Universidad de Costa Rica

Sistema de Estudios de Posgrado

“EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA, RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN”

Trabajo Final de Graduación aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magíster en Administración y Dirección de Empresas con énfasis en Auditoría de Tecnologías de Información.

Rodolfo González López

Carné A46776

Ciudad Universitaria “Rodrigo Facio”, Costa Rica

Año 2007

DEDICATORIA

A mi Dios, quien me enseñó que la verdadera sabiduría radica en su temor,
y en su conocimiento, la inteligencia.

A mis Padres y hermanas, cuyo sacrificio es la base sólida de cada peldaño alcanzado en la escalinata de mi vida.

A mi esposa Martha, por su apoyo y comprensión ante las interminables horas de soledad que tuvo que soportar.

AGRADECIMIENTOS

Agradezco de una manera muy especial a mi equipo asesor, Master Sergio Espinoza Guido, quien como profesor me orientó, apoyó en mi trabajo y veló por su mejora continua; igualmente a los lectores Master Ricardo Arce Sandí y Lic. Luis Fernando Sequeira Solís, por su colaboración y profesionalismo en el desarrollo del presente trabajo.

Agradezco también a la Lic. Amelia Quirós Salinas por sus acertados comentarios y recomendaciones, y por el permanente intercambio de ideas que contribuyó con la mejora del presente documento.

HOJA DE APROBACIÓN

Este Trabajo Final de Graduación fue aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar al grado de Magister con énfasis en Auditoría de Tecnologías de Información.

_____	_____
Dr. Aníbal Barquero Chacón	MAI. Sergio Espinoza Guido
Director Programa de Maestría	Profesor Coordinador
_____	_____
Master. Ricardo Arce Sandí	Lic. Luis Fernando Sequeira Solís
Lector Académico	Lector Institucional

_____

Lic. Rodolfo González López

Estudiante

CONTENIDO

TÍTULO: "EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA, RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN"

Índice de Anexos Complementarios viii

ÍNDICE DE SIGLAS Y ABREVIATURAS

Tecnologías de Información y Comunicación	TIC
Tecnologías de Información	TI
Superintendencia General de Entidades Financieras	SUGEF
Objetivos de Control para la Información y las Tecnologías Relacionadas	COBIT

RESUMEN

González López, Rodolfo

"EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN"

Programa de Posgrado en Administración y Dirección de Empresas. –San José, C.R.

El objetivo general del trabajo es evaluar los aspectos referentes a la seguridad física y lógica de aplicación por parte de una entidad pública en su ambiente de tecnologías de información y obtener un informe sobre los aspectos observados que constituyan oportunidades de mejora en dichos procesos, así como las recomendaciones respectivas.

La organización investigada forma parte de la estructura estatal de instituciones públicas de naturaleza autónoma, que se rigen por una ley constitutiva, el marco jurídico que tutela el accionar del sector público costarricense, tal como la Ley General de la Administración Pública, Ley de Administración Financiera y Presupuestos Públicos, Ley General de Control Interno y otras. Además, del marco normativo de naturaleza vinculante emitido por la Contraloría General de la República.

El proyecto desarrolla una investigación de tipo auditoría, mediante la evaluación de los procesos generales de seguridad física y lógica relativa con las tecnologías de información y comunicación de la institución.

Dentro de las principales conclusiones se tienen:

1. De la evaluación realizada, se determinaron aspectos de mejora en las áreas de seguridad lógica y física, de acuerdo con los objetivos estratégicos de la institución, los cuales han sido recientemente replanteados por la nueva administración dada las variaciones y competitividad en el mercado internacional.

2. Al no haber adoptado la Institución un marco de referencia procedimental para la realización del trabajo propuesto, y ser la normativa del sector público aplicable a la organización ayuna en el tema, se definió como fuentes de criterio la utilización de las mejores prácticas incluidas en los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), a sabiendas de que, por ser una normativa internacional generalmente aceptada para el uso cotidiano de gerentes de empresas y auditores, podría ser de aplicación en el proyecto por desarrollar, con la salvedad de que constituyese una adaptación de sus mejores prácticas y no una adopción de la metodología en forma integral. Igualmente la normativa de carácter obligatorio para las instituciones públicas, emitida por la Contraloría General de la República.

3. Se identificó un entorno del TI con un ciclo de madurez que favorece las oportunidades de reforzar la arquitectura de tecnología de información alineada con los objetivos estratégicos institucionales.

4. La situación actual de la organización en relación con el uso de las Tecnologías de Informática es insuficiente para alcanzar los objetivos estratégicos de la entidad.

Con base en lo anterior, se recomienda:

1. Establecer un plan estratégico de las TI alineado con los objetivos de la entidad.

2. Elaborar un programa de acción para atender las necesidades de arquitectura en hardware y software con la capacidad que se requiere para automatizar los procesos pertinentes que coadyuvarán a alcanzar los objetivos estratégicos institucionales.

3. Considerar en el plan estratégico las acciones respectivas para fortalecer la seguridad física y lógica de las tecnologías de información, tales como:

3.1 Que la administración realice esfuerzos orientados hacia una mejor capacitación de su personal, en procura de establecer un índice satisfactorio de conciencia y cultura organizacional, las mismas que contribuirán con una mejor eficiencia, eficacia, uso y aprovechamiento de las tecnologías de información institucionales.

3.2 Que se proceda con la elaboración de los procedimientos que se encuentran en condición pendiente, y que los existentes sean revisados a efecto de complementarlos con los lineamientos necesarios

3.3 Que la administración considere los aspectos de mejora relacionados con seguridad física; tales como: Cámaras de vídeo, vigilancia, registro de personal que ingresa al Centro de Cómputo, alarmas contra robos, sistemas de detección de incendio, control de humedad, sistema detector de líquidos, piso falso, bitácoras de registro, entre otros.

3.4 De conformidad con la disponibilidad de sus recursos, sus planes estratégicos, estructura administrativa y operativa del recurso humano del Departamento de Tecnologías de Información, es necesario que la administración evalúe la conveniencia de implantar la figura del administrador de la seguridad de TI, como una función específica.

3.5 Se debe crear, comunicar y probar un plan de contingencia para mantener la continuidad de los sistemas críticos de la institución en caso de que ocurra una eventualidad que interrumpa la fluidez de las operaciones del negocio.

3.6 Se debe procurar la adecuada segregación de funciones para prevenir la posibilidad que una única persona sea la responsable por diversas funciones críticas, de forma tal que errores o modificaciones puedan ocurrir y no ser detectados oportunamente dentro del curso normal de los procesos operativos.

3.7 Para asegurar el servicio continuo, la organización debe satisfacer los requerimientos del negocio, asegurando que los servicios de TI estén disponibles y procurar un impacto mínimo en las actividades de la organización, en caso que ocurriera una interrupción mayor.

Palabras clave: Evaluación, auditoría, seguridad física, seguridad lógica, procedimiento.

Director de la investigación:
MAI: Sergio Espinoza Guido

Unidad Académica:
Programa de Posgrado en Administración y Dirección de Empresas
Sistema de Estudios de Posgrado

Introducción

El uso de las tecnologías de información en toda entidad “per se” involucran la utilización de una combinación de recursos tecnológicos, humanos y de capital, así como la convergencia de elementos datos que constituyen valor para las organizaciones, y riesgo en caso de que sean de posible acceso por parte de terceros no autorizados. Ante el riesgo de un evento de dicha naturaleza las organizaciones se encuentran obligadas a establecer una serie de políticas, procedimientos, prácticas, utilización de recurso tecnológico de software y hardware que les permitan enfrentar situaciones no deseadas ante posibles intentos de acceso a información sensible de su organización.

Las organizaciones gubernamentales no se eximen de constituirse víctimas de un ataque a sus sistemas de información, ya sea para extraer información con fines dolosos o bien, por el simple hecho de probar la robustez de su seguridad. Adicionalmente, por la naturaleza de cada una de las organizaciones gubernamentales, son variados los tipos de información sensible que puede ser utilizada, sea esta información bancaria, propiedad de bienes, salud, entre otros.

Una de tantas instituciones es la evaluada, que se caracteriza por ser una institución autónoma con más de una década de haber sido constituida.

Aunque la información en los archivos de la institución son de libre acceso por parte de cualquier ciudadano interesado, prevalecen condiciones durante las cuales la información reviste carácter de confidencialidad, en tanto no exista una resolución firme sobre ella; siendo en este punto en donde mayormente se requiere del debido resguardo y protección de la misma en su naturaleza física, así como la contenida en los equipos y servidores.

Mediante la realización del proceso de auditoría, para cumplir con el Curso PF 2511 Práctica Profesional I de la Maestría Profesional en Auditoría de Tecnologías de Información, se procuró determinar los distintos elementos que constituyen áreas críticas para el debido manejo y custodia de la información relacionada con los procesos internos, identificar la situación real, analizar y evaluar las posibles condiciones factibles de ser mejoradas y brindar las recomendaciones pertinentes.

La oportunidad de poder aplicar los conocimientos adquiridos en los distintos cursos recibidos durante la maestría, permitió aportar a la institución, y de manera indirecta a la sociedad costarricense; insumos que al ser adoptados y aplicados por la administración, coadyuvarán a obtener una seguridad razonable de que la información procesada y custodiada por la entidad es confiable, íntegra y se encuentra disponible, en tanto así sea requerida.

El proyecto de auditoría se desarrollará con una participación directa del personal del área de Tecnologías de Información, desde donde se obtendrá la mayor parte de la información requerida, que constituirá la base fundamental para determinar las condiciones existentes en la institución en cuando a seguridad física y lógica de las TI, y que permitirá suministrarle a la administración, un análisis de su condición actual y las acciones más adecuadas para mejorarlas.

Como limitaciones que presenta el trabajo de auditoría propuesto, se cita lo siguiente:

1. Por la naturaleza del trabajo a realizar y la formación del estudiante en ciencias económicas, se requiere del soporte de un experto en informática para la posible realización de algunas pruebas u obtención de algún tipo de evidencia.

2. Al igual que muchas organizaciones públicas y privadas, el organismo sujeto de evaluación no escapa de las influencias del

comercio internacional que implica la globalización, por lo que se encuentra inmersa en un proceso agresivo de cambio tecnológico y organizacional para lograr competir con las nuevas corrientes y poder enfrentar los cambios que experimentará el país, como producto de la entrada en vigencia del Tratado de Libre Comercio. Por dicha razón los resultados de este proyecto y la información que de él se genere, debe ser manejada bajo condiciones de estricta confidencialidad, y sin opción para que la misma pueda ser divulgada, publicada, exhibida o extraída del recinto institucional. Cabe mencionar que para efectos de revisión por parte del Director del Proyecto de Graduación y los lectores académico e institucional, el resultado del trabajo se presentó en forma íntegra y considerando todos los detalles informativos necesarios.

Es oportuno destacar que si la Comisión del Programa de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica requiere información adicional, se pone a disposición según lo requiera.

Objetivos

Objetivo General

Evaluar los aspectos generales referentes a la seguridad física y lógica de aplicación por parte de la entidad en su ambiente de tecnologías de información, y obtener un informe sobre las condiciones observadas que constituyan oportunidades de mejora en dichos procesos, así como las recomendaciones respectivas.

Objetivos Específicos

1. Determinar el marco de referencia a utilizar como parte del proceso de auditoría.
2. Identificar el entorno de TI en el que se desenvuelve la organización.
3. Describir la situación actual de la institución en relación con el uso de las TI.

4. Analizar el estado actual descrito, elaborando un diagnóstico general de la situación de las tecnologías de información.
5. Evaluar los aspectos relativos a la seguridad física y lógica por medio de un programa de auditoría aplicable a la institución seleccionada.
6. Obtener mediante los resultados de la evaluación de los controles y las pruebas de campo pertinentes, las conclusiones y sus respectivas recomendaciones.

I. Aspectos Generales de seguridad

1.1 Seguridad

1.1.1 Definición

En relación con un mecanismo en general, se define la seguridad como aquella que asegura algún buen funcionamiento, evitando que éste falle, se frustre o se violente.[1]

1.1.2 Seguridad informática[2]

Se considera la seguridad informática como aquella "característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas, a efectos de que dicha información cumpla criterios de confidencialidad, integridad y disponibilidad". La seguridad en la informática abarca los conceptos de seguridad física, seguridad lógica y seguridad en las comunicaciones de los datos.

1.1.3 Seguridad Física

Está asociada con procedimientos para el desarrollo de infraestructura y acceso a los centros de cómputo y comunicaciones. La seguridad física a su vez tiene que ver con la continuidad de los procesos y servicios, y con el reestablecimiento de éstos, cuando por factores internos o externos, los mismos han sido suspendidos.
La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, amenazas o ataques con bomba, robos, catástrofes naturales, fallas de energía, picos de energía, fuentes de energía complementarias, fallas en los sistemas de aire acondicionado, sistemas de

[1] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=seguridad, 16/03/07
[2] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml , 20-03-07

control de humedad y temperatura, fallas de equipo, inundaciones, plan de contingencia, plan de continuidad del negocio, controles de acceso, entre otros.

1.1.4 Seguridad Lógica y acceso a los datos

Considera el sistema de seguridad para la confiabilidad de los datos, proceso de otorgamiento de claves de usuarios, los estándares de acceso a la red, controles para evitar el ingreso externo (paredes de fuego) y la regulación del uso de software no autorizado y el correo electrónico.

También incluye el control de acceso a Internet, procedimientos de encripción y protección de la integridad y exactitud de los datos transmitidos, la autenticación y derechos de acceso acompañado de los atributos de acceso (lectura, escritura, borrado).

La seguridad lógica tiene como objetivo garantizar que todos los equipos de la red, las aplicaciones y los datos solo sean accedidos y en general, usados por personal autorizado. Toma en cuenta aspectos relacionados con: cuentas de usuario, passwords, perfiles de usuario, backups, acceso a aplicaciones y bases de datos, pruebas de acceso y parametrización de la seguridad en los sistemas operativos, aplicaciones y bases de datos, bitácoras, protección de archivos del sistema, entre otros. Además, se consideran procesos, políticas, procedimientos y normas para la separación en las áreas de desarrollo y producción.

1.1.5 Seguridad en las comunicaciones de los datos

Las redes son sistemas de almacenamiento, procesamiento y transmisión de datos.

Están compuestas de elementos de transmisión conformados por cables, enlaces inalámbricos, satélites, conmutadores y servicios de apoyo como un sistema de nombres de dominio que incluyen los servidores raíz, servicios de identificación de llamadas y autenticación.

En las redes existe un número cada vez mayor de aplicaciones conectadas, tales como el sistema de entrega de correo electrónico, navegadores, así como equipos terminales entre los cuales se encuentran teléfonos, computadoras, teléfonos móviles, organizadores personales, aparatos electrodomésticos y máquinas industriales.

Los requisitos generales de seguridad de las redes y los sistemas de información presentan las siguientes características generales interdependientes:

a. Disponibilidad: Significa que los datos y los servicios operativos son accesibles, aún en caso de alteraciones del tipo de cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red de comunicaciones, pueda provocar interrupciones en otras redes críticas como el transporte aéreo o el suministro de electricidad.

b. Autenticación: Es la confirmación de la identidad declarada de usuarios o entidades jurídicas. Existen métodos de autenticación adecuados para muchos servicios y aplicaciones, tales como la conclusión de un contrato en línea, el control del acceso a determinados servicios y datos, los sitios Web, por ejemplo, en el caso de los bancos en Internet. Esta debe contemplar la posibilidad de mantener el anonimato, dado que muchos servicios no necesitan la identidad del usuario y sólo requieren la confirmación fiable de determinados criterios (las denominadas credenciales anónimas) como la capacidad de pago.

c. Integridad – Confirmación de que los datos enviados, recibidos o almacenados son completos y sin modificación. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica (datos médicos, diseño industrial, fórmulas industriales, entre otras).

d. Confidencialidad – Es la protección de las comunicaciones o de los datos almacenados contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es especialmente necesaria para la transmisión de datos sensibles y uno de los requisitos a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Con base en lo anterior, la seguridad de las redes y de la información puede entenderse como la capacidad de las mismas, o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los incidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y los correspondientes servicios que éstos ofrecen.[3]

1.1.6 Fuentes de Criterio

Definición de Criterio

Los criterios son normas razonables contra las cuales los controles financieros y administrativos y los sistemas de información pueden ser evaluados[4].

Son políticas o lineamientos generales dictados por una autoridad superior, que tienen como propósito orientar la acción, en este caso, de la seguridad de los sistemas de información computadorizados, como componentes para el cumplimiento de los objetivos y metas de una organización. Las políticas que se dicten deberán ser documentadas y divulgadas en los niveles pertinentes de la organización y objeto de actualización permanente.

[3] http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_es.pdf, 2-04-07
[4] Curso Proceso de Auditoría de TI/SI, UCR, Maestría en Auditoría de Tecnologías de Información

Los objetivos, metas y acciones constituyen los criterios orientadores para dirigir el desarrollo informático y su administración en todos sus aspectos, los cuales deberán ser concordantes y derivados de los objetivos, estrategias y metas organizacionales.

1.1.7 Normativa del sector público

Al igual que en algunos países, el sector público costarricense experimenta algún grado de escasez de normativa relacionada con aspectos de tecnologías de información. Como normativa de carácter general se dispone del Manual Sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados emitida por la Contraloría General de la República en noviembre del 1995, la misma que en su contenido no hace mayor énfasis a aspectos de la seguridad de tecnologías de información; contrario a lo que ocurre en el sector financiero, en el cual la SUGEF sí ha concretado más este aspecto, por medio de la Normativa de Tecnología de Información para las Entidades Fiscalizadas por la Superintendencia General de Entidades Financieras.

Como normativa complementaria, es común observar la utilización de fuentes de criterio como lo son COBIT, BS-7799, ISO – 17799, la misma normativa de la SUGEF, el uso de sanas prácticas y como última fuente, el sentido común.

Más recientemente la Contraloría General de la República ha hecho esfuerzos por actualizar la normativa del sector público, elaborando el “Manual de Normas técnicas de control interno para la gestión de las tecnologías de información (TI) que deben ser aplicadas por la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización”. Dicho manual, aunque ya fue elaborado se encuentra en etapa de revisión y aprobación, por tanto, aunque puede utilizarse como fuente de criterio, no puede ser utilizado como referencia formal.

1.1.8 Las normas de tecnología de información y los servicios de auditoría

Casi todas las normas de tecnologías de información están vinculadas con los servicios de auditoría interna o externa.

Cuando se trata de una normativa específica de tecnología de información, se establece un recargo en la función del auditor interno, si no es que se crea una auditoría interna de tecnologías de información, y además se profundiza en la necesidad de que la auditoría externa audite los sistemas de información de una manera más integral que como lo hacen cuando ofrecen servicios de auditoría tradicional (como es el caso de las auditorías de empresas de cualquier naturaleza).

Los auditores internos de sistemas de información, preferiblemente deben ser certificados por asociaciones especializadas en Sistemas de Información, quienes desarrollan un proceso de entrenamiento al amparo de las normas específicas relacionadas con TI y emiten un atestado de amplio reconocimiento mundial. .

Además, en el medio hay una sentida necesidad de que firmas de auditoría desarrollen consultorías ("*outsourcing*") de seguridad informática para las organizaciones, a efecto de fortalecer el control interno y mitigar los riesgos que entren en conflicto con los objetivos del negocio.
Las auditorías de los sistemas de información suelen ser bastante complejas abarcando entre otros temas los siguientes:

- Confirmar que la tecnología de información esté acorde con los objetivos estratégicos de la compañía;
- Evaluar la infraestructura tecnológica con base en los estándares actuales, las políticas y procedimientos en materia de tecnología y seguridad;
- Identificar los riesgos y áreas de mejora relacionadas con la seguridad;
- Evaluar las redes a nivel de vulnerabilidad y parámetros de seguridad;

- Capacidad de administración de los nuevos proyectos de desarrollo o migraciones a otras aplicaciones
- Valorar los aspectos relacionados con los recursos humanos de tecnología y sus espacios de decisión en relación con las demandas de formación y toma de decisiones de las tecnologías vigentes;
- Apoyar la construcción de planes de contingencia para superar las brechas identificadas según la priorización que determinan los riesgos y las estrategias de negocio.

1.1.9 Impacto en costos de la normativa de tecnología de información

Las normas de tecnologías de información establecen un nivel superior en la gestión del proceso informático, con niveles de seguridad y control mucho más consistentes e intensos que los que se desarrollarían en ausencia de la norma, motivo por el cual tienen un impacto directo en la estructura de costos de las empresas, en cuanto a la formación de activos de uso específico y exclusivo, así como a los costos directos para su gestión.

La normativa produce un aumento de las capacidades de las organizaciones para gestionar las tecnologías acordes con estándares de calidad y seguridad. Dicho aumento de capacidades tienden a la uniformidad en los procesos entre las organizaciones.

Algunos de los conceptos de gasto e inversión que afectan son los siguientes:

- Espacio físico adicional para separar los procesos de tecnología de información, agregando seguridad a los mismos.
- Equipos adicionales y con más capacidad, tanto de proceso como de almacenamiento.

- Software adicional para procesar la información y garantizar su adecuado almacenamiento, recuperación (restablecimiento) en caso de ser necesario y seguridad.
- Además, contratos de actualización de software más integrales que los que se tendrían en ausencia de una normativa.
- Mayor capacidad de archivo, tanto en hardware como en espacio físico, y arrendamiento de capacidad externa a la organización.
- Mayor personal para atender la división del trabajo propia de un sistema de mayor seguridad (desarrollo, implantación, mantenimiento, soporte, seguridad). A su vez, una escala salarial que se ubica en un rango alto dentro de la organización, para los responsables de las tecnologías de información con el consecuente mayor costo laboral.
- Mayores gastos en capacitación y entrenamiento del personal, tanto del área de tecnología de información como el de la organización para el manejo de las tecnologías y sus actualizaciones.
- Seguros encarecidos para los equipos informáticos, dado que en algunos países dichos seguros no existen o son de muy poca aplicación.
- Fuente de energía alternativa para enfrentar la ausencia de energía de la red pública.

La normativa establece en sí una mejora en la capacidad de gestión y aprovechamiento de las tecnologías que redundarán en mayor seguridad, competitividad y capacidad de proceso, la que a su vez permitirá mayor volumen de operación, dados los recursos existentes, costos de proceso inferiores, e incluso menos recursos destinados a revisión y corrección. Además contribuye con el logro de los objetivos institucionales de una manera eficiente y eficaz.

1.1.10 Estructura operativa para aplicar la normativa

Las organizaciones deben definir y mantener una estructura organizacional, normas de seguridad y procedimientos que les permita administrar adecuadamente los riesgos asociados a la tecnología de información, consistente con su tamaño y naturaleza, así como con la complejidad de las operaciones que realizan. Dentro de la estructura organizacional, el área de sistemas de información debe depender funcionalmente de un nivel tal que le permita garantizar su independencia de las áreas usuarias.

Las normas de tecnología de información que se derivan y sostienen en fuentes de criterio preestablecidos como las que son parciales y asociadas con el riesgo operativo, establecen diversos niveles de estructuras operativas para su atención y relación con la organización.

1.1.11 Gerencia de servicios de tecnologías de información.

Esta gerencia aparece como la culminación o maduración en una organización de los servicios de tecnologías de información. Se supone que el área de TI debe tener el rango suficiente para evolucionar de manera apropiada, tanto en lo operativo como en lo estratégico, contando con presupuestos suficientes y adecuada inserción en las actividades.

Lo que se pretende es que las gerencias en tecnologías de información asuman un rol más proactivo en la gestión de la organización, desempeñando un papel altamente participativo en los diferentes procesos, alineadas a las finanzas, las operaciones, el mercadeo, entre otros; dejando el nivel operativo que tradicionalmente ha venido ejerciendo.[5]

[5] Normativa sobre tecnología de información por parte de las Superintendencias Bancarias –Su aplicación en las cooperativas de Ahorro y Crédito. Confederación Alemana de Cooperativas. San José, C.R. http://www.dgru.org/docs/53.Normas TIC-junio final02.pdf

1.1.12 Comité de riesgos de tecnología de información.

El comité de riesgos de TI es una instancia especializada y de alto dominio del tema que normalmente está constituida por personal remunerado de la organización (la gerencia general, el gerente de servicios de información y el gerente financiero), dedicado a la gestión de la norma (o sea los riesgos) y la rendición de cuentas ante terceros, con sanciones claramente expresas si se da la circunstancia de que fallen. En algunos casos es también llamado comité de sistemas.[6]

1.1.13 Auditoría de servicios de información.

Es una instancia que se crea o se separa a partir del personal de auditoría interna de la empresa (en los casos en que exista todo un departamento como tal).

Normalmente en algunas organizaciones no existe una estructura operativa muy grande, ni una clara división de funciones, razón por la que no se refleja el área de TI, menos aún, un nivel jerárquico acorde con las aspiraciones de los estándares, ya que éstos afectan la organización e impacta en los costos.

[6] Ídem nota 5

II: Situación Actual de la Institución

2.1 Generalidades

2.1.1 Marco Legal (Reglamentos relacionados)

La entidad, en su condición de institución autónoma, se rige por su propia ley constitutiva, la normativa del derecho público aplicable a las instituciones de dicha naturaleza y debe tomar en consideración las normas de derecho privado aplicables. El marco jurídico corresponde al siguiente orden de prelación: la Constitución Política, los convenios internacionales, las leyes y los decretos ejecutivos, la jurisprudencia administrativa y judicial, los contratos, acuerdos, y la costumbre.

La Constitución Política define los derechos y deberes de los ciudadanos, del Estado y su organización, sus formas posibles de asociación, donde cabe resaltar su obligación de servir de una manera eficiente y eficaz.

Los Convenios Internacionales tocan una gran diversidad de temas, desde la Declaración Universal de Derechos Humanos hasta, más recientemente, los Tratados de Libre Comercio.

El conjunto de leyes concernientes al accionar de la institución también es una lista extensa. Se pueden mencionar en un contexto general, por ejemplo:

- Ley General de Administración Pública
- Ley de Contratación Administrativa
- Ley de Administración Financiera y de Presupuestos Públicos
- Ley General de Control Interno
- Ley contra la Corrupción y el Enriquecimiento Ilícito

Igualmente es amplia y variada la lista de leyes específicas, decretos ejecutivos, casos derivados de la jurisprudencia administrativa y judicial, y todavía más aún los contratos y acuerdos públicos, privados y mixtos. Por tanto, se requiere un dominio cada vez mayor del marco jurídico público.

En lo referente a las tecnologías de información aplicables a la entidad, la reglamentación relacionada se limita a lo establecido en el Manual Sobre Normas Técnicas de Control Interno Relativas a Los Sistemas de Información Computadorizados[7] y lineamientos, procedimientos, normas y guías internas que a la fecha se tienen definidos, los cuales seguidamente se enuncian:

LINEAMIENTOS

SI-01 – ADMINISTRACIÓN

LI-SI-01-01 Definición del Plan Estratégico

LI-SI-01-02 Arquitectura de la Información

LI-SI-01-03 Dirección Tecnológica

SI-02 – Adquisición e Implementación

LI-SI-02-06 Administración de Cambios

SI-03 – Soporte

LI-SI-03-04 Seguridad de los Sistemas

LI-SI-03-06 Administración de la Configuración

SI-04 – Monitoreo y Seguimiento

LI-SI-04-01 Monitoreo Proceso

NORMAS

[7] Manual Sobre Normas Técnicas de Control Interno Relativas a Los Sistemas de Información Computadorizados emitido por la Contraloría General de la República en el año 1995.

SI-01 – Seguridad

NO-SI-01-01 Creación de Usuario local con privilegio avanzado

NO-SI-01-02 Longitud claves privadas para acceso a la red institucional

NO-SI-01-03 Administración de claves privadas de usuario

NO-SI-01-04 Cifrado de Información

NO-SI-01-05 Respaldo de Información

NO-SI-01-06 Seguridad Física Equipos uso personalizado

SI-03 - Interno

SI-03-01 – Seguridad

NO-SI-03-01-01 Acceso al Departamento de SI

NO-SI-03-01-02 Cambio de Claves

NO-SI-03-01-03 Programa Antivirus

NO-SI-03-01-04 Conexión al firewall institucional

NO-SI-03-01-05 Pruebas de programas desconocidos

NO-SI-03-01-06 Activación de Alertas de la UPS, vía e mail

NO-SI-03-01-07 Acceso al cuarto de servidores

NO-SI-03-01-08 Acceso a Cuartos de Telecomunicaciones

NO-SI-03-01-09 Ingreso de equipo al departamento SI

SI-04 – Aplicaciones

SI-04-02 – Seguridad

PROCEDIMIENTOS

SI-01-02 – Seguridad

PR-SI-01-02-01 Administración de Usuarios

PR-SI-01-02-02 Administración Claves de acceso

PR-SI-01-02-03 Cifrado de Archivos y Carpetas en Windows

SI-01-03 – Respaldos

PR-SI-01-03-01 Entrega y recepción de respaldos (cintas)

SI-04 – Aplicaciones

SI-04-02 – Seguridad

PR-SI-04-03-02 Modificación de Datos en los Sistemas

GUÍAS

SI-01-02 – Seguridad

GU-SI-01-02-01 Cifrado de Información

GU-SI-01-02-02 Aplicación Contraseña Protección de Pantalla

GU-SI-01-02-03 Guía General de Seguridad

SI-04-02 – Seguridad

GU-SI-04-02-01 Asignación Seguridad Sistemas SIF y RH

2.2 Aspectos Administrativos

La administración enfrenta un marco operativo que procura el equilibrio de sus necesidades y transparencia en la gestión pública. Esto demanda la existencia de adecuados sistemas de información que aseguren la aplicabilidad de los preceptos de la seguridad como lo son disponibilidad, integridad y confiabilidad de la información.

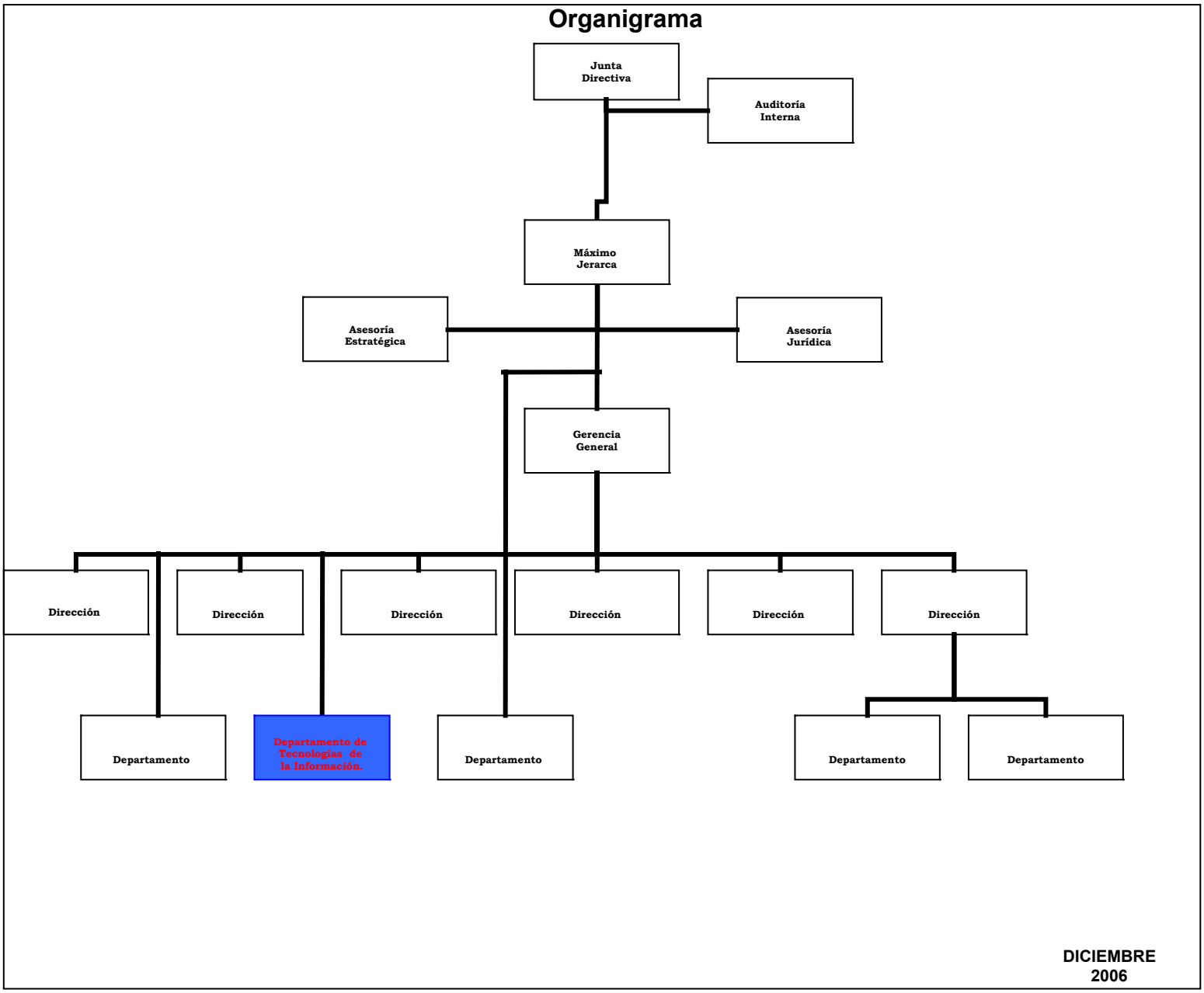
La organización de dichas responsabilidades recae en la figura del Departamento de Tecnologías de Información, quien a su vez reporta a la Gerencia General uno de los niveles más altos dentro de la estructura administrativa.

2.2.1 Estructura orgánica

La estructura organizacional de la entidad está compuesta de la siguiente forma: El nivel superior de la organización esta ocupado por la Junta Directiva, quien esencialmente define políticas. En el plano ejecutivo la estructura se apoya en el máximo jerarca a quien corresponde el control y representación de la organización. Para tal fin, además de unidades funcionales convencionales de apoyo, agrupa en direcciones especializadas distintos tópicos de su misión. Esta estructura general se aprecia en el organigrama que seguidamente se presenta.

La figura No.1 esquematiza el organigrama de la organización.

Figura No. 1


Organigrama
Junta Directiva
Auditoría Interna
Máximo Jerarca
Asesoría Estratégica
Asesoría Jurídica
Gerencia General
Dirección
Dirección
Dirección
Dirección
Dirección
Dirección
Departamento
Departamento de Tecnologías de la Información.
Departamento
Departamento
Departamento
DICIEMBRE 2006

La estructura ubica al Departamento de Tecnologías de Información en una posición elevada, lo que le permite una participación activa y mayor facilidad y agilidad en la toma de decisiones relacionadas con el desarrollo y mantenimiento de la infraestructura tecnológica.

Problemas operativos que se han dado en la puesta en marcha de ciertos proyectos de gran importancia para la institución, impulsaron la toma de dicha decisión, cuya importancia radicó en procurar lograr una objetividad, independencia y autoridad que coadyuvara en la forma de cumplir con sus objetivos de servicio y apoyo a la Institución como un todo y no sólo a una unidad determinada.

La tecnología de información ha venido escalando un nivel de importancia cada vez mayor en las organizaciones, hasta llegar a ocupar un lugar preponderante en los niveles jerárquicos, como facilitador en la toma de decisiones desde la perspectiva tecnológica. Recientemente se puede constatar que en el conglomerado de instituciones específicamente del sector público, estas unidades dependen directamente del nivel jerárquico superior, a efecto de garantizar un adecuado servicio de apoyo a los sistemas operativos y de soporte a los usuarios, que garanticen soluciones de tecnología de información efectiva y adecuada.

2.2.2 Proyectos en desarrollo

Dentro de los proyectos en desarrollo están las modificaciones a sistemas ya existentes, catalogados para estos efectos como microproyectos, que se encuentran en diversas etapas de desarrollo y entre los que se mencionan:

- **i.** Sistema de Control de Juicios, actualmente está en producción y se está confeccionando el manual de usuario.
- **ii.** Sistema de Atención de Solicitudes, el que se encuentra en desarrollo.
- **iii.** Sitio Web, en espera de la contratación de servicios profesionales para su modificación.
- **iv.** Sistema de Registro de Cobro, el cual está en etapa de desarrollo.

v. Sistema de impresión de Acciones de Personal, actualmente en proceso de desarrollo.

También existen otros proyectos de mayor magnitud que son medulares para el eficiente y eficaz desempeño de la entidad y que por su nivel de importancia son de especial análisis por parte de la administración.
Algunos de estos proyectos son los siguientes:

i. Corrección e implantación de los módulos del Sistema Administrativo Financiero y de Recursos Humanos.
ii. Diseño e implantación de Sistema de Producción y Subsistemas.
iii. Diseño e implantación del Sistema de Información de la Dirección Jurídica.

2.2.3 Aspectos Tecnológicos

En los próximos años será cada vez más relevante la aplicación de las Tecnologías de Información y Comunicaciones (TIC) en todos los campos. En ese sentido cabe tener presente que la revolución de la electrónica comenzó en la segunda mitad del siglo XIX y dio paso a las telecomunicaciones, la informática se inició a mediados del siglo XX. La conjugación de ambas, a juicio de muchos, es detonante del proceso de globalización que vivimos hoy. Su acelerado proceso de innovación tecnológica impone un ritmo de cambio tan rápido que en ocasiones es calificado como causante de crisis en otras dimensiones de la sociedad.

El aprovechamiento de las TIC se considera así parte esencial de la innovación tecnológica que demandan los mercados competitivos actuales. Por el contrario, su desaprovechamiento se perfila como mecanismos de exclusión social. Las TIC aseguran el tránsito de la información y por ende del conocimiento, reconocido éste último, hoy, no sólo como uno, sino como el principal factor de la producción.

Esta entidad no escapa a esa corriente y en los últimos años ha incurrido en inversiones cuantiosas en hardware y software, en procura de que las mismas coadyuven con el logro de sus metas y objetivos.

III. Análisis de la Situación Actual de las TIC en la organización.

3.1 Estructura organizacional del Departamento de TI

La forma en que está organizado el departamento de Tecnologías de Información lleva una connotación plana en la que en primera instancia existe un profesional jefe encargado de los aspectos administrativos de la unidad.

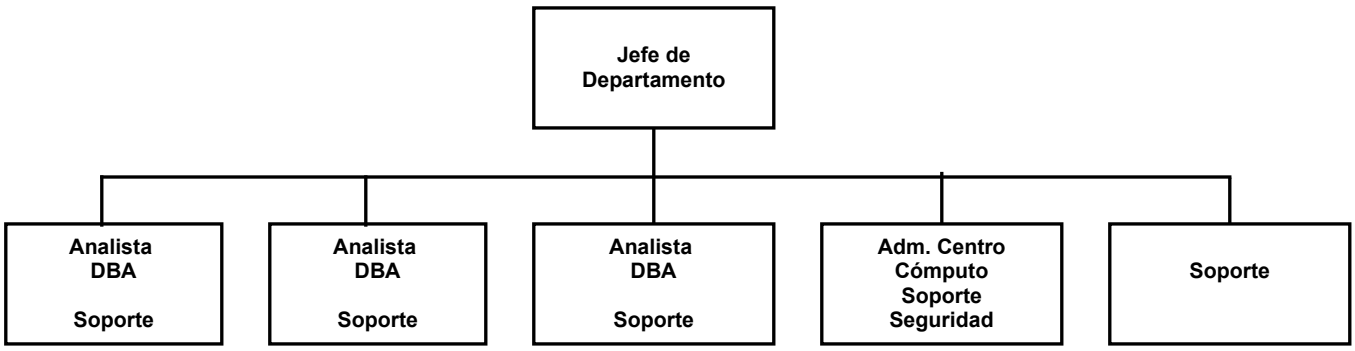
El equipo laboral está compuesto por tres analistas de sistemas cuyas funciones conllevan actividades de análisis y programación, complementadas con administración de algunas bases de datos específicas.

También existe un funcionario encargado de la administración operacional de la estructura informática, en lo que se refiere a administración y monitoreo de red, actividades relacionadas con respaldo de información y actividades de soporte en general.

Dispone además de un funcionario adicional, quien ejecuta actividades de soporte de naturaleza menor, como se aprecia en la figura siguiente.

La figura No. 2 muestra una idea gráfica de la Estructura organizacional del Departamento de TI.

Figura No. 2



3.1.1 Plan Estratégico del Departamento de TI

El Departamento de Tecnologías de Información no dispone a la fecha de un Plan Estratégico de Tecnologías de Información. Con las nuevas disposiciones de la actual Junta Directiva, se está a la espera de la elaboración del Plan estratégico de Tecnologías de Información institucional, del cual se desprenderá la plataforma de metas para elaborar el correspondiente plan a nivel del departamento de TI.

3.1.2 Plan Estratégico de Tecnologías de Información (Institucional)

Desde el año 1996 la institución ha venido elaborando el Plan Estratégico de Tecnologías de Información institucional, el mismo que a la fecha no ha sido implementado como corresponde.

En el periodo 2007 el plan estratégico de TI quedó incluido dentro del Plan Institucional, como parte de los distintos proyectos de desarrollo de software y adquisición de equipos que se consideran necesarios. Posteriormente la Junta Directiva, elaboró uno nuevo, a partir del cual se confeccionará el correspondiente al Departamento de TI, procurando su alineación con las nuevas estrategias.

3.1.3 Plataforma de TI existente

La estructura de las tecnologías de información de la organización se condensa de la siguiente manera:

3.1.3.1 Área de servidores

1. Cantidad de servidores (File Server, Mail Server, DB Server, etc.).

Servidor	Marca	Modelo	Aplicación	Producto
Antispam	Dell	Power Edge	Revisión de paquetes	Windows 2000 Server
Correo	Dell	Power Edge	Envío y recepción de correo	Sist. Operativo Linux
Servidor Web	Fujitsu Siemmens	Primergy	Archivos Web	Windows 2003 Server
Controlador Dominio Primario	Dell	Optiplex	Adm. Cuentas de usuario	Windows 2002 Server
Controlador Dominio Secundario	Dell	Optiplex	Servidor de respaldo I	Windows 2000 Server
Servidor de Respaldos y antivirus	Dell	Power Edge	Actualizaciones de antivirus	Windows 2002 Server
Servidor BD	Dell	Power Edge	BD otros	Windows 2000 Server
Servidor BD	Dell	Optiplex	BD Clientes	Windows 2003 Server
Servidor Archivos	Hewleth Packard	Compaq	Almacena Archivos diversos	Windows 2002 Server
Servidor Sistema Contable	Fujitsu Siemmens	Primergy	Almacena y permite acceso a información que se genera en el sistema. Administra y almacena logs del firewall	Sist. Operativo Linux
Servidor de archivos generales	Dell	Compaq Proliant	Almacena de las diferentes direcciones y de carácter público	Windows 2000 Server
Servidor de Pruebas	Dell	Power Edge	Pruebas	Windows 2002 Server
Unidad de respaldo	Hewleth Packard	Compaq	Unidad de respaldos	

Nota: La información de este cuadro y siguientes fue modificada para efectos de guardar la confidencialidad.

2. Cantidad de sistemas operativos y su aplicación. [Función en la que se utilizan. (Windows 2000, NT, Unix, Linux, etc.)].

Producto	Aplicación
Windows NT	Base de Datos, Antispam, Web, controlador de dominio, Respaldos, Antivirus, Sistema Contable, Archivos Generales, Pruebas.
Sist. Operativo Linux	Correo, Contabilidad
Windows 2003 Server	Web institucional
Windows NT	Uso en las distintas PC´s de usuarios de la red

3. Cantidad de tipos bases de datos, entiéndase Data Base Manager System. (Oracle, SQL, Sybase)

Base de Datos	Uso
Microsoft SQL	Los mismos según cuadros anteriores
SyBase Data Base	Sistema contable y mismos según cuadros anteriores

4. Herramientas disponibles a lo interno para desarrollo de sistemas.

Lenguaje de programación
Microsoft:
Visual Basic
Power Soft:
Power Builder

3.1.3.2 Área de comunicaciones Lan

1. Cantidad y marca de equipos de comunicación (Router, Switch, Hubs, etc.)

Cantidad	Componentes	Marca	Función
1	Enrutador	D Link	Conexión LAN –Internet
1	Firewall	Sonicwall	Protección contra ataques,

			denegación sitios Internet
1	Pix Firewall	Sonicwall	No está en operación por causas desconocidas
4	Switch (Primer piso)	Varias	Conexión de los dispositivos de la red
4	Switch (Segundo piso Rack del Sistema)	Varias	Conexión de los dispositivos de la red
4	Switch (Rack II)	Varias	Conexión de los dispositivos de la red
		Varias	Conexión de los dispositivos de la red
1	Tercer piso Switch	Varias	Conexión de los dispositivos de la red

2. Cantidad y tipos de enlaces de comunicación (Frame Relay, ISDN (PRI/BRI), Dedicados, E1, etc.)

   Sólo se cuenta con un único enlace de 2mbps.

3. Tipo de cableado.

a) Cable UTP categoría 5B
b) Líneas de Fibra óptica
c) Acceso inalámbrico

3.1.3.3 Área perimetral (Internet)

1. Se dispone de cuatro direcciones públicas utilizadas para el enlace principal, servidor Web, antispam, y servidor de correo.

2. Cantidad y tipo(s) de conexión a Internet.

Cantidad	Tipo de enlace
1	E1

3. El Tipo de administración del Web es Local (Costa Rica).

4. Uso de Firewall.

Tipo de Firewall	Marca	Definición	En uso
Hardware	Sonicwall	Software	No
Hardware	Sonicwall	Software	Sí

5. Servicios públicos o privados por Internet.

Tipo de Servicio	Público o Privado
Acceso a correo electrónico	Ambas
Acceso a servidor Web	Ambas

3.1.3.4 Área interna

1. Se dispone de 350 estaciones de trabajo (PC's) y 71 equipos portátiles.

2. La Cantidad de sistemas operativos en las estaciones de trabajo (Windows 95/98, Windows 2000, Windows XP Profesional, etc.).

Cantidad	Marca	Modelo	Sistema Operativo	Programas	Cantidad
75	Dell	GX260	Windows XP	Microsoft Office 2003	75
150	HP	D530	Windows XP	Microsoft Office 2003	150
50	Dell	GX 620	Windows XP		50
125			Windows XP	Microsoft Office 2003	125

3. Existe todo un compendio de políticas, lineamientos y procedimientos relacionados con la administración, control, seguridad y monitoreo de las TI.

IV. Proceso de Auditoría

4.1 Objetivos

Tanto los objetivos generales como específicos, se han definido detalladamente en la sección introductoria.

4.2 Alcance

Tal como se detalla en el apartado de desarrollo del informe, el estudio se orientará a verificar las generalidades de un entorno de seguridad física - lógica y en las áreas sensibles de la organización (Departamento de Tecnologías de Información, cuarto de servidores, racks de comunicación).

4.3 Criterios Generales de Auditoría.

Los criterios constituyen las normas, estándares y procedimientos razonables, contra los cuales los controles de seguridad física y lógica, aplicados a los sistemas de información pueden ser evaluados, y éstos deberán ser definidos de previo a la iniciación de la evaluación.

Como principal fuente de criterio a utilizar durante el desarrollo del trabajo, como marco de referencia, será los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), por cuanto al reunir las buenas prácticas en el uso de las tecnologías de información, reúne los mejores principios que una organización como la evaluada, ausente de la adopción de un estándar internacional en ese sentido, puede utilizar, aplicando de él aquellas condiciones que puedan ser aplicables a su entorno.

También se utilizarán, de conformidad con las situaciones que se detecten, criterios que estén respaldados en normativa del sector público costarricense que sea aplicable.

En el Capítulo IV, sección 4.7, apartado 1.4 del informe se detallan ampliamente los criterios utilizados.

4.4 Planificación

El objetivo en esta etapa es proveer al auditor un entendimiento de la importancia de TI en la organización por auditar, para establecer el enfoque de la auditoría con base en la selección de los componentes significativos de TI, la indagación o exploración de los más prioritarios y la determinación de los proyectos de auditoría para el examen y verificación de los criterios y el cumplimiento de las metas de auditoría.[8]

La planificación del trabajo de auditoría específicamente incluye las siguientes fases:

4.4.1 Planificación Preliminar

4.4.1.1 Un conocimiento de la entidad con énfasis en la seguridad de las tecnologías y sistemas de información.

Se define el conocimiento como un conjunto de datos sobre hechos, verdades o de información ganada a través de la experiencia o del aprendizaje (a posteriori), o a través de introspección (a priori). El conocimiento es una apreciación de la posesión de múltiples datos interrelacionados que por sí solos poseen menor valor cualitativo.[9]

[8] Curso Proceso de Auditoría de TI/SI, UCR, Maestría en Auditoría de Tecnologías de Información

[9] http://www.google.co.cr/search?hl=es&defl=es&q=define:Conocimiento&sa=X&oi=glossary_definition&ct=title, 03-04-2007

En el caso sujeto de estudio, el conocimiento de entidad está integrado por el análisis general de todos los elementos relacionados con TI, de los cuales dispone la organización, y que considera aspectos como planes estratégicos institucionales y de TI, estructura organizacional y departamental de TI, plataforma de TI, estándares internacionales relacionados, normativa, políticas, procedimientos y demás aspectos que fueron cubiertos y detallados en el capítulo III: Análisis de la Situación Actual de las TIC.

También comprende la realización de las siguientes actividades:

i. Revisión de las metas globales y objetivos por medio de un examen de la legislación relevante de la entidad, auditorías anteriores y archivos permanentes de auditoría de estudios similares.
ii. Revisión del proceso de planificación y presupuesto, particularmente los relativos a las tecnologías y sistemas de información.
iii. Revisión de la estructura de la organización, particularmente estructura del Departamento de Tecnologías de Información, su integración y conformación funcional.
iv. Realización de entrevistas preliminares con el personal clave de TI.
v. Realización de una inspección preliminar a las instalaciones.
vi. Identificación y selección de áreas de potencial importancia de TI para ser exploradas con detalle.

vii. Preparación de un Programa de Planificación Detallada con los componentes significativos de TI por explorar.

4.4.1.2 Identificación y selección de aspectos de seguridad que constituyen elementos significativos de TI, con base en criterios preestablecidos.

Para la identificación de los elementos de seguridad física y lógica sobre los cuales se orientarán los recursos, se realizó una evaluación de riesgo cuyos resultados se visualizan en el Anexo No. 1

Para realizar el análisis de riesgo se utilizó la metodología que proporciona el modelo de riesgos de negocios PROTIVITI. Se definió un mapa conceptual de riesgos (ver Anexo No. 2), el cual se aplicará únicamente para el proceso de seguridad física y lógica del TI y se medirá con los criterios de valuación que se detallan en el Anexo No. 3. De conformidad con los resultados obtenidos, se considera pertinente incluir en la evaluación de los riesgos con un valor alto (con rango entre 9 y 15 inclusives).

4.4.1.3 Elaborar un Programa de Planificación Detallada

Conlleva la preparación de un programa detallado con los componentes significativos de TI por explorar.

4.4.2 Planificación Detallada

Esta parte de la planificación comprende, mediante técnicas de recopilación de información, realización de reuniones, observación, aplicación de cuestionarios y una evaluación de la información obtenida, para identificar las áreas de potencial importancia y decidir si

corresponden ser revisadas con mayor profundidad en la etapa de examen y pruebas de auditoría. Sobre ellas se aplicarán las herramientas como guías de auditoría, procedimientos de investigación, listas de chequeo, entrevistas, reuniones, pruebas a los distintos sistemas, que el auditor considere necesarias para realizar su trabajo.

Comprende las siguientes etapas:

4.4.2.1 Preparación de papeles de trabajo (PT's)

4.4.2.2 Examen o Verificación

- Preparación de programas de auditoría
- Efectuar pruebas de control
- Efectuar pruebas sustantivas
- Desarrollo de oportunidades de mejora
- Preparar el borrador del informe

4.5 Preparación de papeles de trabajo (PT's)

Los papeles de trabajo son documentos de distinta naturaleza que registran el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor, y los resultados y conclusiones extraídas de la evidencia obtenida.

Se utilizan para controlar el progreso del trabajo realizado y para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.[10]

Este informe ha sido sustentado en resultados obtenidos a partir de la información analizada y plasmada en el legajo de papeles de trabajo existente, mediante documentos físicos y electrónicos.

[10] http://www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indp.htm,, 03-04-07

4.6 Examen o Verificación

La etapa de examen o verificación resume la actividad generadora de insumos para la redacción del documento respectivo y la comunicación de resultados al auditado. En esta fase se elaboran los programas respectivos, se ejecutan las pruebas de control y sustantivas que le permiten al auditor desarrollar las oportunidades de mejora detectadas, la cuales serán expuestas e informadas al auditado por medio de un informe de auditoría.

4.7 Comunicación de resultados

De acuerdo con lo que establece las normas 2400[11] de Comunicación de Resultados, los auditores internos deben comunicar las derivaciones del trabajo oportunamente, y la comunicación debe contener, entre otros aspectos, los siguientes:

- Los objetivos y alcance del trabajo así como las conclusiones correspondientes
- Las recomendaciones
- Los planes de acción
- Debe incluir, si corresponde, la opinión general del auditor interno.
- Se debe reconocer cuando se observa un desempeño satisfactorio.
- Las comunicaciones deben ser precisas, objetivas, claras, concisas, constructivas, completas y oportunas.
- Comunicar los resultados finales a las personas que puedan asegurar la debida consideración.

[11] De acuerdo con las Normas para el Ejercicio Profesional de la Auditoría Interna de The Institute of Internal Auditors, http://www.imai.org.mx/servicios/Definicion/normprof.html, 03-04-2007

Comunicación de resultados.- De conformidad con la Ley General de Control Interno # 8292 artículo 35, los hallazgos, las conclusiones y recomendaciones de los estudios realizados por la Auditoría interna, deben comunicarse oficialmente al jerarca o a los titulares subordinados de la administración activa, con competencia y autoridad para ordenar la implantación de las respectivas recomendaciones, los cuales deberán regirse por las directrices emitidas por la Contraloría General de la República. Se elaborará el borrador del informe para ser discutido con los jerarcas de la empresa, hasta llegar al informe definitivo; el cual presentará esquemáticamente en forma de matriz, cuadros o redacción simple y concisa que destaque los problemas encontrados, los efectos y las recomendaciones de la Auditoría.

Seguidamente se presenta el informe elaborado como producto de la revisión efectuada.

“INFORME DE REVISIÓN DE LA EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN”

1. INTRODUCCIÓN

1.1 Origen

El presente estudio de realizó de conformidad con lo dispuesto en el plan anual de trabajo de la Auditoría Interna para el año 2007.

1.2 Objetivos.

1.2.1 Objetivo General y Específico

Tanto los propósitos populares como concretos, se han definido detalladamente en la sección introductoria.

1.3 Alcance.

El estudio se orientará a verificar las generalidades del entorno de seguridad física y lógica, partiendo de la existencia de normativa, políticas y procedimientos para los procesos vinculados con la parte física, existente en las áreas sensibles de la organización (Departamento de Tecnologías de Información, cuarto de servidores, racks de comunicación). En lo correspondiente al área lógica, se revisará lo adecuado de la normativa existente, así como las condiciones generales de la normativa relacionada con la configuración de algunos servidores, la asignación de contraseñas y claves de acceso para usuarios y administración de servidores.

1.4 Criterios Generales de Auditoría.

Como principal fuente de criterio a utilizar durante el desarrollo del trabajo, serán los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), por cuanto al reunir las buenas prácticas en el uso de las tecnologías de información, incorpora los mejores principios que una organización como la revisada, ausente de la adopción de un estándar internacional en ese sentido, puede utilizar y tomar como marco de referencia, adoptando de él aquellas condiciones que puedan ser aplicables a su entorno.

También se utilizarán, de conformidad con las situaciones que se detecten, criterios que estén respaldados en normativa del sector público costarricense que sea aplicable.

Seguidamente se detallan los criterios utilizados:

1. La institución debe contar medidas de protección relacionadas con seguridad física .y demás factores no deseados del ambiente.
2. La organización debe poseer un adecuado proceso de administración de medidas de seguridad física y lógica
3. Se debe proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas.
4. Deberán establecerse procedimientos apropiados que aseguren que las personas que no formen parte del grupo de funcionarios de Tecnologías de Información, sean escoltadas por algún miembro de ese grupo, cuando deban permanecer en las instalaciones de cómputo.
5. La seguridad en TIC deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos del negocio.
6. Deberán establecerse los mecanismos necesarios de control de identificación, autenticación y acceso que faculten el ingreso lógico a los recursos de TIC, sólo a personal autorizado.

7. Se deberá disponer de procedimientos necesarios para asegurar acciones oportunas en lo relacionado con la solicitud, establecimiento, emisión y suspensión de cuentas de usuario.
8. La organización debe contar con la capacidad para administrar los incidentes de seguridad física y lógica, debiendo establecer las responsabilidades y procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los acontecimientos de seguridad.
9. Todo elemento de TI relacionado con seguridad debe estar protegido contra intromisiones no autorizadas para proteger su integridad.
10. Se deberá contar con sistemas adecuados de seguridad que protejan a la organización en un ambiente de Internet, Intranet, Extranet y accesos inalámbricos.
11. Se debe asegurar que los servicios de TI estén disponibles cuando se requieran y asegurar el impacto mínimo en el negocio cuando un evento que se presente produzca una interrupción mayor.
12. La unidad de TI debe implementar procedimientos acordes con políticas de seguridad que garanticen el control de acceso, que tome como base las necesidades individuales demostradas de hacer y no de saber.
13. La administración deberá realizar mantenimiento preventivo sobre las UPS y generadores de energía para las aplicaciones críticas de TI, con el fin de asegurarse contra fallas y fluctuaciones eléctricas.
14. La organización debe proteger la integridad de todos los dispositivos que son utilizados para almacenamiento o traslado de información sensitiva y que tome en consideración el tipo de información a movilizar, dispositivos empleados y métodos de protección utilizados.
15. Se debe tener una adecuada segregación de labores, la definición de políticas, funciones y responsabilidades, así como la asignación de personal[12]

[12] (Norma 4.6 *Separación de funciones incompatibles*, Manual de Normas Generales de Control Interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización).

16. La prestación óptima de los servicios de TI debe apoyarse en una estructura organizacional que garantice una adecuada segregación de funciones.
17. La Gerencia deberá asegurar que todos los datos incluso aquellos que no requieran protección, sean clasificados en términos de sensibilidad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación previamente definido.
18. Las prácticas de administración de seguridad lógica de la red deben ser comunicadas, comprendidas e impuestas.
19. La administración debe asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada (Administración de operaciones).
20. Las funciones de control de la red deben ser realizadas por operadores técnicamente calificados.
21. Debe disponerse de planos de telecomunicaciones que permitan una adecuada administración, eliminación, reparación y ampliación de la red.
22. La organización debe disponer de políticas, normas y procedimientos relativos a la seguridad física y lógica que incluya el correo electrónico, acceso a la Web, protección de la infraestructura, datos y comunicaciones.
23. Se deben establecer estrategias para culturizar permanentemente a los usuarios sobre la importancia de la seguridad física y lógica.

2. ASPECTOS DETECTADOS QUE CONSTITUYEN OPORTUNIDADES DE MEJORA

FACTORES AMBIENTALES	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 1	**C/I**

	TITULO: Seguridad Física dentro del centro de cómputo
	CONDICION: Al momento del estudio, se determinó que el centro de cómputo presenta una serie de oportunidades de mejora relacionadas con controles ambientales y de acceso. Algunas de ellas son: Carencia de: Alarma contra robo Alarma contra humo Sistema detector de incendio Sistema detector de líquidos Un extintor de incendios dentro del centro de cómputo, de un tamaño adecuado para los equipos en ella contenidos. Un sistema supresor de incendios Piso falso a prueba de inundaciones Controles de humedad Medidores de humedad Bitácora donde se registre la entrada de terceros al centro de cómputo Salidas de emergencia Otras condiciones: El cielorraso no es a prueba de filtraciones Existencia de ventanas con celosías dentro del centro de cómputo Inexistencia de políticas y directrices al respecto por parte de la administración
	CRITERIO: Deberá disponerse de adecuadas medidas de protección contra factores ambientales. La seguridad en TIC deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos del negocio.
	CAUSA: Dentro de las prioridades de la administración no ha sido considerada la necesidad de reforzar estos aspectos.
	EFECTO: Las exposiciones físicas f y ambientales del centro de cómputo podrían tener como consecuencia afectación en la atención al público, pérdidas financieras para la institución, derivadas de interrupción de operaciones, menoscabo de credibilidad ante clientes internos y externos.
	CONCLUSIÓN: El centro de cómputo de la entidad carece de una serie de controles ambientales y de acceso físico, necesarios para asegurar una razonable continuidad de las operaciones y por ende del servicio que se presta a la comunidad.
	RECOMENDACIÓN: **Al máximo jerarca.** Realizar y ejecutar las acciones pertinentes para implementar los controles ambientales y de acceso restringido que sean necesarios. Crear, documentar, aprobar, publicar, y divulgar políticas y normativas que incluyan lineamientos en

	cuanto a las condiciones óptimas en que se debe mantener el centro de cómputo, así como la periodicidad de revisiones de equipo de control ambiental como aires acondicionados, extintores y otros. Asignar la responsabilidad de la aplicación, revisión, mantenimiento y actualización a funcionarios del centro de cómputo, quienes deberán velar por su cumplimiento. Se deberá implantar el uso de una bitácora en la puerta de entrada al centro de cómputo, en donde se registre el ingreso de terceros debidamente autorizados. Dichas bitácoras deben procurar obtener la siguiente información: Nombre del visitante, motivo de ingreso, persona que lo acompañará durante su permanencia, fecha y hora de ingreso y salida. Deberá nombrarse un responsable de revisar periódicamente la bitácora para asegurar que todo visitante tenga un motivo laboral válido que justifique su ingreso. Al ser el centro de cómputo el lugar donde se almacenan los componentes más críticos que soportan la plataforma tecnológica de la institución, es de suma importancia que ésta tenga todos los controles de restricción de acceso y controles ambientales para proteger el equipo contra desastres y así mitigar el impacto de una eventualidad.
	REACCIÓN DE LA ADMINISTRACIÓN: La administración reconoce existencia de las debilidades mencionadas y se encuentra en proceso de una reestructuración de toda la estructura de TIC.

FACTORES AMBIENTALES	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 2	C/I

	TITULO: Puesto y función de administración de la seguridad informática
	CONDICION: Dentro de la estructura organizacional del departamento de TI de la entidad no se define el puesto de administración de la seguridad informática y aunque la función como tal se encuentra asignada "de hecho" a una funcionaria, también es responsable de otras actividades como lo son administración del centro de cómputo, soporte, monitoreo de red, lo que limita su disponibilidad para ejecutar actividades propias de un administrador de seguridad.
	CRITERIO: 3. Una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas, acordes con el negocio y que facilita la estrategia y provee una dirección efectiva y un control adecuado, con el fin de disponer de una segregación de funciones óptima.
	CAUSA: El departamento no dispone de recurso humano suficiente como para realizar la segregación de funciones de manera específica y distribuye actividades afines entre el personal existente.
	EFECTO: No se le da el debido control, monitoreo y seguimiento a eventos que puedan constituir riesgo para los sistemas informáticos institucionales. Carencia de disponibilidad para llevar a cabo proyectos y tareas propias de administración de la seguridad, lo que disminuye la eficacia o efectividad con que se ejecuten las mismas.
	CONCLUSIÓN: El centro de cómputo de la institución no dispone de un puesto de administración de la seguridad y las funciones son compartidas con otras que compiten con la disponibilidad de recurso humano y de tiempo.
	RECOMENDACIÓN: Efectuar una evaluación de las necesidades reales del recurso humano para el departamento de tecnologías a efecto de que se tomen las medidas necesarias para que las funciones de administración de la seguridad puedan ser otorgadas a un responsable que pueda ejecutar dicha función bajo estándares de seguridad acordes con las mejores prácticas y requerimientos de la entidad.
	REACCIÓN DE LA ADMINISTRACIÓN: La administración reconoce la necesidad y mediante la contratación de una consultoría, espera definir y solucionar ésta y otras necesidades de TI.

FACTORES AMBIENTALES	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 3	**C/I**

	TITULO: Ausencia de un plan de contingencia
	CONDICION: La INSTITUCIÓN carece de un plan de contingencia formalmente documentado, divulgado, aprobado, probado y funcional, que esté alineado con el plan de contingencia del negocio, relacionado con sus requerimientos; en el que se formalicen los roles, responsabilidades y procedimientos que se deberán seguir en caso de una eventualidad.
	CRITERIO: 3. La organización debe poseer un adecuado proceso de administración de medidas de seguridad.
	CAUSA: Dado el ciclo de madurez de TI en que se encuentra la institución, no se ha dado la orientación adecuada y suficiente, a nivel institucional, para atender la necesidad de contingencias.
	EFECTO: Acciones correctivas insuficientes e ineficientes ante situaciones emergentes no previstas voluntarias e involuntarias; tal como fallos que interrumpan las operaciones críticas de la institución por un periodo indefinido, generando consigo pérdidas financieras, de reputación frente a los clientes internos y externos, daño de los equipos y pérdida de información clave para la continuidad del negocio.
	CONCLUSIÓN: La carestía de un plan de contingencia expone los recursos institucionales de TI, la información, el procesamiento de la información que debe ser recuperada y la continuidad de las operaciones y sistemas.
	RECOMENDACIÓN: Es necesario que la administración activa promueva la elaboración, comunique y divulgue el plan de contingencia para mantener la continuidad de los sistemas institucionales más críticos en caso de que ocurra una eventualidad que afecte la fluidez de las operaciones del negocio. Dichos planes deberán definir detalladamente los procesos alternativos a seguir para minimizar el impacto de las fallas y la interrupción de las operaciones, así como definir los responsables de ejecutar las diversas acciones. Este plan deberá ser probado en forma periódica mediante simulacros y revisado anualmente cada vez que surjan cambios significativos en las operaciones o estructura de TI, notificando a cada una de las personas involucradas siempre que se presente una modificación. .
	REACCIÓN DE LA ADMINISTRACIÓN: La administración es consciente de la necesidad y sus consecuencias. Mediante la definición del plan estratégico 2007-2010 espera definir y solucionar ésta y otras necesidades de TI.

	TÍTULO: Acceso a los archivos y programas de producción por parte de los programadores, analistas y operadores.
	CONDICIÓN: Como parte de la evaluación de las actividades de control interno, se observó que los analistas realizan funciones de DBA, programación y soporte, teniendo acceso a las bases de datos de producción como administradores y usuarios.
	CRITERIO: La unidad de TI debe implementar procedimientos acordes con políticas de seguridad que garanticen el control de la seguridad de acceso, tomando como base las necesidades individuales demostradas sobre la necesidad de hacer y no de saber. Deberán separarse y distribuirse entre los diferentes puestos, las funciones que, si se concentraran en una misma persona, podrían comprometer el equilibrio y la eficacia del control interno y de los objetivos y misión institucionales, de tal manera que el control por la totalidad de su desarrollo no se concentre en una única instancia.
	CAUSA: El departamento no posee el recurso humano suficiente para atender esta necesidad. Carencia de una adecuada segregación de funciones y controles complementarios para garantizar el control interno
	EFECTO: El hecho que los analistas de sistemas tengan acceso al ambiente de producción, como usuarios y DBA podría implicar la materialización de los siguientes riesgos: Pérdida o corrupción de datos Pérdida financiera Afectación de la confiabilidad, exactitud, confidencialidad y disponibilidad de la información
	CONCLUSIÓN: Inadecuada segregación de funciones en las actividades de análisis de sistemas y programación, así como el acceso por parte de los analistas al ambiente de producción, incumple con lo que establecen los lineamientos sobre sanas prácticas que sugieren la separación de los ambientes de pruebas y producción, así como la restricción por parte de los analistas a este último.
	RECOMENDACIÓN: Tal como lo establecen las sanas prácticas, el acceso al código y datos debe ser restringido para los analistas, por lo que la jefatura de TI debe responsabilizarse de efectuar la debida segregación de funciones de tal forma que garantice la integridad del dato en todo momento. Para una efectiva segregación de funciones, se debe definir el perfil de puesto y asignación de responsabilidades por escrito. Conviene incluir la figura de supervisión que vele por el correcto desempeño del personal. No se debe permitir el ingreso de analistas y programadores a producción a menos que sea supervisado por la unidad usuaria que eventualmente se vería afectada. Cuando las necesidades de personal no lo permiten, deberán establecerse controles compensatorios que disminuyan el riesgo resultante de una inadecuada segregación de funciones. Dentro de los controles compensatorios por implementar se citan:

	Rastros de auditoría: Deberán proveer un mapa que muestre la secuencia de las transacciones realizadas por los funcionarios, indicando usuario que la realizó, punto de origen, fechas y horas de inicio y terminación, tipo de transacción, campos afectados y archivos actualizados. Estos rastros de auditoría deben ser monitoreados por un tercero ajeno al Departamento de Tecnologías de Información. Reconciliación: Sugiere la realización de un proceso de verificación de la información, principalmente de carácter financiero – contable, de tal forma que permita comprobar que las transacciones se encuentran adecuadamente balanceados, por ende, las aplicaciones corrieron de manera correcta. . Revisiones independientes: Tienen como fin ayudar a identificar errores, fallas intencionales o irregularidades, además de comprobar el adecuado cumplimiento de los procedimientos vigentes.
	REACCIÓN DE LA ADMINISTRACIÓN: Son conocedores de la situación

OPORTUNIDAD DE MEJORA
No. 5

	TITULO: Factores ambientales relacionados con el ambiente de TI
	CONDICION: Al momento del estudio, se determinó la existencia de algunas prácticas humanas que crean riesgo para las tecnologías de información de la institución, tales como: √ Ausencia de sistema de alarmas para la detección de intrusos en horas no laborales √ Ausencia de dispositivos para la identificación de usuarios en la entrada al centro de cómputo √ Aunque existe vigilancia 24 horas al día, la misma no es continua en el centro de cómputo √ Ventanales sin protección con verja o cortinas de acero
	CRITERIO: 3. Deberá disponerse de adecuadas medidas de protección contra factores ambientales. La administración debe garantizar la seguridad de sistemas que satisface los requerimientos de negocio procurando salvaguardar la información contra uso no autorizado, divulgación, modificación, daño o pérdida.
	CAUSA: Por el grado de madurez en que se encuentran las tecnologías de información, la administración no ha considerado el nivel de importancia para establecer controles al respecto.
	EFECTO: Las exposiciones físicas constituyen focos de riesgo tales como intentos de ingreso no deseados cuya materialización podría ocasionar pérdidas financieras derivadas de interrupción de operaciones , de credibilidad ante clientes internos-externos, por deterioro de su infraestructura y equipos; y posibilitan los actos no autorizados, fraude, robo, divulgación de información, daño a los activos institucionales, entre otros.
	CONCLUSIÓN: La infraestructura de la entidad carece de una serie de controles de acceso físico, necesarios para una satisfactoria seguridad de las tecnologías de información ubicadas dentro de su edificio.
	RECOMENDACIÓN: La Gerencia General debe evaluar la conveniencia de que se establezcan controles que permitan solventar las deficiencias detectadas, procurando establecer controles compensatorios (Vg. incremento de rondas de vigilancia, incremento de puntos de control para dichas rondas), para aquellos casos en los cuales es posible por alguna razón, implantar un control específico. Igualmente se debe implementar sistema de alarmas para la detección de intrusos en horas no laborales, así como dispositivos para la identificación de usuarios en la entrada al centro de cómputo y verja o cortinas de acero para aquellos ventanales que se encuentran sin protección.
	REACCIÓN DE LA ADMINISTRACIÓN: Medidas correctivas al respecto podrían ser consideradas dentro del plan estratégico 2007-2010 que está en proceso de elaboración.

PLANTA FÍSICA	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 6	**C/I**

	TITULO: Elementos que constituyen oportunidad de mejora en cuanto a planta física
	CONDICION: Se detectaron aspectos que pueden ser mejorados relacionados con condiciones de acceso y naturaleza de planta física, entre las cuales se citan: √ Aunque es común que se revise el ingreso y salida de personas a la institución, no se lleva un control estricto de ellas y no se usan dispositivos de identificación. √ Se carece de un generador de emergencia en caso de fallo en el fluido eléctrico √ Insuficiencia de luces de emergencia en el centro de cómputo. √ El centro de cómputo carece de red eléctrica independiente. √ Se carece de dispositivos para liberar energía estática.
	CRITERIO: 3. La seguridad en TIC deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos del negocio. La organización debe poseer un adecuado proceso de administración de medidas de seguridad. Se debe proporcionar un ambiente físico conveniente que proteja al equipo y al personal de TI contra peligros naturales o fallas humanas. La administración deberá evaluar regularmente la necesidad de generadores y baterías de suministro ininterrumpido de energía para las aplicaciones críticas de TI, con el fin de asegurarse contra fallas y fluctuaciones de energía.
	CAUSA: Por el grado de madurez en que se encuentran las tecnologías de información, la administración no ha considerado el nivel de importancia para establecer controles al respecto.
	EFECTO: Las exposiciones físicas mencionadas constituyen elementos que pueden afectar significativamente la continuidad de las actividades críticas, deterioro o daño de los equipos con pérdidas financieras para la organización, y pérdida de imagen.
	CONCLUSIÓN: La existencia de condiciones deficientes en cuanto a equipos y componentes complementarios a la actividad de TI, podrían afectar la eficiencia y eficacia de las operaciones y la salvaguarda de los activos (hardware, software e información)
	RECOMENDACIÓN: La administración deberá evaluar, a la luz de las fallas de energía y otras necesidades que haya experimentado en el último periodo, si es justificable la instalación de equipos e infraestructura o que coadyuve con la mejoría de las condiciones detectadas, y proceder con su adquisición. Caso contrario, establecer los controles complementarios pertinentes que disminuyan los posibles riesgos relacionados. Se debe implementar los mecanismos de control necesarios que permitan evidenciar la admisión y salida de aquellas personas ingresan a la institución, así como la debida identificación que permita detectar en cualquier momento y lugar, que se trata de un visitante.
	REACCIÓN DE LA ADMINISTRACIÓN: Estos aspectos serán considerados y evaluados mediante la definición del plan estratégico de TI 2007-2010 en proceso de elaboración.

OPORTUNIDAD DE MEJORA
No. 7

	TITULO: Control de dispositivos de almacenamiento
	CONDICION: Prácticas de manejo y administración de los dispositivos de almacenamiento pueden ser mejoradas ya que durante la revisión la administración manifestó, mediante cuestionario, no llevar una bitácora de control para aquellos dispositivos que son eliminados del centro de cómputo, no hay un responsable de transportar los equipos y dispositivos dentro y fuera de la institución, salvo en casos en que medie una garantía, y algunos dispositivos de almacenamiento no están siendo controlados en cuanto a su uso e información que se transfiere. (Barras de memoria).
	CRITERIO: La organización debe proteger la integridad de todos los dispositivos que son utilizados para almacenamiento o traslado de información sensitiva, tomando en consideración el tipo de información a movilizar, dispositivos empleados y métodos de validación utilizados.
	CAUSA: El departamento no dispone de políticas y lineamientos en cuanto al uso, manejo y desecho de dispositivos de almacenamiento.
	EFECTO: El uso, carente de todo control para algunos dispositivos de almacenamiento, constituye riesgo de fuga de información, manipulación y utilización de la misma con fines no autorizados, con el posible riesgo de pérdida de imagen, información y daños financieros para la institución.
	CONCLUSIÓN: Existen prácticas de manejo y administración de los dispositivos de almacenamiento que requieren ser mejoradas mediante la implantación de controles diversos.
	RECOMENDACIÓN: Deben establecerse y poner en práctica políticas y lineamientos en cuanto al uso, manejo y desecho de dispositivos de almacenamiento, a efecto de que se procure un adecuado uso y custodia de la integridad de la información institucional.
	REACCIÓN DE LA ADMINISTRACIÓN: La administración reconoce la necesidad de mejora en cuanto al control de dispositivos y componentes varios.

POLÍTICAS DE SEGURIDAD	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	**C/I**

OPORTUNIDAD DE MEJORA
No. 8

	TITULO: Controles de acceso de funcionarios de TI a los recursos del centro de cómputo
	CONDICIÓN: El proceso de evaluación del control interno evidenció que el departamento de TI carece de controles de seguridad que registren las horas de entrada y salida de los funcionarios del centro de cómputo así como el recurso que fue utilizado.
	CRITERIO: La organización debe poseer un adecuado proceso de administración de medidas de seguridad. La seguridad en TIC deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos del negocio.
	CAUSA: Falta de conciencia por parte del departamento de TI sobre la necesidad de establecer controles al respecto.
	EFECTO: Ante una eventualidad, no se tendría conocimiento cuál funcionario fue el que ingresó al centro de cómputo, cuáles fueron sus fines y cuál fue el recurso utilizado, por lo que no se podrían tomar las acciones correctivas y además, sentar las responsabilidades del caso.
	CONCLUSIÓN: Se observó que las prácticas de manejo y administración de los recursos carecen de un registro de accesos al centro de cómputo y los recursos utilizados, lo cual requiere de la implementación de controles que permitan identificar claramente quién, cuándo y para qué se ingresó al centro de cómputo.
	RECOMENDACIÓN: Deben establecerse y poner en práctica políticas, lineamientos y controles que procuren el registro de entrada y salida de cualquier persona del centro de cómputo, indicando el recurso que fue utilizado y con qué fines.
	REACCIÓN DE LA ADMINISTRACIÓN: Son conocedores de la situación

	TITULO: Acceso y administración de las Bases de Datos.
	CONDICION: El departamento de TI carece de un administrador de base de datos, de tal forma que la función esté asignada de manera exclusiva; por el contrario, dicha función la realizan tres analistas quienes a su vez realizan labores de soporte. También existen usuarios finales con derechos de administrador de bases de datos, en contradicción con la sana práctica de segregación de funciones.
	CRITERIO: Deberán separarse y distribuirse entre los diferentes puestos, las funciones que, si se concentraran en una misma persona, podrían comprometer el equilibrio y la eficacia del control interno y de los objetivos y misión institucionales, de tal manera que el control por la totalidad de su desarrollo no se concentre en una única instancia. La prestación óptima de los servicios de TI debe apoyarse en una estructura organizacional que garantice una adecuada segregación de funciones.
	CAUSA: Falta de conciencia por parte de la administración activa sobre la necesidad de establecer un adecuado perfil de puestos.
	EFECTO: Las condiciones expuestas conllevan el riesgo de integridad, confiabilidad y disponibilidad de información, con los consecuentes costos financieros para la organización y exposición de la imagen institucional ante clientes internos y externos.
	CONCLUSIÓN: Los sistemas de información existentes se ven expuestos a riesgos que pueden comprometer la confiabilidad, integridad y exactitud de la información. Adicional a ello, no existe una adecuada segregación de funciones y roles de administración, lo cual atenta contra la veracidad de la información.
	RECOMENDACIÓN: La Gerencia General debe establecer un adecuado proceso de segregación de funciones que permita la asignación de la administración de las bases de datos a un único funcionario, quien tendrá la responsabilidad por su administración, monitoreo, depuración, ajustes, modificaciones y mejoras. Igualmente debe definir la normativa que regule la actividad del DBA, así como la actualización de dicho marco legal. . Asimismo, deben establecerse mecanismos de control específicos o compensatorios según sea el caso para que la institución disponga de sistemas de información que le suministren información confiable y oportuna para la toma de decisiones.
	REACCIÓN DE LA ADMINISTRACIÓN: Se espera que con la elaboración del plan estratégico de TI en proceso, las condiciones expuestas sean cubiertas.

POLÍTICAS DE SEGURIDAD, IDENTIFICACIÓN Y AUTENTICACIÓN	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 10	**C/I**

	TITULO: Ausencia de documento para creación de cuentas de usuario
	CONDICION: Aunque la entidad dispone de un Procedimiento de Administración de Usuarios (PR-SI-01-02-01) el mismo carece de un documento formal para la solicitud de creación, modificación y cancelación. Asimismo, no considera lineamientos ni indicaciones referentes a la revocación de accesos por transferencia a otro departamento en el cual no se requiera de los permisos de ingreso otorgados anteriormente en condición permanente, temporal, o bien, porque el mismo deje de prestar servicios para la institución.
	CRITERIO: Se deberá disponer de procedimientos necesarios para asegurar acciones oportunas en lo relacionado con la solicitud, establecimiento, emisión y suspensión de cuentas de usuario.
	CAUSA: Falta de normativa, lineamientos y documentación formales mediante los cuales se rija los procesos de asignación, modificación y revocación de accesos a usuarios.
	EFECTO: Se podría aumentar la posibilidad de que se materialicen los siguientes riesgos: √ Existencia de cuentas activas para funcionarios que ya no laboran para la institución, con el consecuente riesgo de acceso. √ Facultando el acceso no autorizado a la información y potencial afectación a la integridad y confiabilidad de ésta, con accesos a sistemas no requeridos para el desempeño de sus funciones.
	CONCLUSIÓN: El procedimiento de Administración de Usuarios presenta necesidad de ser mejorado, complementado con normativa que regule el proceso de revocación de accesos y con los formularios necesarios para documentar los distintos procesos implícitos en la actividad.
	RECOMENDACIÓN: Se recomienda la creación, aprobación y establecimiento de lineamientos y procedimientos institucionales que rijan la revocación de accesos a usuarios de los sistemas. Dichas directrices deberán contemplar las acciones requeridas a la mayor brevedad, dejando documentadas las transacciones que ello implica. Además se deberá coordinar con Recursos Humanos para que éstos informen al Departamento de TI acerca de los cambios de puesto o terminaciones ocurridas y así asegurar la oportunidad de desactivación de roles, a través de herramientas que el usuario final pueda utilizar.
	REACCIÓN DE LA ADMINISTRACIÓN: Son conocedores de la situación

POLÍTICAS DE SEGURIDAD, BITÁCORAS	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	**C/I**

OPORTUNIDAD DE MEJORA
No. 11

	TITULO: Procedimiento de revisión de bitácoras
	CONDICION: La entidad no dispone de un procedimiento para la revisión de las bitácoras en caso de sospechas de accesos no autorizados a los sistemas.
	CRITERIO: La organización debe poseer un adecuado proceso de administración de medidas de seguridad. La organización debe contar con la capacidad para administrar incidentes de seguridad computacional, debiendo establecer las responsabilidades y procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.
	CAUSA: Falta de normativa y lineamientos formales mediante los cuales se rijan los procesos de revisión de bitácoras.
	EFECTO: La carencia de procedimientos para la revisión de bitácoras en las condiciones expuestas, podrían generar como consecuencia las siguientes condiciones adversas: Ausencia de roles y responsabilidades formalmente asignadas al personal incentiva el hecho de que nadie se encargue de la solución de la anomalía, permitiendo que la misma se convierta en un riesgo mayor. Pérdida de eficiencia en el diagnóstico y solución de este tipo de incidentes. Inexistencia de una administración de la información y conocimiento, producto de incidentes anteriores. Atención inefectiva e ineficiente de algunos incidentes. Pérdidas financieras. Pérdida de imagen y reputación.
	CONCLUSIÓN: La entidad carece de un procedimiento para la revisión de las bitácoras en caso de sospechas de accesos no autorizados a los sistemas y con ello se faculta la omisión de prácticas de control y supervisión sobre los incidentes de seguridad que se reporten, dando pie a que estos se incrementen con la posibilidad de que se conviertan en situaciones de mayor impacto para la organización.
	RECOMENDACIÓN: Se recomienda establecer los lineamientos y procedimientos institucionales que rijan el proceso de revisión de bitácoras. De igual forma se deberá crear uno que indique los pasos a seguir para registrar, investigar, solucionar y documentar casos de sospechas de accesos no autorizados a los sistemas, así como asignar los roles y funciones del personal de TI cuya participación es requerida.
	REACCIÓN DE LA ADMINISTRACIÓN: Será considerado dentro del Plan Estratégico de TI, mismo que considera lo relacionado con contingencias.

ADMINISTRACIÓN CUENTAS DE USUARIO	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 12	**C/I**

	TITULO: Administración y control de cuentas de usuario
	CONDICIÓN: La organización está ayuna de un responsable para la administración de las cuentas de accesos a los sistemas y bases de datos y carece de un reporte de cuentas de usuario que indique su perfil, ubicación, sistemas a utilizar u otra información relacionada.
	CRITERIO: Se deberá disponer de procedimientos necesarios para asegurar acciones oportunas en lo relacionado con la solicitud, establecimiento, emisión y suspensión de cuentas de usuario.
	CAUSA: Carencia de una adecuada segregación de funciones y controles complementarios para garantizar el control interno.
	EFECTO: La falta de un responsable de la administración de cuentas de usuario puede generar para la administración riesgos como: ✓ Existencia de cuenta activa para funcionarios que ya no laboran para la institución, con el consecuente riesgo de acceso. ✓ Usuarios con accesos a sistemas no requeridos para el desempeño de sus funciones. ✓ Duplicación de cuentas de usuario.
	CONCLUSIÓN: La institución no tiene asignadas las funciones de administración de las cuentas de accesos a los sistemas y bases de datos y carece de un reporte control de cuentas de usuario.
	RECOMENDACIÓN: Se recomienda la asignación de las funciones de administración de cuentas de acceso a los sistemas y bases de datos, a un funcionario responsable de su control, monitoreo y depuración permanente. Se deben establecer mecanismos de control mediante el cual se disponga de la información general de las distintas cuentas de usuario que permitan conocer con el mayor grado posible, información general de las calidades de éste, tales como: nombre, apellidos, departamento, perfil, ubicación, sistemas autorizados a utilizar.
	REACCIÓN DE LA ADMINISTRACIÓN: Son conocedores de la situación

ADMINISTRACIÓN Y CONTROL DE ALMACENAMIENTO DE INFORMACIÓN	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	**C/I**

OPORTUNIDAD DE MEJORA
No. 13

	TÍTULO: Planes de respaldo y control de bitácoras de respaldo
	CONDICION: La organización no ha contemplado dentro de sus políticas de seguridad informática un plan de respaldos de información para ser usado en un caso de confrontación de un desastre natural, siniestro, o falla de equipos. Además carece de una bitácora de respaldos.
	CRITERIO: Se debe asegurar una adecuada administración de datos garantizando que éstos permanezcan completos, precisos y válidos durante su entrada, actualización y almacenamiento.
	CAUSA: Falta de normativa y lineamientos formales mediante los cuales se rijan los procesos de planes de respaldo y control de bitácoras.
	EFECTO: El riesgo de pérdida de información por desastres sobrenaturales y accesos indebidos.
	CONCLUSIÓN: La institución no tiene dentro de sus políticas de seguridad informática un plan de respaldos de información para utilizar en caso de desastres, ni un control de bitácoras de respaldo.
	RECOMENDACIÓN: Se recomienda elaborar las políticas de respaldo específicos para ser utilizados en una contingencia. Dicha política deberá incluir controles para el seguimiento de bitácoras de respaldo.
	REACCIÓN DE LA ADMINISTRACIÓN: Son conocedores de la situación

	TÍTULO: Clasificación de la información.
	CONDICIÓN: La organización carece de una clasificación de la información para los procesos de almacenamiento, de acuerdo con las prioridades de la organización.
	CRITERIO: La Gerencia deberá asegurar que todos los datos incluso aquellos que no requieran protección, sean clasificados en términos de sensibilidad, mediante una decisión explícita y formal del dueño de los datos, de acuerdo con el esquema de clasificación previamente definido.
	CAUSA: Carencia de políticas institucionales al respecto y culturización por parte del usuario y la administración activa, en su quehacer diario.
	EFECTO: La inexistencia de parámetros para clasificar la información según su sensibilidad y el riesgo de acceso a la misma por personas no autorizadas, así como la falta de procedimientos que guíen la manipulación, uso y transmisión de datos catalogados como secretos o confidenciales, presenta un riesgo alto para la institución, ya que aumenta considerablemente las posibilidades de que terceras personas tengan acceso a ellos, dadas las debilidades en su manejo. También puede darse su extracción por parte de terceros no autorizados, pérdida de documentos o medios portátiles con información crítica que podría ser alterada o manipulada. La carencia de clasificación de los activos de información incrementa el riesgo y el costo de sobreproteger o sub-proteger estos recursos al no vincular la seguridad con los objetivos del negocio.
	CONCLUSIÓN: La organización carece de una clasificación de la información para los procesos de almacenamiento, de acuerdo con las prioridades de la organización.
	RECOMENDACIÓN: Deberá elaborarse, aprobarse, publicarse, divulgarse y capacitar al personal en cuanto a políticas y procedimientos referentes a seguridad de activos de información, en donde se debe establecer un esquema acorde con el impacto que representa su alteración, pérdida y divulgación. Esta podría ser clasificada y etiquetada en las siguientes categorías: secreta, confidencial, de uso interno, pública; para poder determinar los recursos necesarios y protegerla. Deberá contener la etiqueta de clasificación en el encabezado o pie de cada página. Se recomienda el inventario de estos activos, la clasificación, manejo y etiquetado de conformidad con directrices / lineamientos preestablecidos.
	REACCIÓN DE LA ADMINISTRACIÓN: La administración reconoce la necesidad de políticas institucionales y su adecuado cumplimiento por parte de los usuarios.

	TÍTULO: Condiciones del Cableado Estructurado
	CONDICIÓN: De conformidad con lo manifestado por la administración, mediante la aplicación de cuestionarios de control interno y listas de chequeo, la revisión de documentos fuente y verificación física de la red de datos institucional, se observaron las siguientes oportunidades de mejora: Aunque se dispone de un diagrama de diseño de red artesanal, no está revestido de la oficialidad institucional ni cuenta con fechas y cronograma de actualización. Se desconoce cuál es la topología de red que se tiene definida. Una indefinición de una topología de red dificulta la planificación de la mejor disposición del cableado de los dispositivos físicos. El sistema de cableado estructurado no es confiable porque presenta deficiencias de empalmes, falta de identificadores para localizar los diferentes enlaces, falta de estandarización en el uso de los componentes de sistema en los cordones de interconexión, cables cortados que presentan riesgo de corto circuito, cables amarrados con mecates, entre otros. El sistema de cableado no está debidamente etiquetado. No se dispone de personal debidamente capacitado para el mantenimiento del sistema de cableado estructurado. Se desconoce el nivel de protección de los distintos enlaces contra agentes perniciosos. (Roedores, insectos, intervención humana). Las terminales de cada puerto de red y los cables de servicio de red que se tienen (correo electrónico, base de datos, aplicaciones de respaldo, impresoras), no se encuentran identificadas.
	CRITERIO: Las prácticas de administración de seguridad de la red deben ser comunicadas, comprendidas, impuestas y adoptadas por el personal. La administración debe asegurar que las funciones importantes de soporte de TI estén siendo llevadas a cabo regularmente y de una manera ordenada (Administración de operaciones) Las funciones de control de la red deben ser realizadas por operadores técnicamente calificados.
	CAUSA: Deficiente diseño, instalación y administración de la red organizacional de datos constituyéndose en un riesgo para la infraestructura de la información.
	EFECTO: Entre los distintos efectos que las condiciones observadas conllevan se citan: ✓ No se puede asegurar la disponibilidad de la información. ✓ Probables violaciones a la seguridad física de red ✓ La falta de protección de los datos que viajan por la red. ✓ La exposición a la actividad externa a través de una red vulnerable ✓ Posible revelación indebida de datos causados por debilidades en el entorno de red. ✓ Suspensión de la comunicación por accidentes (tropiezos con cables, y otros).

	✓ Dificultad para la debida administración de la red ✓ Dificultad para localizar fallas y errores al no estar el cableado de red debidamente identificado.
	CONCLUSIÓN: La condiciones observadas en el entorno físico de red, denota vulnerabilidades que atentan contra la continuidad del servicio.
	RECOMENDACIÓN: Se deben establecer los lineamientos necesarios para la debida asignación y delegación de la administración de la red de datos a un solo funcionario responsable de la implementación de acciones correctivas y monitoreo constante para asegurar su operatividad, confiabilidad y disponibilidad. Se debe disponer de un diagrama de diseño de red en el que se evidencia claramente su fecha de actualización, así como un definir formalmente un cronograma para su debida revisión y actualización. Se debe definir y documentar la topología de red para la organización, acorde con los planes organizacionales para el cableado de los dispositivos físicos. Debe brindarse la debida capacitación al personal necesario para que realice las labores pertinentes con fin de disponer de un cableado estructurado confiable, protegido, seguro y de acuerdo con las normas internacionales que rigen dicha actividad en lo relacionado con condiciones del cableado, rutas y espacios de telecomunicaciones, administración su infraestructura y puestas a tierra a efecto de que se pueda certificar la instalación realizada.
	REACCIÓN DE LA ADMINISTRACIÓN: Las condiciones existentes se espera que sean solucionadas con la elaboración del plan estratégico de tecnologías de información 2007-2010.

COMUNICACIONES DE DATOS	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN OPORTUNIDAD DE MEJORA No. 16	C/I

	TÍTULO: Planos de telecomunicaciones
	CONDICIÓN: La organización no cuenta con planos de telecomunicaciones. Los planos constituyen elemento importante que forma parte de un diseño. La función de los planos es la de mostrar la localización del trabajo requerido en relación con otros elementos necesarios, así como la cantidad y el tamaño.
	CRITERIO: Debe disponerse de planos de telecomunicaciones que permitan una adecuada administración, eliminación, reparación y ampliación de la red.
	CAUSA: El nivel de madurez de las TI en la institución no le ha permitido a la administración inquirir en la importancia de los planos para asegurar la continuidad del negocio.
	EFECTO: Sin planos de telecomunicación, se dificulta las labores de detección de fallas, desplazamiento de estaciones, eliminación de sectores en la red, adiciones y cambios en el cableado estructurado.
	CONCLUSIÓN: La institución carece de planos de telecomunicación lo que conlleva riesgo de no poder atender oportunamente posibles incidentes a nivel físico que se presenten, así como un adecuado mantenimiento y administración de la misma.
	RECOMENDACIÓN: La Administración debe efectuar las gestiones necesarias a efecto de contar con los planos correspondientes a la red de telecomunicaciones, los mismos que deben cubrir al menos los siguientes conceptos: ✓ Sitios del Edificio ✓ Trayecto exterior del cableado ✓ Nodos principales del sistema ✓ Ubicación de las zonas de servicio, disposición de las salas de equipos de telecomunicaciones, puntos de acceso. ✓ Etiquetado del cableado
	REACCIÓN DE LA ADMINISTRACIÓN: La administración reconoce la necesidad de mejora y está en procura de un plan integral para enfrentar las condiciones en que se encuentran las TI

	TÍTULO: Políticas de correo electrónico
	CONDICIÓN: La institución carece de políticas de seguridad, normas, procedimientos y controles para el uso del correo electrónico.
	CRITERIO: La organización debe disponer de políticas, normas y procedimientos relativos con la seguridad y uso del correo electrónico.
	CAUSA: El nivel de madurez en que se encuentran las tecnologías de información en la organización, induce a una escasa conciencia institucional y a la ausencia de procedimientos.
	EFECTO: La ausencia de políticas de correo electrónico puede generar problemas como los siguientes: Saturación de correo Uso del mismo para fines distintos a los de la organización, comprometiendo su imagen. Fomenta el envío de cadenas de mensajes a múltiples usuarios Fomenta el acceso indebido a los correos electrónicos por parte del Administrador del Servicio de Correo u otros usuarios, incurriendo en violaciones a los derechos de la confidencialidad de la información y secreto de las comunicaciones personales. Prácticas insanas como compartir contraseñas Uso irracional del servicio Envío de SPAMS de información (correo basura), o enviar anexos (attachments) que pudieran contener información nociva para otro usuario como virus o información no deseada.
	CONCLUSIÓN: La ausencia de políticas de seguridad, normas, procedimientos y controles relacionadas con correo electrónico, expone el riesgo de la prestación óptima del servicio de correo.
	RECOMENDACIÓN: Se deben establecer las políticas, normas y procedimientos necesarios que regulen la actividad y uso de correo electrónico, en procura de la salvaguarda de los activos e información institucional.
	REACCIÓN DE LA ADMINISTRACIÓN: Están en proceso de definición de las políticas relacionadas con el uso del correo electrónico.

CAPACITACIÓN	EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN	**C/I**

OPORTUNIDAD DE MEJORA
No. 18

	TÍTULO: Programas de capacitación
	CONDICIÓN: La organización adolece de programas de capacitación a los usuarios, orientados al uso del servicio de correo electrónico y a la realidad de los virus informáticos, para fomentar una mayor cultura de protección y conciencia de los riesgos.
	CRITERIO: Se deben establecer planes de capacitación permanente a los usuarios sobre diversos temas de seguridad. (Virus, uso de correo electrónico, seguridad física, seguridad lógica, planes de contingencia, políticas de evacuación).
	CAUSA: El nivel de madurez en que se encuentran las tecnologías de información en la organización, induce a una escasa conciencia institucional y a la ausencia de procesos de capacitación constante de los usuarios en temas relacionados con seguridad en TI.
	EFECTO: La falta de una adecuada capacitación de los usuarios finales, principalmente en lo relacionado con uso de correo electrónico y virus informático, expone a desaprovechamiento y usos indebidos esta herramienta y al riesgo de virus en los sistemas de la institución.
	CONCLUSIÓN: Carestía de adecuados procesos de capacitación de usuarios en temas de seguridad relacionados con el uso de correo electrónico y virus informático no permiten maximizar el uso de los recursos.
	RECOMENDACIÓN: Se deben establecer programas de capacitación permanente para los usuarios, en procura de asegurar que estos hagan un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades que ello involucra y la necesidad de su adecuada protección.
	REACCIÓN DE LA ADMINISTRACIÓN: Son conocedores de la situación

V. CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Se puede definir una conclusión como un juicio razonado, basado en una síntesis de resultados producto del análisis de una situación específica.

Los auditores, por la naturaleza de sus funciones, deben entonces basar sus conclusiones en adecuados análisis, evaluaciones, y el registro de información relevante, que les permita soportar los resultados del trabajo. Seguidamente se detallan los desenlaces del estudio.

5.1.1 De la evaluación general practicada al área de seguridad física y lógica se encontró una oportunidad para fortalecerla, de acuerdo con los objetivos estratégicos de la institución, los cuales han sido recientemente replanteados por la nueva administración, dada las variaciones y competitividad en el mercado internacional.

5.1.2 Al no haber adoptado la Institución un marco de referencia que fungiera como marco procedimental para la realización del trabajo propuesto, y ser la normativa del sector público aplicable a la organización, ayuna al tema, se definió como fuentes de criterio la utilización de las mejores prácticas que resumen los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), a sabiendas de que, tanto la auditoría como el departamento de Tecnologías de Información, son conscientes que por ser una normativa internacional generalmente aceptada para el uso cotidiano de gerentes de empresas y auditores, podría ser de aplicación en el proyecto por desarrollar, con la salvedad de que constituyese una adaptación de sus mejores prácticas y no una adopción de la metodología en forma integral. Igualmente la normativa de carácter obligatorio para las

instituciones públicas, emitida por la Contraloría General de la República.

5.1.3 Se identificó un entorno del TI con un ciclo de madurez incipiente, lo que favorece las oportunidades de reforzar la arquitectura de tecnología de información alineada con los objetivos estratégicos institucionales sin haber incurrido en inversiones de alto costo que a la postre, no aporten mayor utilidad para las necesidades actuales de la organización.

5.1.4 La situación actual de la institución en relación con el uso de las Tecnologías de Información se ve inmersa en los riesgos importantes que la exponen, ante determinadas eventualidades no deseadas que afecten la continuidad del servicio o integridad de la información administrada, con el consecuente incumplimiento de los - objetivos estratégicos de la entidad.

5.1.5 Se diagnosticó la siguiente situación, referente a la seguridad física y lógica de las Tecnologías de Información:

1.1.1 Existe una escasa conciencia institucional con respecto a la seguridad informática, la que podría relacionarse con ausencia de algunos procedimientos, políticas, lineamientos, así como necesidad de capacitación formal a los usuarios acerca de las amenazas, riesgos e impactos posibles para el negocio, ante un incidente de seguridad física o lógica.

1.1.2 Se determinaron aspectos susceptibles de mejora relacionados con seguridad física, que exponen a riesgo la información, los sistemas y la infraestructura tecnológica institucional.

1.1.3 La inexistencia de condiciones óptimas de carácter administrativo como ausencia de un administrador de la seguridad, carencia de un plan de contingencia y una inadecuada segregación de funciones, todas ellas contrarias a las sanas prácticas en un entorno informático, generan condiciones adversas al ambiente de TI organizacional.

1.1.4 Aspectos relacionados con el manejo y administración de los dispositivos de almacenamiento, clasificación de la información para los procesos de almacenamiento, los respaldos de información para ser utilizados en caso de desastre, constituyen temas que deben ser mejorados por parte de la organización en procura de una adecuada protección de los datos.

1.1.5 Se evidencia la necesidad de mejorar aspectos relacionados con procedimientos de administración de usuarios, revisión de las bitácoras, administración de las cuentas de accesos a los sistemas y bases de datos, así como reportes y formularios necesarios para documentar los distintos procesos implícitos en las diversas actividades.

1.1.6 Las condiciones observadas en el entorno general de red, denotan vulnerabilidades que atentan contra la eficiencia y continuidad del servicio.

1.1.7 La ausencia de políticas de seguridad, normas, procedimientos y controles relacionados con el correo

electrónico, expone al riesgo los recursos institucionales y la prestación óptima de su servicio.

1.1.8 Carestía de adecuados procesos de capacitación de usuarios en temas de seguridad relacionados con el uso de diversas aplicaciones y en el uso de sanas prácticas, no permiten maximizar el empleo de los recursos informáticos. También la administración relega toda acción correctiva sobre las situaciones de mejora identificadas a la materialización del PLAN DE TI del 2007, de lo cual podría desprenderse que no hay un propósito ni conciencia de enmienda; descansando toda solución para después, sin importar el riesgo que implique para la organización.

5.2 Recomendaciones

La actividad de auditoría demanda evaluar y hacer las recomendaciones apropiadas para mejorar los distintos procesos, actividades o sistemas procurando el cumplimiento de los siguientes objetivos:

- Promover la ética y los valores apropiados dentro de la organización.
- Asegurar la gestión y responsabilidad eficaces en el desempeño de la organización.
- Comunicar eficazmente la información de riesgo y control a las áreas adecuadas de la organización
- Coordinar eficazmente las actividades y la información de comunicación entre el Consejo de Administración, los auditores internos y externos y la dirección.
- Promover un adecuado sistema de control interno mediante una serie de recomendaciones para que la administración activa implemente acciones que proporcionen la seguridad en:
    - ✓ Proteger u conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.
    - ✓ Exigir confiabilidad y oportunidad de la información
    - ✓ Garantizar eficiencia y eficacia de las operaciones
    - ✓ Cumplir con el ordenamiento jurídico y técnico.

Como producto de los objetivos planteados y con base en la revisión efectuada, se emiten las siguientes recomendaciones:

5.2.1 Establecer un plan estratégico de las TI alineado con los objetivos de la entidad.

5.2.2 Elaborar un programa de acción para atender las necesidades de arquitectura en hardware y software con la capacidad que se requiere

para automatizar los procesos pertinentes que coadyuvarán a alcanzar los objetivos estratégicos institucionales.

5.2.3 Considerar en el plan estratégico las acciones respectivas para fortalecer la seguridad física y lógica de las tecnologías de información, tales como:

5.2.3.1 Fortalecer la capacitación de su personal, en procura de establecer un índice satisfactorio de conciencia y cultura organizacional, las mismas que contribuirán con una mayor eficiencia, eficacia, uso y aprovechamiento de las tecnologías de información institucionales.

5.2.3.2 Considerando las sugerencias ofrecidas en las situaciones observadas, es necesario que se proceda a elaborar los procedimientos pendientes y que los existentes sean revisados a efecto de complementarlos con los lineamientos necesarios, así como con los formularios que cada uno de ellos requiera para su debida actualización, vigencia y aplicabilidad. Igualmente se deben establecer políticas de seguridad, normas, procedimientos y controles relacionados con el correo electrónico, a efecto de disminuir el riesgo inherente y procurar una prestación óptima de este servicio.

5.2.3.3 La administración debe considerar los aspectos de mejora relacionados con seguridad física; tales como alarmas contra robos, cámaras de vigilancia, ventanas sin celosías, registro de ingresos, sistema detector de incendio, control de humedad, sistema detector de líquidos, piso falso, bitácoras de registro, extintores de incendio, rondas de vigilancia, entre otros que fueron identificados y proceder con la aplicación de medidas

correctivas y controles necesarios que permita su gobierno por parte de la entidad, en procura de sean disminuidas; a efecto de obtener una seguridad satisfactoria para sus tecnologías de información.

5.2.3.4 De conformidad con la disponibilidad de sus recursos, sus planes estratégicos, estructura organizacional y operativa del recurso humano del Departamento de Tecnologías de Información, es necesario que se evalúe la conveniencia de implantar la figura del administrador de seguridad de TI como responsable de la función específica, acorde con las mejores prácticas y requerimientos de la entidad.

5.2.3.5 Se debe crear, comunicar y probar mediante simulacros un plan de contingencia para mantener la continuidad de los sistemas críticos de la institución en caso de que ocurra una eventualidad que interrumpa la fluidez de las operaciones del negocio. Dichos planes deberán concretar detalladamente los procedimientos alternativos a seguir para minimizar el impacto de las fallas y la interrupción de las operaciones, así como definir las personas responsables por ejecutar las diversas acciones y definir el alcance de su participación. Cabe mencionar que dicha implementación requerirá de la participación de personal de diversos departamentos, y que deberá ser un proyecto prioritario a nivel institucional.

Como mínimo, el plan de contingencia abarcará los siguientes puntos:

i. Análisis de impacto del negocio
ii. Preparación ante el desastre
iii. Procedimientos de evacuación

iv. Identificación de procesos del negocio y recursos de TI que se deben recuperar.

v. Explicar paso a paso la opción de recuperación.

vi. Identificación de los diversos recursos requeridos para los simulacros del plan, la recaudación y operación continua de la organización

vii. Instalaciones alternativas para realizar tareas y operaciones.

El plan deberá asignar responsabilidades específicas a todas las personas involucradas en el mismo. Este deberá ser revisado anualmente e inmediatamente después que se realice un cambio significativo a las operaciones o a los sistemas de información y deberá informarse a las personas involucradas cada vez que el sufra alguna modificación.

También se recomienda mantener un registro de las actividades de mantenimiento del plan de contingencia de la organización, donde se documenten todas las pruebas, entrenamientos y revisiones, así como un directorio actualizado con todos los datos de personal involucrado en su ejecución, incluyendo sus números de teléfono y responsabilidades.

5.2.3.6 Se debe procurar la adecuada segregación de funciones para prevenir la posibilidad que una única persona sea la responsable por diversas funciones críticas, de forma tal que errores o modificaciones puedan ocurrir y no ser detectados en forma oportuna dentro del curso normal de los procesos operativos. Dicha separación es una forma fundamental para desalentar y prevenir actos voluntarios e involuntarios o con dolo y previene el error. La segregación de funciones dentro de un Departamento de TI requiere que los accesos a los sistemas,

programas en producción, documentación y conocimientos de programación, se encuentre limitada según el rol de cada funcionario de TI. Asimismo, debe establecerse mecanismos de control específico o compensatorio, según sea el caso, para que la institución disponga de sistemas de información que le suministren datos confiables y oportunos para la toma de decisiones.

5.2.3.7 Para asegurar el servicio continuo, la organización debe satisfacer los requerimientos del negocio, asegurando que los servicios de TI estén disponibles y procurar un impacto mínimo en las actividades de la organización, en caso que ocurriera una interrupción mayor. Parte de ese proceso es posible a través de adecuados métodos de clasificación de la información con base en su criticidad, probados procesos de respaldo y recuperación, los mismos que conviene sean mejorados por el departamento de TI de la institución.

5.2.3.8 Para garantizar la seguridad en sistemas, referente a procedimientos de administración de usuarios, es necesario documentar fehacientemente mediante formulario único, diseñado para tal fin, cada uno de los cambios o modificaciones que se efectúen en sus perfiles. Igualmente documentar los procesos de manejo, reporte y seguimiento de incidentes, mediante pruebas y reportes de instrucción, siendo sujeto de revisión, análisis, y seguimiento continuo a las bitácoras de administración de las cuentas de accesos, a los sistemas y bases de datos.

5.2.3.9 Deben tomarse acciones correctivas con respecto a las condiciones detectadas en el sistema de cableado estructurado,

capacitar y asignar la gestión de la red a un funcionario específico, y en aspectos meramente técnicos relativos a la debida confección de un diagrama de red, los planos respectivos, la señalización, a efecto de disponer de un sistema confiable, protegido, seguro de acuerdo con las normas que rigen dicha actividad.

5.2.3.10 Es necesario la adecuada capacitación de los usuarios y del personal de operaciones de TI, procurando que ésta sea para el propósito con que fue adquirida, sin incurrir en potenciales riesgos por mal uso, desconocimiento y aplicación de prácticas indebidas que atenten contra la seguridad de la plataforma informática.

Bibliografía

Libros:

- Echenique, J. (2001) **Auditoría en Informática.** Mc Graw Hill.
- Muñoz, C. (2002). **Auditoría en Sistemas Informáticos**. México: Perrazos Educación.

Leyes:

- Ley General de Control Interno; Ley N° 8292 del 18 de julio del 2002.
- Ley General de la Administración Pública; Ley N° 6227 de 2 de mayo de 1978.Versión WEB 2005.

Folletos:

- Sárraga, Alejandro – Durán, Álvaro. (2004). **Normativa sobre tecnología de información por parte de las Superintendencias Bancarias –Su aplicación en las cooperativas de Ahorro y Crédito.** Confederación Alemana de Cooperativas. San José, C.R.

- UCR, **Técnico en Auditoría Informática. Auditoría de Seguridad. Programa De Educación Continua.** Febrero 2004.

- Comité Directivo de COBIT y El IT Governance Institute **COBIT MARCO REFERENCIAL** 3a Edición

- Comité Directivo de COBIT y El IT Governance Institute. **COBIT, DIRECTRICES DE AUDITORIA**. Julio de 2000, 3a Edición.

- Instituto Mexicano de Contadores Públicos **EFECTOS DEL PROCESAMIENTO ELECTRÓNICO DE DATOS (PED) EN EL EXAMEN DEL CONTROL INTERNO** Boletín 5080

- Contraloría General de la República, (1995), Manual **Sobre Normas Técnicas de Control Interno Relativas a Los Sistemas de Información Computadorizados,** San José, Costa Rica.

- Contraloría General de la República (2002), **Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización**, Publicado en La Gaceta Nº 107 del 5 de junio, 2002

- Arce, Ricardo. (Febrero, 2006). Curso Taller "Planeamiento Estratégico de la Auditoría Interna". Modelo de Riesgos de Negocios PROTIVITI. Modelo de definición de riesgos de Negocios. Traducción de Value Management Consulting.

Entrevistas:

- Jefe Departamento de Tecnologías de Información. Condición de las TI en la institución. San José, CR., Entrevista efectuada en marzo 2007. (Comunicación personal)

Otras fuentes:

http://www.mailxmail.com/curso/empresa/auditoriaelemental/capitulo11.htm 19-10-2006.

http://www.citel.oas.org/newsletter/2006/mayo/seguridad_e.asp 02-04-07

http://www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indp.htm 03-04-07

Normas para el Ejercicio Profesional de la Auditoría Interna de The Institute of Internal Auditors, http://www.imai.org.mx/servicios/Definicion/normprof.html, 03-04-2007

http://www.google.co.cr/search?hl=es&defl=es&q=define:Conocimiento&sa=X&oi=glossary_definition&ct=title, 03-04-2007

http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=seguridad, 16/03/07

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml , 20-03-07

http://www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indp.htm, 03-04-07

http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_es.pdf, 2-04-07

ANEXO No. 1
MAPA CONCEPTUAL DE RIESGOS
Evaluación de los Procesos de Seguridad Física y Lógica Relativos a las Tecnologías de Información y Comunicación

CONCEPTUACIÓN DE LOS RIESGOS

<table>
<tr><td colspan="3">RIESGOS DEL ENTORNO</td></tr>
<tr><td colspan="3">RIESGOS DE PROCESOS</td></tr>
<tr><td rowspan="3">OPERACIONES</td><td>DIRECCIÓN</td><td rowspan="3">FINANCIEROS</td></tr>
<tr><td>TECNOLOGÍA DE INFORMACIÓN</td></tr>
<tr><td>INTEGRIDAD</td></tr>
<tr><td colspan="3">RIESGO DE INFORMACIÓN PARA LA TOMA DE DECISIONES</td></tr>
<tr><td>INFORMACIÓN OPERATIVA</td><td>INFORMACIÓN DE GESTIÓN</td><td>INFORMACIÓN ESTRATÉGICA</td></tr>
</table>

Modelo de riesgos de PROTIVITI. Es un esquema integral para entender los potenciales riesgos.

I. RIESGOS DEL ENTORNO

El riesgo del entorno surge cuando hay fuerzas externas que podrían afectar la viabilidad del modelo de la organización que incluye los aspectos básicos que guían los objetivos globales y estrategias que definen a ese modelo.

COMPETENCIA- Las acciones de competidores o de nuevos entrantes al mercado impactan negativamente la ventaja competitiva de la entidad e incluso amenazan su habilidad de sobrevivir, lo que generaría mayor competencia y posible espionaje por parte de las nuevas compañías que ingresan al mercado ofreciendo los mismos servicios en los que tiene injerencia la organización, lo que implica una mayor custodia de la información.

DESEOS DE LOS CLIENTES- Las necesidades y deseos de los clientes cambian y la empresa no es consciente de ello, por ejemplo, mayor demanda por una entrega más rápida y eficiente de servicios.

INNOVACIÓN TECNOLÓGICA- La organización no aplica los avances en la tecnología en su modelo de negocios para lograr o sostener su ventaja competitiva o se expone a las acciones de competidores o sustitutos si lo hacen, obteniendo un mejor desempeño en cuanto a calidad, costo y oportunidad en sus servicios, productos y procesos.

SOBERANO/POLÍTICO-Acciones políticas amenazan los recursos de la empresa y sus flujos de caja futuros en un país en que: la empresa ha invertido significativamente, genera un volumen importante de negocios o cuando se ha establecido un contrato importante con una contraparte sujeta a las leyes de ese país.

LEGAL- Leyes cambiantes amenazan la capacidad de la empresa de consumar transacciones importantes, hacer cumplir acuerdos contractuales o implementar estrategias y actividades específicas.

REGULATORIO- Regulaciones cambiantes amenazan la posición competitiva de la empresa y su capacidad de operar el negocio eficazmente.

INDUSTRIA- Cambios en las oportunidades y amenazas, las capacidades de competidores y otras condiciones que afectan la industria de la empresa amenazan el atractivo o la viabilidad a largo plazo de esa industria.

PÉRDIDA CATASTRÓFICA- Un desastre significativo amenaza la habilidad de la empresa de sostener sus operaciones en funcionamiento, proporcionar productos y servicios esenciales o recuperar sus costos de operación.

II. RIESGOS DE PROCESOS

El riesgo de procesos es el riesgo que los procesos de la organización de la empresa:

- No están adquiriendo, administrando, renovando y disponiendo eficazmente los recursos del negocio.
- No están claramente definidos.
- No están alineados con sus estrategias.
- No están operando eficaz y efectivamente para satisfacer las necesidades del cliente
- No están creando valor

- Están diluyendo el valor al exponer activos financieros, físicos, información e intelectuales importantes a pérdidas, riesgos, malversación o mal uso inaceptables.

Estos riesgos afectan el éxito con que la empresa ejecuta su modelo operacional.

II.I RIESGOS DE OPERACIONES

El riesgo de las operaciones es el riesgo de que sean ineficaces e ineficientes en la ejecución del modelo de la organización, la satisfacción de sus clientes y el logro de los objetivos de calidad, costo y tiempo.

SATISFACCIÓN AL CLIENTE- La falta de enfoque en los clientes en lo referente a la administración de la seguridad, amenaza la capacidad de la organización para cumplir o exceder las expectativas del cliente.

RECURSOS HUMANOS: -Falta de conocimientos, habilidades y experiencias requeridas entre el personal clave de la empresa, amenaza la ejecución de su modelo de seguridad organizacional y el logro de sus objetivos de negocios críticos.

CAPITAL DE CONOCIMIENTO- Los procesos por capturar e institucionalizar el aprendizaje a través de la empresa son inexistentes o ineficaces, produciendo un tiempo de respuesta lento, costos altos, errores repetidos, lento desarrollo de competencias, restricciones en el crecimiento y empleados desmotivados.

EFICIENCIA-Operaciones ineficientes amenazan la capacidad de la empresa de producir servicios a costos iguales o menores a los incurridos por los competidores o negocios de clase mundial.

CAPACIDAD-La capacidad insuficiente amenaza la habilidad de la empresa de cubrir las demandas de los clientes. La capacidad instalada excesiva amenaza la habilidad de la empresa de generar márgenes de beneficios competitivos.

BRECHA DE DESEMPEÑO: La incapacidad para operar a niveles de clase mundial en términos de calidad, costo y/o tiempo debido a procesos operativos inferiores y/o a relaciones externas que amenazan la demanda para los servicios de la empresa.

TIEMPO DE CICLO: Las actividades innecesarias amenazan la capacidad de la organización de desarrollar, producir y entregar bienes o servicios de manera oportuna.

ALIANZAS-Alianzas, afiliaciones y otras relaciones externas ineficientes o inefectivas afectan la capacidad de la organización para competir. Estas incertidumbres resultan de elegir al socio equivocado, la mala ejecución, tomar más de lo que se da y el no aprovechar oportunidades de hacer alianzas.

CUMPLIMIENTO-El incumplimiento con los requerimientos de los clientes, políticas y procedimientos organizacionales, leyes y regulaciones pueden producir baja calidad, costos de producción más altos, ingresos perdidos, retrasos innecesarios, penalidades, multas, etc.

INTERRUPCION: Las interrupciones de operaciones que provienen de la no disponibilidad de materias primas, tecnología de información, personal experimentado, instalaciones u otros recursos amenazan la capacidad de la organización para conducir sus actividades.

FALLA DE SERVICIOS O PRODUCTOS- Productos o servicios defectuosos exponen a la organización a quejas de los clientes, aplicación de garantías, reparaciones en el campo, devoluciones, litigios y pérdidas de ingresos, participación en el mercado y reputación institucional.

MEDIO AMBIENTE-Actividades dañinas al medio ambiente exponen a la organización a obligaciones por daños personales, daños materiales, costo de reparación y remoción, daños y perjuicios punitivos, etc.

SALUD Y SEGURIDAD- No proporcionar un ambiente de trabajo seguro al personal expone a la organización a compensación por daños, pérdida de reputación y otros costos.

II.II RIESGOS DE DIRECCIÓN

Es el riesgo que los gerentes y empleados:

- No estén debidamente liderados
- No sepan qué hacer
- Excedan los limites de autoridad asignadas
- Se le incentiva a hacer lo correcto

LIDERAZGO- El personal de la empresa no es liderado eficazmente, lo que puede resultar en una falta de dirección, enfoque en el cliente, motivación, credibilidad y confianza en la gerencia a través de la organización.

AUTORIDAD / LIMITE- Líneas de autoridad no efectivas pueden causar que los gerentes y personal hagan cosas que no deben hacer o dejen de hacer lo que deberían. El no establecer o verificar el cumplimiento de los límites en las acciones del personal puede causar que los empleados cometan actos no autorizados o no éticos, o asuman riesgos no autorizados o inaceptables.

TERCERIZACIÓN- Las actividades de tercerización pueden dar lugar a que los terceros no actúen dentro de los límites de autoridad establecidos o no realicen sus tareas de manera consistente con las estrategias y objetivos de la empresa.

INDICADORES DE DESEMPEÑO- Indicadores de desempeño mal elaborados, mal entendidos, subjetivos o no accionables pueden causar que gerente y personal actúen de manera inconsistente con los objetivos, estrategias y normas éticas de la organización, o prácticas de negocios prudentes.

DISPOSICIÓN AL CAMBIO- El personal de la organización no puede implementar mejoras a procesos y productos/servicios lo suficientemente rápido como para guardar el paso con los cambios del mercado.

COMUNICACIONES- Canales de comunicación ineficaces pueden producir mensajes que son inconsistentes con las responsabilidades autorizadas o los indicadores de desempeño establecidas.

II.III RIEGOS DE TECNOLOGÍA DE INFORMACIÓN

El riesgo de tecnología de información usada en la organización:

- No está operando según lo planeado

- Está comprometiendo la integridad y confiabilidad de los datos e información
- Está exponiendo activos importantes a pérdidas o mal empleo
- No soporta apropiadamente los procesos críticos

RELEVANCIA- Información irrelevante creada o resumida por cualquier sistema aplicativo puede afectar negativamente las decisiones de usuarios.

INTEGRIDAD-Todos los riesgos asociados con la autorización, integridad y exactitud de las transacciones que son ingresadas, procesadas, resumidas y reportadas por los distintos sistemas aplicativos de la empresa.

ACCESO- El no restringir el acceso a la información (datos o programas) adecuadamente puede producir el conocimiento y uso no autorizado de información confidencial. La excesiva restricción del acceso a la información puede impedir que el personal realice sus tareas asignadas eficaz y eficientemente.

DISPONIBILIDAD- La no disponibilidad de información importante cuando se le necesita amenaza la continuidad de las operaciones y procesos críticos de la empresa.

INFRAESTRUCTURA- El riesgo que la empresa no tenga la infraestructura de tecnología de información (por ejemplo, hardware, redes, software, procesos y personal) que necesita para soportar eficazmente los requerimientos de información de negocios actuales y futuros de la organización, de manera eficaz, costo efectivo y bien controlado.

II. IV RIESGOS DE INTEGRIDAD

El riesgo de integridad es el riesgo de fraude gerencial, fraude de personal, actos ilegales y actos no autorizados, los cuales podrían resultar en la pérdida de reputación.

FRAUDE GERENCIAL. La presentación intencional de estados financieros incorrectos o de información incorrecta sobre las capacidades o intenciones puedan afectar adversamente las decisiones.

FRAUDE DE EMPLEADOS/TERCEROS- Actividades fraudulentas perpetradas por empleados, clientes o proveedores, agentes corredores o terceros contra la organización para beneficio personal, que exponen a la empresa a la pérdida financiera.

ACTOS ILEGALES- Actos ilegales cometidos por gerentes o empleados exponen a la organización a multas, sanciones y pérdidas de clientes, ganancias y reputación.

USO NO AUTORIZADO- El uso no autorizado de los activos físicos, financieros e información de la organización por los empleados u otros la exponen al gasto innecesario de recursos y la pérdida financiera.

REPUTACIÓN- El daño a la reputación de la empresa puede exponerla a la pérdida de clientes, ganancias y la habilidad de competir.

III. RIESGOS DE INFORMACIÓN PARA LA TOMA DE DESICIONES

El riego de información para la toma de decisiones es el riesgo de que la información utilizada para apoyar a la ejecución del modelo de negocios, la generación de reportes internos y externos de la empresa no sea relevante o confiable.

Estos riesgos se relacionan con todos los aspectos de las actividades de creación de valor de la empresa.

III.I RIESGOS DE INFORMACIÓN OPERATIVA

CONDICIONES DE PRODUCTO O SERVICIO- La falta de información relevante y/o confiable que soporte las decisiones de fijación de condiciones puede producir cálculos que el cliente no quiere pagar, no cubre los costos de desarrollo o no cubre el costo de los riesgos asumidos por la organización.

ALINEAMIENTO- El no alinear los objetivos de los procesos de negocio y las medidas de desempeño con objetivos y estrategias corporativas o de unidad de negocios puede producir actividades antagónicas y descoordinados en toda la empresa.

III.II RIESGOS DE INFORMACIÓN DE GESTIÓN

PRESUPUESTO- Información de planeamiento y presupuestaria inexistente, poco realista, irrelevante o no confiable puede causar decisiones y conclusiones financieras incorrectas.

INFORMACIÓN CONTABLE- Énfasis excesivo en la información de contabilidad financiera para administrar el negocio, puede producir la manipulación de resultados para lograr los objetivos financieros a costa de cubrir los objetivos de satisfacción al cliente, calidad y eficiencia.

III.III RIESGOS DE INFORMACIÓN ESTRATÉGICA

MONITOREO DEL ENTORNO- La falta de monitoreo del entorno o la formulación de supuestos poco realistas o erróneos sobre los riesgos del entorno puede causar a la organización que retenga estrategias que se hayan vuelto obsoletas.

PORTAFOLIOS DE NEGOCIOS-La falta de información relevante y confiable que permita a la gerencia priorizar sus productos eficazmente o equilibrar sus negocios en un contexto estratégico puede evitar que una organización diversificada maximice su desempeño.

ESTRUCTURA ORGANIZACIONAL- La gerencia carece de la información necesaria para evaluar la efectividad de la estructura orgánica de la empresa, lo que amenaza su capacidad para el cambio o para lograr sus estrategias de largo plazo. La estructura no sustenta las estrategias de la organización.

MEDICIÓN DE DESEMPEÑO- Indicadores de desempeño inexistentes, irrelevantes, no confiables e inconsistentes con las estrategias establecidas de la organización, amenazan la habilidad de ejecutarlas.

ASIGNACIÓN DE RECURSOS- Un proceso de asignación de recursos e información de soporte inadecuados puede evitar que la empresa establezca y sustente una ventaja competitiva o maximice su valor (por ejemplo, asignar recursos escasos hacia oportunidades que sean más rentables).

PLANEAMIENTO- Un proceso de la planificación estratégica falto de imaginación e innecesariamente complejo puede producir información irrelevante, amenazando la capacidad de la empresa para formular estrategias de negocios viables.

CICLO DE VIDA- La falta de información relevante y confiable que permita a la gerencia gestionar el movimiento de sus líneas de productos y monitorear la evolución de su industria a lo largo del ciclo de vida, amenaza la capacidad de la empresa de permanecer competitiva.

EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TIC
Anexo No. 2
Criterios de valoración

PROBABILIDAD			IMPACTO		
PUNTAJE	DESCRIPCION	COLOR	PUNTAJE	DESCRIPCION	COLOR
1	BAJA		1	NULO SIN RIESGO	
2	MEDIA		2	MANEJABLE	
3	ALTA		3	REQUIERE ATENCION	
			4	ALTO	
			5	CRITICO	

Niveles del Riesgo

1 a 3	Bajo
4 a 9	Medio
9 a 15	Alto

ANEXO No. 2.1
EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TIC
CRITERIOS DE VALORACIÓN
GLOSARIO DE RIESGOS

			OBJETIVOS**								
			ESTRATEGICOS						CONTROL INTERNO		
No	Portafolio de Riesgos	CODIFICACIÓN DE RIESGOS	EFICIENCIA	CALIDAD	UNIVERSALIDAD	COMPETITIVIDAD	SOSTENIBILIDAD	Protección contra Pérdida Despilfarro, uso indebido, irregularidad y acto ilegal	Confiabilidad oportuna e integridad de la información	Garantizar Eficacia y Eficencia	Cumplir ordenamiento Jurídico y Técnico
	I. Riesgos del Entorno										
1	Competencia	**R001**	X	X	X	X	X	X	X	X	X
2	Deseo de los clientes	**R002**	X	X	X	X	X	X	X	X	X
3	Innovación tecnológica	**R003**	X	X	X	X	X	X	X	X	X
4	Soberano Político	**R004**	X	X	X	X	X	X	X	X	X
5	Legal	**R005**	X	X	X	X	X	X	X	X	X
6	Regulatorio	**R006**	X	X	X	X	X	X	X	X	X
7	Industria	**R007**	X	X	X	X	X	X	X	X	X
8	Pérdidas Catastróficas	**R008**	X	X	X	X	X	X	X	X	X
	II. Riesgos de Procesos										
	II.I Riesgo de Operaciones										
1	Satisfacción de clientes	**R009**	X	X	X	X	X	X	X	X	X
2	Recursos Humanos	**R010**	X	X	X	X	X	X	X	X	X
3	Capital de Conocimiento	**R011**	X	X	X	X	X	X	X	X	X
5	Eficiencia	**R012**	X	X	X	X	X	X	X	X	X
6	Capacidad	**R013**	X	X	X	X	X	X	X	X	X
7	Brecha de Desempeño	**R014**	X	X	X	X	X	X	X	X	X
8	Tiempo de ciclo	**R015**	X	X	X	X	X	X	X	X	X
10	Alianzas	**R016**	X	X	X	X	X	X	X	X	X
11	Cumplimiento	**R017**	X	X	X	X	X	X	X	X	X
12	Interrupción	**R018**	X	X	X	X	X	X	X	X	X
13	Falta de Productos/Servicios	**R019**	X	X	X	X	X	X	X	X	X
14	Medio Ambiente	**R020**	X	X	X	X	X	X	X	X	X
15	Salud y Seguridad	**R021**	X	X	X	X	X	X	X	X	X
	II.II Riesgos de Dirección										
1	Liderazgo	**R022**	X	X	X	X	X	X	X	X	X
2	Autoridad/Límite	**R023**	X	X	X	X	X	X	X	X	X
3	Tercerización	**R024**	X	X	X	X	X	X	X	X	X
4	Indicadores de desempeño	**R025**	X	X	X	X	X	X	X	X	X
5	Disposición al cambio	**R026**	X	X	X	X	X	X	X	X	X
6	Comunicaciones	**R027**	X	X	X	X	X	X	X	X	X
	II.IV Riesgos de tecnología de Inf										
1	Relevancia	**R028**	X	X	X	X	X	X	X	X	X
2	Integridad	**R029**	X	X	X	X	X	X	X	X	X
3	Acceso	**R030**	X	X	X	X	X	X	X	X	X
4	Disponibilidad	**R031**	X	X	X	X	X	X	X	X	X
5	Infraestructura	**R032**	X	X	X	X	X	X	X	X	X
	II.V Riesgos de Integridad										
1	Fraude Gerencial	**R033**	X	X	X	X	X	X	X	X	X
2	Fraude de Empleados/terceros	**R034**	X	X	X	X	X	X	X	X	X
3	Actos Ilegales	**R035**	X	X	X	X	X	X	X	X	X
4	Uso no autorizado	**R036**	X	X	X	X	X	X	X	X	X
5	Reputación	**R037**	X	X	X	X	X		X	X	X
	III. Riesgos Informac. Toma Desic.										
	III.I Riesgos Informac. Operativa										
1	Condiciones Servicio/Producto	**R038**	X	X	X	X	X	X	X	X	X
3	Alineamiento	**R039**	X	X	X	X	X	X	X	X	X
	III.II Riesgos de Informac. Gestión										
1	Presupuesto	**R040**	X	X	X	X	X	X	X	X	X
2	Información Contable	**R041**	X	X	X	X	X	X	X	X	X
	III. II Riesgos Informac. Estratégica										
1	Monitoreo del Entorno	**R042**	X	X	X	X	X	X	X	X	X
3	Portafolio de negocios	**R043**	X	X	X	X	X	X	X	X	X
5	Estructura organizacional	**R044**	X	X	X	X	X	X	X	X	X
6	Medición del desempeño	**R045**	X	X	X	X	X	X	X	X	X
7	Asignación de Recursos	**R046**	X	X	X	X	X	X	X	X	X
8	Planeamiento	**R047**	X	X	X	X	X	X	X	X	X
9	Ciclo de vida	**R048**	X	X	X	X	X	X	X	X	X

** **Fuente**: Plan estratégico institucional 2007 - 2010, aprobado por la Junta Directiva, acuerdo 001-076-2006, Sesión 076-2006 del 6-12-2006.

Anexo No. 3
EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TIC
SELECCIÓN UNICAMENTE DE RIESGOS ALTOS

Descripción	Código de Riesgo	Valuación	Prioridades	Observaciones
Brecha de Desempeño	**R014**	13,50	1	
Fraude de Empleados/terceros	**R034**	13,50	2	Políticas de seguridad, identificación y autenticación
Fraude Gerencial	**R033**	13,50	3	Políticas de seguridad, identificación y autenticación
Innovación tecnológica	**R003**	13,50	4	Virus informático. Correo electrónico
Actos Ilegales	**R035**	13,50	5	
Alineamiento	**R039**	12,00	6	
Autoridad/Límite	**R023**	12,00	7	Políticas de seguridad Roles de usuario. Niveles de seguridad.
Disposición al cambio	**R026**	12,00	8	
Comunicaciones	**R027**	12,00	9	Seguridad en las comunicaciones de datos
Relevancia	**R028**	12,00	10	Políticas de seguridad Transacciones
Integridad	**R029**	12,00	11	Dispositivos de almacenamiento. Servicios de seguridad
Acceso	**R030**	12,00	12	Seguridad General. Roles de usuario. Políticas de seguridad bitácoras. Servicios de seguridad. Adm. Cuentas de usuario. Accesos remotos
Disponibilidad	**R031**	12,00	13	Políticas de seguridad transacciones
Infraestructura	**R032**	12,00	14	Seguridad General Planta Física
Condiciones Servicio/Producto	**R038**	12,00	15	
Ciclo de vida	**R048**	12,00	16	
Tiempo de Ciclo	**R015**	12,00	17	
Planeamiento	**R047**	10,50	18	Políticas de seguridad. Administración de políticas. Correo electrónico. Virus informático
Estructura organizacional	**R044**	10,50	19	Políticas de seguridad Roles de usuario. Niveles de seguridad.
Capacidad	**R013**	10,50	20	Virus informático
Medio Ambiente	**R020**	10,50	21	Factores ambientales
Cumplimiento	**R017**	10,50	22	
Interrupción	**R018**	10,50	23	Adm. Control de almacenamiento de información. Virus informático
Pérdidas Catastróficas	**R008**	10,00	24	Seguridad General

Nota:
La priorización de los riesgos se estableció seleccionando únicamente aquellos que quedaron en el rango de alto riesgo. Posteriormente se consideró los valores descendentemente por bloques, y se determinó la prioridad de acuerdo con los objetivos que persigue la administración de la seguridad informática.

Por razones de limitación de tiempo, sólo se considerarán en el estudio el 50% de los riesgos en el proceso de la administración de la seguridad.

Anexo No. 3.1
CALCULO DE RIESGOS INSTITUCIONALES

Cuantificacion del Riesgo
Unidad **U001** **Administración de la Seguridad**
Departamento Proceso **Tecnologías de Información**

			Amelia		Rodolfo		Promedio		Riesgo
			P	I	P	I	P	I	
	I. Riesgos del Entorno								
1	Competencia	**R001**	2	3	2	4	2	3,5	8,00
2	Deseo de los clientes	**R002**	1	4	2	3	1,5	3,5	5,25
3	Innovación tecnológica	**R003**	3	5	3	4	3	4,5	13,50
4	Soberano Político	**R004**	1	3	2	3	1,5	3	4,50
5	Legal	**R005**	1	2	1	2	1	2	2,00
6	Regulatorio	**R006**	2	3	2	3	2	3	6,00
7	Industria	**R007**	1	2	1	2	1	2	2,00
8	Pérdidas Catastróficas	**R008**	2	5	2	5	2	5	10,00
	II. Riesgos de Procesos								
	II.I Riesgo de Operaciones								
1	Satisfacción de clientes	**R009**	2	3	3	3	2,5	3	7,50
2	Recursos Humanos	**R010**	2	4	1	3	1,5	3,5	5,25
3	Capital de Conocimiento	**R011**	2	3	2	3	2	3	6,00
4	Eficiencia	**R012**	3	4	2	3	2,5	3,5	8,75
5	Capacidad	**R013**	3	3	3	4	3	3,5	10,50
6	Brecha de Desempeño	**R014**	3	5	3	4	3	4,5	13,50
7	Tiempo de ciclo	**R015**	3	4	3	4	3	4	12,00
8	Alianzas	**R016**	1	2	1	1	1	1,5	1,50
9	Cumplimiento	**R017**	3	3	3	4	3	3,5	10,50
10	Interrupción	**R018**	3	3	3	4	3	3,5	10,50
11	Falta de Productos/Servicios	**R019**	2	4	2	2	2	3	6,00
12	Medio Ambiente	**R020**	3	3	3	4	3	3,5	10,50
13	Salud y Seguridad	**R021**	2	4	1	2	1,5	3	4,50
	II.II Riesgos de Dirección								
1	Liderazgo	**R022**	2	3	2	4	2	3,5	7,00
2	Autoridad/Límite	**R023**	3	4	3	4	3	4	12,00
3	tercerización	**R024**	1	2	1	2	1	2	2,00
4	Indicadores de desempeño	**R025**	2	4	3	3	2,5	3,5	8,75
5	Disposición al cambio	**R026**	3	4	3	4	3	4	12,00
6	Comunicaciones	**R027**	3	4	3	4	3	4	12,00
	II.IV Riesgos de tecnología de Inf								
1	Relevancia	**R028**	3	4	3	4	3	4	12,00
2	Integridad	**R029**	3	4	3	4	3	4	12,00
3	Acceso	**R030**	3	4	3	4	3	4	12,00
4	Disponibilidad	**R031**	3	4	3	4	3	4	12,00
5	Infraestructura	**R032**	3	4	3	4	3	4	12,00
	II.V Riesgos de Integridad								
1	Fraude Gerencial	**R033**	3	5	3	4	3	4,5	13,50
2	Fraude de Empleados/terceros	**R034**	3	5	3	4	3	4,5	13,50
3	Actos Ilegales	**R035**	3	5	3	4	3	4,5	13,50
4	Uso no autorizado	**R036**	2	4	2	3	2	3,5	7,00
5	Reputación	**R037**	2	4	2	3	2	3,5	7,00
	III. Riesgos Informac. Toma Desic.								
	III.I Riesgos Informac. Operativa								
1	Condiciones Servicio/Producto	**R038**	3	4	3	4	3	4	12,00
2	Alineamiento	**R039**	3	4	3	4	3	4	12,00
	III.II Riesgos de Informac. Gestión								
1	Presupuesto	**R040**	2	2	1	2	1,5	2	3,00
2	Información Contable	**R041**	2	4	2	3	2	3,5	7,00
	III. II Riesgos Informac. Estratégica								
1	Monitoreo del Entorno	**R042**	2	3	2	3	2	3	6,00
2	Portafolio de negocios	**R043**	2	2	2	3	2	2,5	5,00
3	Estructura organizacional	**R044**	3	3	3	4	3	3,5	10,50
4	Medición del desempeño	**R045**	2	3	2	3	2	3	6,00
5	Asignación de Recursos	**R046**	2	3	3	4	2,5	3,5	8,75
6	Planeamiento	**R047**	3	4	3	3	3	3,5	10,50
7	Ciclo de vida	**R048**	3	4	3	4	3	4	12,00

Anexo No. 3.2
EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TIC
PRIORIZACION DE RIESGOS POR BLOQUE

Unidad **U001** **Administración de la Seguridad**
Departamento Proceso **Tecnologías de Información**

			Amelia		Rodolfo		Promedio		Riesgo
			P	I	P	I	P	I	
I. Riesgos del Entorno	**I. Riesgos del Entorno**								
	Innovación tecnológica	**R003**	3	5	3	4	3	4,5	13,50
	Pérdidas Catastróficas	**R008**	2	5	2	5	2	5	10,00
	Competencia	**R001**	2	3	2	4	2	3,5	8,00
	Regulatorio	**R006**	2	3	2	3	2	3	6,00
	Deseo de los clientes	**R002**	1	4	2	3	1,5	3,5	5,25
	Soberano Político	**R004**	1	3	2	3	1,5	3	4,50
	Legal	**R005**	1	2	1	2	1	2	2,00
	Industria	**R007**	1	2	1	2	1	2	2,00
II. Riesgos de Procesos	**II. Riesgos de Procesos**								
	II.I Riesgo de Operaciones								
II.I Riesgo de Operaciones	Brecha de Desempeño	**R014**	3	5	3	4	3	4,5	13,50
	Tiempo de ciclo	**R015**	3	4	3	4	3	4	12,00
	Capacidad	**R013**	3	3	3	4	3	3,5	10,50
	Cumplimiento	**R017**	3	3	3	4	3	3,5	10,50
	Interrupción	**R018**	3	3	3	4	3	3,5	10,50
	Medio Ambiente	**R020**	3	3	3	4	3	3,5	10,50
	Eficiencia	**R012**	3	4	2	3	2,5	3,5	8,75
	Satisfacción de clientes	**R009**	2	3	3	3	2,5	3	7,50
	Capital de Conocimiento	**R011**	2	3	2	3	2	3	6,00
	Falta de Productos/Servicios	**R019**	2	4	2	2	2	3	6,00
	Recursos Humanos	**R010**	2	4	1	3	1,5	3,5	5,25
	Salud y Seguridad	**R021**	2	4	1	2	1,5	3	4,50
	Alianzas	**R016**	1	2	1	1	1	1,5	1,50
	II.II Riesgos de Dirección								
II.II Riesgos de Dirección	Autoridad/Límite	**R023**	3	4	3	4	3	4	12,00
	Disposición al cambio	**R026**	3	4	3	4	3	4	12,00
	Comunicaciones	**R027**	3	4	3	4	3	4	12,00
	Indicadores de desempeño	**R025**	2	4	3	3	2,5	3,5	8,75
	Liderazgo	**R022**	2	3	2	4	2	3,5	7,00
	Tercerización	**R024**	1	2	1	2	1	2	2,00
	II.IV Riesgos de tecnología de Inf								

Anexo No. 3.2
EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA RELATIVAS A LAS TIC
PRIORIZACION DE RIESGOS POR BLOQUE

Unidad **U001** **Administración de la Seguridad**
Departamento Proceso **Tecnologías de Información**

			Amelia		Rodolfo		Promedio		Riesgo
			P	I	P	I	P	I	
II.IV Riesgos de tecnología de Inf	Relevancia	**R028**	3	4	3	4	3	4	12,00
	Integridad	**R029**	3	4	3	4	3	4	12,00
	Acceso	**R030**	3	4	3	4	3	4	12,00
	Disponibilidad	**R031**	3	4	3	4	3	4	12,00
	Infraestructura	**R032**	3	4	3	4	3	4	12,00
II.V Riesgos de Integridad	**II.V Riesgos de Integridad**								
	Fraude Gerencial	**R033**	3	5	3	4	3	4,5	13,50
	Fraude de Empleados/terceros	**R034**	3	5	3	4	3	4,5	13,50
	Actos Ilegales	**R035**	3	5	3	4	3	4,5	13,50
	Uso no autorizado	**R036**	2	4	2	3	2	3,5	7,00
	Reputación	**R037**	2	4	2	3	2	3,5	7,00
III. Riesgos Informac. Toma Desic.	**III. Riesgos Informac. Toma Desic.**								
III.I Riesgos Informac. Operativa	**III.I Riesgos Informac. Operativa**								
	Condiciones Servicio/Producto	**R038**	3	4	3	4	3	4	12,00
	Alineamiento	**R039**	3	4	3	4	3	4	12,00
III.II Riesgos de Informac. Gestión	**III.II Riesgos de Informac. Gestión**								
	Información Contable	**R041**	2	4	2	3	2	3,5	7,00
	Presupuesto	**R040**	2	2	1	2	1,5	2	3,00
III. II Riesgos Informac. Estratégica	**III. II Riesgos Informac. Estratégica**								
	Ciclo de vida	**R048**	3	4	3	4	3	4	12,00
	Estructura organizacional	**R044**	3	3	3	4	3	3,5	10,50
	Planeamiento	**R047**	3	4	3	3	3	3,5	10,50
	Asignación de Recursos	**R046**	2	3	3	4	2,5	3,5	8,75
	Monitoreo del Entorno	**R042**	2	3	2	3	2	3	6,00
	Medición del desempeño	**R045**	2	3	2	3	2	3	6,00
	Portafolio de negocios	**R043**	2	2	2	3	2	2,5	5,00