deben estar detallados con claridad para cada sistema, proceso o función en la entidad. Los respaldos deben ser operaciones contínuas y regulares y también pueden ser operaciones especiales o excepecionales, todas deben llevarse a cabo con exactitud para asegurar una buena estrategia de respaldo y recuperación de datos.

La **periodicidad** de la generación de los resguardos debe ser acorde a la criticidad de la información y la frecuencia de cambios.

La información restaurada desde una copia de respaldo debe siempre dar como resultado el estado de los datos al último respaldo. Para ello es necesario verificar el estado de las cintas o medios de respaldo y reemplazarlas apenas sufrieran un error físico o cuando las especificaciones de uso recomendadas por el fabricante lo señalen.

4.1.2 Recuperación

La fuente principal de recuperación la constituyen las copias de respaldo o backups almacenados para proteger la información. Adicionalmente, se cuenta con otras fuentes, entre las que podemos contar con los Logs de transacciones, caso común en los sistemas de bases de datos relacionales como Oracle, SQL Server, Informix, etcétera. Este procedimiento es aplicable a sistemas de alto grado de actualización diaria, en los que el conocimiento de los últimos datos es crítico.

Deberá existir un **procedimiento de recuperación** de copias de respaldo, donde se incluya la metodología a seguir y el responsable de la realización. Deberán realizarse **chequeos** para comprobar que los procedimientos de restauración son eficientes.

4.1.3 Procedimientos periódicos de backup

Los archivos de datos y el software deben ser resguardados en backups en forma periódica. El período en el que se programa el backup puede diferir según el programa de aplicación o sistema. Por ejemplo, ciertos sistemas de aplicación que corren en forma mensual, en los que se actualizan archivos maestros o de transacciones, requerirán que se programe el backup luego de la corrida mensual en producción. Sin embargo, el software de sistemas o de aplicación que se actualiza frecuentemente, puede requerir backups semanales o diarios. A menudo los sistemas on-line/en tiempo real, que procesan un gran volumen de transacciones, exigen backups cada noche o de inmediato o la utilización de espejado (imágenes especulares o "mirroring") de las actualizaciones a los archivos maestros en una instalación de procesamiento separada.

La programación periódica de los backups puede hacerse por medio de un sistema de administración automatizada de cintas o medios de respaldo y software de "job-scheduling" automatizado. La automatización del procedimiento de backup evitará ciclos erróneos u omitidos debido a errores del operador.

Un procedimiento de respaldo aplicable para entidades que no pueden parar sus operaciones por más de algunos segundos, e incluso en aquellas que no pueden parar ante una catástrofe, es contar con instalaciones de respaldo, las que por lo general son una réplica actualizada (en menor escala) del centro de proceso habitual. Estas entidades pueden acudir a esta instalación de respaldo cuando es necesario y continuar operando sus servicios de informática.

De la misma manera, debe mantenerse toda la documentación que se necesite para una operación continua y exitosa, en la instalación de respaldo en sede alternativa. Ello incluye los documentos fuente que se necesitan para la restauración de la base de datos de producción. De la misma manera que con los archivos de datos, las copias en las sedes alternas deben mantenerse actualizadas para asegurarse de que sean útiles.

Los procedimientos de backup de uso regular son dos: **Total** e **Incremental o Acumulativo** , el primero es útil para realizar copias de respaldo históricas y para protección de información que es actualizada en períodos regulares de tiempo, por ejemplo una vez al mes. El segundo es útil para protección de información que se actualiza diariamente, generalmente este tipo de procesos actualizan los datos de forma interactiva o "en línea".

Las copias de respaldo deben ser almacenadas en medios físicos (cintas, diskettes, discos compactos, etc) fuera del computador. Al respecto, conviene precisar los siguientes conceptos:

- Volúmen: Es la unidad lógica completa de un archivo de respaldo.
- Medio: Es una unidad física, un diskette, una cinta, un disco compacto, etcétera.
- Multi-volúmen: Es un archivo de respaldo (unidad lógica) que por su tamaño, ocupa más de un medio físico, por ejemplo: 2 cintas, 5 discos compactos, etcétera.

- Medio Multi-respaldo: Es un medio físico en el cual se han almacenado varios archivos de respaldo, esto para aprovechar el espacio del medio con archivos de respaldo que son pequeños.

Las copias de respaldo deben estar almacenadas en medios físicos de uso común y en un formato de backup también de uso común, a fin de garantizar su recuperación en otro centro de computo o equipo si fuere necesario.

4.1.4 Frecuencia de rotación de los medios físicos

Para determinar la frecuencia de rotación y el cronograma de los backups se debe tener en cuenta los siguientes aspectos:

- Debe determinarse la frecuencia del ciclo de backup y período de retención para cada sistema o función y si es necesario para cada archivo de datos dentro de éste.
- La estrategia de backup debe anticipar fallas en cualquier paso del ciclo de procesamiento, los procesos de actualización deben incluir elementos de protección para garantizar que el proceso continue luego de una falla, aplicando copias de respaldo, por ejemplo en otro disco del mismo servidor, copias que deben ser reemplazadas por cada versión resultante de la conclusión de un proceso de actualización.
- Los archivos maestros deben ser "respaldados" en momentos convenientes, como al finalizar un procedimiento de actualización.
- Los archivos de transacciones deben conservarse conciliados con los archivos maestros, de manera que pueda actualizarse una generación previa de un archivo maestro para recrear el archivo maestro actual.
- Los archivos en tiempo real requieren técnicas de backup especiales, tal como la registración de transacciones en un log, la utilización de imágenes previas y/o posteriores a la actualización de registros maestros, identificación de las transacciones con la hora, simulación de comunicación, etc.
- Los sistemas de Administración de Base de datos (DBMS) como los ya mencionados, emplean funciones de backup especializado, generalmente provistas como una función integral del propio DBMS.
- Debe conservarse descripciones de los archivos de los cuales se hace backup; para los sistemas que estén en la base de datos, estas descripciones pueden ser reemplazadas por una versión de los diccionarios de datos.
- Debe conservarse copia de los procedimientos (Querys SQL de creación de estructuras) para re-crear las estructuras de las bases de datos, con todos los elementos definidos para acceso y seguridad.
- Puede ser necesario asegurarse de la licencia para utilizar ciertos utilitarios en una sede alterna y los arreglos deben hacerse con antelación.
- El Backup del software debe incluir tanto las bibliotecas de código fuente como los ejecutables y todas las librerias y componentes del software. Debe incluir mecanismos para guardar los parches a los programas en forma actualizada en todas las sedes de backup.

4.2 Respaldo de la información de usuario

Utilización: Usuarios en general
Descripción: Normas generales de protección de información del usuario común

Los backups de información de usuario contenida en su estación de trabajo, se realizan a solicitud de cada usuario. No hay un máximo de backups que pueda solicitar un usuario, pero es aconsejable eliminar los almacenados de un sólo usuario en cantidades mayores a dos, o antigüedad mayor a seis meses. Solamente se debe almacenar la información relevante.

Para ello el usuario deberá seguir las recomendaciones de usar directorios estándares para almacenar su información.

4.3 Respaldos fuera de la Institución

Utilización: Departamento de Soporte Técnico
Descripción: Normas generales de respaldo de información fuera de la Institución.

La Entidad debe contar con bóvedas especializadas para almacenamiento de información en un local externo a la misma, perferentemente en una institución financiera o de resguardo de valores. Debe existir una copia de la información importante en esta bóveda, idéntica a la que existe dentro de la oficina, que permita:

- Recuperar la información almacenada en backups históricos de los sistemas multiusuario importantes.
- Recuperar programas fuente y ejecutables de los sistemas multiusuario importantes.
- Reconstruir la información del día anterior en conjunción con los backups diarios.

La información almacenada debe estar contenida en un medio magnético y formato comunes, y no en cintas legibles desde pocos equipos. Esto se debe a que esta información está almacenada con el propósito de salvar la información en caso de cualquier catástrofe en el centro de cómputos. Puede además, existir una gaveta portátil en el Centro de cómputos, que debe ser salvada con celeridad en caso de alguna emergencia. Entre ambos se logra respaldar y recuperar la información anterior.

La información de respaldo se debe recopilar según el detalle del Log de Operación. Se pasa una comunicación interna al jefe de la Dirección de Informática y al Administrador de la Institución detallando el contenido. También se almacena un detalle en el Log de cada Sistema. El transporte de las cintas debe ser obligatoriamente por una persona de Administración y una de la Unidad TIC, que tengan las autorizaciones respectivas. Puede ser aconsejable, en ciertas ocasiones, solicitar la compañía de un guardia de seguridad.

4.4 Archivo Magnético

Utilización: Departamento de Soporte Técnico
Descripción: Normas generales de servicio del Archivo Magnético.

El Archivo Magnético es una sala especialmente acondicionada para el almacenamiento de documentación en papeles y medios magnéticos. En el Archivo Magnético se almacenan:

- Información de respaldo
- Software desarrollado en la Entidad o adquirido de terceros
- Software de marca (Sistemas operativos, base de datos, utilitarios, aplicaciones, etc.)
- Manuales
- Varios, incluyendo materiales

El archivo debe contar con un encargado de su organización y acceso, quien es absolutamente responsable de mantener en buen estado la información archivada. Debe ser la única persona que tiene acceso, a excepción de la Administración que podrá contar con una llave.

El responsable es el encargado de llevar los registros de:

- Existencia de software
- Existencia de información
- Préstamos/devoluciones de información
- Manuales

Cada mes se debe identificar aquello que debe ser enviado a los depósitos de la Institución, siguiendo los procedimientos de envío exigidos por Administración; al mismo tiempo enviando una comunicación interna al Jefe de la Unidad TIC.

4.5 Gavetas de Información Especial

Utilización: Departamento de Soporte Técnico
Descripción: Contenido de las Gavetas de Información Especial.

El Centro de cómputos debe contar con dos Gavetas de Información Especial.

Una de las gavetas debe ser portátil, de tal manera que en caso de emergencia se pueda trasladar con prontitud fuera de la Institución, debe contener:

- Ultimos backups de datos y software de los sistemas en producción
- Passwords de todos los equipos servidores y PC´s de la institución, incluidos los de la Unidad TIC.
- Passwords de Administración de los Sistemas Multiusuarios.
- Licencias de Software.

Los guardias de seguridad deben conocer el procedimiento de evacuación de la gaveta portátil del Centro de cómputos.

La otra gaveta debe estar empotrada, de ser posible, y bajo llave, pues es la que almacenará principalmente los paswords y licencias de software, por razones de mayor seguridad. La llave debe estar en poder del responsable del Centro de cómputos y del Jefe de la Unidad TIC.

Debe nombrarse entre los operadores, un responsable de cada una de las gavetas, quien estará encargado de conservar la información necesaria dentro de cada una.

5. SOFTWARE DE MARCA Y DESARROLLADO

Utilización: Unidad TIC, Departamento de Desarrollo de Sistemas
Descripción: Normas para la implantación de software, propio y adquirido

Todo el software en uso en la Institución debe ser oficialmente desarrollado o comprado, deben eliminarse las copias "piratas" de software en uso. Toda instalación de software debe contar con la licencia respectiva.

Todo software desarrollado por la Institución deberá respetar los estándares de diseño, desarrollo y documentación, establecidos por la entidad.

La recepción de Software se realizará inmediatamente después de haber sido probado. El encargado del Departamento de Soporte Técnico debe darlos de alta en sus registros. Los operadores deben encargarse de hacer una copia de seguridad del Software y guardar una copia en las gavetas del centro de cómputos.

Cada paquete de software en las gavetas del centro de cómputos debe tener una tarjeta de identificación visible, de modo de hacer más rápida su ubicación. En caso de que el Software se preste, debe guardarse la tarjeta anotando en ella el nombre del prestatario.

Los paquetes de Software deben probarse inmediatamente después de su recepción. Únicamente en caso de ser inservibles o estar dañados para el propósito con que se compraron, se hará un rechazo, con una comunicación interna al Jefe de la Unidad TIC.

Todo software que se ponga en producción debe ser transferido formalmente del área de desarrollo al área de producción, incluyendo las copias de respaldo realizadas en el momento de entrega. El analista responsable del desarrollo debe quedar sin acceso a los fuentes, ejecutables y librerías del sistema entregado.

Para ponerlos en funcionamiento se aconseja únicamente organizarlos en los directorios estandarizados para la institución. No se dicta ninguna norma para esto, pero se aconseja uniformar todos los equipos. Por ejemplo:

Aplicaciones WIN : directorio/msoffice
Archivos de datos WIN : directorio/archivos/excel
/archivos/Word
/archivos/otros

Aplicaciones UNIX	:	directorio/usr
Desarrollos UNIX	:	directorio/users/usrdes
Datos usuarios	:	directorio/users/usrcom

El mantenimiento de software comprado debe hacerse por la empresa proveedora en caso de contar con contrato. El mantenimiento de programas desarrollados e implementados se realizará por el personal de Desarrollo asignado para el mantenimiento de sistemas.

Todo Software será dado de baja en decisión conjunta con el Jefe de la Unidad TIC y los interesados en él. Para darlo de baja se debe enviar una comunicación interna dirigida al Jefe de la Unidad TIC. El software debe ser enviado al depósito de la Institución.

Se dará de baja un software por los siguientes motivos:

- No utilización actual y futura
- Reemplazo por una nueva versión
- Desactualización de soporte por el proveedor

6. SEGURIDAD EN LOS EQUIPOS DE HARDWARE Y LA RED

6.1 Seguridad del hardware

Utilización: Unidad TIC
Descripción: Organización y cuidado del hardware de toda la Institución.

Se describen a continuación un conjunto de normas en favor de la protección de hardware. Este punto es muy importante, pues si bien el centro de cómputos debe contar con un servicio de mantenimiento permanente para cada uno de los equipo servidores y de comunicaciones, y para el resto de equipos de la Institución con un servicio correctivo, es problemático en extremo suspender el servicio informático para reparar equipos en horas de trabajo. Con este conjunto de normas de protección, se minimizará la posibilidad de faltas y aumentará el grado de disponibilidad del servicio.

- Todos los equipos de la Institución deben contar con servicio de mantenimiento. Para los equipos principales como servidores se debe establecer un contrato de mantenimiento preventivo y correctivo permanente, en cambio para los equipos de usuario podría ser suficiente con un contrato de mantenimiento correctivo por llamada.

- Los equipos de hardware del Centro de cómputos y del resto de la Institución se deben ubicar en sitios que ofrezcan la mayor protección posible a los rayos de sol, humedad, polvo, interferencia magnética, cambios térmicos y vibraciones. Deben protegerse sus conexiones y cableado, separando al máximo los grupos de líneas eléctricas de las líneas de comunicaciones y datos. Deben evitarse tensiones en los cables. No pueden haber líneas de datos defectuosas, ni conectores en peligro de fallar en alguna situación; de lo contrario, debe acudirse al servicio de mantenimiento. Toda conexión debe realizarse de acuerdo a las especificaciones técnicas del equipo. Deben protegerse los accesos a los interruptores de encendido para evitar apagados accidentales. Los usuarios no deben tener acceso a las consolas de equipos ni deben prestarse los equipos del centro de cómputo. La temperatura del centro de cómputo debe ser aproximadamente 24°C (75°F), evitando cambios violentos de temperatura, pues se corre riesgo de daños con los equipos instalados.

- Deben protegerse los equipos con cobertores plásticos cuando estén apagados.

- El horario de disponibilidad de los equipos servidores de datos es el de trabajo efectivo en la Institución que no necesariamente coincide con la jornada oficial laboral del personal de la entidad. El resto del tiempo se puede disponer de los equipos para tareas de mantenimiento y reparación. Debe lograrse la mayor disponibilidad del servicio de los equipos, evitando hacer reparaciones en horarios de trabajo del personal usuario.

- Generalmente los equipos servidores están diseñados para funcionamiento contínuo. Si no es este el caso, pueden dejarse encendidos los equipos servidores de datos, en la noche, los fines de semana y feriados a solicitud de los usuarios, considerando que no haya tareas administrativas o de mantenimiento.

- Deben apagarse los monitores de los equipos que están en funcionamiento en horarios no laborales, para evitar que se queme la pantalla en exposiciones estáticas continuas, dejándose firme una nota sobre el teclado advirtiendo que el equipo está encendido.

- En caso de emergencias relacionadas con la alimentación eléctrica o situaciones de riesgo se deben apagar los equipos sin previo aviso. No será así cuando el margen de tiempo para desconectar los equipos ofrece la oportunidad de informar a los supervisores de área. Ellos deben estar al tanto del estado general de los sistemas todo el tiempo.

- Fuera del horario de servicio y cuando los equipos no vayan a ser utilizados por un tiempo considerable, deben apagarse todos los equipos, si es posible desde el UPS mismo o un interruptor especialmente instalado para tal efecto, para evitar mover cables en equipos que no cuentan con interruptores de apagado.

- El personal del Area de Administración debe designar un encargado de verificar los equipos encendidos y que permanecen por largo tiempo sin utilización por ningún usuario. Estos equipos deben ser apagados por el operador de turno u otra persona designada.

- Ante cualquier falla debe llamarse al servicio técnico. Si el equipo pertenece al centro de cómputos, debe anotarse la falla y la solución en el Log del Sistema. Si el equipo es de un usuario del resto de la Institución, se registra la falla y la solución del servicio técnico en la bitácora de cada equipo.

6.2 Seguridad de la red

Utilización: Departamento de Soporte Técnico
Descripción: Organización y cuidado de los componentes de la red

Adicionalmente a las medidas de protección del hardware de la institución, se recomienda incorporar las siguientes para los componentes de la red.

- Los cables de comunicación deben ser tendidos aplicando la técnica de cableado estructurado de categoría 5 o superior.

- Los equipos de comunicación instalados fuera del Centro de cómputo, deben estar debidamente protegidos en cajas o compartimentos que sean accesibles únicamente por el personal del Departamento de Soporte Técnico.

- Debe instalarse una red redundante mínima que cubra servicios a los usuarios cuya función con los sistemas es crítica para la Institución.

6.3 Seguridad de las comunicaciones

Utilización: Departamento de Soporte Técnico
Descripción: Confidencialidad de los datos transmitidos.

Es necesario asegurar la **integridad, exactitud, disponibilidad y confidencialidad** de los datos transmitidos, ya sea a través de los dispositivos de hardware, de los protocolos de transmisión, o de los controles de aplicativos. Para ello se sugieren las siguientes medidas:

- Deberá existir **documentación** detallada sobre los diagramas topológicos de las redes, tipos de vínculos y ubicación de nodos.

- Deberán existir **medios alternativos de transmisión** en caso de que alguna contingencia afecte al medio primario de comunicación.

- Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un **firewall** prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.

- El firewall de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los **protocolos y servicios**, habilitando únicamente los necesarios.

- La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una **autorización de la Gerencia**. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior.

6.4 Equipo de protección eléctrica

Utilización: Departamento de Soporte Técnico
Descripción: Protección del hardware con equipo eléctrico.

Para la protección eléctrica de todos los equipos en general se recomiendan las siguientes medidas:

- Instalación de UPS, con regulador de voltaje y con baterías de por lo menos 45 minutos de funcionamiento ininterrumpido para todos los servidores de datos, unidad de Cinta, impresoras principales y algunas estaciones de trabajo, se recomienda en este aspecto que no más del 20% de los equipos periféricos deben estar conectados al UPS (su potencia se debe calcular sobre estos parámetros).

- La red eléctrica debe estar polarizada con conexión a tierra y de acuerdo a las normas de conexión del fabricante.

- La electricidad de todo el equipamiento debe de estar aislada de las conexiones eléctricas del edificio (luces, equipos adicionales, etc.). Para este caso también deberá instalarse un transformador directo de la corriente externa hacia las conexiones de los equipos de computación.

- Con el objeto de la protección ante caídas prolongadas en el suministro de energía eléctrica, se puede contar con una planta eléctrica y un tablero de transmisión automática que transfiera el control del UPS hacia la planta eléctrica.

- Debe instalarse equipos de protección de rayos para evitar el ingreso de descargas a la red de los equipos.

7. PRINCIPALES PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DEL MANUAL

Ante cualquier contingencia, el presente Manual recomienda el uso conjunto de tres elementos complementarios:

- Herramientas de recuperación
- Acciones periódicas
- Acciones continuas

Cada uno de estos se describe en detalle más adelante. Brevemente, podemos citar sus funciones.

a) Las Herramientas de recuperación son un conjunto de elementos físicos que pudieran auxiliar en la solución de cualquier problema.

b) Para prevenir, además una posible falla, definimos un conjunto de Acciones periódicas de prevención masiva.

c) Para complementar el grado de satisfacción en la solución, las acciones continuas maximizan la probabilidad de solución total.

7.1 Situaciones previsibles

Ante las situaciones previsibles, el plan presente centra su objetivo en la preservación de los datos y los elementos que hacen posible su existencia y conservación. Citamos, así:

- Destrucción de los datos (causada ya sea por un error desde la operación/transcripción, hasta por una catástrofe).
- Destrucción de programas (fuentes, y ejecutables).
- Fallas de Hardware/Eléctricas/Mecánicas/Comunicacionales.
- Otros (personas ausentes/fallas del sistema/etc.).

7.2 Herramientas de recuperación

Este grupo de herramientas debe estar disponible el 100% del tiempo, para lo cual se describe su ubicación física.

Documentación:

- Log de Sistema y de Operación (Bitácoras en uso): Centro de cómputos
- Manuales de Operación: Centro de cómputos
- Documentación de cada sistema: Archivo Magnético
- Manuales de software original: Archivo Magnético
- Diccionarios de datos: Centro de cómputos
- Mapas de cableado: Centro de cómputos
- Logs de Operación con información de backups: Centro de cómputos

Hardware/ software de apoyo:

- Computadores/PCs: Archivo magnético
- Tarjetas PC, otros componentes de varios tipos: Almacén
- Periféricos: Archivo magnético
- Material auxiliar: Centro de cómputos
- Medios auxiliares (Cintas) de arranque del sistema: Centro de cómputos
- Herramientas: Centro de cómputos
- Bipers: Con el personal de informática

Archivos de respaldo

- Copias de respaldo de datos y programas: Archivo magnético, archivo remoto

7.3 Acciones periódicas

Las acciones períodicas que la Institución debe realizar para garantizar la seguridad y prever eventos de contingencia, incluyen las siguientes:

- Archivar en bóvedas externas a la Entidad una copia de un backup histórico de datos, para cada sistema o función.
- Revisar y actualizar los contratos de mantenimiento y seguros.
- Capacitar al personal en los temas relacionados con el buen uso de los recursos informáticos y su seguridad.
- Verificar y probar los distintos procedimientos del Plan de Contingencia.

7.4 Acciones contínuas

Las acciones contínuas, que están orientadas a la seguridad y la recuperación inmediata ante un evento de contingencia, y que deben ser realizadas extríctamente por la Institución incluyen las siguientes:

- Realizar los procedimientos de respaldo de información en todos los sistemas o funciones, de acuerdo a la metodología definida para cada caso y siguiendo el manual de operaciones del sistema.
- Realizar los respaldos de archivos de los proyectos de desarrollo de sistemas de acuerdo a la metodología de respaldo incremental.
- Llevar un registro en el Log de operaciones, de todos los procesos de respaldo realizados.
- Verificar toda copia de respaldo con las herramientas propias del software de respaldo empleada, antes de ser almacenada.
- Realizar backups mensuales o a solicitud, de los datos de los sistemas en PC, bajo responsabilidad del usuario.
- Realizar un backup trimestral de programas fuentes y ejecutables y guardarlos directamente en las bóvedas externas de la Entidad.
- Realizar un backup de programas fuentes y ejecutables cada vez que se instale una versión nueva del sistema o aplicación.

7.5 Procedimientos de seguridad

A continuación se presentan un conjunto de propuestas de seguridad a ser evaluadas según su funcionalidad. Todas apuntan a la seguridad en general, protección de los datos y previsión de contingencias.

7.5.1 Para la seguridad del centro de cómputos

El centro de cómputos debe estar mantenido bajo llave durante todo el tiempo en el que no esté ningún funcionario. No pueden quedarse a cargo personas ajenas a éste ni a la Institución. Las llaves estarán en poder de una sola persona del grupo y se entregará una copia a la Administración. Se sugiere que se instale un sistema de ingreso electrónico, por la flexibilidad que tiene en el cambio de claves, y la velocidad de acceso.

El acceso al centro de cómputos está prohibido a personal de otras áreas. Los usuarios deberán, en lo posible, evitar el ingreso y solicitar cualquier servicio por teléfono. Esta medida apunta a proteger el cableado y el acceso del usuario a cualquier equipo o medio contenedor de información. Debe instalarse una puerta que impida el acceso a usuarios que no pertenezcan al área.

Para evitar incendios, el centro de cómputos debe contar con extinguidores dentro de su perímetro. Se deben instalar detectores de humo que, en caso de incendio, accionen sirenas. Con esto se evitarán problemas en horarios fuera de oficina, cuando los equipos deban permanecer encendidos, y causen algún fuego.

Se debe realizar mantenimiento periódico de los equipos de emergencia instalados en el centro de cómputos: ventiladores, luces de emergencia, UPS, líneas de comunicación de emergencia, extinguidores, etc. Todos los servicios de mantenimiento se registrarán en el Log del Sistema.

En caso de emergencia, cuando haya que salir del edificio, se deben evacuar, en orden de importancia los siguientes componentes:

Del Centro de cómputos:

- Gaveta de Cintas con últimos backups de los sistemas.
- Discos del servidor de datos de los principales sistemas.
- Servidores de los Sistemas principales.
- Servidores de Comunicación.
- Registros de Software.
- Equipos Costosos.
- Resto de los equipos.

Para este objeto, se debe tener definida un área dentro del centro de cómputos, que sea de alta accesibilidad, donde se ubique una gaveta con la información más valiosa de la Entidad.

Del Archivo Magnético:

- Cintas, diskettes u otros medios con los sistemas
- Resto de información de la Entidad
- Software desarrollado
- Manuales de los sistemas desarrollados
- Software original
- Manuales de software original

7.5.2 Para la seguridad de los equipos de protección eléctrica

La central eléctrica UPS se desconectará en situaciones de riesgo eléctrico y funcionamiento prolongado inútil, como por ejemplo, casos de lavado general de pisos o un feriado prolongado. En estos casos, debe comunicarse la desconexión a los usuarios. Por lo tanto, si el acceso de un usuario a los datos de los sistemas en red implica el encendido del UPS, los servidores de comunicación y los servidores de datos, se debe solicitar autorización del supervisor respectivo.

Los procedimientos detallados de desconexión del UPS deben estar descritos en el Log de Operación. Es obligación de todo el personal de la Unidad TIC el conocerlos.

Debe chequearse continuamente el estado de la línea eléctrica y el cable de tierra, para evitar problemas eléctricos.

Es necesario que el centro de cómputos tenga una unidad UPS propia, para evitar depender de otras áreas, en caso de emergencia.

En caso de cortarse el suministro eléctrico, debe desconectarse todo computador, aplicando un esquema de prioridades para apagar cualquier equipo que no sea el que use energía eléctrica para completar un proceso. Siempre debe seguirse el procedimiento normal de apagado de equipos, tomando en cuenta el margen de tiempo que provee el sistema UPS.

7.5.3 Para la seguridad del archivo magnético

El Archivo magnético estará siempre a cargo del área de operaciones. Solamente estas personas debe tener las llaves, deberá existir una copia de emergencia en la Administración general de la Entidad.

Todos los archivos resguardados en el archivo magnético deben estar ordenados en las gavetas destinadas para ello.

7.5.4 Para la seguridad de los equipos servidores

Los equipos servidores de datos generalmente están diseñados para operar por largos periodos de tiempo sin desconectar o apagarse. Sin embargo, es recomendable que en periodos largos de receso (feriados u otros) sean desconectados. En caso de acceso por algún usuario, se dejarán encendidos durantes estos periodos, evitando que el monitor pueda dibujarse por quemazón de la pantalla, apagándolo o quitándole todo el contraste. Aun así, los servidores deben apagarse por lo menos de acuerdo con las recomendaciones del fabricante.

Deben resguardarse todos los equipos contra la humedad, polvo y humo de cigarrillo. Esta prohibido fumar en el centro de cómputos. En la noche, momento en que se realiza la limpieza del alfombrado, se deben proteger los equipos contra el polvo que se levanta en el ambiente utilizando cobertores plásticos.

Los servidores de comunicación, al igual que los otros servidores, se apagarán en periodos de receso prolongados, quedando encendidos en caso de necesidad de algún usuario.

En caso de cualquier emergencia en la que sea necesario apagar los equipos, se lo hará sin previo aviso. No así cuando el apagado de los equipos ofrezca un cierto margen de tiempo para informar a los usuarios y pedir autorización.

El mantenimiento preventivo de equipos servidores debe ser realizado por una empresa especializada una vez cada tres meses. Semestralmente deben abrirse completamente los equipos para revisar su estado general y limpiarlos.

En caso de fallos en cualquier equipo del centro de cómputos, se debe llamar inmediatamente al servicio técnico para que realice su reparación o reemplazo. Todos los equipos en el centro de cómputos deben estar en perfecto funcionamiento. Debe también describirse en el Log del Sistema la solución encontrada.

Todos los equipos del centro de cómputos deben contar con un servicio de mantenimiento externo a la Institución. Los equipos nuevos vienen con un período de garantía, pasado este período, se debe exigir su inclusión inmediata a un contrato de mantenimiento externo.

Durante el tiempo de operación, se debe registrar en el Log del Sistema toda falla eventual que sea difícil de hallar y no perjudique la operación normal, para informarla a los técnicos el día del mantenimiento.

Las normas de apagado y encendido deben estar registradas en los manuales de operación de cada equipo. Estas normas deben ser conocidas por todos los integrantes del Departamento de Soporte Técnico y cumplirse al pie de la letra.

Todo cambio de configuración del sistema operativo o utilitarios principales de cada servidor debe ser registrado en el Log del Sistema. En él también estará registrada la información de configuración de las cintas de backup en cada equipo.

Como se indicó anteriormente, los equipos deben ser protegidos al final de la jornada de trabajo con cobertores plásticos, y mantenidos en funcionamiento a una temperatura aproximada a los 24ºC. En la noche la temperatura debe mantenerse constante, evitando en lo posible el apagado del ventilador y los cambios de temperatura, ya que los chips de alta temperatura de cualquier circuito pueden quebrarse.

Los passwords de los sistemas deben ser cambiados cada tres meses. Deben registrarse en clave (cifrados o encriptados) en el Log del Sistema. Las cuentas de los usuarios retirados deben ser removidas en un plazo máximo de dos meses, pero sus passwords deben cambiarse el día del retiro del funcionario.

Semanalmente se verificarán los archivos de sistema (file systems) de cada servidor y las bases de datos, para comprobar su consistencia. En caso de haber fallas, el administrador del sistema es el responsable de corregirlas. Los Filesystems se deben mantener al 80% de su capacidad y las bases de datos al 90% como máximo. Puede modificarse la prioridad de los procesos elevándola a un grado que no perjudique a los usuarios.

El acceso a los sistemas por parte de los usuarios está sujeto a la presentación de un volante interno firmado por los supervisores de área encargados de los sistemas. La Unidad TIC no debe tener acceso a ninguna información, aspecto que corresponde establecer a los supervisores de área encargados de los sistemas.

Deberá utilizarse al menos una herramienta antivirus en los **servidores**, para así disminuir el riesgo de infección.

Los esquemas de seguridad de los Sistemas y Administradores de Bases de Datos deben definir claramente los accesos que puede lograr un usuario. Aunque esta protección es secundaria, pues la principal protección está implícita en los sistemas desarrollados, no debe olvidarse en ningún caso. No debe existir un usuario que pueda emular el acceso de otro. Los passwords que pudieran permitir este paso deben estar únicamente en poder del administrador.

Las prioridades en el uso de los equipos servidores están definidas en el siguiente orden de importancia:

1. Proceso de datos
2. Consulta de datos
3. Procesos de programación y administración
4. Procesos propios de los sistemas o aplicaciones

Todos los datos se almacenan en backups y se resguardan en el Archivo magnético y bóvedas externas. El acceso a estas localizaciones físicas está restringido al administrador de datos y al Jefe de la Dirección.

7.5.5 Para la seguridad de los equipos PC en general

La limpieza de las PC de las unidades externas al centro de cómputos debe realizarse de la siguiente forma:

- Monitores y CPU: limpieza externa a cargo del usuario.
- Teclados: limpieza externa a cargo del mismo usuario.
- CPU y teclados: limpieza interna a cargo de Unidad TIC. debe realizarse al menos tres veces al año.

Los monitores no reciben limpieza interna por el personal de la entidad, debido a que ésta exige personal especializado.

Los usuarios deben tener cobertores plásticos para cpu, monitor y teclado, que deben usarse cada noche.

Todo trabajo que se realice en una PC, debe almacenarse en directorios fácilmente diferenciables de los de la máquina y aplicaciones propias del sistema operativo y software de oficina. Esta medida apunta a poder recuperar los archivos en caso de cualquier problema y cualquier transferencia de datos, sin que exista la posibilidad de extraviarlos al confundirse con los de alguna aplicación.

Debe prohibirse el traslado de equipos sin contar con la colaboración de un integrante de la Unidad TIC, para evitar daños en el equipo y fallas en la conexión.

Debe instruirse a los usuarios sobre la forma y materiales que deben utilizar para realizar un mantenimiento básico.

Todo equipo con fallas debe llevarse a mantenimiento inmediatamente. En caso de que la falla pueda provocar demoras largas, debe reemplazarse el equipo, y cargarlo con los datos y programas necesarios, del usuario. El sistema de backups debe estar diseñado para lograr una recuperación máxima de los datos de hasta el día anterior, en el peor de los casos.

Se deberán **documentar** no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen. Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados.

En el momento en que un nuevo usuario ingrese a la empresa, se le deberá **notificar y éste deberá aceptar** que tiene prohibida la instalación de cualquier producto de software en los equipos. Se deberán realizar **chequeos periódicos** en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.

7.5.6 Para la seguridad del proceso de datos

El proceso de datos debe ser responsabilidad del área de operaciones, ningún otro usuario ajeno a operaciones debe tener acceso a los menús de proceso. Todo proceso de datos debe ser realizado siguiendo las instrucciones contenidas en el manual de operaciones de cada sistema o aplicación.

Los analistas y programadores no deben tener acceso a los datos de producción. Ellos solamente pueden manejar datos de prueba en bases de datos especialmente diseñadas para tal fin. Tampoco deben tener acceso a la ejecución de procesos reales de producción.

Se debe registrar la salida de toda información hacia los usuarios, con la firma de estos. Toda esta información debe almacenarse en archivos de los cuales se realiza un backup diario.

7.5.7 Para la seguridad de los backups

Los backups de datos de los sistemas se deben proteger en gavetas cerradas. Una copia se mantendrá fuera de la institución, como se indica en Acciones periódicas.

Los backups se realizarán de acuerdo con los esquemas y metodología definidos por la entidad, de esta manera se protegerá todo cambio en los datos y programas.

Toda copia de respaldo o backup debe ser verificada antes de archivarla.

Debe mantenerse documentación adecuada para cada sistema, backups y sus datos. Todo documento debe estar indexado y ubicado en un lugar visible.

7.5.8 Para la seguridad de los procedimientos internos

Si bien no es imprescindible la rotación de tareas en la Unidad TIC, es una buena opción, puesto que se busca que el funcionamiento de los sistemas y procesos de datos no dependan únicamente de una persona. En consecuencia, todo proceso debe ser conocido por todos los integrantes de la Unidad.

Es aconsejable el uso de bipers o celulares para localización del personal de la Unidad TIC. Además estarán al alcance del guardia de turno los teléfonos de éstos y su posible ubicación, así como los de las empresas que prestan mantenimiento a la Entidad.

Deben crearse dos cuadernos o Logs, ambos ubicados en el Centro de cómputos, con el siguiente contenido:

LOG DEL SISTEMA:

- Registro de mantenimiento de hardware y equipo de emergencias, describiendo el problema y soluciones encontradas.

- Registro de fallas eventuales y pequeñas en hardware y software.
- Registro de procesos ejecutados y accesos de usuarios.
- Registro de la configuración de variables de Sistemas Operativos y Aplicaciones principales.
- Registro de la codificación en clave de los passwords.

LOG DE OPERACIONES

- Registro de Backups en la sede principal y fuera de la institución.
- Registro de procedimientos de encendido y apagado de UPS.
- Registro de la procedimientos de evacuación.
- Registro de procedimientos de apagado y encendido de todos los equipos.
- Registro de procedimientos de creación de cuentas de acceso a cada sistema.
- Registro de procedimientos de rotación de personal.
- Registro de la atención de requerimientos a los usuarios.
- Registro de instalación, reemplazo, anulación de software desarrollado y comprado.

7.5.9 Para la seguridad del software: adquirido, desarrollado y su documentación

Todo sistema desarrollado debe entregarse al Departamento de Soporte T'ecnico en diskettes, cintas o discos compactos; rotulados, junto con los respectivos manuales, para que sean registrados, almacenados e instalados.

Los sistemas desarrollados por la Institución deben tener un esquema de seguridad propio más un registro de accesos y operaciones de los usuarios.

El software original comprado y desarrollado, más toda su documentación, debe almacenarse en el Archivo magnético. Todo préstamo debe registrarse en el Centro de cómputos.

Los fuentes del software en desarrollo deben almacenarse en cintas de backup cada día. El acceso a los programas fuentes debe estar permitido únicamente a los programadores.

MANUAL DE SEGURIDAD Y CONTINGENCIAS

PARTE II: PLAN DE CONTINGENCIAS

Toda entidad y en especial las del sistema financiero deben contar con un Plan de Contingencias que permita la continuidad de sus operaciones. Como se visto en el capítulo anterior, existen muchas posibles contingencias relacionadas con el procesamiento de datos que podrían afectar a esta continuidad de operaciones.

Este capítulo, pretende organizar un contenido mínimo de acciones preventivas y correctivas basadas en la guía de referencia brindada en el Capítulo I. Cada entidad deberá decidir cuales de estas acciones pueden y deben ser implementadas en su institución para preservar a salvo y operando su servicio informático

1. CONCEPTOS

Acciones de Emergencia: Referidas a los procedimientos para reaccionar a la crisis, desde los procedimientos de activación de alarmas, hasta las evacuaciones de emergencia.

Notificación: Procedimientos para notificar a los funcionarios en caso de desastre.

Declaración del desastre: Procedimientos para la evaluación del daño que sigue al desastre.

Recuperación de Sistemas: Procedimientos para restaurar los sistemas críticos y vitales a nivel de servicio de emergencia dentro de un marco de tiempo determinado. Incluye la documentación e instrucciones para el procesamiento manual de información, si es necesario.

Recuperación de red: Procedimientos para reactivar las comunicaciones de voz y de datos a niveles de emergencia dentro de un tiempo determinado.

Recuperación de usuarios: Procedimientos para recuperar las funciones de usuarios que sean críticas y vitales dentro de un marco de tiempo determinado.

Operaciones de salvamento: Los procedimientos para salvar las instalaciones, los registros, el hardware, incluyendo la determinación de la viabilidad de ocupar el sitio del desastre y las gestiones para reponer temporalmente el equipamiento.

Reubicación: Los procedimientos para reubicar las operaciones de emergencia (sistema, red y procesamiento de usuarios).

Niveles de desastre: No todas las interrupciones del servicio se clasifican como desastre, por ello, es necesario conceptualizar los diferentes niveles de desastres. Esta conceptualización debe ser dada por la entidad. La siguiente puede ser una definición básica de los diferentes niveles de desastre a considerar dentro del Plan de Contingencias:

- No desastres: La interrupción del servicio que surge de un mal funcionamiento del sistema u otras fallas que exige una acción concreta y posible para recuperar el nivel operativo y reanudar el servicio en muy corto plazo, minutos u horas como máximo.

- Desastres: Interrupciones que provocan que toda la instalación se ponga en situación no operativa por un largo periodo de tiempo, generalmente más de un día. En algunos casos exige recuperar el status operativo por medio de una instalación alternativa.

- Catástrofe: Interrupciones mayores que son producto de la destrucción de la instalación del procesamiento. Se requiere pasar a una instalación alternativa en el corto o largo plazo.

2. ACTIVIDADES

2.1 Organización y asignación de responsabilidades

2.1.1 Definición de equipos de trabajo y responsabilidades

A fin de implementar las estrategias del Plan de Contingencias debe definirse la organización y responsabilidades del personal asignado de la ejecución del Plan y los grupos de trabajo. La siguiente puede ser una estructura básica para la ejecución del Plan Contingencias:

Equipo de acción ante una emergencia
Equipo de primera respuesta. Se los denominan puesto de vigilancia de incendio o "equipo contraincendios" cuya función es enfrentarse a "fuegos" o situaciones de extrema emergencia. Una de sus funciones primarias es la evacuación ordenada del personal y proteger la vida humana. Se recomienda que, como mínimo, una persona dentro de cada área de la Entidad participe dentro de este grupo.

Equipo de evaluación de daños
La función de este equipo es la de evaluar los daños del desastre a posteriori. El equipo debe incluir personas que tengan la capacidad de evaluar el daño y estimar el tiempo que se requerirá para recuperar las operaciones del servicio informático. En este equipo debe incluirse personal calificado para la utilización de equipos de pruebas, con conocimientos de redes y tecnología. Asimismo, este equipo tiene la responsabilidad de identificar las posibles causas del daño o derivar a especialistas técnicos de otro nivel para la evaluación de las causas del daño.

Equipo de administración de la emergencia
La función de este grupo es la de coordinar las actividades de todos los equipos de recuperación y se encarga de las decisiones claves. Determina la activación del Plan de Contingencia. Actúa como supervisor del desastre y se requiere que el mismo coordine las siguientes actividades:

- Recuperar los datos críticos y vitales incluso desde el almacenamiento alternativo.
- Instalar y probar el software de sistemas y aplicaciones en la sede habitual o en la de alternativa.
- Identificar, comprar e instalar el hardware en la sede habitual o alternativa.
- Reconstruir las bases de datos.
- Proveer toda la logística necesaria para continuar operando.
- Operar desde la sede habitual o alternativa.

- Re-direccionar el tráfico de comunicaciones de la red si es necesario.
- Restablecer la red usuario-sistema.
- Transportar a los usuarios a la sede alternativa, si es necesario.
- Coordinar los horarios y utilización de los sistemas por parte de los usuarios y operadores.

Equipo de Sede alternativa de almacenamiento

Responsable de obtener, acondicionar para transporte y enviar los medios magnéticos y los registros a la sede alternativa, así como establecer y supervisar el cronograma de almacenamiento de la información que sea creada durante las operaciones en la sede alternativa.

Equipo de software y aplicaciones

Responsable de restaurar los paquetes de sistemas, carga y prueba del software de sistema operativo y resolver problemas a nivel de sistema. Se traslada a la sede alternativa, si es necesario y restaura los paquetes de usuarios y los programas de aplicaciones en el sistema de back-up. A medida que progresa la recuperación, este equipo puede llegar a tener la responsabilidad de monitorear el rendimiento de las aplicaciones y la integridad de la base de datos.

Equipo de seguridad

Monitorea en forma contínua la seguridad del sistema y los enlaces de comunicaciones; también resuelve los conflictos de seguridad que impiden la recuperación rápida del sistema. Se asegura de la instalación correcta y el funcionamiento del paquete de software de seguridad.

Equipo de operaciones de emergencia

Constituido por los operadores de turno y los supervisores de turno que actuarán en la emeregencia, ya sea en la sede habitual o la alternativa. Administra la operación del sistema durante el desastre y recuperación. Otra responsabilidad puede incluir coordinar la instalación de hardware si no se ha designado como sede alternativa a un “hot-site” o una instalación lista para operar.

Equipo de recuperación de la red y comunicaciones

Responsable de redireccionar el tráfico de comunicaciones de voz y el tráfico de las comunicaciones de datos y restablecer el control de la red, incluyendo acceso a la sede alternativa, si es necesario. Da soporte contínuo para las comunicaciones de datos y supervisa la integridad de las comunicaciones. Se traslada a la sede alternativa donde trabaja para establecer una red de usuarios/sistema. También es responsable de solicitar e instalar el hardware de comunicaciones en la sede alternativa y trabajar con los operadores de centrales telefónicas y proveedores de gateways u otros equipos en el redireccionamiento de servicio local y acceso por estos.

Equipo de transportes

Actúa como un equipo de instalaciones para ubicar la sede alternativa de usuarios, en caso de no haber una predeterminada y es responsable de coordinar el transporte de los empleados de la empresa a dicha sede. También asiste en ponerse en contacto con los empleados para informarles de las nuevas ubicaciones del trabajo y horarios y hacer arreglos para residencia de los empleados.

Equipo de hardware para usuarios
Ubica y coordina la entrega e instalación de terminales de usuarios, impresoras, máquinas de escribir, fotocopiadoras y otro equipo que sea necesario. Ofrece respaldo al equipo de comunicaciones y a cualquier esfuerzo destinado a salvar el hardware e instalaciones.

Equipo de reparación de datos y registros
Actualiza la base de datos de aplicaciones. Supervisa el personal encargado de la carga de datos y ayuda a los esfuerzos destinados a salvar registros, adquirir los documentos primarios y otras fuentes de información de entrada a los sistemas.

Equipo de soporte administrativo
Brinda respaldo administrativo a todos los otros equipos y actúa como centro de mensajes para la sede alternativa de usuarios. Se encarga de la logística durante la emergencia o desastre y la recuperación. Da respaldo a los esfuerzos de los otros equipos, al realizar contactos con los vendedores y coordinar la logística de la provisión continua de insumos necesarios de oficina y computación. Administra el Proyecto de reubicación, para lo cual:

- Realiza una evaluación del daño a las instalaciones y equipo, evaluación más detallada que la realizada por el equipo de .evaluación de daños.
- Provee al Equipo de Administración de Emergencia la información requerida para determinar si la planificación debe ser dirigida a la reconstrucción o reubicación.
- Provee la información necesaria para presentar los reclamos de los seguros (los seguros son la fuente primaria de fondos para los esfuerzos de recuperación).
- Coordina los esfuerzos necesarios para el salvamento de registros (es decir, recuperar documentos, medios electrónicos, etc.).

2.1.2 Organización de los equipos y responsabilidades en la Entidad

Los equipos mínimos recomendados para la entidad debieran tener las responsabilidades y estructura siguientes:

Equipo de vigilancia, evaluación y administración de emergencia
Funciones:
- Administración de la emergencia
- Evaluación de daños
- Coordinacíon de la instalación en la sede alternativa
- Coordinación de transportes
- Coordinación de soporte administrativo

Equipo de recuperación tecnológica

Funciones:
- Recuperación de la red y comunicaciones
- Hardware para usuarios
- Seguridad

Equipo de recuperación de software y aplicaciones
Funciones:
- Restaurar software y aplicaciones

Equipo de operación de emergencia y logística
Funciones:
- Operación de la emergencia
- Acciones ante una emergencia
- Reparación de datos y registros
- Procurar insumos y acciones de salvamento

Los grupos o equipos propuestos debieran incluir al menos la asignación de los siguientes funcionarios:

- Equipo de vigilancia, evaluación y administración de emergencia:
  - Gerente de la Unidad TIC
  - Gerentes de área
  - Administrador general
  - Jefe departamento de Soporte Técnico
- Equipo de recuperación tecnológica
  - Jefe del departamento de Soporte Técnico
  - Administrador del Sistema y redes
  - Administrador de la Base de Datos
  - Responsable de servicio o soporte a usuarios
- Equipo de recuperación de software y aplicaciones
  - Jefe del departamento de Desarrollo de Sistemas
  - Administrador de la Base de Datos
  - Analistas programadores
  - Jefes de los Departamentos usuarios de cada sistema o aplicación
- Equipo de operación de emergencia y logística
  - Jefe del departamento de Operaciones
  - Responsables de producción u operadores
  - Funcionario de administración dedicado a logística
  - Funcionarios usuarios de los sistemas

2.2 Evaluación del riesgo de los sistemas, funciones o procesos en uso

Para que se tenga un control adecuado sobre los impactos que pueden tener las contingencias en la utilización y procesamiento de los sistemas, se debe tener muy en claro la clasificación de riesgos de cada uno de ellos, con el objeto de que se puedan evaluar rápidamente los daños y consecuencias y tomar las medidas adecuadas.

En este contexto, es importante mencionar que un desastre es cualquier suceso que tiene un componente de azar o incertidumbre, que cuando ocurre tiene potencial como para interrumpir el funcionamiento normal de la Entidad. Tales interrupciones a menudo se asocian con desastres naturales como terremotos, inundaciones, tornados, huracanes, incendio, etc., o con situaciones de conmoción civil.

Sin embargo, lo hechos desastrosos pueden ocurrir cuando no se brindan más los servicios esperados por la Entidad, a causa de una falta de energía, pérdida de capacidad de comunicaciones, etc. Aunque la pérdida de tales servicios puede deberse a un desastre natural, también puede deberse a un hecho aislado. Un buen plan de contingencias deberá tener en cuenta todos los tipos de hechos desastrosos.

2.2.1 Metodología de clasificación de riesgos

Para clasificar el grado de tolerancia a interrupciones de cada sistema o aplicación, la Entidad deberá considerar varios aspectos en términos del impacto que causaría a la Institución el no poder operar sus sistemas por un período de tiempo. Principalmente deberá considerar el valor tangible e incluso intagible que representa tener detenido un sistema, tanto al interior de la Institución como para los usuarios externos.

Con estos factores en consideración, se deberá clasificar la importancia de los sistemas y funciones en una de las siguientes categorías:

i) Críticos

Sistemas cuyas funciones no pueden llevarse a cabo, y que reemplazarlas por métodos manuales no ofrece la mismas capacidades y funciones. La tolerancia a la interrupción es muy baja por lo que el costo de la interrupción es muy alto.

ii) Vitales

Sistemas cuyas funciones pueden ser realizadas manualmente pero solamente por un período breve. Existe una tolerancia mayor a la interrupción que con los sistemas críticos y, por ende, costos de interrupción ligeramente menores, siempre y cuando se restauren las funciones dentro de un marco temporal determinado (generalmente 5 días o menos).

iii) Sensibles

Sistemas cuyas funciones pueden realizarse en forma manual, con costos tolerables, por un largo período. Sin embargo, los procesos manuales involucrados son complejos y exigen mano de obra adicional, generalmente bien calificada, para su ejecución.

iv) No críticos

Sistemas cuyas funciones pueden ser interrumpidas durante un lapso largo, con poco o sin costo para la entidad y exigen poco o ningún esfuerzo de "ponerse al día" cuando se restauran.

2.2.2 Clasificación de riesgo en los sistemas, funciones y procesos de la entidad

Tomando en consideración los aspectos señalados en la metodología de evaluación del riesgo, se plantea para la Entidad el siguiente caso de ejemplo:

Dada una contingencia que provoque una interrupción en el sistema de Créditos, se podrá valorar lo que representa para la imágen de la Entidad el hecho de que sus clientes no puedan realizar operaciones y que los analistas y oficiales de negocios no cuenten con esta información al interior de la Institución, y estén sin trabajo por el tiempo que dure la interrupción.

En este escenario una clasificación resultante podría ser:

a. Proceso de atención de las operaciones de clientes en Créditos: CRITICO
b. Proceso de consulta interna de información de Créditos: VITAL

Esto en el entendido que la Entidad ha decidido ofrecer una imágen de servicio de alta eficiencia para el cliente y que los analistas y oficiales de negocios pueden ocuparse de otros asuntos miestras está interrumpido el servicio de consulta interna del sistema de Créditos.

El cuadro a continuación, presenta el ejemplo de resultado de una evaluación de parte de los sistemas, procesos y funciones típicos de una Entidad Financiera.

Procesos, funciones o sistemas críticos

N°	Proceso o aplicación	Código	Estado actual	Clasificación	Periodo Actualiz	Dias Actualiz	Crítico en epoca
	Sistemas operativos						
1	Créditos	Cred	E	C	D	-	Siempre
2	Caja de Ahorro	Caja	E	C	D	-	Siempre
3	Contabilidad	Conta	E	V	D	1/2	Actualización
	Sistema administrativos						
4	Recursos Humanos	RRHH	E	V	D	-	Fin mes
4	Planilla de sueldos	Plan	E	V	D	-	Fin de mes
6	Activo fijo	Act	E	V	D	-	-
7	Inventarios	Inv	E	V	D	-	-
8	Desarrollo de sistemas		E	C	D	-	Diario

Estado actual: E=En explotación, D=En desarrollo, P=En pruebas, X=Rutina diaria.
Clasificación: C=Críticos, V=Vitales, S=Sensibles, N=No críticos.
Periodo actualización: D=Diario, S=Semanal, Q=Qincenal, M=Mensual, T=Trimestral, S=Semestral, A=Anual.
Días de actualización: Días del período en que se actualiza la información.

El ejemplo de clasificación general otorgada a los sistemas de la Entidad, es que todos corresponden a la categoría "V" o vitales, excepto los sistemas de Créditos y Caja de Ahorro, debido a la política de la entidad de ser eficientes en el servicio a los clientes. También se han considerado otros factores, como el tiempo de actualización de la información y la necesidad de los usuarios de contar con esta información.

En general, los sistemas de la Entidad, debieran tener mayor protección y mayores posibilidades de recuperación en las etapas de actualización de información. También es importante que la información histórica de los sistemas esté bien resguardada y que sea fácil hacerla disponible cuando es requerida.

Por otro lado, la prioridad de un sistema sobre otro es también irrelevante, puesto que las necesidades de uso de información para análisis principalmente, cubren al mismo tiempo temas relacionados con varios de los sistemas. Otra vez, en este punto se debe otorgar privilegios a los sistemas que sirven a la entidad para atender de manera eficiente sus políticas.

La clasificación otorgada al proceso de desarrollo de sistemas es de "C" o Crítico, que debe mantenerse mientras se desarrolle un proyecto, puesto que no se deberían admitir demoras en los calendarios de desarrollo e implantación de sistemas.

Esta clasificación que se aplica a todo los sistemas, procesos y funciones que estén automatizados, es la base para que a partir de ella se elaboraren los cuadros de tiempos de proceso e interrupción permitidos y de estrategias de respaldo aplicables. La clasificación no debe ser inmutable puesto que las necesidades de la Institución podrán modificarse con el tiempo y la evolución de sus servicios.

2.3 Evaluación del tiempo crítico de recuperación

El “tiempo crítico de recuperación” es la “ventana” o marco de tiempo en que debe reanudarse el procesamiento de sistemas, antes de arriesgarse a incurrir en problemas serios dentro y fuera de la Entidad.

2.3.1 Determinación del tiempo de recuperación para las aplicaciones

Deben identificarse cuidadosamente las aplicaciones, el software de base y los archivos de datos que han sido definidos como críticos. Esto es, aquellos cuyo uso, consulta y modificación son contínuos y de importancia gravitante para la labor institucional, que tienen una muy baja tolerancia a la interrupción y que en consecuencia deben ser recuperados en primer término. El carácter crítico de las aplicaciones, el software de base y los archivos de datos puede estar en función de la época del mes o del año en la que ocurre el desastre. Debe realizarse un análisis del carácter crítico del tiempo, al identificar las aplicaciones críticas, el software de sistemas o los archivos de datos a recuperar.

Siguiendo el ejemplo planteado, los tiempos de interrupción y recuperación determinados para los sistemas, procesos y funciones críticas en la Entidad podrían ser los siguientes:

Tiempos de proceso, interrupción y recuperación permitidos
(en días calendario)

Nro	Proceso o aplicación	Tiempo del proceso	Tiempo máximo interrupción	Tiempo máximo recuperación
	Sistemas operativos			
1	Créditos			
	Actualización de operaciones	Minutos	1 Hora	1 Hora
	Generación de productos (estados de cartera)	1	1	1
	Puesta en línea para consulta interna	Minutos	1/2 día	1/2 día
	Generación de estados de cierre	2	1	1
2	Caja de Ahorro			
	Actualización de operaciones	Minutos	1 Hora	1 Hora
	Generación de productos (estados de cartera)	1	1	1
	Puesta en línea para consulta interna	Minutos	1/2 día	1/2 día
	Generación de estados de cierre	2	1	1
3	Contabilidad			
	Actualización datos del período	1	5	1
	Generación de productos	1	5	1
	Puesta en línea para consultas	-	5	1
	Sistema administrativos			
4	Recursos Humanos	-	5	1
5	Planilla de sueldos	-	5	1
6	Activo fijo	-	5	1
7	Inventarios	-	5	1
8	Desarrollo de sistemas	-	1	1

Los tiempos máximos de interrupción y recuperación, se plantean para todos los casos ante la eventualidad de una contingencia del tipo "no desastre". Para los casos de desastre o catástrofe, se estima razonable que la interrupción y recuperación no sea mayor a una semana calendario, debido a que luego de ese tiempo la información de las operaciones diarias se hace muy grande en cantidad.

2.3.2 Interrelación entre los usuarios y procesamiento de datos

Es necesario hacer participar al usuario final en la identificación de todas las funciones críticas. La realización de back-ups y el almacenamiento en sedes externas se convierte en una práctica esencial a fin de sobrevivir a un desastre. Las copias de resguardo de archivos y prevención de capacidad de computación para los usuarios finales requerirá el almacenamiento de archivos y servidores de archivos duplicados en la sede alternativa. El equipo de recuperación debe proveer máquinas de microcomputación, conexiones de telecomunicaciones, incluyendo voz, hardware y software de red necesarios para reinstalar la computación crítica para los usuarios finales.

2.3.3 Prioridades de procesamiento

Se debe desarrollar una planilla formalizada de procesamiento para todos los sistemas. Esta planilla debe estar trazada por días del año, a fin de facilitar la recuperación de los sistemas que son críticos en el momento que ocurra un desastre. La identificación de la planilla debe estar detallada hasta el punto de indicar el orden de procesamiento a seguir para ordenar en una cola de procesamiento los trabajos que necesiten procesamiento.

Por lo general, los procesos masivos de los sistemas en la Entidad son de dos tipos: actualización de datos y generación de productos; eventualmente puede existe un tercer tipo de proceso que es el de transferir información vía telecomunicaciones. A efectos de programar las prioridades en los procesos, conviene considerar este último tipo como un proceso de generación de productos. Por otra parte, algunos sistemas requieren de información de otros sistemas para la generación de productos, principalmente productos de validaciones cruzadas o indicadores para análisis de gestión.

Otros factores a tomar en cuenta son: a) Los plazos o periodos de actualización de la información en los sistemas, por lo general los datos de los sistemas operativos se actualizan en cuanto ocurren las operaciones (por ejemplo, minuto a minuto); b) Los volúmenes de información en la actualización son sustancialmente diferentes entre los sistemas; y c) Los procesos regulares, por ejemplo de cierre, hacen que en tanto no se ejecuten, los usuarios finales no pueden contar con esta información, por lo general los usuarios tienen acceso a la información del último cierre.

En atención a estas consideraciones, siguiendo el ejemplo planteado y la clasificación de sistemas o procesos definida, se plantea la siguiente priorización de procesos:

1ro Actualización de datos de los sistemas de Créditos y Caja de Ahorro,
2do Actualización de datos del sistema de Contabilidad,
3ro Actualización de datos de los sistemas administrativos,
4to Generación de productos de los sistemas de Créditos y Caja de Ahorro,
5to Generación de productos de Contabilidad
6to Generación de productos de los sistemas administrativos
7mo Generación de productos con información cruzada

Adicionalmente, se deberán programar estas prioridades sin perjudicar a los usuarios en sus actividades de acceso y consulta a la información. Esto es, los procesos de actualización masiva o cierres (batch) deben programarse preferentemente en horarios fuera del período regular de trabajo diario, que es el horario en que los usuarios accesan a los sistemas.

2.4 Actividades para el Backup de medios magnéticos y documentación

Un elemento crucial de un plan de contingencia en la sede original o alternativa, es la disponibilidad de datos adecuados. La duplicación de datos importantes y de la documentación es un pre-requisito para cualquier tipo de recuperación, incluyendo almacenamiento de los datos de back-up y documentación fuera de la sede habitual.

2.4.1 Procedimientos periódicos de backup

Siempre siguiendo el ejemplo planteado, para definir la estrategia de respaldo se ha identificado el ciclo de proceso de cada sistema o función, encontrándose que todos los sistemas operacionales corresponden a ciclos de actualización variables durante el día. Por ejemplo, en el momento en que ocurre una operación para los sistemas de Créditos y Caja de Ahorro. Contabilidad es una excepción ya que puede actualizarse una vez al día. En cuanto a los sistemas administrativos, todos son actualizados también en forma permanente y diaria, y requieren de cierres de fin de período (fin de día y fin de mes).

El ideal en esta caso es realizar operaciones de respaldo en el momento en que ocurren las transacciones. Sin embargo, esto resulta tan costoso que casi ninguna entidad podría soportarlo. Por otro lado, las bases de datos relacionales, permiten realizar de manera automática este procedimiento para periodos de tiempo relativamente cortos, por ejemplo las operaciones del día. Por lo tanto, el proceso de respaldo sugerido toma en cuenta estos aspectos.

En todos los casos se debe realizar un respaldo **total** semanal, al fin de una semana o luego de un cierre mensual. Luego, debe realizarse un respaldo **acumulativo o incremental** al final de cada día de la semana. El primero permite obtener una copia completa de la información a una fecha y el segundo una copia de todos los cambios ocurridos en el día.

El siguiente cuadro muestra el ejemplo de la estrategia de respaldo definida para cada sistema o función:

Estrategia de respaldo por sistema o función

N°	Proceso o aplicación	Período	Dirección fuente de contenido	Momento estimado respaldo	Tipo de respaldo
	Sistemas operativos				
1	Créditos				
	Datos de operaciones	D		Fin día	Acumulativo
	Datos sistema en general	S		Fin actualiz.	Total
2	Caja de Ahorro				
	Datos de operaciones	D		Fin día	Acumulativo
	Datos sistema en general	S		Fin actualiz.	Total
3	Contabilidad	M		Fin actualiz.	Total
	Datos de operaciones	D		Fin día	Acumulativo
	Datos sistema en general	S		Fin actualiz.	Total
	Sistema administrativos				
4	Recursos Humanos	D		Fin día Al Cierre	Acumulativo Total
5	Planilla de sueldos	D		Fin día Al Cierre	Acumulativo Total
6	Activo fijo	D		Fin día Al Cierre	Acumulativo Total
7	Inventarios	D		Fin día Al Cierre	Acumulativo Total
8	Desarrollo de sistemas	D		Fin día	Acumulativo

Período: D=Diario, S=Semanal, Q=Quincenal, M=Mensual, T=Trimestral, A=Anual
Dirección: Describir los dispositivos y directorios que contienen la información a respaldar
Momento: Indica el momento más oportuno para realizar la copia de respaldo
Tipo respaldo: Indica el tipo de procedimiento de respaldo más apropiado.

Los respaldos totales de los sistemas en producción, deben incluir los programas ejecutables, para ello existen varias alternativas: incluir en cada copia lo programas ejecutables o incluir estos únicamente en la copia inmediata a una modificación del sistema, o finalmente generar la copia por separado. En el primer caso se cuenta con la ventaja de acceso inmediato a los programas, en cambio se gasta más en espacio de almacenamiento. En el segundo caso ocurre lo contrario, ubicar la copia de los programas requerirá de mayor tiempo y los respaldos consumirán menos espacio.

Los repaldos de las bases de datos deben tomar en cuenta las capacidades y limitaciones de la base de datos relacional que se esté utilizando. Son de especial consideración las capacidades de respaldo automático provistas con las herramientas de "transaction log" que le permite a estas bases de datos realizar recuperaciones automáticas luego de una caida en el sistema, esto es muy útil para bases de datos que tienen alto volumen de actualizaciones durante el día, que en general es el caso de sistemas de Créditos y Caja de Ahorro. Por otro lado, las herramientas de respaldo (dump, backup, etc) y recuperación (load, restore, etcétera) operan sobre toda la base de datos, esto impide la realización de respaldos selectivos de tablas maestras o de transacciones de una aplicación, esta característica obliga a obtener copias de respaldo "total" de cada base de datos. En una sesión ordinaria de actualización diaria, estos procedimientos de respaldo y recuperación tienen aplicación cuando la falla es en el disco o medio que almacena la base de datos.

El uso apropiado de las herramientas de respaldo y recuperación permite configurar un plan del tipo "total" e "incremental". Realizar un “dump o backup” de la base de datos equivale a realizar una copia de respaldo total. Realizar un "dump o backup" del “log de transacciones” equivale a realizar una copia de respaldo incremetal de los cambios a la base de datos.

También es de vital importancia considerar que los archivos de backup obtenidos, muchas veces no pueden ser recuperados con restore en otra plataforma, versiones anteriores de base de datos e incluso con configuraciones diferentes de las bases de datos.

Finalmente, se deben realizar copias de respaldo de las estructuras de las bases de datos cada vez que se modifica la estructura de una base de datos. Estos backups deben extenderse a las bases de datos maestras de la propia base de datos relacional ("master", "model", "systemprocedures", “systemobjects”, etcétera), cada vez que se realicen cambios en ellas para prever recuperaciones cuando éstas sean afectadas por un fallo.

2.4.2 Frecuencia de rotación de las copias de respaldo

Por regla general se debe mantener información por el tiempo dispuesto legalmente, la Entidad debe guardar los archivos de respaldo total por este tiempo, que actualmente en Bolivia es de 10 años. Esto significa que los respaldos totales deben almacenarse en lugar seguro por un tiempo no menor a 10 años. Adicionalmente, cabe analizar el hecho de que la base de información de la Entidad es una primerísima fuente de datos históricos para realizar estudios acerca del comportamiento de sus operaciones y clientes, lo que la convierte en depositaria de información histórica con alto valor agregado.

Para los requerimientos de respaldo acumulativo o incremental, se plantea el esquema de respaldo en "tres generaciones", que cubre períodos semanales (día a día), mensuales (semana a semana) y anuales (mes a mes).

Para este procedimiento se requiere contar con:

- Un (juego) volúmen de unidades físicas de respaldo (cintas, CDW, otro) por cada mes,

- Un (juego) volúmen de unidades de respaldo por cada una de tres semanas del mes, la cuarta corresponde al volumen del mes.
- Un (juego) volúmen de unidades de respaldo por cada uno de cuatro días de la semana, el quinto corresponde al volumen de la semana. Si la entidad genera información durante los días sábado y domingo, el ciclo debe incluir unidades para estos días también.

Las unidades deben etiquetarse "Dia 1 a Día 4" para las de la semana, "Semana 1 a Semana 3" para las del mes y las anuales con el mes calendario correspondiente.

El proceso se realiza de la sigiente manera:
- Iniciar con una copia Total en la unidad de la semana 1, preferentemente en viernes.
- Continuar con la copia de cada día de la semana utilizando la unidad correspondiente al día. En este proceso respaldar únicamente los datos o archivos nuevos o modificados en el día (respaldo incremental).
- Al final de la semana realizar la copia total en la unidad de la semana 2.
- Continuar con el procedimiento hasta el último día de la última semana del mes.
- En este punto se habrá completado el ciclo de un mes. Continuar con el procedimiento para cada mes.

En este proceso las unidades o volúmenes que se reciclan son las correspondientes a cada día y a cada semana. Las unidades correspondientes al mes no se reciclan, se mantienen como respaldo histórico permanente.

2.4.3 Tipos de medios magnéticos y documentos que se deben rotar

Los archivos magnéticos o electrónicos con el software (sistemas operativos, lenguajes de programación, compiladores, utilitarios y programas de aplicación) deben ser conservados en una sede alterna en su versión actual.

La información bajo la forma de registros, archivos de datos, bases de datos y documentos de entrada/salida, brindan el material en bruto y los productos terminados para el ciclo de procesamiento de datos. Entre la documentación de la que se debe respaldar y almacenar en la sede remota, se debe incluir:
- **Procedimientos operativos:** Libros de corrida de aplicaciones, manuales de operación para ejecutar los procesos, manuales del sistema operativo y procedimientos especiales.
- **Documentación de sistemas y programas:** Documentación de diseño de sistemas tales como flujogramas, listados de código fuente de programa, descripciones de lógica del programa, condiciones de error y otras descripciones.
- **Procedimientos especiales:** Cualquier procedimiento o instrucciones que salen de lo común, tales como procesamiento de excepciones, variaciones de procesamiento, procesamiento de emergencia.
- **Documentos fuente o de entrada:** Duplicados de archivos, fotocopias de documentos, microfichas, microfilm.

- **Documentos de salida:** Informes o resúmenes que se necesitan con objeto de auditoría, análisis histórico, realización de tareas vitales, cumplimiento de requisitos legales, la documentación necesaria sobre seguros para efectuar y acelerar los reclamos a la compañía aseguradora.

2.4.4 Contabilización del almacenamiento en la sede de backups

Se debe llevar un inventario del contenido de los back-ups residentes en el Centro de cómputos y en la sede de almacenamiento alternativa. Ese inventario debe incluir información como:

- Nombre de los archivos, número serial de volumen, fecha de creación, período de contabilidad y número de depósito de almacenamiento en la sede alternativa para todas las unidades de back-up, y
- Nombre del documento, ubicación, sistema al que corresponde, última fecha de actualización.

2.4.5 Procedimiento de recuperación

El procedimiento de recuperación de información desde una copia total difiere de la de una copia incremental. Para recuperar los datos desde una copia de respaldo total, simplemente se cargan desde la última copia de respaldo total. En cambio para la recuperación de un respaldo incremental se debe proceder de la siguiente manera:

- Obtener el respaldo del último log de transacciones, de las bases de datos que fallaron.
- Eliminar o borrar las bases de datos que se tengan que recuperar.
- Eliminar e inicializar el dispositivo que falló.
- Re-crear las bases de datos a recuperar, una a una.
- Cargar los datos de la última copia de respaldo **total**.
- Cargar los datos desde las copias de respaldo incremental desde la 1ra generada luego de la copia **total** utilizada, hasta la última, estas son las copias incrementales realizadas en el período transcurrido entre la última copia de respaldo total y el momento en que se realiza la recuperación.

2.5 Contratación de seguros

Una medida importante para asegurar la continuidad de las operaciones y la posible reparación de los daños económicos ocasionados por una contingencia, es tener protegidos todos los equipos y software con una póliza de seguros.

La póliza de seguros de procesamiento de datos es por lo general una póliza multi-riesgo diseñada para brindar diversos tipos de cobertura. Lo negativo de esto, es el alto costo que por lo general cobran las compañias de seguro para otorgar cobertura a datos y programas computacionales.

2.5.1 Alternativas de modalidades de contratación de seguros

Las coberturas específicas o similares que podrían contratarse son las siguientes:

Equipamiento y Centros de cómputo
Da cobertura a daño físico al centro de procesamiento de información y al equipo de propiedad de la Entidad. Se debe tener especial cuidado en revisar las pólizas, dado que muchas pólizas sólo imponen reemplazar el equipamiento no recuperable con equipos "de tipo y calidad semejante", no necesariamente con equipamiento nuevo del mismo proveedor que el equipamiento siniestrado. De otro lado, si la Entidad cuenta con equipos en la modalidad de leasing, es pertinente señalar que en tales casos deben obtenerse y analizarse las respectivas pólizas, cuando el arrendador tiene a su cargo la cobertura de riesgos.

Reconstrucción de medios de almacenamiento (software y datos).
Cubre los daños a los medios del centro de computos y al Sistema de Información que son propiedad de la Entidad y por los cuales el asegurado pueda tener responsabilidad civil. Existen seguros para situaciones dentro del local, fuera del local y en tránsito y dan cobertura al costo real de reproducción de la propiedad. Lo que se tiene en cuenta para determinar el valor de la cobertura que se necesita, son los costos de programación para reproducir los medios dañados, reemplazo físico de los dispositivos o medios (por ejemplo, cintas, cartuchos, CDs, discos, etc.) y gastos de back-up.

Gastos Extras
Diseñada para cubrir los costos extras de continuar las operaciones tras el daño o destrucción del centro de procesamiento. El monto de los seguros por gastos extras se basa en la disponibilidad y costo de los centros de back-up y operaciones. (este seguro debe ser suficientemente adecuado para cubrir el costo de los esfuerzos de contingencia).

Interrupción del negocio
Cubre las pérdidas económicas causadas por los daños a los equipos y medios magnéticos del computador mientras estén interrumpidas las operaciones. En una entidad financiera, podrían eventualmente estar asociadas a servicios de información financiera o de riesgos crediticios, con costo para el cliente de la entidad.

Documentos y registros valiosos
Da cobertura al valor monetario de papeles y registros valiosos (no definidos como medios de almacenamiento) en el local de la Entidad, por pérdida o daño directo.

Errores y omisiones
Este tipo de seguro se creó originalmente para los centros de procesamiento externo pero en la actualidad son ofrecidos por las empresas de seguros para dar cobertura a analistas de sistemas, diseñadores de software, programadores y consultores.

Cobertura de Fidelidad
Dan cobertura por actos deshonestos o fraudulentos de parte de los empleados.

Transporte de medios magnéticos
Da cobertura de protección ante pérdida potencial o daños a los medios magnéticos en tránsito hacia un centro de procesamiento de datos fuera de la sede principal. La cobertura de la póliza en tránsito generalmente especifica que los documentos deben ser copiados o microfilmados.

Finalmente, es pertinente aclarar que las coberturas anteriormente señaladas, han sido tomadas como base de pólizas de seguros universales de equipamiento electrónico.

2.5.2 Modalidad de seguros a contratar recomendada

La cobertura de seguro apropiada para la entidad dependerá de la situación en que se encuentre su servicio de informática. Por ejemplo si se encuentra en un proceso intensivo de desarrollo informático, es conveniente iniciar con un contrato de seguros en la modalidad de **Cobertura para equipamiento y centros de cómputo.** Esta podrá ser ampliada a otras modalidades en un futuro mediato, en función a la evolución de los servicios de información que brinde la Unidad TIC.

2.6 Selección de la Sede Alternativa: seguridad y control

La instalación de procesamiento de información alternativa (off-site) debe ser tan segura y controlada como la sede original. Ello incluye controles de acceso físico adecuados como puertas con cerraduras, vigilancia, etc.

También, la instalación de procesamiento alternativo no debe ser fácilmente identificable desde el exterior, por lo tanto, no deben estar presentes signos que identifiquen al vendedor/empresa y el contenido de la instalación. Esto es a fin de evitar el sabotaje intencional de la instalación alternativa fuera de la sede original en caso de que la destrucción de la sede se hubiera debido a un ataque intencional.

Asimismo, la instalación de la sede alternativa no debe estar sujeta al mismo desastre natural que afectó la sede original. Por ende, su ubicación no debe estar muy próxima a la sede original.

La sede alternativa debe poseer el mismo monitoreo y control constante del ambiente de la sede original. Ello incluye el monitoreo de la humedad, temperatura y el aire, a fin de lograr las condiciones óptimas para el equipo y los dispositivos periféricos. Se incluye entre los correctos controles ambientales, operar en un piso sobre-elevado con adecuados detectores de humo y agua instalados, provisión ininterrumpible de energía y un sistema de extinción de incendios en funcionamiento/probado.

2.7 Determinación de los requerimientos de hardware y software alternativo

2.7.1 Determinación de los requerimientos mínimos de funcionalidad

La Entidad debe determinar los requerimientos de hardware y software alternativo, de acuerdo a las prioridades asignadas a los sistemas y aplicativos. La Entidad en caso de emergencia extrema, deberá poder ofrecer servicios con las funciones operativas mínimas acordes con su política de servicio. Sin embargo, un caso eventual de catástrofe, podría dejar a la Entidad sin su capacidad operativa normal por un período largo de tiempo, más de 2 semanas. Entonces deberá poder operar en un ambiente de contingencia que le permita a sus usuarios internos trabajar con los sistemas de información más importantes. En consecuencia y siguiendo el ejemplo ya planteado, las instalaciones alternativas deberán cubrir:

a. Sistemas y módulos que operarán en situación de emergencia.

Créditos	Servicio a operaciones de clientes
	Consultas locales o internas
Caja de Ahorros	Servicio a operaciones de clientes
	Consultas locales o internas
Contabilidad	Consultas locales

Si la emergencia se dá en tiempo de actualización de datos, será conveniente que además se habiliten las funciones de actualización de los tres sistemas.

Los sistemas administrativos deberán poder operar en el mismo ambiente con todas sus capacidades.

b. Información histórica disponible.
Los datos históricos con que operarán los sistemas de emergencia, son particulares a cada caso:

Créditos	Seis meses de transacciones en operaciones vigentes
Caja de Ahorro	Seis meses de transacciones en operaciones vigentes
Contabilidad	últimas dos gestiones

c. Usuarios que operarán en situación de emergencia.

Externos:

Todas las entidades que usualmente interactuan con la red y sistemas de la entidad.

Internos:

- Gerente general 1
- Secretaría General 1
- Auditoría 1

- Créditos
  - Oficiales de campo 1 - 2
  - Oficiales de oficina 2 - 4
- Caja de Ahorro
  - Oficiales de campo 1 - 2
  - Oficiales de oficina 2 - 4
- Unidad TIC
  - Administrador base de datos 1
  - Operadores 1 - 2

2.7.2 Alternativas de sede alternativa disponibles

La selección adecuada de los requerimientos de hardware y software en la sede alternativa de procesamiento, son indispensables para la buena marcha del Plan de Contingencias.

Para esta implementación se propone que la Entidad del sistema Financiero, estime conveniente la contratación de sedes alternativas de procesamiento con el equipamiento adecuado, para lo cual a continuación se presentan las diversas alternativas de centros de procesamiento de back-up que la Entidad podría considerar en la implementación de su Plan de Contingencias:

HOT-SITES (Alternativas de emergencia).

Este centro de procesamiento debe estar totalmente configurado y listo para operar dentro de unas pocas horas. El equipamiento y el software de sistemas deben ser compatibles con la instalación básica de la Entidad. Las únicas necesidades adicionales son las de personal, programas y archivos de datos.

Los costos de la utilización de hot-sites son generalmente altos pero son justificables para aplicaciones críticas. Para ello se debe planificar correctamente la cobertura de seguros, la cual deberá compensar los costos incurridos por utilizar este tipo de instalación.

El hot-site debe contratarse cuando existan operaciones de emergencia por un período limitado de tiempo y no para un uso extendido a largo plazo. El mismo que debe considerarse como un medio de lograr una continuación de operaciones esenciales por un período de hasta algunas semanas posteriores a un desastre o una grave emergencia.

WARM-SITES

Este centro de procesamiento está parcialmente configurado, generalmente con equipo periférico seleccionado, tal como unidades de disco, cinta y controladores, pero sin el computador principal. Es posible que se seleccione este tipo con una CPU menor.

El supuesto que respalda al concepto de warm-site es que el computador puede obtenerse rápidamente para una instalación de emergencia (siempre que sea un modelo de uso común), y dado que el computador es la unidad más cara, tal arreglo es menos costoso que un hot-site.

Luego de la instalación de los componentes necesarios, el centro puede ser considerado listo para el servicio en cuestión de horas; sin embargo, la ubicación e instalación de CPU y de las otras unidades faltantes puede insumir días o semanas.

COLD-SITES

Estos son centros que tienen el ambiente básico (cableado eléctrico, aire acondicionado, piso, etc.) para operar un centro de procesamiento de información. El cold-site está listo para recibir el equipamiento pero no ofrece ningún componente instalado antes de que sea necesario. La activación del centro puede insumir semanas.

Las principales diferencias entre los tres tipos de centros son el tiempo de activación y el costo. En el caso de desastre a largo plazo, una reducción en los costos operativos es deseable. Ello puede lograrse utilizando un warm-site o un cold-site como centro secundario, luego de utilizar un hot-site por un corto plazo.

2.7.2 Consideraciones para la contratación de centros alternativos

Aun cuando los servicios descritos en el punto anterior no son comunes en Bolivia, las entidades pueden considerar su aplicación. Probablemente sea posible contar con ellos si se busca contratos masivos (varias entidades del mismo tipo contratan un solo servicio), esto debido a que es poco probable que un mismo desastre afecte a más de una entidad a la vez.

Las consideraciones que se deberian tomar en cuenta en la contratación de centros de sede alternativa para el procesamiento, deben cubrir los siguientes puntos:

- **Configuraciones:** Asegurándose de que las configuraciones de hardware sean adecuadas para satisfacer las necesidades de la Entidad. Debido a que las mismas pueden variar con el tiempo, debe asegurarse que el centro contratado esté informado de las actualizaciones.

- **Desastre:** Es la definición de desastre lo suficientemente amplia como para satisfacer las necesidades que se prevén?

- **Rapidez de la disponibilidad:** Qué pronto luego del desastre estará disponible el centro alternativo?

- **Preferencia:** Quién tiene preferencia si se producen desastres comunes? Existe un back-up del centro de back-up? Tiene el proveedor más de un centro disponible?

- **Periodo de uso:** Durante cuánto tiempo se dispondrá del centro? Es adecuado el período? Qué soporte técnico dará el operador de la sede? Es adecuado?

- **Comunicaciones:** Son adecuadas las comunicaciones? Son suficientes las conexiones de comunicaciones en la sede de back-up como para permitir las comunicaciones con la sede alterna si fuera necesario?

- **Garantías:** Qué garantías da el proveedor respecto de la disponibilidad de la sede y la adecuación de los equipos?

- **Prueba:** Qué derechos a hacer pruebas se incluyen en el contrato?

- **Confiabilidad:** El proveedor debe garantizar la confiabilidad de las sedes que se ofrecen. En una situación ideal, el proveedor debe poseer UPS, un número limitado de clientes, una administración técnica razonable y garantías de compatibilidad de hardware y software.

A partir de estas definiciones será posible escoger entre Hot sites, Warm sites y Cold sites, analizando, además, el costo de la mantención stand-by (sin uso) del servicio.

2.7.3 Obtención de centros de procesamiento de información alternativos

a. Opciones disponibles.

Se dispone de diversas alternativas para asegurarse de obtener el hardware e instalaciones físicas:

Reaprovisionamiento por el proveedor de los equipos

En primer lugar debe verificarse con el proveedor de los equipos principales de la Entidad si es posible el procesamiento en equipos del proveedor en caso de Contingencias. Esto para cualquiera de las modalidades HOT SITE, WARM SITE o COLD SITE. Normalmente en la adquisición de equipos se garantiza equipos de respaldo en caso de contingencias, pero debe formalizarse claramente esta contratación.

Hardware listo

Se pueden obtener prontamente componentes de proveedores a corto plazo y con una necesidad mínima de arreglos especiales. A fin de utilizar este enfoque, deben implementarse diversas estrategias.

- Evitar el uso de equipo inusual o difícil de mantener. La Entidad debe cuidar de implantar equipos de uso corriente en el mercado y que cuenten con servicios de respaldo y mantenimiento comprobados.

- Actualizar regularmente el equipo a fin de mantenerlo al día. Los procesos de actualización de tecnología deben seguir lineamientos de compatibilidad y desarrollo apropiados a las necesidades y posibilidades de la Institución.
- Mantener la compatibilidad del software a fin de permitir la operación de equipo más nuevo. Los desarrollos de software deben evitar el uso de técnicas particulares o complicadas que impidan el funcionamiento del software en equipos actualizados.

b. Opción generalmente recomendada a una Entidad.

La Entidad debe negociar con el proveedor de sus equipos principales la posibilidad de contar con un servicio de sede alternativa, en base a las configuraciones actuales y en proceso de instalación, y también a la determinación de servicios mínimos que debe proveer el centro de cómputos en una situación de contingencia. En lo posible, el contrato debe garantizar el uso de Hot sites por un plazo mínimo, y descender gradualmente a Warm sites o Cold sites. Los plazos de uso de cada modalidad deben ser determinados en el momento de ocurrencia de la contingencia y luego de analizadas sus consecuencias y posibilidades de recuperación.

2.8 Red de telecomunicaciones

Las redes de telecomunicaciones también pueden sufrir los mismos desastres naturales que los centros de cómputos, pero también son susceptibles a acontecimientos desastrosos propios de las telecomunicaciones.

Entre ellos se incluyen desastres en las centrales de conmutación, corte de líneas, problemas y errores del software de telecomunicaciones, violaciones a la seguridad relacionadas con la piratería, y una multitud de inconvenientes de origen humano.

Es normal que la propia Entidad tenga la responsabilidad de que se cuente con capacidad constante de comunicación, por lo que debe preverse respaldo de sus funciones de telecomunicaciones.

La capacidad de telecomunicaciones debe incluir los circuitos de voz, redes de área amplia (por ejemplo, conexiones con las sucursales), y fuentes de intercambio electrónico de datos. Deben identificarse los niveles de capacidad críticos para diversos escenarios en caso de salida de la capacidad de telecomunicaciones, por ejemplo, 2 horas, 8 horas, 24 horas, etc. Las fuentes ininterrumplibles de energía deben ser suficientes como para servir de respaldo tanto para el equipo de telecomunicaciones como para el resto de equipo del centro de procesamiento (CPU, periféricos, etc.).

2.8.1 Consideraciones del plan de contingencia para la red

Redundancia en la red local

En este caso la Entidad debe establecer medidas para asegurar una redundancia mínima para que los servicios no se detengan cuando falle la red local principal. Para ello puede considerase la instalación un segundo cableado, por medio de una ruta alterna, para utilizarla en caso de que el cableado primario se dañe.

Estas rutas son un método para enviar la información por un medio alternativo tal como un cable de cobre en reemplazo del dañado. Ello implica utilizar diferentes redes, circuitos y puntos terminales en cada caso. Lo que se recomienda en este aspecto con el objeto de no incurrir el altos costos de un cableado paralelo redundante, es determinar la "red mínima", necesaria para la habilitación de los principales usuarios. Esta red mínima tendría un cableado redundante.

Redundancia o Alternativa de red de largo alcance WAN

Para las redes electrónicas remotas se recomienda establecer convenios con la Entidad proveedora de estos servicios para conseguir rutas alternativas de transmisión de datos y adicionalmente algún proveedor alternativo, que pueda suplir este servicio.

2.8.2 Requerimientos mínimos de la red de contingencia

Redundancia de red en la sede principal

La red local en la sede principal de la Entidad deberá implementar redundancia para los accesos de los usuarios principales o críticos. Por lo general, será suficiente que el personal que realice operaciones vitales con el sistema, sea el que tenga posibilidad de acceso en una contingencia de fallo de la red principal. Este personal corresponde principalmente a las siguientes áreas:

Area	**Estaciones de emergencia**
• Gerencia General	1
• Secretaría General	1
• Auditoría	1
• Créditos	
◦ Oficiales de oficina	2 - 4
• Caja de Ahorro	
◦ Oficiales de oficina	2 - 4
• Unidad TIC	
◦ Administrador base de datos	1
◦ Operadores	1 - 2
• Administración	1
• Informática	
◦ Administrador base de datos	1
◦ Operadores	1 - 2

Una alternativa más económica a considerar, consiste en que toda las estaciones para trabajar con la red de emergencia, puedan ser conectadas desde un mismo ambiente físico, por ejemplo desde una sala de reuniones o capacitación.

Acceso o redireccionamiento de los nodos hacia la sede alternativa

En el contrato de servicios de la Entidad con el proveedor de servicios de comunicación, se debe incluir la posibilidad de redireccionar los accesos a la sede alternativa en caso de contigencias que obliguen el uso de ésta.

3. PRUEBAS DEL PLAN DE CONTINGENCIAS

Deben ejecutarse pruebas regulares para verificar que el Plan de Contingencias funcione en los momentos apropiados. Para estas pruebas se propone lo siguiente:

- Entrenamiento de los grupos de trabajo de emergencia y la verificación del cumplimiento de sus responsabilidades.
- Verificación de los centros de respaldo.
- Verificación de las comunicaciones de respaldo.
- Evaluación de la capacidad de recuperación de datos y programas (Pruebas reales).
- Prueba general del Plan de Contingencias simulando hechos que pudieran producirse.

4. CURSO A SEGUIR EN CASO DE CONTINGENCIA

El plan de contingencias tendrá los éxitos esperados, únicamente si las acciones que se realicen son efectivas principalmente en las tareas de prevención de contingencias. Esto es, llevar a cabo prolijamente las tareas de protección, seguridad y respaldo.

4.1 Acciones preventivas

4.1.1 Del personal y sus funciones

Todo funcionario de la Unidad TIC y fuera de ella, debe realizar sus actividades apegándose por completo a las definiciones del Manual de funciones de la institución y los manuales propios tanto de la Unidad TIC, como de los sistemas o aplicaciones.

Todo funcionario debe respetar las reglas de exclusividad del uso de passwords para accesar a los sistemas y equipos, así como de las llaves de acceso a los ambientes restringidos por seguridad. El poseer una llave de acceso o password más que un privilegio de acceso, representa una responsabilidad identificable, si un funcionario comparte sus claves no podrá compartir del mismo modo las responsabilidades que se deriven de su uso.

La Institución debe diseñar y ejecutar un programa de capacitación masiva e integral del personal de informática y usuarios, en el uso de las herramientas tecnológicas y en los procedimientos de seguridad y contingencia definidos en este manual.

4.1.2 De los estándares en metodología y herramientas en uso

Todas las actividades de la Unidad TIC y su personal deben ser realizadas ajustándose a los estándares de metodologías y herramientas de aplicación aprobados por la Institución. A continuación se señalan algunos ejemplos de estos estándares, metodologías y herramientas:

- La metodología de análisis y diseño de sistemas debe ser exclusivamente la correspondiente al Manual de estándares de diseño y desarrollo, que especifica el uso exclusivo de las herramientas de diseño CASE, definidas por la entidad.

- La metodología de desarrollo de sistemas debe ser exclusivamente la definida en el Manual de estándares de desarrollo, que especifica el uso de las herramientas apropiadas:
    - Visual Basic, Power Builder, InfoMaker, Java, ASP, etcetera;

- Las bases de datos, bases documentales y herramientas similares deben ser aprobadas por la entidad y especificadas en los manuales correspondientes:

- SQL Server, Oracle, Sybase, etcétera, para las bases de datos institucionales,
- Exchange, Lotus Notes, otras, para la bases documentales,
- Access (para archivos de cliente), para aplicaciones de usuario final.

- El usuario debe usar únicamente el software de cliente o de usuario final autorizado por la Unidad TIC, el cual podría incluir por ejemplo:
  - Office: Word, Excel, Power point, Schedule y Outlook
  - MS-Project
  - Lotus Notes

- Toda la documentación de diseño y desarrollo, así como los Manuales de usuario y de operación de los sistemas, debe ser generada en formato de procesadores de texto como Word.

4.1.3 En el Centro de cómputos y su seguridad

Deben instalarse los elementos de seguridad para resguardar el centro de cómputos, cubriendo al menos los siguientes:

- Detectores de humo e incendio.
- Llave de acceso a las instalaciones del Centro de cómputos.
- Instalación de la gaveta portátil de almacenamiento de archivos y de la gaveta fija o empotrada.
- Puesta en práctica de los Logs de Sistemas y Operaciones

Verificar regularmente el funcionamiento de los elementos de seguridad del Centro de cómputos.

4.1.4 De las previsiones de sede alternativa

Verificar, revisar, modificar y aprobar los requerimientos de equipamiento para la sede alternativa, planteados en este manual.

Gestionar lo más pronto posible la contratación de un servicio de sede alternativa que reuna las condiciones de ambiente y equipamiento planteadas en este Manual de Contingencias. El servicio puede ser contratado con el proveedor de los equipos principales.

Mantener actualizados los requerimientos y términos contractuales de uso de la sede alternativa, en función a los cambios y avances tecnológicos en su propia sede principal.

Negociar o renegociar con el proveedor de servicio de comunicaciones, para asegurar de inmediato que las condiciones contractuales del servicio de telecomunicaciones, incluya la posibilidad de redireccionamiento de las comunicaciones hacia la sede alternativa cuando sea necesario.

4.1.5 Acciones de respaldo

Regularmente, de ser posible diariamente, ejecutar los procesos de verificación de los discos (Fcheck o similar) y las bases de datos (dbcheck o similar), para asegurar que estos se encuentran en buen estado.

Periódicamente realizar copias de unidades de arranque de los servidores. Almacenar una copia de la configuración de cada servidor y sus periféricos (directorios de programas, de datos, de bases de datos, usuarios, permisos de acceso, etcétera).

Realizar las copias de respaldo de sistemas de acuerdo a lo dispuesto en los manuales de operación de cada sistema.

Verificar que las copias de respaldo realizadas estén correctas.

Verificar que los medios (cintas, diskettes, discos compactos), en que se realizan los backups están en buen estado.

Registrar los backups realizados, en el Log de operaciones.

Guardar los archivos de backup en las gavetas del Centro de cómputos y enviar las copias a los recintos de resguardo cuando corresponda.

Establecer el programa de respaldos de información en equipos de usuario.

Capacitar a los usuarios en el uso apropiado de directorios de trabajo y procedimientos de respaldo.

Ejecutar el programa de respaldos asesorando al usuario en su aplicación.

4.1.6 Acciones para la red interna LAN

Establecer los requerimientos de conexión mínima de acuerdo a las definiciones de este manual y definir los componentes tecnológicos necesarios.

Realizar la instalación de los componentes de red para la red redundante, incluyendo los dispositivos necesarios para el redireccionamiento de la red.

Mantener actualizadas las especificaciones y manuales de configuración de la red.

Realizar copias de respaldo periódicas de las configuraciones de la red.

4.1.7 Acciones para la seguridad de los equipos

Verificar la vigencia de tiempos de garantía y mantenimiento de los equipos servidores, de comunicación y de usuario. Actualizar los contratos de inmediato si es necesario.

Verificar si los seguros cubren los equipos según las definiciones de este manual, contratar los seguros necesarios si corresponde.

Adquirir e implantar el uso de cobertores y protectores de equipo en toda la Institución.

Realizar el mantenimiento externo de los equipos del Centro de cómputos y verificar la realización del mismo servicio por los usuarios en sus equipos de trabajo.

Establecer y ejecutar un programa de capacitación intensiva para los funcionarios de la Institución, en la aplicación de las acciones de protección y seguridad de los equipos planteadas en este manual.

4.2 Acciones correctivas

Las acciones correctivas, serán necesarias en caso de ocurrir alguna contingencia, prevista o no prevista. Dado que la contingencia puede ser de cualquiera de las tres categorías señaladas (no desastre, desastre y catástrofe), se plantea una guía básica de acciones a seguir:

Enfrentar la contingencia, teniendo como primer objetivo, salvar la vida de las personas. Si el caso lo requiere, debe procederse a la evacuación de la sede siguiendo el orden establecido en el punto "Para la seguridad del centro de cómputo" del capítulo I.

Evaluar las consecuencias de la contingencia. En función a esto se determinará el punto de incicio para la recuperación de la capacidad de funcionamiento. Este punto de inicio puede ser tan sencillo como reconectar el equipo y echar a andar los sistemas o tan complicado como activar y poner en marcha la sede alternativa.

En todo caso, el orden de acciones a realizar, podría ser como sigue:

- Restablecer las condiciones de uso del Centro de cómputos, en la sede principal o alternativa. Este proceso podría incluir las siguientes tareas:
    - Revisión, reparación y/o reemplazo de componentes del equipo auxiliar del Centro de cómputos.
    - Acondicionamiento de la sede alternativa.
    - Prueba de funcionamiento del equipo auxiliar de la sede
- Restablecer el funcionamiento de los equipos y de la red. Este proceso podría incluir las siguientes tareas:
    - Revisión, reparación y/o reemplazo de componentes o equipos
    - Re-instalación del software de base en el equipo
    - Re-configuración de dispositivos periféricos
    - Re-instalación del software de red

    - Re-configuración de la red.
    - Activación de la red local alternativa.
    - Re-configuración de usuarios y permisos de acceso.
    - Pruebas de funcionamiento de los equipos y la red.
- Revisar y determinar las prioridades de procesamiento con base a las definiciones del Manual de contingencia y las capacidades de operabilidad en la emergencia.
- Restablecer los datos a su momento más actualizado:
    - Re-creación de las bases de datos y su configuración.
    - Re-creación de las tablas y vistas, incluyendo tablas, vistas, índices, reglas, usuarios y grupos, permisos, triggers, etcétera.
    - Recuperar los datos de las bases de datos de acuerdo al procedimiento de recuperación definido para cada sistema o aplicación.
    - Recuperar los datos fuente de acuerdo al procedimiento de recuperación definido en los manuales de cada sistema.
    - Probar el funcionamiento de las bases de datos.
- Restablecer el funcionamiento de los sistemas. En este punto se deberán repetar las prioridades establecidas para los sistemas, para poder operar con los sistemas críticos cuando las capacidades de los equipos no sean totales.
    - Recuperar el software de los sistemas o aplicaciones.
    - Probar el funcionamiento de los sistemas o aplicaciones.

Dependiendo de las necesidades de recuperación, producto de la contingencia, el proceso deberá ser iniciado en el punto apropiado.

4.3 Personal requerido para enfrentar las contingencias

El personal que deberá resolver las contingencias, debe ser el mismo personal que trabaja en condiciones normales en la Unidad TIC y deberá contar con el apoyo del personal usuario. Las funciones epecíficas de cada funcionario están detalladas en el punto "Organización de los equipos y responsabilidades en la Entidad". Si la emergencia lo exige, se acudirá a apoyo externo expecífico de proveedores de servicios de mantenimiento y equipos. Esto se determinará una vez evaluada la emergencia.

Los cuadros a continuación explican las responsabilidades paso a paso en las tareas de prevención y corrección ante contingencias:

Asignación de responsabilidades en el Manual de Contingencias
Acciones preventivas

No	Proceso o tarea	Responsable o ejecutor	Herramientas empleadas
	Del personal y estándares		
01	Asignación y control de funciones.	Gerente Unidad TIC Jefe Depto. Desarrollo Jefe Depto. Soporte Técnico	Planificación de funciones.
02	Capacitación a funcionarios de informática.	Gerente Unidad TIC.	Oferta de cursos especializados del mercado.
03	Capacitación a usuarios de la institución.	Personal de soporte a usuarios.	Programas de capacitación y herramientas informáticas.
04	Definición y aplicación de estándares en el diseño y desarrollo de sistemas.	Gerente Unidad TIC Jefe Depto. Desarrollo	Metodología de diseño y desarrollo, Herramientas Case. Power Builder, Infomaker Lotus Notes, Visual Basic, Etcétera.
05	Definición y aplicación de herramientas de usuario estándares.	Jefe Depto. Soporte Técnico	SQL Server, Oracle, Sybase, Lotus Notes, Access, etcetera.
06	Puesta en producción de software	Jefe Depto. Desarrollo Jefe Depto. Soporte Técnico	Control de accesos y passwords Respaldo de información.
	Del centro de cómputos y los procesos		
07	Instalación de equipo de protección y seguridad	Gerente Unidad TIC Jefe Depto. Soporte Técnico	Servicios de proveedores.
08	Operar los equipos y sistemas y registrar los Log de Sistema y Operaciones	Responsable Operaciones	Equipos y sistemas
09	Realizar mantenimiento a los equipos	Jefe Depto. Soporte Técnico Proveedor del servicio	Programa de mantenimiento
10	Realizar mantenimiento de los equipos auxiliares	Responsable Operaciones	Programa de mantenimiento
11	Controlar acceso al Centro de cómputos	Jefe Depto. Soporte Técnico Responsable Operaciones	Llaves de acceso y claves de acceso.
12	Verificar y chequear el funcionamiento de servidores y la red	Jefe depto. Soporte Técnico Administrador Sistema Responsable Operaciones	Software de diagnóstico de servidores y red.
13	Actualizar anti-virus	Responsable soporte a usuarios	Versiones actuales anti-virus
14	Instalar y verificar uso de software autorizado	Responsable soporte a usuarios	Catálogo de software autorizado.
15	Mantenimiento externo de estaciones de trabajo	Usuarios	Manual de contingencia
	De los datos y su protección		
16	Administrar passwords de acceso a los sistemas y red	Administrador Sistema	Software de sistema operativo
18	Administrar passwords y accesos a las bases de datos	Administrador Base de Datos	Software de la base de datos
19	Verificar los medios y datos que se reciben de las entidades supervisadas	Responsable Operaciones	Manual de cada sistema Software de diagnóstico
20	Realizar respaldo de archivos	Responsable Operaciones	Manual de contingencia y Manual de operaciones Softwar de respaldo

21	Realizar respaldo de bases de datos	Administrador Base de Datos	Manual de contingencia y Manual de operaciones Softwar de respaldo de la DB
22	Realizar respaldo de estaciones de usuarios	Usuario Responsable soporte a usuario	Software de respaldo
23	Resguardar las copias de respaldo	Responsable Operaciones	Gavetas del Centro de cómputos
24	Transporte copias a resguardo externo	Administración institución	
	Del hardware y la red		
25	Contratar, verificar cumplimiento y actualizar servicio de mantenimiento	Gerente Unidad TIC Jefe Depto. Soporte Técnico	Especificaciones equipos Contratos de mantenimiento
26	Contratar, actualizar cobertura de seguros	Gerente Unidad TIC Jefe Depto. Soporte Técnico Jefe Dir. Administrativa	Especificaciones equipos Contratos de seguros
27	Instalar la redundancia mínima de la red local LAN	Jefe Depto. Soporte Técnico Administrador Sistemas	Servicio de proveedores
28	Incluir re-direccionamiento de accesos en la red WAN	Jefe Depto. Soporte Técnico Administrador Red	Servicio de proveedores
29	Actualizar la documentación de equipos y red	Administrador Red	Software de documentación
	Del servicio de sede alternativa		
30	Definir y configurar requerimientos de la sede alternativa	Gerente Unidad TIC Jefe Depto. Soporte Técnico	Configuración equipos actuales y en proceso de instalación. Manual de Contingencia
31	Contratar, verificar y probar sede alternativa	Gerente Unidad TIC Jefe Depto. Soporte Técnico Jefe Depto. Desarrollo	Sede instalada Sistemas en producción
	De los equipos de trabajo de emergencia		
01	Asignación formal de responsabilidades en el equipo de trabajo	Gerente o Director General Gerente Unidad TIC	Plan de Contingencia
02	Capacitación a los equipos de trabajo de emergencia	Gerente Unidad TIC	Plan de Contingencia
03	Pruebas del Plan de Contingencia	Todos los equipos de trabajo de emergencia	Plan de Contingencia

Las funciones y responsabilidades asignadas para la fase de prevención, son actividades ordinarias y regulares que cada área y funcionarios de la Unidad TIC, deben llevar a cabo en la Institución.

Asignación de responsabilidades en el Manual de Contingencias
Acciones de emergencia o correctivas

No	Proceso o tarea	Responsable o ejecutor	Herramientas empleadas
01	Enfrentar la contingencia, evacuación si corresponde	Equipo de vigilancia, evaluación y administración de la emergencia. Equipo de operación y logística	Plan de contingencia, Procedimientos de evacuación

02	Evaluar la contingencia y determinar el curso de acción	Equipo de vigilancia, evaluación y administración de la emergencia.	Plan de contingencia
	Restablecer condiciones de uso del Centro de cómputos		
03	Revisión, reparación y/o reemplazo de equipo auxiliar	Equipo de recuperación tecnológica. Equipo de operación y logística Proveedores	Plan de contingencia Evaluación de la contingencia
04	Acondicionamiento de la sede alternativa (si correponde)	Equipo de recuperación tecnológica. Proveedor del servicio	Plan de contingencia Evaluación de la contingencia Contrato de servicio de sede alternativa
05	Pruebas de funcionamiento del equipo auxiliar	Equipo de recuperación tecnológica. Proveedor del servicio	Equipo auxiliar
	Restablecer funcionamiento de equipos y la red		
06	Revisión, reparación y/o reemplazo de equipos o componentes	Equipo de recuperación tecnológica. Proveedor del servicio	Evaluación de la contingencia Equipos y componentes
07	Re-instalación del software de base de los equipos y reconfiguración de los dispositivos periféricos.	Equipo de recuperación tecnológica	Copias de respaldo del software de servidores Procedimientos de recuperación del Plan de contingencia
08	Re-instalación del software de red y reconfiguración de la red	Equipo de recuperación tecnológica	Copias de respaldo del servidor de la red Procedimientos de recuperación del Plan de contingencia
09	Activación de la red local alternativa	Equipo de recuperación tecnológica	Manual de configuración Manual de administración de la red
10	Re-configuración de usuarios y permisos de acceso	Equipo de recuperación tecnológica	Copias de respaldo de servidores
11	Pruebas de funcionamiento de equipos y la red	Equipo de recuperación tecnológica	Equipos y red instalados
	Restablecer los datos a su momento más actualizado		
12	Re-crear las bases de datos y su configuración	Equipo de recuperación de software y aplicaciones	Copias de respaldo de información Procedimientos de recuperación del Plan de contingencia
13	Re_crear la tablas y objetos de la base de datos, usuarios y permisos	Equipo de recuperación de software y aplicaciones	Copias de respaldo de información Procedimientos de recuperación del Plan de contingencia
14	Recuperar los datos de las bases de datos	Equipo de recuperación de software y aplicaciones	Copias de respaldo de información Procedimientos de recuperación del Plan de

			contingencia
15	Recuperar archivos de datos fuente	Equipo de recuperación de software y aplicaciones	Copias de respaldo de información Procedimientos de recuperación del Plan de contingencia
16	Probar funcionamiento de la bases de datos	Equipo de recuperación de software y aplicaciones	Bases de datos recuperadas
	Restablecer el funcionamiento de los sistemas		
17	Recuperar el software de los sistemas y la configuración del mismo	Equipo de recuperación de software y aplicaciones	Copias de respaldo de sistemas Procedimientos de recuperación del Plan de contingencia
18	Probar funcionamiento de los sistemas	Equipo de recuperación de software y aplicaciones	Sistemas recuperados

Dependiendo de la gravedad de la contingencia, el personal participará en mayor o menor grado, por lo general será más bien el personal de la Unidad TIC el que esté dedicado a tareas de recuperación ante emergencia producto de una contingencia.

La Paz, julio, 04 .

MANUAL DE ESTANDARES

UNIDAD DE TECNOLOGIA DE INFORMACION Y COMUNICACIONES (Unidad TIC)

ESTRUCTURA, ORGANIZACIÓN Y FUNCIONES

DAI/SEFIR/R.Tapia/G.Simon
Enero, 2003

Unidad de Tecnología de Información y Comunicaciones (TIC)
Estructura, Organización y Funciones

Tabla de Contenidos

Unidad de Tecnología de Información y Comunicaciones
Estructura, Organización y Funciones

Las Unidades de Tecnología de Información y Comunicaciones (Unidad TIC) tienen una misión que cumplir, independientemente del nombre, rango o jerarquía, dentro de la estructura organizacional de toda empresa. Para ello deben contar también con políticas, objetivos, estructura funcional y otros elementos típicos que hacen al buen funcionamiento de toda organización. El presente documento, recoge estos elementos de la manera más general posible y los presenta como una referencia sugerida. Cada entidad puede ajustar los mismos de acuerdo a sus propias características y objetivos de negocios.

Misión

Proveer información veraz y eficaz en tiempo real a la empresa, o apoyar y agilizar la prestación de servicios a los usuarios, la toma de decisiones y las actividades operativas / administrativas de la organización, mediante sistemas de información y servicios de computación efectivos y eficientes.

Políticas

Políticas de organización

Es política de la Unidad TIC, mantener una organización que preste servicios de Informática, Computación y Comunicación de datos efectivos, eficientes y cónsonos con sus demas objetivos, políticas y requerimientos.
En función de lo anterior, la Unidad TIC, estimula la adquisición de herramientas tecnológicas avanzadas y la contratación y desarrollo de personal especializado, debidamente justificado por análisis de costo/beneficio y aprobado por la alta dirección de la Entidad.

Políticas sobre centralización de actividades

En la Unidad TIC se crean y desarrollan las actividades de Planificación, Evaluación, Justificación, Propuestas de Contratación, Administración y Control de Equipos de Computación, Telecomunicaciones, Sistemas de Información, para toda la Entidad.

Políticas sobre datos

La Entidad, considera los datos (data) como un **Activo Fijo** corporativo. La Unidad TIC, por lo tanto, tiene las siguientes responsabilidades en cuanto a su administración y control: "Proveer mecanismos adecuados para su captación, procesamiento, almacenamiento, respaldo, seguridad y confiabilidad".

Políticas de costos de informática

Los costos de Informática y sus recursos (instalaciones, equipos, programas, personal y materiales) serán distribuidos entre los usuarios de acuerdo al mecanismo aprobado para tal fin. Un buen ejemplo para ello es usar el concepto de los centros de costos bajo el esquema de cargos en función de recursos usados.

La Unidad TIC es responsable de garantizar su productividad de forma tal que el costo de sus servicios no exceda el costo de servicios equivalentes, que puedan ser contratados o adquiridos externamente.

Objetivos

Objetivos generales

En cuanto a la información: Proveer a toda la organización de la Institución, de información organizada, sumarizada y sistemática, que le facilite el desempeño de sus funciones.

En cuanto a eficiencia y efectividad: Efectuar el procesamiento de la información recibida en el menor tiempo posible, y hacer disponibles sus resultados a las áreas usuarias dentro de los límites de tiempo establecidos.

En cuanto a costos: Capturar, procesar, almacenar y distribuir la información a las áreas usuarias con el menor costo por transacción posible.

Objetivos específicos

Los objetivos especificos de la Unidad TIC, cuyo cumplimiento conllevará a la realización de los objetivos generales expuestos antes, son:

En cuanto a organización: Desarrollar y mantener la estructura de organización más adecuada e idónea para el desarrollo de sus funciones; evaluar dicha estructura periódicamente para adaptarla a las necesidades del momento y de acorde a los cambios tecnológicos y necesidades a mediano plazo y evolución de las instituciones.

En cuanto a planificación: Planificar el uso adecuado de personal, recursos, equipos de procesamiento y apoyo, de programación y de archivos. Evaluar y reajustar periodicamente dicha planificación.

En cuanto a control: Establecer y mantener un mecanismo de control que garantice la exactitud de todas las operaciones efectuadas por la Unidad TIC.

En cuanto a sistemas: Participar con las áreas usuarias en la definición y ejecución de proyectos para innovar, mejorar y/o simplificar los sistemas y procedimientos operativos de aquellas.

En cuanto a estándares: Desarrollar y mantener normas y estándares para el análisis, diseño, programación, documentación y operación de los sistemas instalados.

En cuanto a documentación: Documentar los sistemas, programas, trabajos y controles correspondientes, en la forma más sencilla y completa posible y de acuerdo a los estándares definidos por la entidad. De igual manera desarrollar los manuales para los usuarios en función no solo del aspecto técnico sino operacional con las implicaciones de reingeniería o cambio de procesos/procedimientos que el nuevo sistema pueda introducir,

así mismo que sirva de herramienta de entrenamiento para los nuevos usuarios y manual de consulta en un momento dado.

El material de la documentación debe ser actualizado con la periodicidad de los cambios que se efectúen a los sistemas.

En cuanto a investigación: Evaluar periodicamente la nueva tecnología disponible, tanto en equipos de procesamiento como en programas y sistemas operativos, a la luz de la factibilidad operativa y económica de su uso, y de sus posibles beneficios.

En cuanto a educación: Mantener la capacidad técnica de todo el personal a un nivel cónsono con la tecnología disponible en la Unidad TIC.

En cuanto a ventas: Promover en las áreas operativas de la Institución el uso de sistemas y métodos de computación, cuando ello se justifique, y motivar al personal gerencial de aquellas a la investigación e implantación de tales sistemas.

Medios para el cumplimiento de objetivos

Para el cumplimiento de los objetivos expresados, la Unidad TIC contará con los medios suficientes para garantizar que:

- Opera como un área de servicio independiente de las otras áreas funcionales de la Institución.
- Provee información diferenciada a los niveles operativos, gerenciales y de planificación de la Institución.
- Mantiene un personal con la capacidad técnica necesaria y adecuada para la prestación de servicios de óptima calidad.
- Encamina la utilización de sus recursos humanos y materiales hacia la aplicación de los mejores métodos de procesamiento y el empleo de los equipos más idoneos.
- Participa, junto con las áreas usuarias, en la planificación de automatización de nuevos servicios y/o sistemas.

Factores a considerar

Entre los factores más importantes a considerar para el cumplimiento de los objetivos de la Unidad TIC, están:

- Número y tamaño de los usuarios de los servicios de informática. Determinar cuales son las caraterísticas de los usuarios y sus necesidades ¿Hay muchos usuarios pequeños? ¿Hay pocos usuarios grandes? Cuales son las características que determinan el tamaño de un usuario? Determinar si está balanceada la distribución de carga de trabajo para atender las necesidades de los usuarios.
- Dependencia de la gerencia usuaria en los servicios suministrados por la Unidad TIC. Determinar si los resultados de informática son escenciales para la planificación gerencial y toma de decisiones ¿Debe tener la gerencia acceso rápido a la información?
- Dependencia de los usuarios operacionales en informática. Determinar si la Unidad TIC es parte integral del trabajo del usuario ¿Debe estar la información disponible instantaneamente en operaciones?.

- Clase de trabajo en la Unidad TIC. De acuerdo con las determinaciones anteriores se debe determinar la clase de servicio informático que debe proveer la Unidad TIC ¿Están los negocios de la Entidad orientados a procesamiento de base de datos? ¿Procesamiento computacional científico? ¿Sistemas de control de procesos basados en sensores? Etcétera.
- Grado en que los usuarios participan en el desarrollo y/o implementación de sistemas. Determinar si la actividad de informática es manejada como un centro de servicios, si provee Informática personal técnico, si todo el trabajo de desarrollo es efectuado por la Unidad TIC.
- Proporciones del trabajo de desarrollo de sistemas y mantenimiento. ¿Es la actividad el medio del desarrollo de sistemas mayores? ¿Es el mantenimiento de sistemas y modificaciones de programas la demanda mayor de analistas y programadores?
- Predicción de carga de trabajo y programación. ¿Pueden las operaciones de de la Unidad TIC ser rapidamente programadas? ¿Puede ser la actividad preparada para ser aceptada y dar un rápido giro del trabajo con una muy poca notificación?
- Clase de entradas al sistema de procesamiento. Determinar si los sistemas están orientados a transacciones en línea, tiempo compartido interactivo, etcétera. También si los datos deben ser convertidos a formato procesable.

Responsabilidades de la Unidad TIC

La Unidad TIC tiene autoridad y responsabilidad sobre las siguientes funciones:

- Participar en la elaboración y actualización de los planes de informática a corto, mediano y largo plazo;
- Evaluar y seleccionar equipos, sistemas operativos, programas de apoyo y paquetes de aplicaciones;
- Administrar el centro de computación;
- Controlar la entrada y procesamiento de los datos;
- Producir la información correspondiente a los usuarios y distribuirla oportuna y adecuadamente;
- Diseñar, instalar y afinar las redes de comunicación de datos;
- Desarrollar, implementar y hacer cumplir normas y procedimientos de informática;
- Distribuir los costos de informática a los departamentos usuarios de acuerdo a la política establecida;
- Realizar análisis e investigación sobre sistemas, métodos y equipos que potencialmente puedan mejorar la relación beneficio/costo o ampliar las utilidades de la Institución;
- Velar por la seguridad y confidencialidad de todas las operaciones de informática;
- Evaluar y recomendar adquisiciones de equipos o servicios y contratos externos de procesamiento de datos para toda la Institución;
- Participar en la elaboración del presupuesto de informática;
- Administrar el presupuesto de informática;
- Participar en la evaluación y formulación de prioridades para el desarrollo e implementación de sistemas;
- Reportar periodicamente a la alta gerencia los resultados de sus actividades en sus áreas de responsabilidad;

- Cualquier otra responsabilidad inherente a la Unidad TIC.

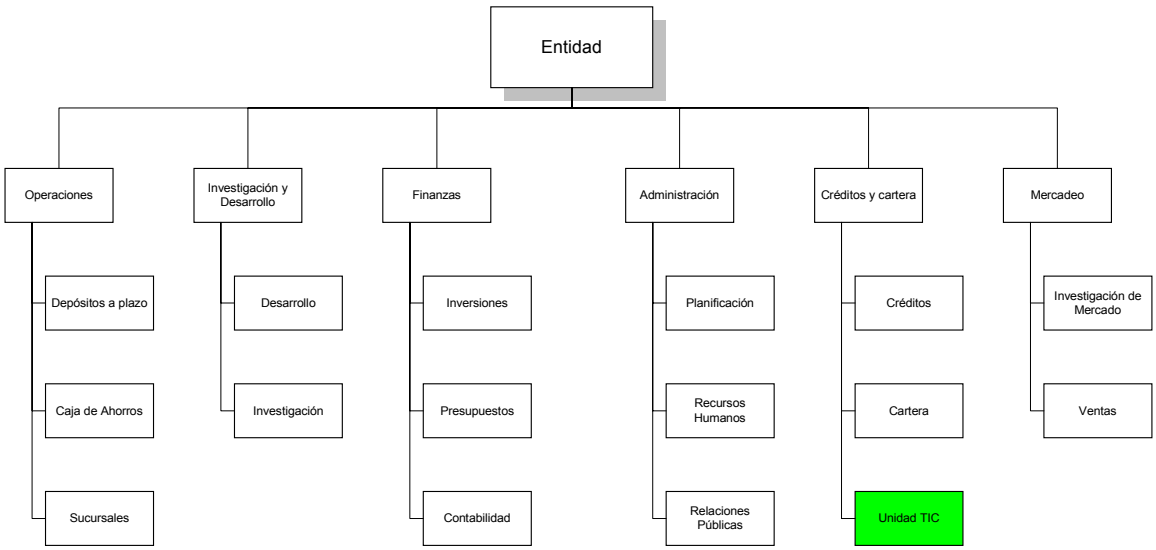
Organización de la Unidad TIC

La naturaleza de servicios provistos por la actividad de informática, hace que la ubicación adecuada del la Unidad TIC, dentro de una organización sea de importancia primaria. Existen tres enfoques básicos que determinan la ubicación de una Unidad de TIC, estos son:

1. Ubicación dentro del departamento que es el mayor usuario.
2. Distribución de pequeñas Unidades TIC dentro de cada departamento usuario.
3. Ubicación dentro del departamento de servicio (generalmente administración), separada de las unidades organizacionales a las cuales presta servicio.
4. Ubicación como un departamento propio, reportando al mismo nivel que los otros departamentos operacionales.

Los siguientes diagramas ilustran ejemplos de estos enfoques.

Figura 1: La Unidad TIC es parte de la unidad que mayor peso tiene en la entidad, no siempre resulta ser la de mayor importancia en el negocio de la entidad.



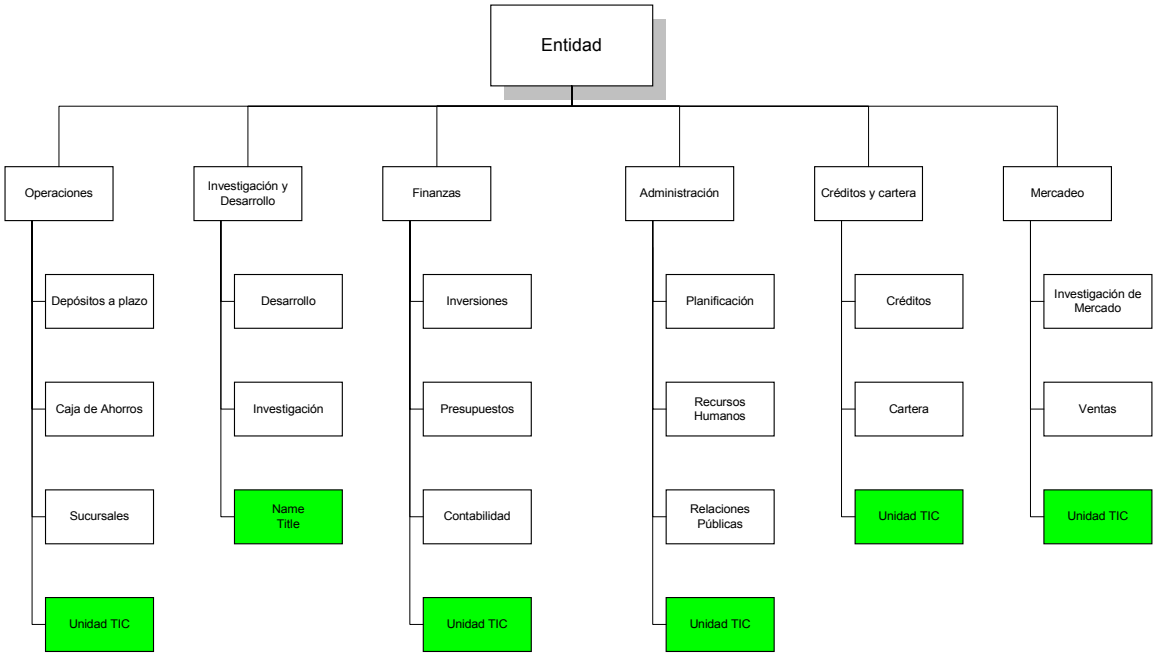
Algunas ventajas.

- Si está ubicada dentro de la unidad más estratégica para la Entidad, el usuario principal tiene el control del servicio, que puede favorecer a la entidad.
- La Unidad TIC puede tener el respaldo pleno de su cliente principal.

Algunas desventajas.

- Las otras unidades son desatendidas por presión de la unidad a cargo de la función de informática.
- Las funciones operativas y administrativas de las otras áreas pueden convertirse en un cuello de botella en la función global de la entidad.

Figura 2: La Unidad TIC es parte de las unidades operativas. Es muy común que esta estructura se derive de la primera a causa de la desigualdad de atención de la Unidad TIC a las diferentes áreas usuarias.



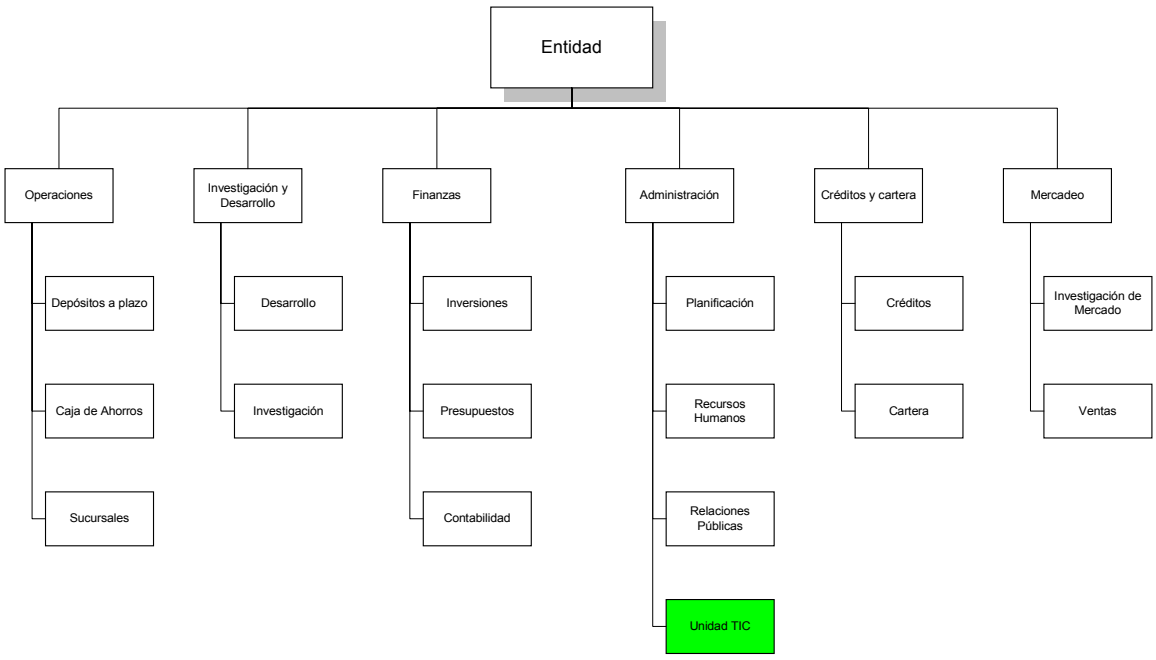
Algunas ventajas.

- Los grupos operacionales tienen el control directo de las facilidades de Informática para las operaciones del día a día.
- Cada Unidad TIC requiere el mínimo necesario de equipamiento y personal para los propósitos que sirve.
- Se enfatiza la contabilidad por centro de costo o ganancia.

Algunas desventajas.

- Puede ser un derroche de personal y recursos de equipos.
- La integración de las funciones de Informática, consolidación de las bases de datos y la coordinación planificada de estas funciones, puede ser dificil.
- La estandarización de políticas y prácticas corporativas para Informática, se hace dificil.
- Medidas especiales son necesarias para ejercer control sobre los sistemas, ya que cada unidad usuaria tiene el control completo sobre todas las fases de procesamiento.

Figura 3. La Unidad TIC es parte de una unidad de servicios.



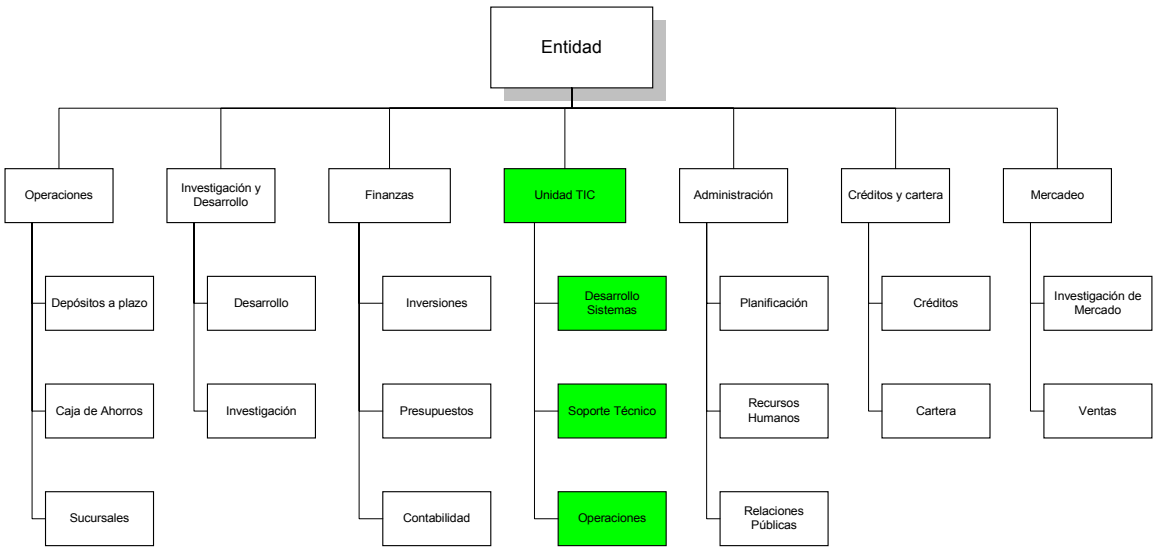
Algunas ventajas

- Todos los departamentos tienen igual consideración de la Unidad TIC.
- Mayor poder de computación puede estar disponible para todo tipo y tamaño de usuario y se tiene una mejor utilización del equipamiento.
- La planificación y desarrollo de sistemas de información esta concentrada y bien integrada.
- La alta gerencia controla la Unidad TIC y sus usos están simplificados.
- El número de gerentes y supervisores necesarios para la actividad total de Informática, es generalmente menor que los necesarios para las unidades separadas.
- Expansión en los requerimientos de cualquier usuario puede en general facilmente ser acomodado dentro de la capacidad existente o mediante adiciones modulares.

Algunas desventajas

- El personal de analistas y programadores centralizados de la Unidad TIC puede no estar suficientemente familiarizado con las necesidades de las áreas operativas; puede ser necesario implementar programas de entrenamiento contínuo.
- Si no hay contabilidad por uso de Informática, el usuario puede llegar a ser desperdiciador en cuanto a la colocación de demandas en el departamento central.
- El establecimiento de las prioridades de los usuarios es un problema dificil y sensitivo.
- A menos que los usuarios mantengan muy bien informado a la Unidad TIC en cuanto a sus planes y demandas esperadas a mediano y largo plazo, la planificación de recursos en la Unidad TIC puede llegar a ser ineficaz.

Figura 4. La Unidad TIC es un departamento independiente.



Algunas ventajas

- La Unidad TIC es un departamento reportando directamente a la cabeza de la organización.
- Disfruta de la misma importancia, independencia y atención gerencial como los otros departamentos.
- Este enfoque y sus variaciones son similares a los enfoques previos, en el cual la actividad de Informática está localizada dentro de un grupo general de soporte.
- Este tipo de ubicación es deseable cuando la actividad de Informática es básica en el logro de los objetivos de la organización; esto es, Informática es el método o sistema de producción.
- El procesamiento de datos es un "service bureau".

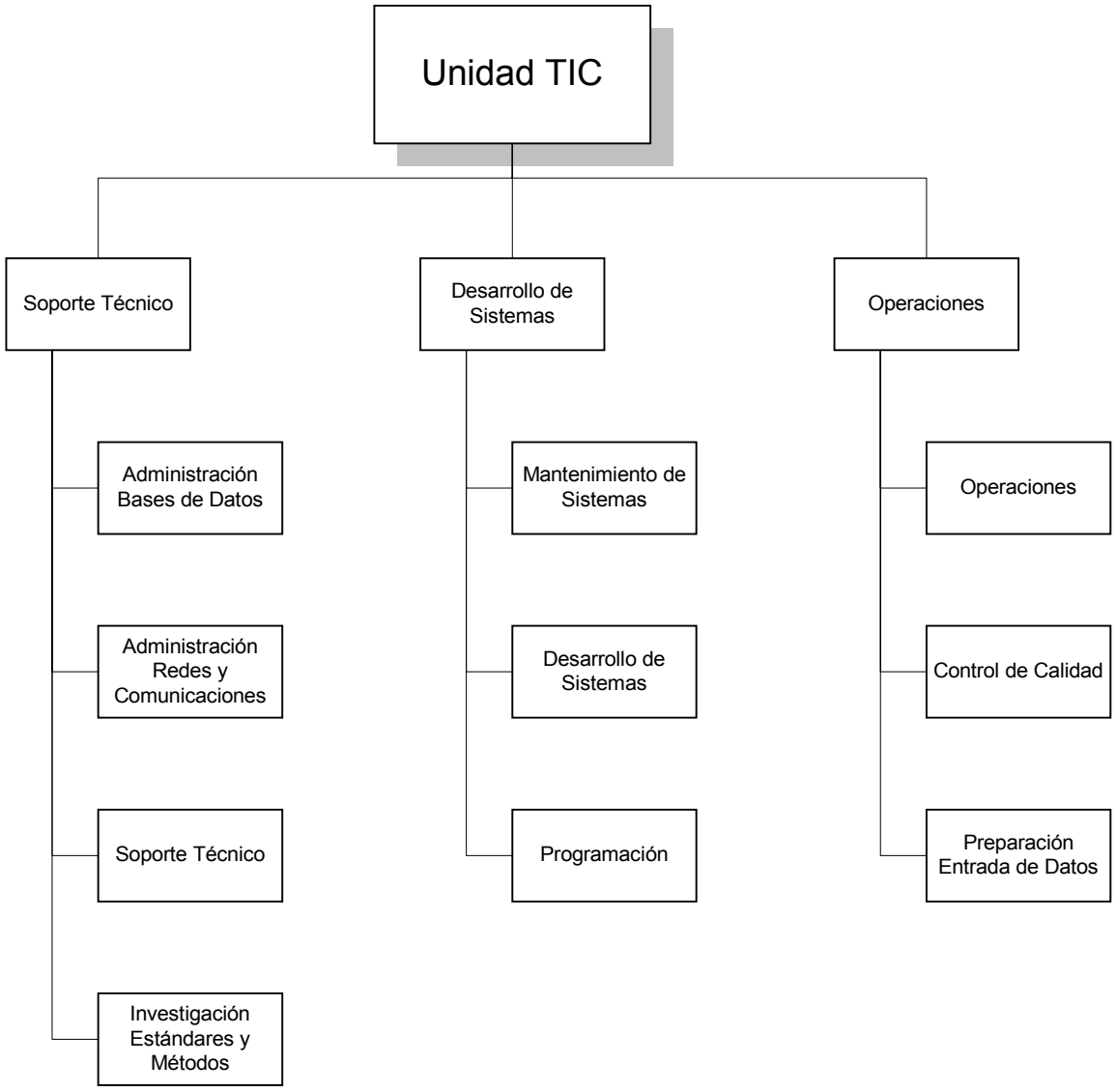
Algunas desventajas

- La alta independencia de la Unidad TIC podría generar, "desvios" de los objetivos del servicio con relación a los de la Institución.

Para entidades financieras con operaciones que dependen en gran medida de los servicios informáticos, es recomendable que la estructura del servicio informático, Unidad TIC, corresponda con el cuarto caso o una variante de este. Se pueden encontrar muchos ejemplos de estos, principalmente en bancos comerciales, compañias de seguros, líneas aéreas, etcétera.

Estructura organizacional interna de la Unidad TIC

El siguiente es un ejemplo de una organización típica para una Unidad TIC, dependiendo de los objetivos y factores señalados previamente, cada área dentro de la estructura tendrá un peso específico.



Funciones de la Unidad TIC

Una estructura organizacional es un agrupamiento lógico de funciones y de la gente que las realiza. Antes que una actividad pueda ser organizada es esencial que sus funciones esten definidas y totalmente entendidas, por quienes las realizan.

Desarrollo de sistemas

Un sistema es definido aqui como un conjunto de programas y procedimientos que operan sobre datos de entrada y archivos para producir resultados deseados. Todo este proceso debe ser guiado por las metodologías y estándares que la entidad haya adoptado para el desarrollo de sistemas.

Cada sistema debe ser:

1. Analizado

2. Diseñado
3. Programado
4. Probado
5. Instalado
6. Mantenido
7. Evaluado periodicamente

Analisis de sistemas. El análisis de las necesidades y recursos para seleccionar y planificar aplicaciones de procesamiento de datos eficaces y el equipamiento y recursos humanos necesarios para realizarlos.

Diseño de sistemas. El diseño detallado y especificaciones de un sistema de procesamiento de datos para realizar los objetivos y requerimientos del sistema previamente definidos.

- Las entradas al diseño del sistema son los requerimientos especificados en el análisis del sistema.
- Las salidas (resultados) en el diseño de sistemas son un conjunto de especificaciones detalladas de las cuales el programador puede proceder con poca o ninguna referencia exterior.

Programación de aplicación. Es la ttraducción de las especificaciones del sistema definido en un proceso lógico y un conjunto de instrucciones de computación para operación de un paso dado dentro del sistema.

Pruebas del sistema. Determinación del éxito de un conjunto completo de programas y procedimientos en alcanzar los requerimientos definidos para el sistema.

Instalación del sistema. Poner un sistema nuevo o modificado en operación.

Mantenimiento del sistema. Efectuar cambios menores a un sistema operacional para cumplir con los requerimientos que surjen en el curso normal de los eventos.

Evaluación del rendimiento del sistema post-instalación (auditoría). Algun momento predeterminado para despues de la instalación del sistema y de tiempo en tiempo durante el ciclo de vida del sistema, mediciones del rendimiento del sistema y evaluación del exito en alcanzar los objetivos y requerimientos originales establecidos.

Operaciones

Las funciones de operaciones en informática pueden ser comparadas a aquellas de una planta de manufactura.

- Programación de equipos
- Mantenimiento de inventarios
- Recepción de ordenes de trabajo
- Preparación de ordenes
- Operación de equipos
- Inspección de productos

- Envio a “usuarios”

En informática podemos agrupar estas tareas en los grupos funcionales siguientes:
1. Programación de eventos y control
2. Operación de equipos
3. Soporte a producción (Control de calidad, Preparación entrada de Datos).

Soporte técnico
Las actividades de informática en la actualidad requieren de un soporte técnico considerable.
- Estandares de procesamiento
- Asistencia técnica
- Sistemas operativos
- Administración de base de datos
- Administración de recursos de teleprocesamiento y comunicaciones
- Administración de los recursos de equipos y sistemas operativos

Gerencia y administración
La gerencia y administración de informática incluye la mayoria de las funciones de supervisión y administración de cualquier actividad operativa compleja. La naturaleza técnica relacionada con desarrollos en la actividad de informática, sin embargo pone énfasis en ciertos aspectos del proceso gerencial.
1. Supervisión y gerencia de proyectos
2. Planificación
3. Seguridad
4. Reportaje e informes
5. Gerencia financiera
6. Gerencia de personal
7. Coordinación - comunicación
8. Soporte administrativo

Posiciones o cargos en informática
Los títulos de posiciones (trabajo) y definiciones de estos, varian de acuerdo a los objetivos de las actividades de informática asi como otros factores en el ambiente, tales como tamaño, clase de desarrollo de sistemas, clase de trabajo a ser ejecutado y la carga de trabajo. Sin embargo es posible definir cierta familia de trabajos y posiciones generalmente asociadas con ellos.
Familia de trabajo son agrupaciones de trabajos que cubren un rango de funciones relacionadas y tienen similares requisitos y calificaciones, habilidades y conocimiento necesario para realizar las funciones.
1. Análisis y diseño de sistemas
2. Programación
3. Operación
4. Soporte técnico
5. Administración

6. Gerencia

1. Análisis y diseño de sistemas. Trabajos en esta familia establecen los requerimientos para sistemas de informática y los diseños de información y procesos. Algunos títulos típicos para estas funciones pueden ser:

- Analista de sistemas
- Diseñador de sistemas
- Analista de sistemas de información gerencial
- Consultor de sistemas
- Analista de procedimientos y métodos

2. Programación. Posiciones en esta familia de trabajo, son responsables de preparar programas operacionales para el computador. Algunos títulos típicos para estas funciones pueden ser:

- Programadores
- Programador de aplicaciones
- Programador de mantenimiento

3. Operación. Esta familia cubre trabajos de personas quienes operan directamente o controlan las operaciones de los equipos de informática. Algunos títulos típicos para estas funciones pueden ser:

- Operador de consola
- Operador de consola maestra
- Operador de equipo periférico
- Operador de terminales
- Programador de carga de trabajo
- Coordinador de producción

4. Soporte técnico. Esta familia de trabajo cubre trabajos de personas cuyo conocimineto técnico y habilidades soportan la actividad total de informática. Algunos títulos típicos para estas funciones pueden ser:

- Administrador de base de datos
- Administrador de comunicaciones
- Programador de sistemas operativos
- Gerente de configuraciones
- Controlador de estandares y procedimientos de informática

5. Administración. Esta familia de trabajo incluye las posiciones que soportan las funciones de informática. Las personas en estos trabajos tienen habilidades que pueden no ser informáticas. Estos trabajos soportan ciertas funciones en operaciones, en desarrollo de sistemas y gerenciales. Algunos títulos típicos para estas funciones pueden ser:

- Oficinista de control
- Oficinista de suministros
- Bibliotecario de operaciones
- Asistente de operaciones

- Bibliotecario técnico
- Asistente de programación
- Coordinador de entrenamiento
- Especialista en presupuesto y costos

6. Gerencia. Esta familia de trabajo incluye posiciones que requieren habilidades gerenciales, asi como experiencia en informática. La persona debe estar calificada en ambos aspectos. Las funciones de supervisión y gerencia son ejecutadas por este grupo. Algunos títulos típicos para estas funciones pueden ser:

- Gerente de informática
- Gerente de desarrollo de sistemas
- Gerente de operaciones
- Gerente de producción
- Gerente de programadores
- Gerente de soporte técnico
- Supervisor de captura de datos
- Supervisor de turno
- Gerente de proyecto
- Especialista de planificación de informática.

Descripción de cargos ó puestos

La siguiente representa una proposición básica de la descripción de cargos o puestos en una organización estructural de la Unidad TIC que incluye las dos divisiones básicas de funciones y descripciones de trabajo de cada una de las áreas establecidas en la misma.

GERENTE DE INFORMÁTICA

El gerente de informática tiene que reportar directamente al Gerente de nivel superior en la estructura de su entidad, por ejemplo, al Gerente Administrativo o al Gerente General. La supervisión del Gerente de Informática es directamente sobre:

- El asistente de Informática
- El Gerente de Desarrollo de Sistemas
- El Gerente de Soporte Técnico
- El Gerente de Operaciones

Descripción del trabajo del Gerente de informática

- Planificar y dirigir todas las actividades de informática de la empresa.
- Preparar planes para mejorar las actividades de la empresa a través de sistemas mejorados o nuevos.
- Dirigir el cumplimiento de los servicios de operaciones, desarrollo y producción mediante enlace con usuarios de informática.
- Proveer soporte para mejorar las actividades organizacionales mediante métodos mejorados y técnicas con la utilización de mejores recursos tecnológicos.
- Organizar los recursos de informática para proveer servicios eficientes y útiles a los usuarios.

Responsabilidades del Gerente de Informática

- Proveer sistemas y servicios computacionales eficientes y seguros para cumplir con las necesidades organizacionales.
- Desarrollar y entrenar al personal de informática.
- Comunicar a la alta gerencia de los progresos en el desarrollo de los proyectos, utilización de recursos y rendimiento de producción.
- Proyectar los requerimientos de recursos de informática, incluyendo personal, equipos y provisiones asociados con costos y coordinarlos con el ciclo de planificación y presupuesto de la entidad.
- Medir de rendimiento del personal, equipos y sistemas.
- Evaluar nuevas técnicas de desarrollo con vista en los planes y objetivos de la organización.

Obligaciones y deberes del Gerente de Informática

- Planificar y participar en la educación gerencial en sistemas y conceptos de procesamiento de datos.
- Analizar la utilización de recursos e iniciar programas de mejoramiento.
- Identificar áreas potenciales de mejoras a través de sistemas mejorados y nuevos.
- Evaluar sistemas propuestos y recomendar las acciones apropiadas.
- Revisar requisiciones para servicios adicionales de informática e identificar sus impactos en recursos actuales y planificados.
- Evaluar la tecnología de nuevos equipos y sistemas y valorar su aplicabilidad a los requerimientos de la organización.
- Informar a la alta gerencia lo relacionado al rendimiento de los recursos de personal y equipos, e identificar tendencias importantes.
- Aplicar métodos de análisis de costo / beneficio de aplicaciones en uso y configuraciones de equipos y sistemas operativos, estructura organizacional y administración de personal.
- Supervisar el trabajo de la Unidad TIC.
- Contratar y desarrollar personal para Unidad TIC.
- Controlar y planificar las redes y comunicación.
- Desarrollar e implementar aspectos de seguridad en informática.

Experiencia requerida para el Gerente de Informática

- Licenciado o Ingeniero en Informática.
- Entrenado en prácticas gerenciales avanzadas, habilidades y conceptos, gerencia administrativa, control de proyectos, técnicas avanzadas de análisis y diseño.
- Tener mínimo dos a tres años de experiencia comparable al asistente de Gerente de informática.
- Tener de seis a ocho años de experiencia laboral en informática
- Tener conocimiento del idioma ingles.

GERENTE DE DESARROLLO DE SISTEMAS

El Gerente de Desarrollo de Sistemas reporta directamente al Gerente de Informática. La supervisión del mismo es directamente sobre:

- Mantenimiento de sistemas
- Desarrollo de sistemas
- Programación

Descripción del trabajo del Gerente de Desarrollo de Sistemas

- Dirigir las actividades del desarrollo de sistemas de la Unidad TIC, incluyendo análisis de sistemas, dirección de sistemas, diseño de sistemas y programación.
- Planificar y administrar una plana calificada de analistas y programadores.
- Proporcionar servicios de planificación, consultoría y asesoría en desarrollo de sistemas a los departamentos usuarios.
- Vigilar proyectos de largo alcance para desarrollo o modificación mayor de sistemas de información, desde su concepción hasta su implantación operacional total.

Responsabilidades del trabajo del Gerente de Desarrollo de Sistemas

- Ejecutar con éxito los proyectos de desarrollo de sistemas de información y modificaciones a tiempo y dentro del presupuesto.
- Mantener una plantilla adecuada y calificada de especialistas en desarrollo de sistemas y programación, para servir como recurso técnico clave en la institución.
- Utilizar de forma efectiva los recursos de desarrollo de sistemas en cumplir los planes y objetivos de sistemas de información de la organización.

Obligaciones y Deberes del Gerente de Desarrollo de Sistemas

- Supervisar las funciones que le reportan.
- Planificar el nivel de recursos necesarios en cada función y proveer el personal adecuado por selección y entrenamiento.
- Planificar y procurar el uso de metodologías y herramientas de desarrollo modernas y apropiadas para la institución.
- Establecer la programación general y prioridades para los proyectos de desarrollo de sistemas y servicios de soporte.
- Revisar los resultados de los sistemas desarrollados, tomar acciones necesarias.
- Informar y asesorar al gerente de informática de los planes, proyectos y funciones bajo su responsabilidad.

Experiencia requerida para el Gerente de Desarrollo de Sistemas

- Licenciado o Ingeniero en Informática (Programación de Lenguajes y Bases de datos)
- Entrenado en prácticas gerenciales avanzadas, habilidades y conceptos, gerencia administrativa, control de proyectos, técnicas avanzadas de análisis y diseño.
- De seis a ocho años en el área de informática con responsabilidad de gerencia de desarrollo de sistemas.
- Dominio de metodologías de análisis y diseño de sistemas.
- Dos años mínimo de experiencia comparable a: Gerente de Análisis y Diseño de Sistemas, Gerente de Programación o Gerente de Sistemas Operacionales.

- Conocimiento del idioma Ingles.

Analista Programador

El Analista Programador reporta directamente al Gerente de Desarrollo de Sistemas y tiene responsabilidad sobre su propio trabajo y sobre los analistas y programadores a su cargo durante la ejecución de proyectos, si éste es lider del proyecto. Las funciones de Analistas programdores son similares tanto en tareas de desarrollo como de mantenimiento de sistemas.

Descripción del trabajo del Analista Programador

- Liderar por encargo del Gerente de Desarrollo de Sistemas, proyectos específicos de sistemas.
- Diseñar y desarrollar los programas de los sistemas.
- Dar un mejor mantenimiento a los programas, códigos de los programas. Preparar los diagramas de flujos y codificación de rutinas para el procesamiento de datos. Realizar la programación de tareas según las normas establecidas y completar las pruebas del funcionamiento de los programas e integración con otros.
- Documentar los sistemas y programas de acuerdo a metodologías y estándares establecidos por la entidad.

Responsabilidades, obligaciones y deberes del trabajo del Analista Programador

- Diseñar y desarrollar eficazmente los programas que requiera el sistema.
- Mantener el conocimiento actual del sistema con un lenguaje estándar codificando los métodos y requisitos del funcionamiento.
- Evaluar completamente los programas.
- Analizar las especificaciones del programa para la integridad y conformidad a las normas establecidas.
- Tener la programación en el idioma adecuado.
- Documentar los programas de acuerdo a las normas y estándares de la institución.
- Entregar los reportes requeridos por la administración.
- Preparar una evaluación de los datos y una prueba de codificación de los programas para validar la exactitud.

Experiencia requerida para el Analista Programador

- Licenciado o Ingeniero en Informática.
- Habilidad en diseñar y programar en base de datos actuales.
- Fuertes fundamentos de metodologías de diseño y programación.
- Conocimientos completos de base de datos y herramientas automatizadas de diseño y desarrollo de sistemas.

Programador

El Programador reporta regularmente al Gerente de Desarrollo de Sistemas, sin embargo, durante el ciclo de ejecución de un proyecto de sistemas reporta al lider del proyecto, por lo general un Analista Programador.

Descripción del trabajo del Programador

- Apoyar al Analista Programador en Diseñar los programas de los sistemas.
- Programar los sistemas de la institución.
- Dar un mejor mantenimiento a los programas, códigos de los programas. Preparar los diagramas de flujos y codificación de rutinas para el procesamiento de datos. Realizar las pruebas del funcionamiento de los programas y su integración con otros.
- Documentar los sistemas y programas de acuerdo a metodologías y estándares establecidos por la entidad.

Responsabilidades, obligaciones y deberes del trabajo del Programador

- Desarrollar eficazmente los programas que requiera el sistema.
- Mantener el conocimiento actual del sistema con un lenguaje estándar codificando los métodos y requisitos del funcionamiento.
- Evaluar completamente los programas.
- Analizar las especificaciones del programa para la integridad y conformidad a las normas establecidas.
- Tener la programación en el idioma adecuado.
- Documentar los programas de acuerdo a la instalación estándar.
- Entregar los reportes requeridos por la administración.
- Preparar una evaluación de los datos y una prueba de codificación de los programas para validar la exactitud.

Experiencia requerida para el Programador

- Graduado en Ingeniería o Licenciatura de Sistemas, o como Técnico Superior en Informática.
- Habilidad en programar en base de datos actuales con fuertes fundamentos de programación, conocimientos completos de base de datos.
- Habilidad en programación avanzada en base de datos recientes.
- Habilidad de elaboración de manuales de los programas elaborados en un idioma adecuado y estándar.
- Habilidades de diseños de programas e integración de los mismos.
- Habilidad en desarrollo de sistemas en herramientas modernas orientadas a objetos.
- Habilidad en desarrollo de sistemas en las herramientas específicas empleadas por la institución.

GERENTE DE SOPORTE TÉCNICO

El gerente de soporte técnico reporta directamente al Gerente de Informática y supervisa directamente los trabajos de:

- Administradores y operadores de red y comunicaciones
- Adminsitradores de Bases de datos
- Oficiales de soporte técnico y servicio a usuarios
- Oficiales de investigación, estándares y métodos

Descripción del trabajo del Gerente de Soporte Técnico

- Programar las actividades de administración, mantenimiento y soporte técnico de todos los componentes tecnológicos empleados en la entidad.
- Controlar y administrar el acceso y buen uso de los sistemas y equipos por parte de los usuarios.
- Verificar las actividades de soporte técnico de todo el departamento de informática y la entidad, incluyendo red local como red de comunicación, sistemas operativos, administración de base de datos, administración y evaluación de sistemas (operativos) y servicios de soporte y limpieza.
- Inventariar todo equipo de Software y Hardware.
- Impartir capacitaciones a personal en el cual se detecte deficiencia en alguna área de los sistemas que ocupan en el quehacer diario.

Responsabilidades del trabajo del Gerente de Soporte Técnico

- Mantener en buen funcionamiento las estaciones de trabajo, servidores, impresores, UPS, equipos de comunicaciones y cualquier otro equipo del cual la entidad posea.
- Mantener en buen resguardo la información y sistemas de la entidad, administrando los accesos a las mismas.
- Instalar y administrar las redes locales y de comunicación.
- Suministrar y transmitir a otros en el departamento de tener conocimiento y experiencia en informática y sus técnicas.

Obligaciones y deberes del Gerente de Soporte Técnico

- Supervisar las funciones que le reportan.
- Planificar el nivel de soporte técnico necesario en cada función.
- Seleccionar personal calificado para ese nivel de soporte y entrenar personal existente y nuevo cuando y como sea requerido.
- Establecer la programación general y prioridades para la operación de sistemas operativos, comunicaciones, base de datos, aplicaciones de la institución, estándares y otros proyectos de soporte.

Experiencia requerida para el Gerente de Soporte Técnico

- Licenciado o Ingeniero en Informática.
- Entrenamiento en prácticas gerenciales.
- Un mínimo de dos años de experiencia en el área de Soporte Técnico.
- Completamente familiar con el diseño, programación, mantenimiento, instalación, configuración de programas de computación.
- Completamente familiar con la instalación y funcionamiento de redes, sistemas operativos y bases de datos.
- Conocimiento del idioma ingles.

Administrador de Base de Datos

El Administrador de Base de Datos reporta directamente al Gerente de Soporte Técnico y tiene responsabilidad sobre su trabajo.

Descripción del trabajo del Administrador de Bases de Datos

- Administrar y mantener en funcionamiento adecuado las bases de datos de la entidad
- Afinar y ajustar el funcionamiento de las bases de datos de acuerdo a los parámetros establecidos por el proveedor de las mismas,
- Administrar el buen uso y acceso de los usuarios a las bases de datos institucionales
- Asistir o asesorar a los funcinonarios de la Unidad TIC en el uso de las mejores técnicas de acceso y uso de las bases de datos.

Responsabilidades, obligaciones y deberes del trabajo del Administrador de Bases de Datos

- Mantener siempre disponibles las bases de datos para el uso apropiado de la información institucional
- Asegurar la capacidad de operación sin interrupciones de las bases de datos institucionales
- Asegurar la aplicación de procedimientos de respaldo y recuperación de la información de las bases de datos
- Apoyar la investigación de herramientas adecuadas para el uso y explotación de la información institucional.

Experiencia requerida para el Administrador de Bases de Datos

- Ingeniero o Licenciado en Sistemas.
- Experiencia en bases de datos relacionales de última generación.
- Habilidad para afinar y depurar bases de datso relacionales.
- Capacidad para crear los procedimientos de la seguridad y permisos de acceso a los datos con que contaran los usuarios.
- Habilidad de anticipar cualquier problema que pueda surgir en la administración de las bases de datos.

Administrador de Redes y Comunicaciones

El Administrador de Redes y Comunicaciones reporta directamente al Gerente de Soporte Técnico.

Descripción del trabajo del Administrador de Redes y Comunicaciones

- Administrar y mantener en buen estado de funcionamiento la red nacional y las redes locales existentes en toda la institución.
- Instalar y mantener el hardware y software que es necesario dentro de la red.
- Elaborar el diseño y la arquitectura de las redes.
- Monitorear y evaluar el trafico de las redes utilizando las herramientas necesarias.
- Implementar la mejor seguridad y los permisos adecuados para los usuarios en la red.
- Controlar los recursos de acceso de cada uno de los usuarios desarrollando encriptaciones de entrada a la red.
- Elaborar manuales de respaldo y recuperación de la red.
- Elaborar planes de entrenamiento para el mejor uso de las redes.

Responsabilidades, obligaciones y deberes del trabajo del Administrador de Redes y Comunicaciones

- Mantener en funcionamiento regular las redes de la institución.
- Mantener segura y libre de daños e intrusiones las redes de la institución.
- Poner a la disposición de los usuarios los impresores, aplicaciones y datos, y todos los recursos compartidos de las redes que estos tienen que utilizar.

Experiencia requerida para el Administrador de Redes y Comunicaciones

- Ingeniero en telecomunicaciones o similar.
- Habilidad en los conocimientos necesarios que posee el sistema operativo que estará a cargo del manejo de la red.
- Habilidad en los conocimientos del software que se utilizara para proveer la comunicación de los usuarios
- Capacidad para crear los procedimientos de la seguridad y permisos con los que contaran las redes.
- Habilidad de anticipar cualquier problema que pueda surgir en la administración de las redes.
- Conocimiento de sistemas operativos y aplicativos, instalación de equipo de hardware, habilidad con el manejo de sistemas de comunicaciones.

Oficial de Soporte Técnico

El oficial de Soporte Técnico reporta diréctamente al Gerente de Soporte Técnico y tiene responsabilidad sobre su propio trabajo.

Descripción del trabajo del Oficial de Soporte Técnico

- Mantener en buen funcionamiento las estaciones de trabajo, servidores, impresoras, UPS, equipos de comunicaciones de datos y cualquier otra clase de hardware.
- Transmitir a otros departamentos los conocimientos y experiencia en el área de computación, relacionada al buen uso de los equipos.
- Instalar software: sistemas operativos, software de escritorio y las herramientas necesarias, en las estaciones de trabajo.
- Inventariar todo el equipo de software y hardware de la institución.
- Impartir capacitaciones al personal cuando se detecte deficiencia en alguna área de los sistemas y herramientas que deben usar para su trabajo.
- Establecer prioridades para sistemas operativos y comunicaciones

Responsabilidades, obligaciones y deberes del trabajo del Oficial de Soporte Técnico

- Mantener el buen funcionamiento de las estaciones de trabajo, servidores, impresoras, UPS y cualquier otra clase de hardware.
- Dar el mejor soporte a los usuarios en cualquier problema que ocurra con el equipo en el que trabajan, mantenimiento y limpieza de todo el equipo que se encuentra instalado en la institución, instalación de máquinas, impresoras, scanner, etc.
- Mantener actualizados a los usuarios en el uso de equipos, software y herramientas de estaciones de trabajo.

- Controlar el uso de software autorizado en cada una de las estaciones de trabajo.

Experiencia requerida para el Oficial de Soporte Técnico

- Graduado en Ingenieria de Sistemas, Informática o Técnico Superior
- Conocimiento de sistemas operativos, software y herramientas de escritorio, habilidad de instalación en cualquier máquina, conocimiento de limpieza física de equipos, de archivos y habilidades de impartir capacitaciones.
- Habilidad de arreglar cualquier problema que pueda enfrentarse en las estaciones de trabajo, impresores o cualquier otro tipo de hardware.
- Habilidad de elaboración de un plan de mantenimiento adecuado para cada una de las estaciones de trabajo y equipo que se encuentre en las oficinas.
- Capacidad de crear los procedimientos para las capacitaciones necesarias para los usuarios.

Oficial de Investigación, Estándares y Métodos

El Oficial de Investigación reporta directamente al Gerente de Soporte Técnico, es responsable de su propio trabajo, sin embargo, interactúa permanentemente con los oficiales de las otras áreas de la Unidad TIC.

Descripción del trabajo del Oficial de Investigación, Estándares y Métodos

- Investigar los mejores estándares, métodos y herramientas tecnológicas para el desarrollo de las actividades de informática en la entidad.
- Evaluar el uso de las herramientas tecnológicas en la Unidad, a objeto de determinar su utilidad práctica.
- Capacitar a los oficiales de la Unidad y de otras unidades operativas, en el mejor uso de los estándares, metodologías y herramientas.

Responsabilidades, obligaciones y deberes del trabajo del Oficial de Investigación, Estándares y Métodos

- Mantener actualizados, de acuerdo al avance tecnológico y la viabilidad de su uso, los mejores estándares, métodos y herramientas tecnológicas, que emplea la Unidad TIC.
- Sugerir mejoras y/o cambios en las herramientas tecnológicas en la Unidad, a objeto de mejorar su utilidad práctica.
- Mantener actualizados a los oficiales de la Unidad y de otras unidades operativas, en el mejor uso de los estándares, metodologías y herramientas.

Experiencia requerida para el Oficial de Investigación, Estándares y Métodos

- Ingeniero o Licenciado en Sistemas.
- Habilidad en organización, métodos y en manejo de proyectos.
- Conocimientos profundos de las herramientas tecnológicas empleadas en la entidad.
- Habilidad para desarrollar procedimientos para los procesos de la Unidad TIC.
- Conocimiento de sistemas operativos, bases de datos, aplicativos y herramientas en uso en la entidad.
- Habilidad para transmitir conocimientos técnicos.

GERENTE DE OPERACIONES

El Gerente de Operaciones reporta directamente al Gerente de Informática y tiene responsabilidad sobre las siguientes funciones:

- Administradores y Operadores de sistemas
- Oficiales de Control de Calidad
- Oficiales de Entrada de Datos

Descripción del trabajo del Gerente de Operaciones

- Planificar y programar la operación de los equipos y procesos automatizados de la entidad.
- Planificar y programar la incorporación, puesta en marcha y operación de todos los equipos en la entidad.
- Verificar la ejecución de registro, procesamiento y control de calidad realizadas por sus oficiales.

Responsabilidades, obligaciones y deberes del trabajo del Gerente de Operaciones

- Asegurar que los procesos regulares de la entidad se llevan a cabo regularmente.
- Asegurar que los equipos computaciones operan regularmente, de acuerdo a lo programado.
- Asegurar que la información producida por las aplicaciones de la entidad tienen la calidad esperada, de acuerdo a los estándares definidos para ella.
- Asegurar que todos los datos necesarios son registrados en los sistemas o aplicativos y que toda la información necesaria es producida.

Experiencia requerida para el Gerente de Operaciones

- Ingeniero o Licenciado en Informática.
- Habilidades de gestión y administración de personal.
- Habilidades en programación de operaciones.
- Conocimientos de sistemas operativos, bases de datos y herramientas en uso en la entidad.

Operador

El Operador reporta directamente al Gerente de Operaciones, y es reponsable de su propio trabajo.

Descripción del trabajo del Operador

- Operar las aplicaciones de la entidad.
- Generar los reportes y productos regulares de las aplicaciones de la entidad
- Operar los equipos servidores y periféricos de uso compartido.

Responsabilidades, obligaciones y deberes del trabajo del Operador

- Asegurar que la información es producida a tiempo, y de acuerdo con los estándares de producción de la Unidad TIC.

- Asegurar que los equipos servidores y periféricos están operables y disponibles para los usuarios.

Experiencia requerida para el Operador

- Graduado en Ingeniería, Informática, o Técnico Superior
- Conocimientos profundos de sistemas operativos.
- Conocimientos de bases de datos y de la red de comunicaciones
- Conocmientos de las aplicaciones de la entidad

Oficial de Control de Calidad

El Oficial de Control de Calidad reporta directamente al Gerente de Operaciones, y es reponsable de su propio trabajo.

Descripción del trabajo del Oficial de Control de Calidad

- Verificar la calidad de los datos que alimentan las aplicaciones de la entidad.
- Verificar la calidad de la información que se genera en los reportes y productos regulares de las aplicaciones de la entidad.

Responsabilidades, obligaciones y deberes del trabajo del Oficial de Control de Calidad

- Asegurar que la información es producida con calidad, y de acuerdo con los estándares de producción de la Unidad TIC.
- Asegurar que los datos que alimentan las aplicaciones cumplen con los estándares de calidad de las mismas.

Experiencia requerida para el Oficial de Control de Calidad

- Técnico Superior en Informática.
- Conocimientos de sistemas operativos.
- Conocimientos de bases de datos y de la red de comunicaciones.
- Conocmientos de las aplicaciones de la entidad.

Oficial de entrada de datos

El Oficial de Entrada de Datos reporta directamente al Gerente de Operaciones, y es reponsable de su propio trabajo.

Descripción del trabajo del Oficial de Entrada de Datos

- Realizar la carga de datos (transcripción) que alimentan las aplicaciones de la entidad.

Responsabilidades, obligaciones y deberes del trabajo del Oficial de Control de Calidad

- Asegurar que los datos son cargados con calidad y precisión, de acuerdo con los estándares de producción de la Unidad TIC.

Experiencia requerida para el Oficial de Control de Calidad

- Técnico Superior en Informática.

- Conocimientos de sistemas operativos.
- Conocimientos de bases de datos y de la red de comunicaciones.
- Conocimientos de las aplicaciones de la entidad.

La Paz, Enero de 2003.