UNIVERSIDAD DE COSTA RICA

SISTEMA DE ESTUDIOS DE POSGRADO

PROGRAMA DE POSGRADO EN MAESTRÍA EN DIRECCIÓN DE EMPRESAS

"AUDITORÍA DE LOS SISTEMAS ADMINISTRADORES DE BASE DE DATOS"

TRABAJO FINAL DE INVESTIGACIÓN APLICADA, SOMETIDO A LA COMISIÓN DEL PROGRAMA DE ESTUDIOS DE POSGRADO EN DIRECCIÓN DE EMPRESAS, PARA OPTAR POR EL GRADO DE *MAGÍSTER EN AUDITORÍA DE TECNOLOGÍAS DE INFORMACIÓN.*

Autor

LUIS ANTONIO SEGURA SUÁREZ

Ciudad Universitaria Rodrigo Facio, San José, Costa Rica

2007

Dedicatoria

Desde lo más profundo de mi propio ser, ofrezco este proyecto a la persona que hace muchos años me trajo al mundo. Ella sin ningún interés desde mi nacimiento se ha preocupado y ha buscado lo mejor para mí, por eso hoy le agradezco de todo corazón.

Comenzando con los primeros pasos en ámbito de la educación: escuela, colegio y posteriormente en la universidad, siempre has estado ahí. En este caminar se ha sentido un apoyo, una colaboración, una compresión y un sin número de consejos en todos los momentos buenos y malos.

Principalmente, doy gracias a Dios por haber puesto en el camino una madre tan ejemplar y buena, digna de imitar. Este y todos los éxitos en la vida estarán marcados con su imagen.

Gracias Madre.

Agradecimientos.

Correspondo a Dios por darme su fortaleza para mantenerme firme en cada una de mis metas. En esta lucha he logrado superar los momentos más difíciles, porque siempre se cuenta con su apoyo incondicional.

Nunca, se podría dejar de lado a todas aquellas personas que de una ú otra manera han brindado su apoyo y ayuda sin esperar nada a cambio; sin ellos jamás se hubiera llegado hasta la cúspide de la montaña. No podemos mencionar nombres, pues sería injusto dejar alguna persona sin agradecer su colaboración.

Por eso, no queda más que pedir a Dios bendición, fortaleza y protección para la vida de todas estas personas.

Hoja de Aprobación del Trabajo Final de Investigación Aplicada

Este Trabajo Final de Investigación Aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Dirección de Empresas de la Universidad de Costa Rica, como requisito para optar por el grado de Magíster en Auditoría de Tecnologías de Información.

Máster Xiomar Delgado Rojas
Tutor

Máster Yorleny Salas Araya
Lectora

Licenciado Ronny La Touche Arguello
Empresa

Doctor Aníbal Barquero Chacón
Director de Programa de Estudios de Posgrado en Dirección de Empresas

Licenciado Luis Antonio Segura Suárez
Sustentante

CONTENIDO CAPITULARIO

LISTA DE GRÁFICOS

LISTA DE TABLAS

PRÓLOGO

I. Tema.

Auditoría de los Sistemas Administradores de Base de Datos (DBMS) en el Instituto Nacional de Aprendizaje (INA).

CAPÍTULO I

Aspectos introductorios

I. Introducción al tema.

Actualmente la información es el principal activo de toda organización. Tal es así, que día con día el procesamiento y manejo de la información se realiza de manera automatizada. Los Sistemas Administradores de Base de Datos juegan un papel crucial en este proceso.

II. Justificación del tema.

Las bases de datos contienen información sensitiva y privada, por lo que deben ubicarse en un lugar seguro. Si esto no sucede, muchas actividades incorrectas podrían pasar, ya que personas no autorizadas podrían acceder de manera inapropiada la información, por algún método. Para evitar esto, se debe lograr mantener monitoreado el acceso y privacidad de los datos. Pero, esto es solamente parte de las actividades que involucra el proceso. La protección de la información no es una ocurrencia, sino una exigencia por regulaciones internacionales, como lo son el HIPAA, Sarbanes Oxley Act, Gram-Leanch-Bliley.

Algunas de estas organizaciones exigen grabar y monitorear el acceso a la información confidencial. Por ejemplo, una empresa de gran tamaño debe guardar las pistas de auditoría de los 365 días del año por varios años; por ello se puede deducir que se requiere gran capacidad de almacenamiento, pero, lo peor es que la información debe estar accesible y debe ser completa. Por tanto, se debe definir un mecanismo de respaldo adecuado que permita administrar el alto volumen de almacenamiento provocado por la alta frecuencia de acceso.

Otras organizaciones asientan sobre la organización: la responsabilidad y contabilidad de los datos. Por tal razón, las empresas deben establecer medidas de control que requieren evidencia de seguridad y control sobre el tiempo, establecer medidas de control que permitan monitorear amenazas, tanto internas como externas, de accesos sin autorización, todo bajo la filosofía de que la información sea completa sobre el acceso a la base de datos, entre esto las pistas de auditoría.

Por otro lado, dentro de la administración de las Tecnologías de Información, es necesario considerar diferentes aspectos para mantener el funcionamiento dentro de los márgenes normales. La mayoría de empresas consideran que lo más importante es mantener su buena reputación. Para ello, los siguientes elementos serían críticos:

- ✓ Evitar riesgos del negocio y conjuntos de demandas de los clientes y socios.
- ✓ Implementar las mejores prácticas, con ello satisfacer a los auditores.
- ✓ Evitar penas civiles y criminales.
- ✓ Seleccionar la mejor propuesta de auditoría.

En la selección o desarrollo de una política de seguridad, se debe considerar el desarrollo de un marco de auditoría como un sistema homogéneo que expande las diferentes aplicaciones. Pero, lo más importante es cuánto valor genera para la organización.

En las organizaciones surge la necesidad de las auditorías, tanto internas como externas. Buscan que personas que no se relacionan directamente con la actividad, puedan emitir opiniones válidas referentes a la correcta operación y funcionamiento de un área o proceso específico de la organización. Adicionalmente, en el momento en que exista o se determine una

oportunidad de mejorar, se expongan las recomendaciones que ayuden a incrementar el valor del área hacia o para a la organización.

Es así, que se llega a la conclusión de que los Sistemas Administradores de Base de Datos son una parte esencial del funcionamiento de la infraestructura de las Tecnologías de la Información y de toda organización. Por tanto, se decidió seleccionar esta área para la realización del proyecto práctico de auditoría. Para tal efecto, se cuenta con los conocimientos y herramientas necesarias para poder llevar a cabo el proceso de evaluación del área.

III. Objetivos.

III.I. Objetivo General.

Realizar una auditoría de los sistemas de administración de base de datos, para determinar la seguridad y una administración razonable de las fuentes de información automatizadas, mediante los sistemas gestores de base de datos en el Instituto Nacional de Aprendizaje.

III.II. Objetivos específicos.

- Conocer aspectos generales de la infraestructura de tecnologías de información y de la organización para fundamentar la auditoría.
- Identificar aspectos críticos de éxito del área de base de datos para su evaluación.
- Determinar oportunidades de mejora del proceso de administración de los sistemas administradores de base de datos para proponer su implementación.

- Generar las conclusiones y recomendaciones del proyecto de auditoría para sintetizar los resultados.

IV. Alcance o delimitación.

El estudio abarcará la evaluación de los sistemas administradores de base de datos en el INA. Este estudio se centrará los DBMS ubicados en la Unidad de Informática y Telemática, sita en La Uruca. Éste se realizará con base en las mejores prácticas de administración y seguridad de Tecnologías de Información (TI) al 10 de agosto de 2007, con la finalidad de lograr determinar la eficiencia y eficacia con que se trabaja, para asegurar una disponibilidad y seguridad razonable de la información en las bases de datos.

Marco Teórico/Posicionamiento Teórico.

Para lograr entender el marco en que se desarrolla el proyecto, es necesario conocer algunos aspectos o conceptos generales relacionados; en este caso, específicamente base de datos, sistema administrador de base de datos y auditoría.

I. Base de Datos.

Michael J. Hernández la define así: “Una base de datos es una colección organizada de datos usada para el propósito de modelar algún tipo de organización o proceso organizacional”. (Hernández, 2003, p. 4)

II. Sistema Administrador de Base de Datos.

Un Sistema Gestor de Base de Datos “es un software computacional usado para crear, almacenar, recuperar, cambiar, manipular, clasificar, dar formato, e imprimir información dentro de una base de datos. Además, es el

software que controla la organización, el almacenamiento, la recuperación, la seguridad, y la integridad de los datos dentro de una base de datos" (Vallabhaneni, 2006, p 1301).

En otras palabras, es el software que sirve de interfaz entre la Base de datos y el usuario, o sea las aplicaciones que la utilizan.

III. Auditoría.

El Instituto de Auditores Internos define la Auditoría como "una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno".

Esta auditoría revisa la confiabilidad e integridad de la información, cumplimiento con políticas y regulaciones, la salvaguarda de activos, el uso económico y eficiente de los recursos y que se hayan establecido objetivos y metas operacionales. Igualmente, evalúa las actividades financieras y operaciones incluyendo los sistemas de producción, ingeniería, mercadeo y recursos humanos.

IV. Auditoría de TI.

Por otro lado se ha estudiado en los diferentes cursos de maestría, la auditoría de TI que difiere por su enfoque a las Tecnologías de Información. Esta se puede definir como "*el proceso mediante el cual se evalúa el cumplimiento de los criterios de gestión y control de los recursos tecnológicos de información de una empresa o entidad, con el propósito de concluir sobre el*

grado de economía y eficiencia en la adquisición y uso, y sobre la eficacia para producir información pertinente al negocio, íntegra, correcta, confiable, confidencial y oportuna, para la toma de decisiones de la organización, bajo criterios de ética, legalidad y cuidado por el ambiente".

Y como resultado de este proceso se espera coadyuvar a los miembros de la organización para un desempeño efectivo de sus responsabilidades.

V. Metodología

Durante todo el desarrollo de la maestría se estudio la metodología de auditoria que se aplicará al proyecto en cuestión. Esta metodología se compone para nuestro proyecto de tres etapas:

1. Planificación
2. Examen
3. Comunicación de Resultados

V.I. Planificación

En esta etapa se pretenderá asegurar la atención apropiada a áreas significativas, identificar los problemas potenciales y el trabajo será completado en forma expedita y la apropiada asignación y coordinación del trabajo del o de los integrantes del equipo. Los objetivos en esta etapa son:

- Lograr un conocimiento del área o áreas de indagación
- Preparar y ejecutar una evaluación preliminar de las áreas de indagación
- Determinar las posibles áreas de críticas
- Preparar un Plan de Auditoría y los correspondientes Programas para la evaluación de las áreas críticas.

V.II. Examen

En esta fase, se realizará un mapeo del universo de controles asociados a cada uno de los procesos que se ejecutan en el área seleccionada (sistemas de administración de base de datos) como área de potencial interés, con el fin de determinar los controles aplicables en operación. Identificados los controles en operación, éstos serán evaluados mediante la aplicación de guías o listas de verificación, diagramas de flujo, cuestionarios de control, técnicas de auditoría asistida por computadora u otras pruebas seleccionadas para tal efecto, con el fin de establecer si los controles están diseñados, así como su cumplimiento y efectividad. Adicionalmente, se hará una evaluación de los riesgos asociados, la cual permitirá establecer una calificación de los riesgos asociados a cada una de esas áreas. Posteriormente, se planeara un enfoque de auditoría eficiente y efectivo que responda a la calificación del riesgo en la auditoría. El cual contiene: un resumen del o de las áreas críticas determinadas que serán evaluadas en la siguiente fase de la auditoría con los objetivos específicos para cada área y global, el plazo que se estima se requerirá para la ejecución de la evaluación, por área y total y una estimación de recursos (humanos, equipo y materiales y suministros) para la ejecución en forma eficiente de esta fase de la auditoría.

V.III. Comunicación De Resultados

El objetivo de está etapa es dar a conocer los principales resultados obtenidos a la administración de la entidad y otros usuarios de los productos de auditoría. Es importante destacar que el proceso de comunicación se va a mantener a través de la ejecución de todo el proceso de la auditoría.

VI. Descripción de Instrumentos manuales a utilizar

Al ser un área muy delicada la que se tiene por evaluada, se deben combinar diferentes instrumentos para lograr el mayor valor agregado al proceso de auditoria. Por lo tanto, se considera esencial la utilización de los siguientes instrumentos:

Observación: Para conocer y entender la entidad auditada, en sus principales actividades.

Encuestas: Para recopilar información concreta y cuantitativa de un gran número de individuos en la Etapa de Ejecución. Para identificar la frecuencia de un evento dado.

Entrevistas: En la Etapa de Planificación, para obtener información que ayude a comprender la entidad e identificar problemas potenciales. En la Etapa de Examen, para obtener información única y específica que se relacione con los objetivos de auditoria, para confirmar hechos o para desarrollar recomendaciones.

Análisis de Costo/Beneficio: Para obtener confianza de que un análisis hecho por la entidad auditada cumple con los estándares profesionales. Para comparar costos y beneficios cuando ambos son conocidos o pueden ser razonablemente estimados. Para comparar costos de alternativas cuando los beneficios se pueden asumir constantes.

Análisis de contenidos programas: Para ayudar a identificar los objetivos de los programas. Estudiar los antecedentes del programa en el expediente legislativo que originó los programas. Un análisis de contenidos puede ser usado para proveer descripción objetiva de las actividades de un programa mediante el

análisis de la documentación. Para determinar resultados positivos o negativos de un programa. Además, será utilizado para sintetizar reportes de evaluación, informes de auditoría, políticas, evaluaciones académicas o independientes de la ejecución de programas.

Análisis del flujo de trabajo y de comunicaciones: Para llegar a comprender cómo funciona una organización o sistema, particularmente cuando el tema de la auditoría involucra varios entes u órganos, unidades o etapas complicadas.

CAPÍTULO II

Planificación.

La planificación, aspecto crítico de éxito en el desarrollo de una auditoría, se debe desarrollar con sumo cuidado para lograr un adecuado control y ejecución del proyecto. Como se explicó en el capítulo anterior la planificación se compone dos fases las cuales se detallan en adelante.

I. Planificación Preliminar.

I.I. Objetivos.

1. Obtener información general preliminar para desarrollar un conocimiento y comprensión general de la entidad y del área y operaciones de TI de la entidad.
2. Definir los principales aspectos y directrices que regirán el trabajo en la fase planificación detallada de la auditoría de TI.
3. Considerar la pertinencia del objetivo general de la auditoría señalado anteriormente y proponer los cambios y/o ajustes que sean necesarios para definir un objetivo más realista y alcanzable.

I.II. Descripción de Procedimientos.

1. Obtenga el conocimiento general de las operaciones de la entidad por auditar, como normativa que regula el ente auditado, organigrama, políticas institucionales, estrategias, plan anual operativo, presupuesto y cualquier otra información importante para comprender mejor las actividades y operaciones, cumplimiento de objetivos y metas de los riesgos de operación.
2. Consolide la información en una Hoja diseñada para Documentar el Conocimiento de las Operaciones de la Entidad Auditada.

3. Complemente la información con el conocimiento del área de Tecnologías de Información, obteniendo la información más relevante de TI, a saber estructura organizacional, funciones, objetivos, personal, sistemas de aplicación, principales equipos, presupuesto.
4. Elabore con la información obtenida un modelo gráfico que facilite la comprensión más detallada y permita descomponer el área de TI en componentes significativos.
5. Elabore una matriz de componentes significados evaluando al menos los siguientes aspectos: impacto sobre los resultados, el riesgo de no auditarlo, recursos involucrados, oportunidad para mejorar el desempeño y factibilidad de la auditoría. Lo anterior con la finalidad de seleccionar los más importantes por ser considerados, en la planificación detallada.
6. Prepare un Informe de Planificación Preliminar destacando los principales esfuerzos de auditoría hechos en esta fase.

I.III. Resultados.

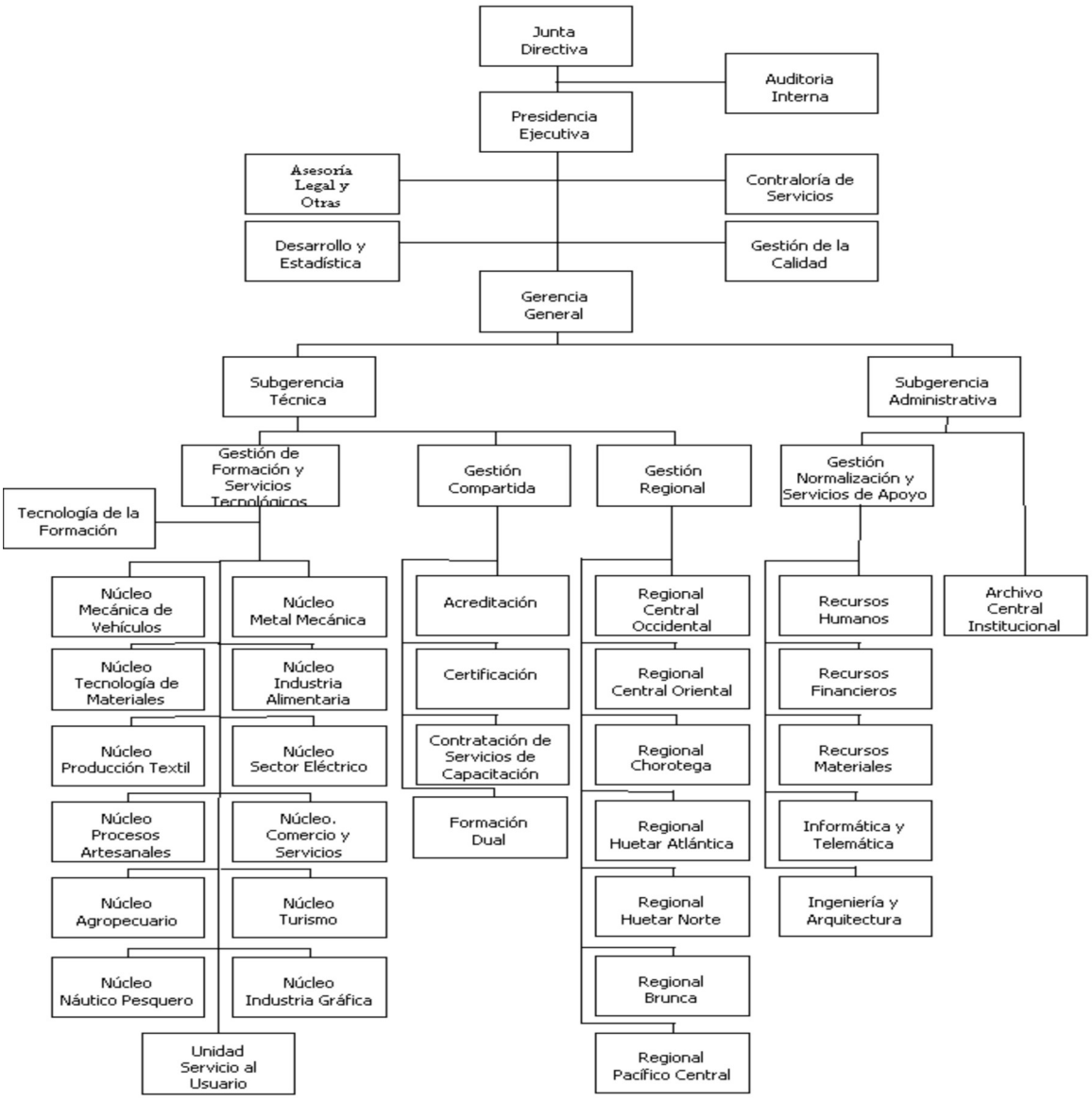
Conocimiento de la organización.
Antecedentes del INA

En 1964, bajo la administración de don Francisco J. Orlich Bolmarcich, el entonces Ministro de Trabajo y Bienestar Social, Lic. Alfonso Carro Zúñiga, mediante un proyecto propone la creación del INA como un organismo descentralizado con personería jurídica y patrimonio propio. Así fue creado el Instituto Nacional de Aprendizaje (INA), es una entidad autónoma creada por la ley No.3506 del 21 de mayo de 1965 y reformada por la Ley Orgánica No.6868 del 6 de mayo de 1983.

Su principal tarea es promover y desarrollar la capacitación y formación profesional de los hombres y las mujeres en todos los sectores de la producción

para impulsar el desarrollo económico y contribuir al mejoramiento de las condiciones de vida y de trabajo del pueblo costarricense.

Estructura Organizacional.



Junta Directiva.

Lic. Francisco Morales Hernández	Ministro de Trabajo y Seguridad Social.
Licda. Olga Cole Beckford	Directora Sector Cooperativo.
Lic. Manuel González Murillo	Director Sector Industrial.
Lic. Edgar Chacón Vega	Director Sector Comercial.
Licda. Xiomara Rojas Sánchez	Director Sector Sindical.
Lic. Eduardo Rojas Gómez	Director Sector Solidarista.
Ing. Luis Fernando Monge Rojas	Director Sector Agropecuario.
Lic. Ricardo Arroyo Yannarella	Gerente General.
Lic. Erick Román Sánchez	Subgerente Administrativo.
Lic. Luis Ramírez Arguedas	Subgerente Técnico.
Lic. Elías Rodríguez Chavarri	Auditor Interno.
Lic. Giovanny Marchena Jara	Asesor Legal.

El INA, como entidad rectora de la formación y capacitación de los recursos humanos que demanda el país, fundamenta su trabajo en los siguientes postulados:

Visión.

"Ser la institución líder en la prestación de los servicios de capacitación y formación profesional, preparando el capital humano calificado que demanda el país"[1].

Misión.

"El Instituto Nacional de Aprendizaje es un ente público que prepara personas mediante la capacitación y formación profesional para el trabajo productivo y propicia la generación de empresas con calidad y competitividad"[2].

Políticas Institucionales.

En marco filosófico institucional definido para el periodo del 2006-2010 establece once políticas con la finalidad de lograr cumplir con la misión y visión:

[1] www.ina.ac.cr
[2] www.ina.ac.cr

1. Creación de los mecanismos que faciliten la accesibilidad a los servicios de formación y capacitación profesional de los sectores de población más vulnerables, propiciando la igualdad de oportunidades y la atención de grupos específicos.
2. Consolidación de los servicios de capacitación y formación profesional, dirigidos a las empresas nacionales e internacionales, cámaras empresariales y organizaciones laborales (sindicatos, cooperativas y asociaciones solidaristas), por medio de programas integrales tendientes a incrementar la productividad, el encadenamiento productivo y la competitividad.
3. Participación activa en los procesos de investigación tecnológica como elemento fundamental para generar nueva oferta de servicios de capacitación y formación profesional, así como valor agregado a la producción de bienes y prestación de servicios.
4. Fortalecimiento del Sistema de Intermediación de Empleo, a nivel institucional, con el propósito de coadyuvar con las políticas nacionales de empleo.
5. Afianzamiento a nivel institucional de una cultura de servicio al cliente, en procura de que los potenciales usuarios encuentren una respuesta oportuna hacia las demandas que se generan.
6. Implementación de servicios de capacitación y formación profesional dirigidos a programas y proyectos de sostenibilidad ambiental, que desarrollen organizaciones públicas y privadas, para un crecimiento económico en armonía con el medio ambiente.
7. Abordaje de proyectos nacionales de inversión y de desarrollo con programas de formación articulados, para atender los encadenamientos productivos que fortalezcan el desarrollo local.
8. Establecimiento de todas las medidas necesarias para garantizar el funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) en sus diferentes procesos, de forma continua,

sistemática y participativa, con el fin de que se cumplan de manera eficiente y eficaz los objetivos institucionales.

9. Desarrollo e implementación de la gestión de conocimiento, la inteligencia de negocios y gobierno digital, partiendo de lo estipulado en el plan estratégico de Tecnología de Información y Comunicación.
10. Articulación con diferentes instancias para el establecimiento de las bases para la creación y operativización del Sistema Nacional de Formación Profesional, propiciando el desarrollo de proyectos conjuntos.
11. Establecimiento de convenios nacionales e internacionales que permitan mejorar los servicios de capacitación y formación profesional que oferta la institución en los diferentes sectores económicos.

Financiamiento y Presupuesto.

Como se establece en la ley orgánica 6868, el Instituto Nacional de Aprendizaje se financia con el 1,5% sobre el monto total de las planillas de salarios pagadas mensualmente por los patronos de todos los sectores económicos cuando ocupen en forma permanente por lo menos a cinco trabajadores con excepción de algunas instituciones públicas o sociales y un cero coma cincuenta por ciento (0,50%), de ese monto para las empresas del sector agropecuario cuando ocupen un número superior a diez trabajadores en forma permanente.

El INA ha tenido un crecimiento para un presupuesto de 35.000 millones de colones para el año 2006 y 39.000 para el 2007, tal y como se representa en el gráfico # 1.

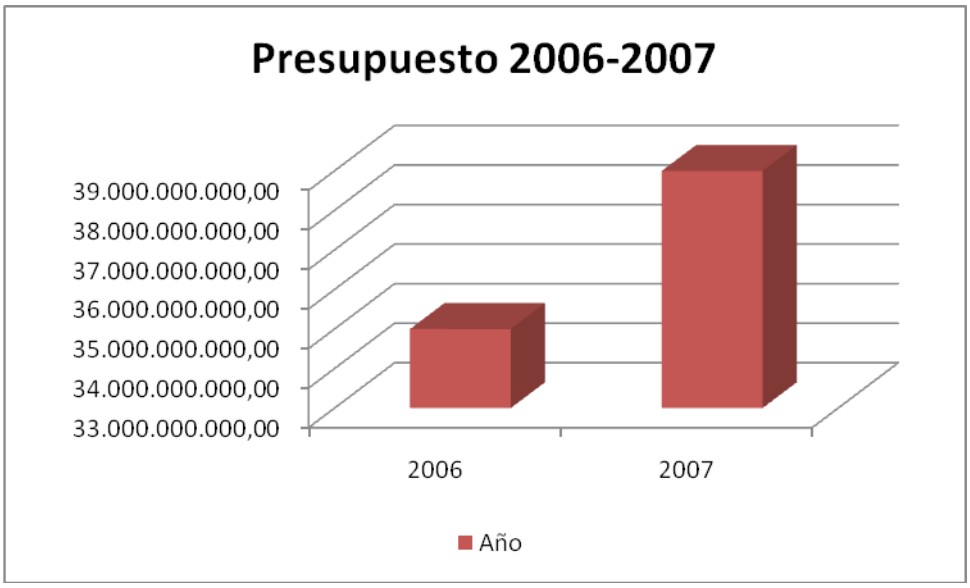


Gráfico # 1 – Presupuesto Ordinario.

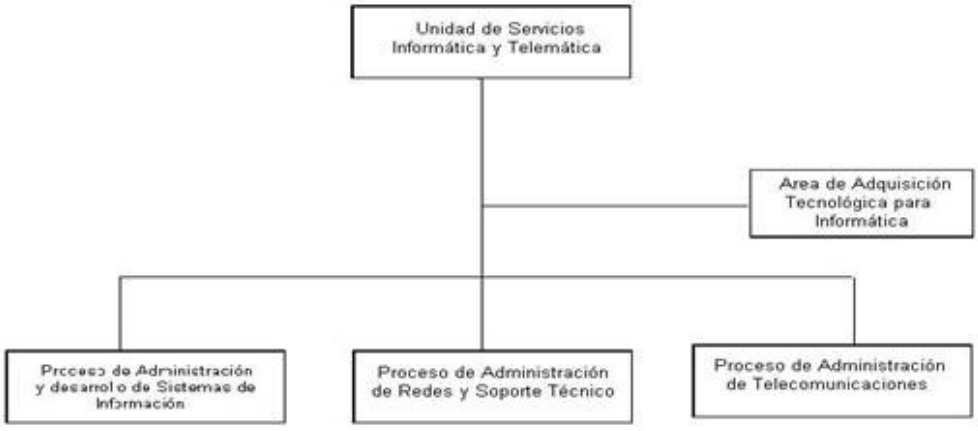
Conocimiento de TI.

Unidad de Servicios de Informática y Telemática.

La Unidad de Servicios de Informática y Telemática (USIT) pertenece al Área de Gestión de Normalización y Servicios de Apoyo. Siendo el superior inmediato la Gerencia General.

La USIT está organizada en tres procesos y un área:

- Proceso de Administración y Desarrollo de Sistemas de Información.
- Proceso de Administración de Redes y Soporte Técnico.
- Proceso de Administración de Telecomunicaciones.
- Área de Adquisición de Tecnología Informática.



Objetivos Generales.

Los objetivos generales de la Unidad son los siguientes:

- Desarrollar y poner en producción los nuevos sistemas de información de acuerdo con las prioridades, políticas y objetivos definidos por las autoridades superiores, así como dar mantenimiento a los sistemas de información, actualmente en operación.
- Administrar la red institucional de datos y sus enlaces a las Unidades Regionales y demás dependencias ubicadas fuera de la Sede Central, así como los servicios de acceso a los servidores, administración de base de datos, comunicación electrónica, seguridad e integridad de la información, utilización de sistemas de información, acceso a Internet y otros recursos y servicios que se brinden a través de la red.
- Administrar los servicios de telecomunicaciones que se brindan en la red de comunicación institucional.

Personal.

En la Unidad de Informática y Telemática del INA trabajan un total de 35 personas en la siguiente distribución:

Área	Cantidad
Dirección	3
Adquisición de TI	5
Redes y Soporte	13
Sistemas	10
Telecomunicaciones	4

Tabla # 1 – Cantidad de Personas por Sección de TI.

En el gráfico # 2 se puede apreciar más claramente el porcentaje de personal asignado a cada área.

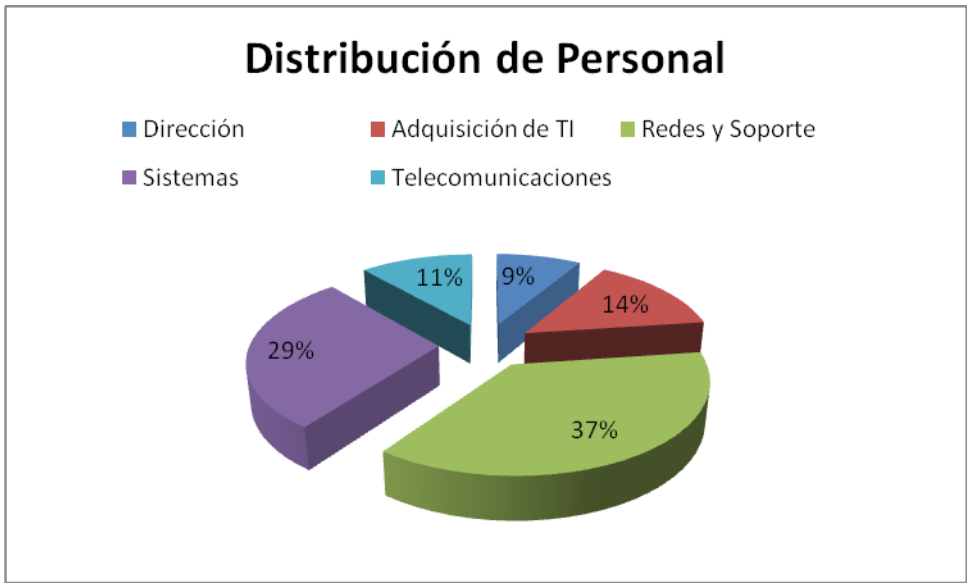


Gráfico # 2 – Distribución de Personal.

Funciones.

Las principales funciones de la Unidad[3] se conciben como las siguientes:

- Mantener una visión estratégica para el desarrollo de la función informática de la Institución.
- Coordinar la formulación y actualización del Plan Informático Institucional, en conjunto con la Comisión de Informática y las autoridades superiores.
- Elaborar el Plan Operativo Anual y el Presupuesto de la Unidad, según el Plan Informático y las políticas Institucionales.
- Diseñar los planes y programas para atender las necesidades de desarrollo informático del INA.
- Supervisar el desarrollo del Plan Informático.
- Definir las normas y estándares técnicos para el desarrollo y producción de los Sistemas de Información y la administración de los procesos informáticos a nivel Institucional.
- Administrar las redes de comunicaciones de datos del INA.
- Definir los lineamentos técnicos de las funciones de los recursos humanos informáticos desconcentrados y brindar la asesoría necesaria para el buen desempeño de sus funciones.
- Garantizar el cumplimiento de leyes, normas y procedimientos que rigen la informática.
- Realizar los estudios y dar las recomendaciones de los estándares para la adquisición de tecnologías informáticas (“hardware”, “software” y comunicaciones) de uso Institucional.
- Investigar y evaluar los adelantos tecnológicos para mantener estándares en la utilización de la informática y computación en el INA.
- Coordinar la contratación de servicios de análisis, desarrollo e instalación de los Sistemas Institucionales y la adquisición de los respectivos equipos computacionales.

[3] Intranet del INA

- Asesorar a todas las Unidades del INA en la implementación de las aplicaciones informáticas específicas.
- Garantizar el correcto funcionamiento de la plataforma de comunicaciones, del nodo Internet y la red de telefonía.
- Velar por la correcta ejecución del Plan Informático, Plan Operativo Anual y el Presupuesto de la Unidad.
- Evaluar y controlar las normas y procedimientos definidos para la administración de sistemas informáticos Institucionales y adquisición de tecnología.
- Evaluar el desempeño de los sistemas redes y tecnologías informáticas del INA.
- Aplicar la filosofía del desarrollo sostenible y los principios de control total de calidad en todas las actividades que le correspondan.

Infraestructura tecnológica.

Servidores:

- Sistema de almacenamiento EVA 3000.
- HP Alpha Servers DS25.
- HP Proliant 360.
- Librería de Respaldos HP MSL5026.
- Switch FC HP Storage works MSA 1000.
- Unidad de Respaldo SDLT.
- Switch KVM.

Clientes:

- Microcomputadora Pentium IV, Dúo.
- Velocidad de 2 GHz o superior.
- Memoria 512 MB.

Sistemas operativos:

- Unix True 64 para servidores de base de datos.
- Windows Server para controladores de dominio y servicios de red.

- Linux para servidores de desarrollo y otros.
- Windows 2000, XP, Vista para clientes.

Software Principal:

- Oracle 7, 8, 9, 10 para base de datos.
- Oracle developer 6i y 9i como herramienta de desarrollo.

Sistemas de Información:

Los principales sistemas de información que tiene el INA son los siguientes:

Nombre	Uso
Sistema de la Asesoría Legal.	Permite llevar un control sobre los documentos que se generan o son de uso del departamento legal.
Sistema Financiero.	Permite llevar un control financiero de la entidad, emisión de pagos, viáticos, etc.-
Sistema de Costos.	Permite realizar un cálculo estimado de los costos por servicio de capacitación impartidos.
Sistema de Calidad.	Lleva el control de los documentos generados por la gestión de calidad (ISO 9001)
Sistema de Cobros.	Permite administrar los cobros de ingresos a empresas que le adeudan al INA.
Sistema de Matricula y Control de Servicios.	Es el sistema que controla el proceso de matricula, control de calificaciones y certificados de los estudiantes para los diferentes servicios de capacitación.
Sistema de Formulación Presupuestaria.	Este sistema permite hacer las proyecciones y generación presupuestaria de las diferentes dependencias del INA.
Sistema de Recursos Humanos.	Sistema para la administración de la información del personal del INA, pagos, información personal, entro otros.
Sistema de Recursos Materiales.	Sistema que controla el proceso de adquisición de bienes y servicios para el INA.

Sistema de Servicios.	Permite la programación y control de servicios de capacitación proyectados durante los diferentes años.
Sistema de Ventas.	Permite administrar las ventas de productos que se realizan en el INA.

Presupuesto.

El Unidad de Informática y Telemática del INA posee un presupuesto mayor a los 1500 millones de colones, presupuesto que equivale al 4% aproximadamente del presupuesto ordinario de la institución.

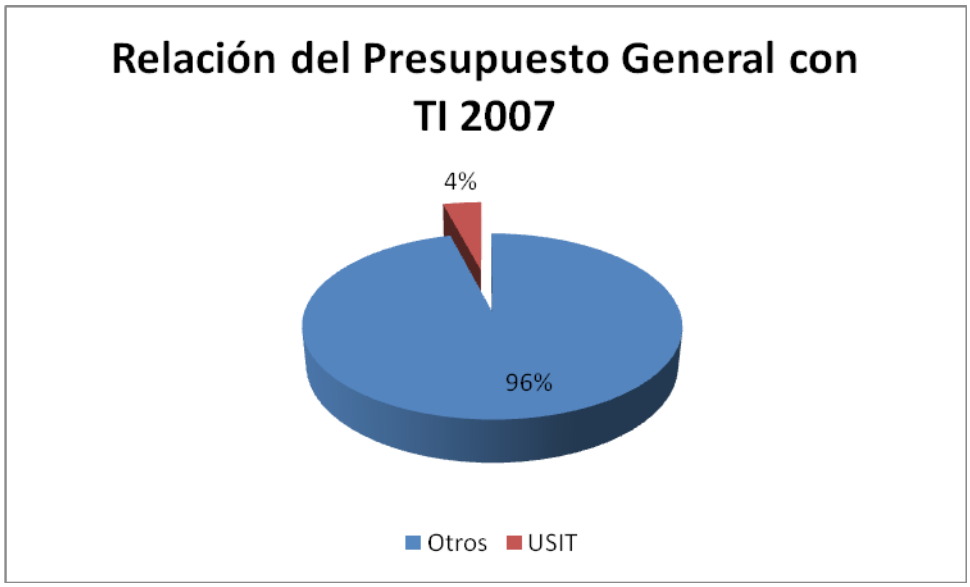


Gráfico # 3 – Relación del Presupuesto General y de TI.

Este 4% del presupuesto general asignado a TI se distribuyó de la siguiente mantera:

Tipo de Gasto.	Presupuesto (millones).
Remuneraciones.	305
Servicios.	467
Materiales. y Suministros.	12
Bienes duraderos.	798

Total	**1582**

Tabla # 2 – Presupuesto en millones de colones por subpartida.

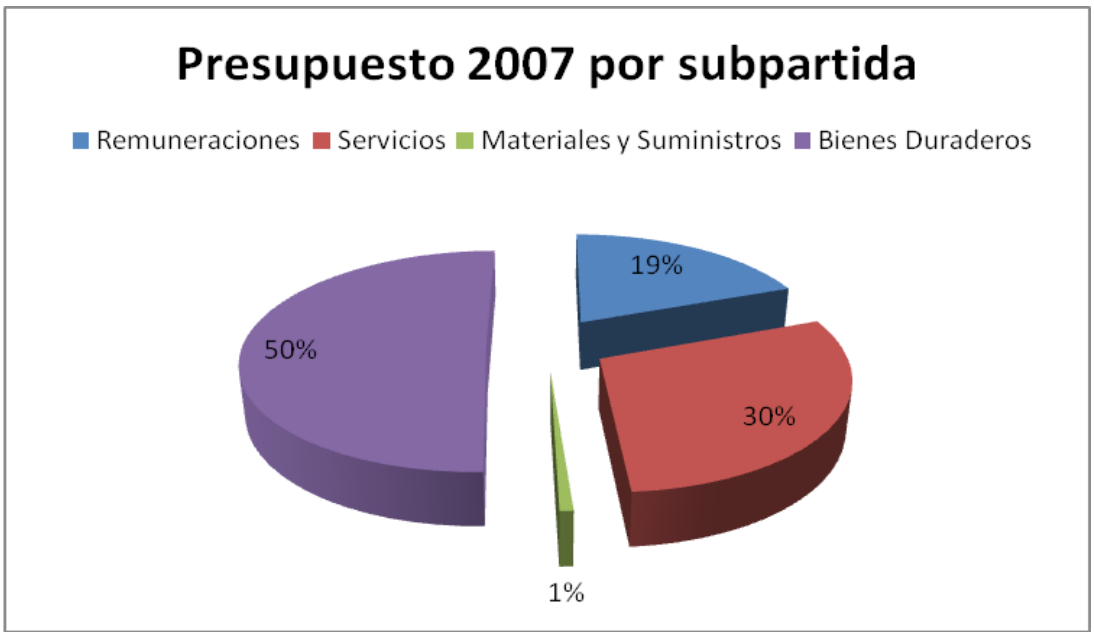


Gráfico # 4 – Presupuesto TI.

Como se puede observar en el gráfico # 4, el 50% del presupuesto general de la USIT corresponde a inversiones en bienes duraderos, seguido con un 30% de la contratación de servicios; otro aporte importante se gasta en salarios, 19 %, y solamente un 1% se presupuesta en materiales de trabajo.

Controles.

Desde año 2002 con la promulgación de la ley de control interno, las instituciones tienen la obligación de implementar y definir las estrategias para mantener y mejorar el funcionamiento de control interno. Es por eso, que desde el año 2003 en los diferentes departamentos se ha realizado una evaluación y mejora del sistema. Es así, que para el año 2007 la USIT presenta un cumplimiento mayor al 90 %.

Eje	SI	NO	PARCIAL

Generalidades.	93%	0%	7%
Ambiente.	89%	0%	11%
Riesgo.	100%	0%	0%
Control.	100%	0%	0%
Información.	97%	0%	3%
Seguimiento.	100%	0%	0%
Total	97%	0%	3%

Tabla # 3 – Cumplimento de la ley de control interno por tema.

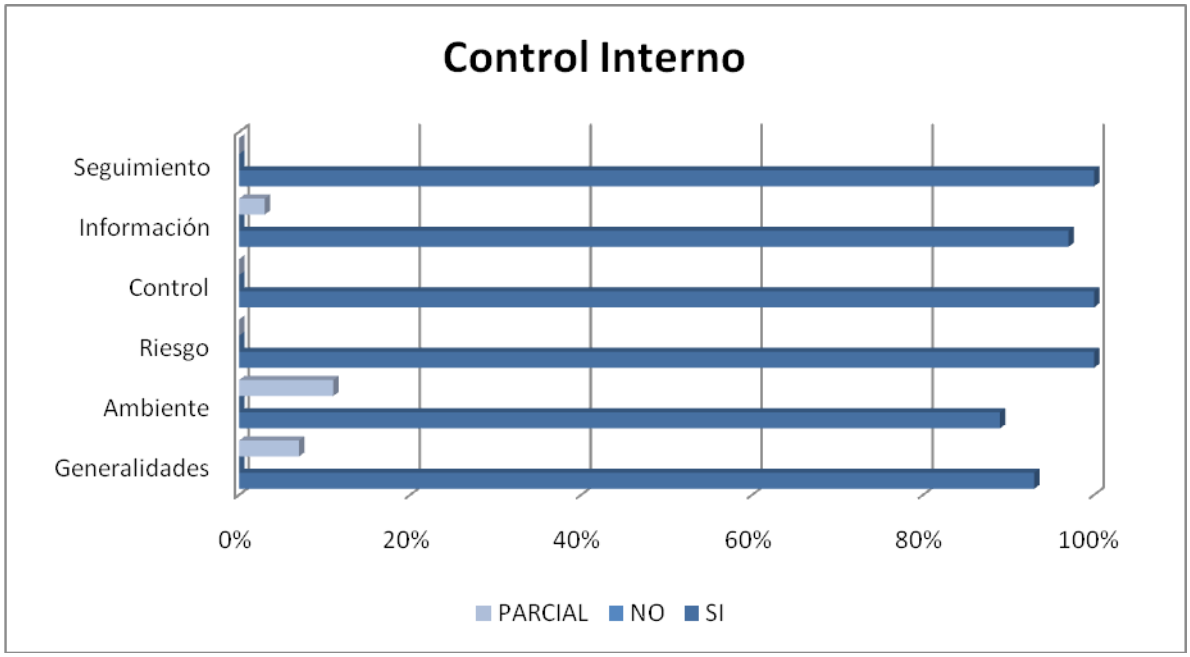


Gráfico # 5 – Cumplimiento de Ley Control Interno 2007.

Riesgos.

Desde el año anterior el INA estableció una metodología de administración de riesgos, con la finalidad de cumplir con lo estipulado por la Contraloría General de la República para la implementación del SERVRI.

Riesgo	Objetivo 1	Objetivo 2	Objetivo 3
Desastres Naturales	0	2	6
Innovación Tecnológica	0	4	3
Requerimientos de los Clientes	6	4	2
Capacidad	0	0	4
Capital de Conocimiento	9	6	0

Interrupción	9	6	4
Recursos Humanos	0	9	4
Acceso	0	6	0
Disponibilidad	0	6	0
Infraestructura	0	6	6

Tabla # 4 – Principales Riesgos de TI.

A pesar de la implementación de una ley de control interno es importante reconocer que no ha sido suficiente para minimizar los riesgos. Es por eso que existen muchos riesgos críticos; en la tabla # 4 se denota claramente que el objetivo # 2 de TI, es el que más riesgos críticos y a nivel medio presenta.

Componentes significativos.

Con base en el conocimiento general y de TI adquirido se procede a determinar cuales son las áreas de TI más importantes para la auditoría. Este procedimiento se basa en la aplicación de cinco factores, a saber: impacto sobre los resultados, riesgo de no auditarlo, recursos involucrados, oportunidad de mejorar el desempeño y factibilidad de auditoría.

OMPONENTES SIGNIFICATIVOS DE LA GESTIÓN TI	FACTORES DE EVALUACIÓN					ASIGNACIÓN DE (PRIORIDAD)
	IMPACTO SOBRE LOS RESULTADOS	RIESGO DE NO AUDITARLO	RECURSOS INVOLUCRADOS	OPORTUNIDAD DE MEJORAR EL DESEMPEÑO	FACTIBILIDAD DE AUDITORÍA	
Área de Adquisición de Tecnología Informática	4	4	4	4	4	20
Proceso de Administración de Telecomunicaciones	5	4	4	4	5	22

Proceso de Administración de Redes y Soporte Técnico	5	4	3	3	3	18
Proceso de Administración y Desarrollo de Sistemas de Información	3	4	3	4	3	17

Tabla # 5 – Análisis de Componentes Significativos de TI.

COMPONENTES SIGNIFICATIVOS DE LA GESTIÓN DE REDES Y SOPORTE	FACTORES DE EVALUACIÓN					ASIGNACIÓN DE (PRIORIDAD)
	IMPACTO SOBRE LOS RESULTADOS	RIESGO DE NO AUDITARLO	RECURSOS INVOLUCRADOS	OPORTUNIDAD DE MEJORAR EL DESEMPEÑO	FACTIBILIDAD DE AUDITORÍA	
Planificación, control y evaluación en la implementación.	2	3	4	2	3	14
Redes de datos en operación.	4	3	3	3	3	16
Asesoría y soporte técnico a Unidades.	2	2	1	1	2	8
Normalización del equipo computacional.	2	4	3	3	3	15
Operación de los servidores	4	4	3	3	3	17
Mantenimiento de los sistemas operativos.	3	3	2	2	2	12
Administración de la Base de Datos	5	5	3	3	3	19
Soporte Técnico a todas las máquinas, impresoras y equipos.	4	3	3	3	3	16

Administración de Correo.	3	3	3	3	3	15
Administración de Antivirus.	4	4	2	3	3	16
Administración del Servicio de Internet	3	3	2	2	2	12

Tabla # 6 – Análisis de Componentes Significativos de Redes y Soporte.

II. Planificación Detallada.

Una vez que se ha logrado determinar las áreas críticas para la indagación de auditoría, se procede a definir los aspectos principales de la planificación detallada, como lo son los objetivos, criterios y procedimientos.

II.I. Objetivo I - Sistemas de Gestión de Base de Datos.

Determinar que los DBMS se instalan, se configuran las bases de datos y mantienen bajo políticas y/o procedimientos establecidos para proveer acceso a los datos.

Criterio.

"El software de gestión de base de datos usado por la organización para proveer el acceso a, la estructura de, y el control sobre los datos, **deberá** instalarse y mantenerse de modo tal que asegure la integridad del software, las bases de datos y las instrucciones de control que definen el entorno de las bases de datos." (Benkus, II-1-1, 1991)

Procedimientos.

- Determine si existe una política o procedimientos para la administración de los DBMS.
- Identifique los objetivos y metas del entorno de base de datos de la organización.

- Determine si se ha establecido un procedimiento para monitorear su funcionamiento.
- Identifique los componentes del entorno de base de datos usados por la organización.
- Identifique la arquitectura de los sistemas de gestión de bases de datos.
- Determine que los Sistemas administradores de base de datos se encuentran ubicados en un lugar seguro y bajo condiciones ambientales adecuadas.

II.II. **Objetivo II -** Responsabilidad de la administración de las bases de datos

Determinar si se han definido por escrito el o los responsables para administrar los DBMS.

Criterio.

"Deberá asignarse la responsabilidad de la administración del entorno de base de datos de la organización" (Benkus, II-1-2, 1991).

Procedimientos.

- Establezca si las responsabilidades relacionadas con la administración de los activos de datos de la organización han sido definidas claramente y por escrito.
- Establezca si las responsabilidades relativas a la administración del entorno de las bases de datos de la organización se han definido claramente y por escrito, incluyendo: coordinación, revisión, documentación, formación, desarrollo y mantenimiento de estándares, seguridad.
- Identifique a la persona nombrada para la posición de administración de las bases de datos de la organización y evaluar la competencia técnica y administrativa de dicha persona y su posición en la organización para asegurar que el interesado tenga independencia y autoridad suficientes para desempeñar las responsabilidades asignadas.

- Determine si la organización aplica la segregación de funciones en el área de base de datos.
- Determine que el administrador de las bases de datos ha establecido estándares y directivas para ayudar al desarrollo de aplicaciones que utilizan bases de datos (debería cubrir tanto aspectos técnicos como de control).

II.III. **Objetivo III –** Creación de base de datos.

Comprobar la existencia y aplicación de un procedimiento para la creación de las bases de datos de la organización.

Criterio.

"Un DBA proactivo desarrolla e implementa un documento con la estrategia para desarrollar bases de datos dentro de la organización" (Craig, p 83, 2002).

Procedimientos.

- Verifique la existencia de un procedimiento documentado para la creación de bases de datos.
- Compruebe que las bases de datos existentes han sido creadas con base en el procedimiento.
- Determine la conformidad del procedimiento en relación con los aspectos básicos de creación base de datos.

II.IV. **Objetivo IV -** Descripción de datos y cambios de datos.

Comprobar si se han establecido por escrito políticas y procedimientos establecidos para garantizar la descripción de los datos y el control de cambios.

Criterio.

"Deberían establecerse, por escrito, los procedimientos a ser usados en la organización para la descripción de datos, los cambios de datos, y el mantenimiento del diccionario de datos" (Benkus, II-1-3, 1991).

Procedimientos.

- Establezca si el proceso de descripción de datos se lleva a cabo de forma manual o utilizando algún software específico.
- Seleccione muestras específicas de descripciones de datos y evalúe adecuación y actualización.
- Establezca la forma en que, en el caso de nuevos nombres para datos se sugiere la adopción de los mismos, se aprueban para ser incluidos en la descripción de datos, se introducen en la descripción de datos.
- Asegure que los cambios a las descripciones de datos se solicitan por escrito, se acuerden entre los usuarios de descripciones de datos compartidos, se aprueban por la dirección, se comunican a todos los usuarios de descripciones de datos compartidos
- Evalúe el papel del administrador de las bases de datos en la creación de descripciones de nuevos datos o en el cambio o supresión de descripciones de datos existentes.
- Determine si los estándares y procedimientos de la organización para incorporar nuevos nombres de datos y para cambiar descripciones de datos están definidos por escrito y si se controla su cumplimiento y utilización.
- Determine los controles incorporados en cualquier software usados para crear descripciones de datos y evaluar si se controla la conciliación y actualización de dichas descripciones de datos.

II.V. **Objetivo V -** Control de Acceso a Datos.

Comprobar que existe una política o procedimientos para garantizar que solamente personas autorizadas acceden los datos que están almacenados en los DBMS.

Criterio.

"Los procedimientos utilizados en la gestión de las bases de datos de la organización deberán contemplar el acceso a los datos en general y el acceso a los datos sensitivos en particular, el control sobre accesos concurrentes a los datos" (Benkus, II-1-3, 1991).

Procedimientos.

- Determine que el acceso a datos significativos sólo puede hacerse a través del sistema de gestión de base de datos de la organización.
- Asegúrese que están identificados los elementos de datos sensitivos contenidos en el sistema de gestión de base de datos y que las autorizaciones para acceder a los mismos son adecuadas y congruentes con la política de la organización.
- Determine que el sistema de gestión de las bases de datos de la organización ofrece sensibilidad adecuada, a nivel de campo.
- Asegúrese que las solicitudes para autorizar acceso a elementos de datos se hacen por escrito y que se aprueban de acuerdo con los procedimientos escritos significativos de la organización.
- Determine que se han establecido en el sistema de gestión de base de datos de la organización controles que aseguran que las actuaciones de elementos de datos, sólo pueden hacerse mediante programas de producción autorizados.
- Determine si el concepto de propiedad de los datos se ha establecido en la organización, si se ha identificado al propietario de cada elemento de datos y si éste es consciente de su responsabilidad de garantizar la integridad de tales datos.
- Asegúrese que el acceso al diccionario de datos está restringido a aquellas personas autorizadas por la organización para efectuar cambios adecuados en su contenido.

II.VI. **Objetivo VI –** Respaldo y recuperación del contenido de las bases de datos.

Demostrar que se han establecido procedimientos para garantizar la recuperación de las bases de datos.

Criterio.

"La alta dirección de la organización deberá establecer procedimientos escritos suficientes para minimizar los fallos, recuperar el entorno de las bases de datos hasta el punto de la caída y minimizar el tiempo necesario para la recuperación" (Benkus, II-1-4, 1991).

Procedimientos.

- Evalúe si existen los procedimientos escritos en la organización para la recuperación tanto física cómo lógica del entorno de las bases de datos.
- Indague si han sido probados los procedimientos de recuperación de las bases de datos de la organización. Si es así, revisar los resultados de las pruebas para evaluar la efectividad de dichos procedimientos para llevar a cabo la recuperación lógica y física de las bases de datos.
- Identifique las prácticas de la organización en cuanto a frecuencia de respaldos de las bases de datos.

II.VII. **Objetivo VII -** Integridad y Disponibilidad de las bases de datos.

Demostrar el establecimiento de los controles, prácticas y/o procedimientos para garantizar la seguridad de información almacenada en las bases de datos de los DBMS.

Criterio.

"Deberán establecerse procedimientos adecuados para asegurar la integridad de los datos contenidos en las bases de datos de la organización" (Benkus, II-1-5, 1991).

Procedimientos.

- Evalúe los procedimientos de control de cambios usados en el software del sistema de gestión de bases de datos de la organización.
- Establezca si se usan periódicamente programas de utilidad adecuados para comprobar los enlaces físicos.
- Establezca si los propios elementos de datos son objeto de balance periódico con los registros de control.
- Establezca si los estándares de programación de aplicaciones de la organización incluyen: la exigencia de que en cada acceso de base de datos se comprueben los códigos de estado, medios para manejar errores y otras disposiciones para mantener la integridad de las bases de datos.
- Revise las disposiciones para el respaldo de equipo y software para las bases de datos, para asegurar la disponibilidad de las bases de datos para aplicaciones críticas en el tiempo.
- Revise la redundancia de la red o las disposiciones que establezcan rutas alternativas para acceder a bases de datos a través de dicha red, para asegurar la disponibilidad de las bases de datos para aplicaciones críticas en el tiempo.

III. Necesidades

Para poder cumplir con el la etapa de planificación y ejecución del proyecto se consideran necesarios contar información y recursos.

III.I. Fuentes de Información.

Para la etapa de planificación y ejecución del proyecto se consideran fundamentales contar con las siguientes fuentes de información:

- Internet.

- Intranet.
- Archivos.
- Publicaciones.
- Entrevistas
- Otros.

III.II. Recursos

Al ser un trabajo que se desarrolla en forma individual se cuenta y se hará uso de los siguientes recursos:

Humanos:

- Especialista en Auditoría de TI.

Equipos:

- 1 computadora.
- 1 impresora.
- 1 escritorio y 1 silla.

Materiales:

- 100 hojas.
- 2 lapiceros.
- 1 lápiz.
- 1 cuaderno.
- 1 ampo.

CAPÍTULO III

Ejecución.

Una vez que hemos llevado a la práctica la planificación detallada de la auditoría mediante la etapa de ejecución, se ha logrado identificar algunos aspectos de suma importancia que requieren ser atendidos por parte de personal de la organización, con la finalidad de mejorar el que hacer diario del área auditada. Estos se conocen como hallazgos de auditoría y se detallan de aquí en adelante.

Para la obtención de estos hallazgos fue necesaria la puesta en práctica de conocimientos y procedimientos de auditoría definidos anteriormente. Los principales actores de entrevistados o con los que hubo mayor interacción fueron: el encargado de administración de los DBMS y sus dos colaboradores, un analista de sistemas y el encargado del proceso de documentación, una persona del área de operación de respaldos y el gerente del área de Redes y Soporte Técnico.

I. Hallazgo # 1 – Monitoreo.

Condición Muchas de las actividades realizadas por las cuentas de base de datos en su mayoría de DBMS no son registradas en las pistas de auditoría, ni tampoco se realiza ninguna revisión sobre los registros de las bases de datos que si registran estas.

Causa El personal de administración de los DBMS no ha establecido un procedimiento para mantener un monitoreo constante del funcionamiento de los DBMS.

Criterio La norma ISO17799:2005 en su apartado 10.10 plantea lo siguiente: "*El sistema debe ser supervisado y los acontecimientos de la seguridad de la información deben ser registrados*".

Efecto Por falta de un procedimiento para monitorear el funcionamiento de los DBMS se puede producir alteración de la información almacenada, además, de fallos que provoquen la falta de disponibilidad servicio que pudieron haberse detectado a tiempo o evitado.

Recomendación *A la Gerencia de TI*

Establecer un procedimiento para crear, mantener almacenadas y revisar los log de auditoría por un tiempo definido.

A la Gerencia de TI y Auditoría de TI

Establecer un procedimiento para el monitoreo de las pistas de auditoría y log de eventos generados en los diferentes DBMS para determinar fallas y cualquier actividad inapropiada. Además, implemente los mecanismos de seguridad para

restringir el acceso y manipulación indebida de estos registros.

II. Hallazgo # 2 – Responsabilidad de Administración de los DBMS.

Condición. Los administradores de los DBMS realizan su trabajo de acuerdo con lineamientos generales y consideraciones personales acerca de la mejor forma de administración.

Causa No existe un área o proceso de base de datos definido, por lo que la administración de TI le ha dificultado la comunicación por escrito las funciones y responsabilidades del personal a cargo de la administración de los DBMS.

Criterio La normas técnicas de control interno en el punto 4.4 define lo siguiente: "*La responsabilidad por cada proceso, actividad, operación, transacción o acción organizacional debe ser claramente definida, específicamente asignada y formalmente comunicada al funcionario respectivo, según el puesto que ocupa*".

Efecto La falta de definición y comunicación de responsabilidades provoca que muchos hechos inapropiados queden impunes al no poderse determinar las responsables de cada caso.

Recomendación *A la Gerencia de TI.*

Analizar la posibilidad de definir formalmente un subproceso o proceso de base de datos.

Revisar las diferentes funciones del personal que trabaja en la administración de los DBMS, para definir y

comunicar por escrito sus responsabilidades.

III. Hallazgo # 3 – Segregación de Funciones.

Condición. Actualmente las diferentes personas que trabajan administrando los DBMS en la mayoría de ocasiones definen, aprueban e implementan los trabajos por sí mismos.

Causa. El poco personal con se cuenta en el área de base de datos dificulta la segregación de funciones.

Criterio. La norma ISO17799:2005 en su apartado 10.1.3 plantea lo siguiente: "*Deberes y responsabilidades de las áreas, se deben segregar para reducir las oportunidades para la modificación o el uso erróneo desautorizado o intencional de los activos de la organización*".

Efecto. El personal administrador de los DBMS tiene libre acceso tanto a nivel de sistema operativo como a nivel de DBMS por lo cual se puede dar uso erróneo accidental o deliberado del sistema.

Recomendación. *A la Gerencia de TI:*

Realizar una análisis del trabajo ejecutado por parte del personal de esta área, y tratar de separar funciones incompatibles.

IV. Hallazgo # 4 – Clasificación de la información.

Condición. Los administradores de base de datos dan la misma atención a toda la información almacenada en los diferentes DBMS.

Causa. El poco involucramiento e importancia que se le brinda a la información por parte de la Administración.

Criterio. La norma ISO17799:2005 en su apartado 7.2 plantea lo siguiente: "*La información se debe clasificar para indicar la necesidad, las prioridades, y el grado previsto de protección al manejar la información*".

Efecto. La falta de una clasificación de la información provoca que información crítica o sensitiva de la organización no reciba el tratamiento adecuado, lo que podría ocasionar una revelación sin autorización, lo que conllevaría a demandas legales y, por ende, una pérdida de imagen.

Recomendación A la Gerencia

Establecer un procedimiento y llevarlo a la práctica para desarrollar un esquema de clasificación de la información, determinando los niveles de protección y las necesidades de medidas de dirección especiales.

V. Hallazgo # 5 – Acceso a Producción por parte de los analistas.

Condición. Los analistas de sistemas están accediendo y modificando la estructura y datos dentro de las bases de datos en producción de los DBMS con el usuario dueño del esquema de cada sistema de aplicación.

Causa. No se le ha dado la importancia de restringir el acceso de los analistas de sistemas a las base datos en producción por parte de la gerencia de TI.

Criterio. La norma ISO17799:2005 en su apartado 10.1.4 plantea lo siguiente: "*Desarrollo, prueba, y las instalaciones operacionales se deben separar para reducir los riesgos del acceso o de los cambios desautorizados al sistema operacional*".

Efecto. El personal del desarrollo y/o de prueba puede introducir código desautorizado y no comprobado, alterar datos operacionales, facilitar fraudes, generar problemas operacionales críticos y/o revelar información confidencial.

Recomendación. *A la Gerencia de TI:*

Tomar las medidas correspondientes para separar completamente el ambiente de desarrollo y producción

Establecer una política de utilización de las cuentas dueñas de los esquemas de los diferentes sistemas operacionales, evitando el uso de estas cuentas por parte de los desarrolladores y deshabilitando las mismas cuando no se utilizan.

VI. Hallazgo # 6 – Políticas de Seguridad.

Condición. La administración no ha definido una política para la gestión de la seguridad de la información.

Causa. Por la falta de tiempo e involucramiento del personal

que gestiona la seguridad de la información.

Criterio. La norma ISO17799:2002 en su apartado 3.1 plantea lo siguiente: "*La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización*".

Efecto. Se pueden producir pérdidas económicas por la desorganización de los esfuerzos e inversiones realizadas en el tema de seguridad de la información.

Recomendación. *A la Gerencia:*

Realizar un análisis de las amenazas y vulnerabilidades de seguridad de la información para determinar los riesgos e implementar los controles necesarios para mitigarlos.

Con base en los resultados del análisis anterior definir lo más pronto posible una política de seguridad de la información para dirigir y dar soporte a la gestión de la seguridad de la información.

VII. Hallazgo # 7 – Administración de las contraseñas.

Condición. Los usuarios de aplicaciones de cuentas de base de datos pueden asignar cualquier contraseña sin importar sus características, por ejemplo nombres propios, número de teléfono, entre otros.

Causa. La administración de los DBMS no ha definido ningún

perfil para la definición y administración de las contraseñas de las cuentas de base de datos.

Criterio La norma ISO17799:2005 en su apartado 11.2.3 plantea lo siguiente: "*La asignación de contraseñas debe controlarse a través de un proceso de administración formal*".

Efecto. Al no existir una política para la administración y definición de contraseñas de cuentas de base de datos facilita la revelación, captura y uso de las contraseñas de las cuentas por parte de personal sin autorización, lo que puede causar la pérdida de integridad de la información.

Recomendación. *A la Gerencia de TI:*

Definir un procedimiento formal para la administración de contraseñas; el mismo debería incluir aspectos relacionados a la responsabilidad de usuarios, revisión de roles y derechos concedidos, formato de calidad para la definición de contraseñas, tiempo máximo de inactividad, entre otros aspectos.

VIII. Hallazgo # 8 – Respaldo y Recuperación.

Condición. La administración de los DBMS ha definido procedimientos para respaldar la información, pero, excluyeron el procedimiento para restauración de los servicios de información.

Causa. La administración de los DBMS no considera un aspecto crítico el procedimiento de restauración de la

información respaldada.

Criterio. Cobit 4 establece en su apartado DS4.8 Restauración y recuperación de Servicios de TI que: "*Un plan de acción debe se establecido para la recuperación de los servicios de información …"*

Efecto. En caso de la pérdida de información por fallas de equipo o desastres naturales, el personal de informática existente puede tener grandes problemas para poder restaurar, de manera oportuna, los servicios de base de datos.

Recomendación. A la Gerencia de TI:

Establecer las medidas pertinentes para incorporar en los planes de contingencia los procedimientos necesarios para restaurar los servicios información.

Establecer una política para determinar la funcionalidad y recuperación de los respaldos creados, al menos una vez al mes.

CAPÍTULO IV

Conclusiones y Recomendaciones

Una vez cumplido con las etapas anteriores de este trabajo, es importante mencionar las principales conclusiones y recomendaciones obtenidas con la puesta en práctica de conocimientos adquiridos y hechos destacados durante el proceso.

I. Conclusiones

1. Se logró cumplir con el objetivo planteado para el proyecto de auditoría al inicio de esta práctica. Lo anterior debido a que se realizaron de manera exitosa todas las fases de la auditoría.

2. La conclusión de la auditoría es que existen algunas deficiencias significativas de seguridad en el área estudiada, ya sea por falta de recursos o por poco interés de la seguridad de información por parte del personal.

3. Las mejores prácticas plantean una recopilación de procedimientos probados con éxito a nivel mundial, sin embargo, al provenir muchas de estas prácticas de países desarrollados, son difíciles de implementar en organizaciones de países subdesarrollados donde no existe una cultura débil sobre estos temas.

4. Con la nueva promulgación de las nuevas normas técnicas para la gestión y control de las tecnologías de información, promulgadas en julio del presente año por parte de la Contraloría General de La República, exige a las organizaciones públicas le implementen algún marco de

control de mejores prácticas. Estas, a su vez, irán creando y fortaleciendo el uso de las mejores prácticas y con ello la fortalecimiento de la cultura de las instituciones.

5. Lo más difícil será cambiar la forma en que es vista la auditoría por parte de los funcionarios públicos, que en lugar de verla como una oportunidad para mejorar el proceso en el cual se desenvuelven, la consideran como una amenaza.

6. Otro aspecto de suma importancia es cambiar la actitud de muchos funcionarios públicos, que desean mantenerse haciendo su trabajo tal y como siempre lo han hecho, sin cambios. Estos no muestran ningún interés por mejorar la eficacia y eficiencia de los procesos, debido a que manejan recursos públicos que son de todos, pero a la vez no son de nadie.

7. A pesar de que se adquieren muchos conocimientos, durante el proceso de maestría, se dificulta en gran medida llevar con éxito esos conocimientos, de la teoría a la práctica.

II. Recomendaciones

1. La universidad debería establecer convenios con organizaciones y/o empresas para facilitar la aceptación y compromiso para con los estudiantes de prácticas profesionales.

2. Para los trabajos de auditoría se debería considera el desarrollo de trabajos grupales de dos o tres personas, con la finalidad de compartir conocimientos y técnicas de auditoría desde puntos de vista diferentes.

3. Creo de suma importancia que la Universidad considere la implementación de sistema de promoción para los profesionales recién egresados en sus diferentes posgrados.

BIBLIOGRAFÍA

Craig S. Mullins. **Database Administration: The Complete Guide to Practices and Procedures.** Editorial Addison Wesley, 2002.

Hernandez, Michael J. **Database Design for Mere Mortals: A Hands-On Guide to Relational Database Design**. Editorial Addison Wesley. Segunda Edición, 2003.

Vallabhaneni, S. Rao. **The MicroMash Certified Information System Auditor Exam Review: Theory Book.** Editorial SRV Professional Publications and ExamMatrix. Edición 2006.

Menkus, Belden. **Objetivos De Control para SDLC**, Editorial The EDP Auditors Foundation Inc**.** Edición1991.

Contraloría General de la República de Costa Rica, **Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización.** La Gaceta, 2003.

ISO / IEC, **International Standard 17799, Information Technology – Security Techniques – Code of practice for Information Security Management,** Segunda Edición, 2005.

ISO / IEC, **International Standard 20000, Information Technology – Service Management.** Primera edición, 2005.

IT Governance Institute, **Control Objectives for Information and related Technology.** Cuarta Edición, 2007.

Sistemas de Gestión de Base de Datos, http://es.wikipedia.org/wiki/SGBD, 15/04/2007

Database Security (Common-sense Principles), Blake Weidman, http://www.governmentsecurity.org/articles/DatabaseSecurityCommon-sensePrinciples.phpm 05/03/2007

Database Auditing Best Practices, Ted Julian, www.appsecinc.com/presentations/db_auditing.pdf, 13/03/2007

7 Keys to Help You, Tango04 Security and Auditing Solutions, www.blackhat.com/presentations/bh-usa-06/BH-US-06-Spradlin.pdf, 15/04/2007

How to keep data private, Bill Bennett, http://www.smh.com.au/news/home-office/how-to-keep-data-private/2006/07/19/1153166452409.html, 29/04/2007

Keeping Data Private, Sean Doherty, http://www.networkcomputing.com/1213/1213ws12.html, 28/05/2007

ANEXOS

I. Cronograma

	Nombre de tarea	Duración	Comienzo	Fin
1	**Planificacación**	**21 días**	**lun 04/06/07**	**lun 02/07/07**
2	**Planificación Preliminar**	**11 días**	**lun 04/06/07**	**lun 18/06/07**
3	Elaboración de Programa	4 días	lun 04/06/07	jue 07/06/07
4	Recopilación de Información de la Entidad	2 días	vie 08/06/07	lun 11/06/07
5	Consolidación de la información	5 días	mar 12/06/07	lun 18/06/07
6	**Planificación Detallada**	**21 días**	**lun 04/06/07**	**lun 02/07/07**
7	Analisis de la información de la Planificación Preliminar	2 días	lun 04/06/07	mar 05/06/07
8	Elaboración del o de los Programas	15 días	mié 06/06/07	mar 26/06/07
9	Revisión y Aprobación del o de los Programas	4 días	mié 27/06/07	lun 02/07/07
10	**Ejecución**	**15 días**	**mar 03/07/07**	**lun 23/07/07**
11	Aplicación de los Programas	5 días	mar 03/07/07	lun 09/07/07
12	Recopilación y Análisis de la Evidencia	5 días	mar 10/07/07	lun 16/07/07
13	Elaboración de Conclusiones y Recomendaciones	5 días	mar 17/07/07	lun 23/07/07
14	**Comunicación**	**12 días**	**mar 24/07/07**	**mié 08/08/07**
15	Elaración del Informe	6 días	mar 24/07/07	mar 31/07/07
16	Presentasión del Informe	1 día	mié 01/08/07	mié 01/08/07
17	Corrección del Informe	3 días	jue 02/08/07	lun 06/08/07
18	Presentasión del Informe Final	2 días	mar 07/08/07	mié 08/08/07
19	**Revisión y ajuste del documento**	**8 días**	**jue 09/08/07**	**lun 20/08/07**
20	Ajuestes Lector	2 días	jue 09/08/07	vie 10/08/07
21	Ajuste Filologo	2 días	lun 13/08/07	mar 14/08/07
22	Ajuste Tutor	2 días	mié 15/08/07	jue 16/08/07
23	Impresión y Empaste del Documento	2 días	vie 17/08/07	lun 20/08/07

II. Guías de Auditoría

II.I. Creación de Base de Datos

Un buen procedimiento establecido para la creación de base de datos ayudara a garantizar la integridad de la información.

Aspecto	SI	NO	Comentarios
Se utiliza el modelo de normalización para creación de las bases de datos			
La creación de las bases de datos esta creada o coordinada por el DBA			
La base de datos física proviene de la transformación de un modelo lógico en la implementación física.			
Mapea cada entidad del modelo de datos a una tabla de la base de datos.			
Los atributos de cada entidad pueden ser mapeados a la columna de cada tabla respectivamente.			
Mapea cada dominio lógico a un tipo de dato físico, los cuales pueden ser acoplados con restricciones adicionales.			
Se especifican las columnas que pueden ser nulas.			
Para cada tabla que se crea se asegura de que cada tabla física posee su clave primaria.			
Se revisa el orden de las columnas en las tablas físicas.			
Las restricciones referenciales ata la llave primaria a la llave foránea.			
Se utiliza la integridad referencial para asegurar			

su integridad.			
Se mapea cada tabla a una estructura para almacenar los datos de la tabla.			
Se realizar una planificación de la capacidad de almacenamiento y uso.			
Se crean los índices en las tablas de la base de datos para un mejor rendimiento.			
Todos los objetos de base de datos físicos son creados usando lenguaje de definición de datos SQL.			
Todos los aspectos de la base de datos y código de aplicación son revisados para verificar la eficiencia y efectividad.			
Se consideran controles específicos para evitar la pérdida de integridad o acceso a las bases de datos dentro del estándar de desarrollo			

II.II. Descripción de datos y cambios de datos

Se puede haber definido e implementado un excelente procedimiento de creación de base de datos, pero, si no existen controles sobre los cambios puede provocar que DBMS y sus bases de datos se conviertan en un problema crítico para su operación y mantenimiento.

Aspecto	SI	NO	Comentarios
Existe un procedimiento escrito para controlar los cambios, tales las migraciones a nuevos DBMS o actualizaciones			
Las solicitudes de cambios se realizan por escrito			
Los cambios son aprobados antes de su			

implementación			
Los cambios se realizan por la persona con autorización para hacerlo			
Se utiliza alguna herramienta que facilite los cambios sobre las base de datos			
Al DBA mantiene una estrecha relación entre soporte para la coordinación de cambios en hardware.			
Para cada cambio en la estructura debe actualizarse la documentación y descripción.			
Existe una sincronización entre los cambios de aplicaciones y estructura de la base de datos.			
Se ha establecido una forma estandarizada para realizar cambios en la base de datos.			
Se cuenta con una política para monitorear y administrar el rendimiento de toda la aplicación.			
Esta incluye aspectos de sistema operativo, hardware (memoria, almacenamiento), sistema y base de datos.			
Se mantiene un registro histórico de análisis de rendimiento y cambios realizados.			
Existe algún procedimiento para implementar nuevas aplicaciones.			
Se ha definido algún estándar para la nomenclatura de base de datos.			
Se documenta cada cambio en la estructura de base de datos			
Solamente el DBA realiza los cambios en la estructura de base de datos			
Se utiliza algún software para modificar las descripciones de datos.			

Se ha implementado el concepto de propietario de los datos.			
Todos los sistemas incluyen métodos para manejar errores			