Universidad de Costa Rica

Sistema de Estudios de Posgrado

“Auditoría de seguridad general en el área de Tecnologías de Información en la empresa Media Gurú”

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.

Oscar Ezzio Reyes Donato

Carné 822937

Ciudad Universitaria “Rodrigo Facio”, Costa Rica

Año 2007

Título

“Auditoría de seguridad general en el área de Tecnologías de Información en la empresa Media Gurú”

DEDICATORIA

A mi esposa Ivón, y a mis hijos Gabriel y Javier
Gracias por su paciencia y apoyo.

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 Magíster con énfasis en Auditoría de Tecnologías de Información.

Dr. Aníbal Barquero Chacón
Director Programa de Maestría

MAI Sergio Espinoza Guido
Profesor Coordinador

Máster Xiomar Delgado Rojas
Profesor Guía

Máster Carlos Luis Boza Araya
Supervisor Laboral

MSc. Oscar Ezzio Reyes Donato
Estudiante

CONTENIDO

ÍNDICE DE SIGLAS Y ABREVIATURAS

Asamblea Legislativa	AL
Banco Interamericano de Desarrollo	BID
Caja Costarricense de Seguro Social	CCSS
Defensoría de los Habitantes de la República	DHR
Estados Unidos de América	EEUU
Fomento y Desarrollo de la Actividad Juvenil	FDAJ
Gestión y Desarrollo Cultural (Fomento y Extensión Cultural)	GDC
Instituto Costarricense de Acueductos y Alcantarillado	AyA
Maestría en Administración y Dirección de Empresas	MADE
Ministerio de Economía, Industria y Comercio	MEIC
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura	UNESCO
Partido Liberación Nacional	PLN
Partido Unidad Social Cristiana	PUSC
United States of America	USA
Universidad de Costa Rica	UCR
INTERNATIONAL ORGANIZATION FOR STANDARDIZATION	ISO
MEDIA GURU SOCIEDADA ANONIMA	MEDIAGURU
INTERNATIONAL ELECTROTECHNICAL COMMISSION	IEC
BRITISH STANDARDS INSTITUTE)	BSI
INTERNATIONAL STANDARD ON AUDITING	ISA

RESUMEN

Reyes Donato, Oscar Ezzio

"Auditoría de seguridad general en el área de Tecnologías de Información en la empresa Media Gurú"

Programa de Posgrado en Administración y Dirección de Empresas. –San José, C.R.:
o. reyes d. – 2007.

El objetivo general del trabajo es evaluar los controles de seguridad del almacén activo de datos de la empresa.

La organización investigada se dedica a realizar auditorías de publicidad, auditarías de contenido, auditorías de información y planeación publicitaria

Para ello el proyecto desarrolla una auditoría de seguridad

Dentro de sus principales conclusiones se encuentra que los controles instituidos hasta el momento han dado resultados adecuados y que ha basado el diseño de su sistema de seguridad en criterios independientes no en ninguna norma ya establecida

Con base en todo lo anterior, se recomienda que fundamenten la selección de controles en una norma establecida, que instituyan un esquema de monitoreo constante de los controles, que se defina y comunique una política de seguridad interna, que se instaure un esquema reiterado de verificación de controles.

Palabras clave: Auditoría, seguridad

Director de la investigación:
MAI: Sergio Espinoza Guido

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

Tema:

La empresa Media Gurú, desde sus inicios ha mantenido un crecimiento sostenido en transacciones a través de veintiún años. Eso los ha obligado a buscar ser más eficientes en sus funciones para poder satisfacer las demandas de sus clientes.

Este crecimiento en eficiencia se ha basado en el uso de las Tecnologías de Información.

A pesar de ser un crecimiento ordenado, hay aspectos de seguridad que se pueden haber dejado de lado.

Por lo anterior es que se plantea la realización de una Auditoría en aspectos de Seguridad General en el área de las Tecnologías de Información, buscando evaluar por medio de la misma, si se han establecido controles con miras a resguardar tanto los datos como los equipos que se emplean, y si existen estos controles, verificar por un lado que se cumplan, y por otro que sean eficaces.

El fin de la auditoría es, después de haber realizado lo propuesto, hacer un veredicto de la razón de la seguridad en la empresa y generar recomendaciones de la misma

Introducción

El objetivo principal de este proyecto es Realizar una Auditoría de Seguridad en el área de Tecnologías de Información en la empresa Media Gurú.

Media Gurú es una empresa dedicada principalmente a la venta de servicios de monitoreo publicitario y servicios afines.

Esta organización se fundó en 1985 y fue pionera en el empleo de computadores en el campo del monitoreo publicitario en nuestro país.

Según fue transcurriendo el tiempo, se transformó en una empresa de envergadura internacional, cuyo mercado abarca varios países de Centroamérica que incluye Nicaragua, Honduras y están próximos a comprar una empresa en Guatemala.

En la actualidad, forma parte del Grupo Ibope Time, que cuenta con más de 3000 empleados a nivel latinoamericano

De la mano con su crecimiento, esta compañía ha tenido que ir buscando soluciones tecnológicas que le permita satisfacer la demanda de sus clientes para poder cumplirles a cabalidad. Estas soluciones involucran desarrollos de *software*, bases de datos e inversiones en comunicaciones entre otras.

Se puede deducir de todo lo anterior, que el producto de esta organización es la información, y, por ende, es altamente dependiente de las tecnologías de información.

Los jerarcas de la institución, conociendo la importancia de proteger su producto, se encuentran preocupados ya que desconocen si el grado de seguridad con que cuentan en sus instalaciones es adecuado.

De la misma forma que las empresas establecen controles de seguridad para proteger sus productos, MediaGurú debe implantar controles para proteger su información.

En este momento, no es claro si se han definido estos controles, o en caso de que estén definidos, si los mismos son lo suficientemente satisfactorios para efectuar con esta función o, en caso que lo sean, si los controles se están llevando a cabo en forma activa.

Con el tema propuesto se busca establecer la razón de la seguridad de las Tecnologías de Información y Comunicaciones de la empresa mencionada.

En lo referente a intereses profesionales, se busca con este proyecto, poner en práctica los conocimientos adquiridos en el transcurso de la Maestría en Auditoría de Tecnologías de Información, especialmente en un área que es de suma importancia como lo es la seguridad.

Esta auditoría se llevará a cabo únicamente en las oficinas que esta empresa tiene en Costa Rica, ubicadas en Curridabat, en San José.

De igual forma, se limita la verificación de controles de acceso físico al área de servidores de la empresa.

En lo que a seguridad lógica respecta, se busca establecer el nivel de seguridad, satisfactorio o no, referente al almacén activo de datos de la empresa.

Como aporte final, como parte del proyecto, se emitirá una serie de recomendaciones para alinear la empresa con las mejores prácticas de la industria en aspectos de seguridad.

Objetivos

Objetivo Principal:

Revisar si los controles establecidos en la empresa MediaGurú para proteger la información del almacén activo de datos son adecuados de acuerdo con las mejores prácticas de la industria.

Objetivos Específicos:

- Verificar la razón de la seguridad física de las instalaciones de servidores de MediaGurú.

- Examinar la razón de la seguridad lógica de los datos de MediaGurú.

- Comprobar por medio de pruebas de cumplimiento si los controles de seguridad están acordes con lo establecido en la normativa vigente.

- Emitir conclusiones y recomendaciones según el resultado de las pruebas de cumplimiento practicadas.

Capítulo I: Definiciones y términos

1.1 Importancia de la Seguridad en Tecnologías de Información

La seguridad en el área de TI se ha convertido en un tema de gran relevancia para todas las empresas u organizaciones. Esto es debido al valor de la información que se genera en cada agrupación.

En la actualidad, las tecnologías de información han generado beneficios diversos, entre los que se pueden mencionar:

- Permitir a personas e instituciones de diversos tamaños, acceder y compartir gran cantidad de datos
- Facilitar la comunicación y cooperación entre partes
- Facilitar transacciones comerciales
- Generación de informes con gran rapidez

Esto ha provocado que las empresas se tornen cada vez más dependientes de este tipo de tecnologías.

Pese a este tipo de dependencias, en algunas organizaciones se obvia el hecho de que existen amenazas que pueden afectar el funcionamiento correcto de las tecnologías de información.

Este tipo de amenazas pueden ser de carácter físico o lógico.

Ahora bien, sin importar el tipo de amenaza, es de suma importancia que las organizaciones cuenten con una serie de controles para evitar o administrar en lo posible, la materialización de una amenaza.

En este punto, es importante aclarar que, sin importar la cantidad de controles que se instituyan garantizar que una organización se encuentra totalmente libre de amenazas o peligros.

La seguridad en Tecnologías de Información está vinculada con los controles que se establecen con el fin de administrar los riesgos, peligros o amenazas.

1.2 Seguridad Física en Tecnologías de Información[1]

Como punto de partida para hablar de seguridad física en tecnologías de información, se citará la siguiente definición, que fue tomada de un curso que se imparte en la Universidad de Valencia:

> "Cuando hablamos de *seguridad física* nos referimos a todos aquellos mecanismos --generalmente de prevención y detección-- destinados a proteger físicamente cualquier recurso del sistema; estos recursos son desde un simple teclado hasta una cinta de backup con toda la información que hay en el sistema, pasando por la propia CPU de la máquina.
>
> Dependiendo del entorno y los sistemas a proteger esta seguridad será más o menos importante y restrictiva, aunque siempre deberemos tenerla en cuenta. "

La seguridad física en tecnologías de información es la parte de la seguridad que se encarga de definir controles contra amenazas o peligros de carácter físico.

[1] http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html

A continuación se mencionan algunos peligros de este tipo:

- Accesos indebidos a los equipos o datos
- Desastres naturales como incendios o inundaciones
- Accidentes ocasionados por el hombre, tanto dentro de la organización como externos a la misma
- Incidentes deliberados tanto internos como externos

Algunos aspectos de la seguridad física pueden ser tan sencillos como mantener una puerta cerrada, el problema es que este tipo de controles, por parecer obvios o simples se olvidan o no se les da la importancia que requieren, de tal suerte que podría ser más sencillo y efectivo para un infractor tratar de irrumpir en un centro de cómputo o sala de servidores y dañar un equipo físico que intentar un ataque de otro tipo como intentar contagiar a la organización con un virus informático.

1.3 Seguridad Lógica

Como ya se ha mencionado, las tecnologías de información no sólo sufren de amenazas de carácter físico sino también lógicos.

A continuación se listan algunas amenazas en esta categoría:

- Acceso no autorizado a aplicaciones
- Acceso a aplicaciones en horas no autorizados
- Virus

- Ataques de Delincuentes Informáticos[2]

En forma análoga a la seguridad física, la seguridad lógica lidia con los controles o barreras que eviten o disminuyan la materialización de amenazas lógicas. De igual forma que el acceso a una sala de servidores debe de estar controlado, el acceso a los datos debe de estar controlado también. Así, la organización debe de contar con barreras contra el ingreso de virus, evitar accesos a sitios de Internet indebidos, entre otros.

Tanto la seguridad física como la lógica deben de estar sustentadas en políticas establecidas por las altas esferas de la organización, no deben ser antojadizas, deben de ser planificadas.

1.4 Auditoría de Seguridad en Tecnologías de Información

La siguiente es una definición de "Auditoría de Seguridad en Informática", tomada de un artículo[3]:

> "La Auditoría de la Seguridad Informática en la informática abarca el concepto de seguridad física y lógica. La seguridad física se refiere a la protección de hardware y los soportes de datos, así también como la seguridad del los edificios y las instalaciones que lo albergan. Esto mismo contempla situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.

[2] Delincuentes informáticos: personas que usan su conocimiento con fines maliciosos, antimorales o incluso bélicos, como intrusión de redes, acceso ilegal a sistemas gubernamentales, robo de información, distribuir material ilegal o moralmente inaceptable, piratería, fabricación de virus, herramientas de Crackeo y elementos de posible terrorismo como la distribución de manuales para fabricar elementos explosivos caseros o la clásica tortura china.

[3] http://www.shellsec.net/articulo/auditoria-empresas/

Por su parte la seguridad lógica se refiere a la seguridad del uso de software, protección de la información, procesos y programas, así como el acceso ordenado y autorizado de los usuarios a la información."

El fin de una Auditoría de Seguridad en Tecnologías de Información es realizar una verificación de las bondades o defectos de la implantación de esquemas de seguridad tanto físicos como lógicos.

1.4 Fuentes de criterios

A la hora de verificar los esquemas de seguridad, surge un problema: ¿contra qué se compara para calificar si un esquema es adecuado o no?

Para poder realizar la verificación de las bondades o defectos de los esquemas de seguridad establecidos, es necesario tomar como punto de comparación a una fuente de criterios.

La definición de criterio, tomada del Diccionario de la Real Academia de la Lengua Española es como sigue:

Criterio.

(Del gr. κριτήριον, de κρίνειν, juzgar).

1. m. Norma para conocer la verdad.

2. m. Juicio o discernimiento.

Un criterio es algo contra que comparar un proceso o situación, constituye el “deber ser”.

Se puede decir que una fuente de criterios es un conjunto de normas definida contra las que se puede comparar un esquema para definir si cumple o no con lo esperado.

Este conjunto de normas son definidas por alguna organización reconocida de carácter internacional.

En el caso que nos compete, se definió emplear como fuente principal de criterios, aunque no necesariamente en forma exclusiva, la norma **ISO/IEC 17799**[4]***.***

Esta norma es un estándar para la seguridad de la información. Fue publicado por primera vez como ISO/IEC 17799:2000 por International Organization for Standardization y por la comisión International Electrotechnical Commission en el año 2000 y con el título de Information technology - Security techniques - Code of practice for information security management. Tras un periodo de revisión y actualización de los contenidos del estándar se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

Capítulo II: La empresa.

2.1 Generalidades

[4] ISO : International Organization for Standardization

MediaGurú es una empresa costarricense que nace en agosto del 2002[5] como resultado de la fusión de tres empresas:

- Servicios Publicitarios Computarizados,
- Medio & Mensaje y
- Media Data.

La organización brinda los mismos servicios que brindaban las tres empresas por separado y se agrupan de la siguiente manera:

- Auditorías de Publicidad: Auditorías, Competencia, Industria
- Auditorías de Contenido: Videoteca (campañas, videos, slogans, texto), Fonoteca, Hemeroteca, Exterior y Promociones
- Auditorías de Información
- Planeación Publicitaria

[5] En la introducción se menciona que la empresa ha funcionado desde 1985 y es por que una de las empresas que la conforman, Servicios Publicitarios Computarizados nació en ese año.

Tiene establecida su misión como sigue:

MISIÓN

“Transformamos en conocimiento la información publicitaria y periodística difundida por los medios de comunicación masivos, para apoyar las acciones de nuestros clientes en sus estrategias de imagen y comercialización.”

Por otro lado, tienen definida su visión como sigue:

VISIÓN

“Ser el mejor proveedor de conocimiento sobre la industria de la comunicación en Centroamérica.”

Desde sus inicios, sus fundadores se abocaron al uso de la tecnología para llevar a cabo su misión. De forma tal que aún iniciando, ya empleaban tecnología de punta para la época. A manera de historia, se transcribe un párrafo del documento "Veinte años más tarde"[6]:

"En ***MediaGurú*** dejamos de usar un Dynabite con *floppy* de 12 pulgadas por 52 computadoras, incluidos ocho servidores: datos, oracle, web, firewall, zoyla, video y audio, backup, respaldo de videos. De Database II a Oracle 9i, de impresoras de matriz a láser, de edición lineal a digital, de siete colaboradores a 34."

De ese párrafo se infiere no sólo la dependencia que tiene la empresa de las Tecnologías de Información, sino también el crecimiento que ha tenido.

Según fue transcurriendo el tiempo, se transformó en una empresa de envergadura internacional, cuyo mercado abarca varios países de Centroamérica, que incluye Nicaragua, Honduras y están próximos a comprar una empresa en Guatemala.

En la actualidad, forma parte del Grupo Ibope Time, que cuenta con más de 3000 empleados a nivel latinoamericano

La vinculación de MediaGurú con la tecnología ha sido permanente. Ha desarrollado sus propios sistemas de monitoreo y competencia, además de sistemas de planificación publicitaria. Ha evolucionado con los avances tecnológicos, reemplazando su software cinco veces en ese lapso.

Hoy dispone de una plataforma Web para distribuir la información cuantitativa y cualitativa de los mercados publicitarios: *Mediatools Advanced* (www.mediaguru.co.cr).

[6] Elaborado por José Francisco Correa Navas, Presidente de MediaGurú

Estructura Orgánica

Esta organización tiene establecida una estructura orgánica de carácter jerárquico definida como sigue:

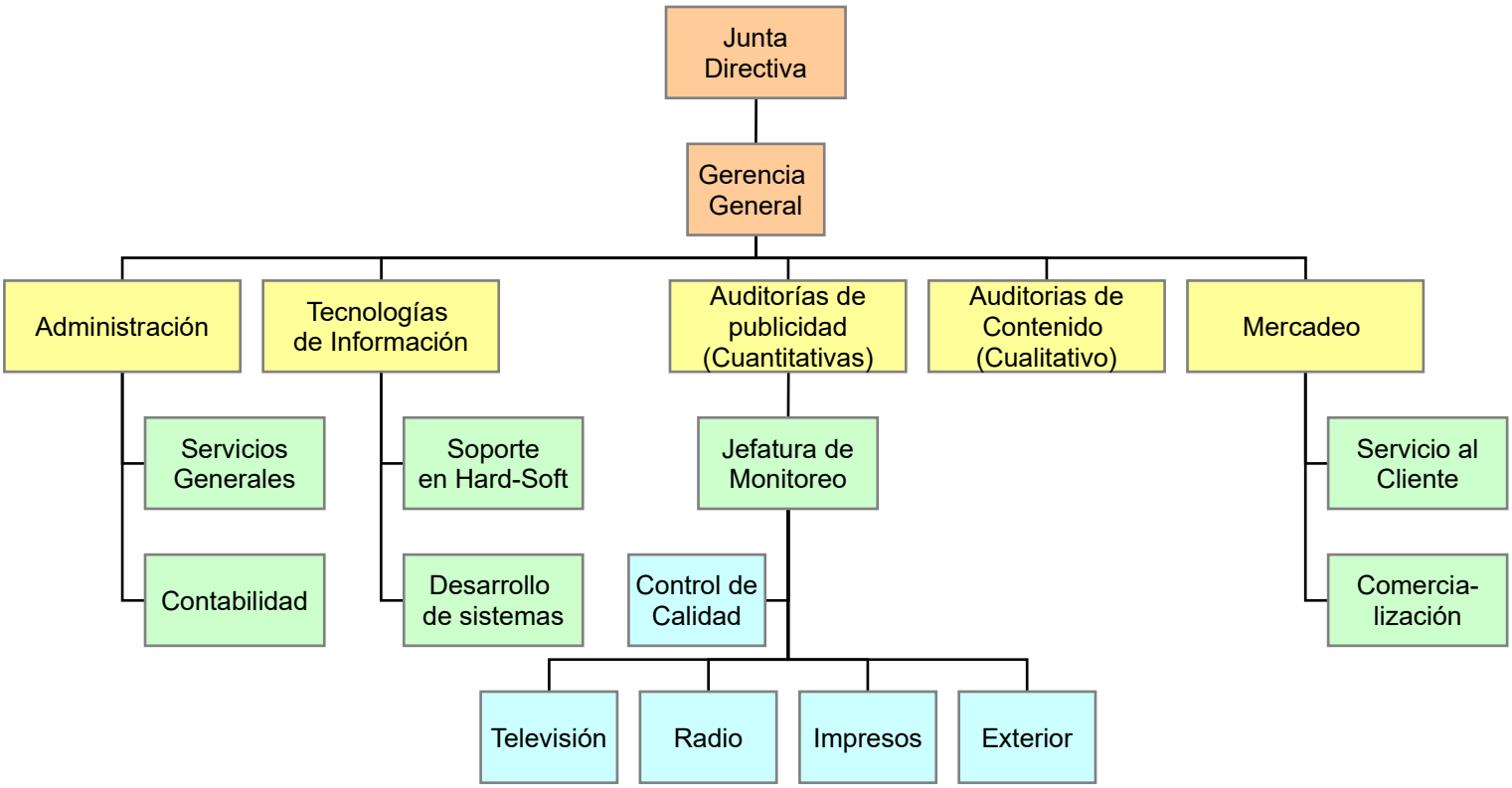

Figura 1[7].

[7] Fuente: MediaGurú

Como se puede observar en el organigrama, la empresa está compuesta por cinco departamentos, dependientes de la gerencia general y de la junta directiva. Estos últimos constituyen la “alta gerencia” de la institución.

2.2 Legislación y normativas

Desde el punto de vista jurídico, la empresa Mediagurú está constituida como una sociedad anónima cuya razón social es “MEDIA GURU SOCIEDAD ANÓNIMA”, con cédula jurídica 3-101-225254, inscrita en el registro nacional en el tomo 1113, folio 006 y asiento 00008.

Por el tipo de institución que es, no está obligada a adherirse a ningún tipo de normativa de control.

Capítulo III: Análisis de la situación actual del departamento de Tecnologías de Información de la empresa.

3.1 Estructura Orgánica del departamento de Tecnologías de Información

Tecnologías de Información está constituido en uno de los cinco departamentos que conforman la empresa.

Dentro de la estructura orgánica, este departamento se encuentra subordinado directamente a la Gerencia General de la empresa.

En cuanto a su ubicación dentro de la estructura orgánica de la institución, este departamento tiene un nivel adecuado para apoyar a la organización a lograr cumplir con los aspectos estratégicos que se plantee.

A continuación se presenta un diagrama para representar la estructura organizativa de dicho departamento:

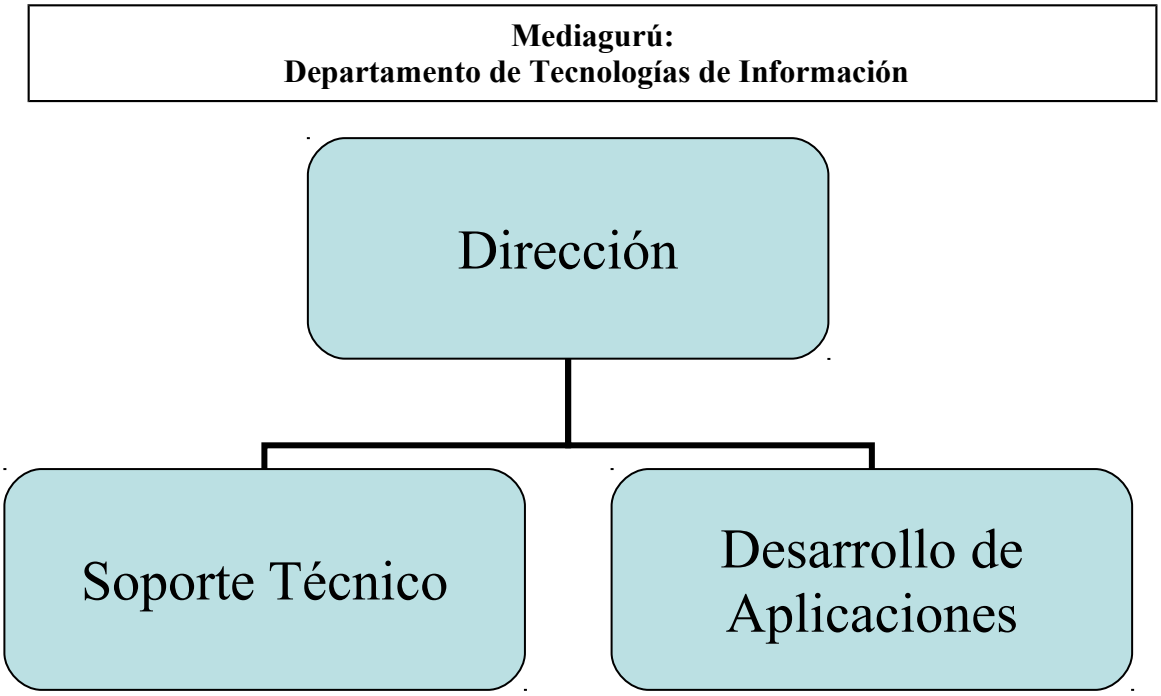

Figura 2.[8]

La dirección de este departamento tiene la función de establecer el planeamiento estratégico del mismo y vigilar que se lleve a cabo.

La unidad de soporte técnico es la encargada de velar por el mantenimiento del equipo de cómputo de la empresa y dar soporte a los usuarios.

La unidad de desarrollo e aplicaciones tiene como función primordial el dar mantenimiento a las aplicaciones existentes y el desarrollo de nuevas.

Dicho departamento se encuentra compuesto por cuatro integrantes, a saber:

[8] Fuente: Departamento de Tecnologías de Información, MediaGurú

- Un director
- Un responsable de la parte técnica (mantenimiento de equipo, red, soporte, etc.)
- Un asistente de la parte técnica y para otros trabajos
- Un desarrollador para las aplicaciones de Internet

Como se ve, las funciones de este departamento son muy amplias, van desde el apoyo operativo a usuarios más simple hasta el desarrollo de aplicaciones y control de calidad de las mismas.

Dada la amplia gama de funciones y la cantidad de funcionarios, no es posible tener una adecuada segregación de funciones.

3.2 Planificación estratégica

Los siguientes son los objetivos planificados por la institución para desarrollar en el corto, mediano y largo plazo:[9]

Corto (2006)

- Calidad continua en procesos de producción y sistemas de información
- Promover en los colaboradores y "stakeholders" el nuevo enfoque empresarial.

[9] Estos objetivos fueron tomados de una presentación desarrollada por la gerencia de la empresa

- Revisión de Política de Recursos Humanos, estudiar el efecto de contratación y rotación.
- Cumplir con las metas de ventas especificadas en el PPto 2007
- Fortalecer el liderazgo en Centroamérica en el ámbito publicitario.
- Aprovechar al máximo la relación con IBOPE-TIME (SINERGIAS)
- Mejorar el servicio al cliente por medio de una capacitación eficaz para que el uso y conocimiento de los sistemas sea máximo
- Incrementar el uso y la eficiencia de Mediatools-Advanced
- Aumentar el valor al cliente
- Información -> Inteligencia -> Conocimiento

Corto (2007)

- Desarrollar el sistema de planeación Web previa consulta a clientes
- Concluir el proceso de compra de Guatemala
- Desarrollar “spotter”, noticias
- Expandir a El Salvador los servicios de información publicitaria.
- Estandarizar información en Centroamérica
- Ampliación de cobertura no tradicional (cine, PP, Internet, movil, indoor)
- Revisión de política de recursos humanos

- Sello de Calidad
- Ingresar El Salvador

Mediano (2008)

1. Expandir a nivel centroamericano el servicio de noticias Nicaragua y planeación
2. Perfeccionar la información gerencial regional
3. Implementación interna MTA
4. Automatización de tareas
5. Encuesta de TV en El Salvador

Largo (2009, en adelante)

1. Reconocimiento automática
2. Sistemas de decisión con simulación
3. Fluido eléctrico 24/7
4. Perfeccionar un modelo de planeación multimedia y ROI
5. El mercado necesitará de otros tipos de investigaciones y de la relación de la info con otras variables cuantitativas

Como se puede inferir por lo detallado de los puntos anteriores, la administración ha invertido tiempo en la planificación y tiene claro el rumbo que desea que siga la empresa. En distintos puntos de esta planificación se destaca la

importancia que se le da a las aplicaciones informáticas, en la calidad y eficiencia de los mismos y en nuevos desarrollos.

Sin embargo, hay poca profundidad en temas referentes a la seguridad de la información o planes de continuidad de negocios, que son aspectos de gran importancia y que deben ir de la mano con los desarrollos en este tipo de sistemas.

3.3 Planificación estratégica del departamento de Tecnologías de Información

En cuanto a lo que se refiere a la planificación estratégica del departamento de tecnologías de información, el último plan de trabajo detallado se hizo en el período 2005.

En dicho plan se estipuló como objetivo general:

> "Continuar con el desarrollo de la infraestructura tecnológica que le permita a la empresa procesar y consolidar la información centroamericana, así como mejorar la eficiencia operativa interna mediante sistemas de información."

Es importante hacer ver en este punto que hay un desfase evidente entre el nivel de la planificación estratégica de la empresa y el del departamento de Tecnologías de Información de la misma.

La falta de un detalle más profundo evita el poder establecer la alineación de los objetivos del departamento con los de la empresa.

3.4 Plataforma Tecnológica

La empresa tiene un ambiente heterogéneo en los que se refiere a sistemas operativos y características de los equipos de cómputo. De igual forma, cuenta con diversos servidores de diferentes características.

En bases de datos y herramientas de desarrollo, también se mantiene un ambiente heterogéneo.

La siguiente es una tabla resumen con datos de los servidores y su función:

Servidor	Marca	Modelo	Año de adquisición	Aplicación
HPLINUX	HP	PROLIANT ML350	10/10/2005	BASE DE DATOS ORACLE PARA INTERNET
SION	HP	MARCA HP, PROLIANT ML110G3, 1GB DE RAM, SERIE: USX54000J7, TARJETA CONTROLADORA RAID 0 Y 1 INTEGRADA SATA, 2 DISCOS DUROS WEST DIGITAL DE 250GB SATA2	07/11/2006	BASE DE DATOS DE SISTEMA PRINCIPAL (EN VISUAL FOX)
5 SERVIDORES DE ARCHIVOS (TIPO A)	CLONES	P4 (procesador)	DEL 2002 AL 2005	SERVIDORES DE ARCHIVOS MULTIMEDIA Y BACKUPS
25 SERVIDORES DE VIDEO Y AUDIO (TIPO B)	CLONES	P3 Y P4 (procesador)	DEL 2001 AL 2005	SERVIDORES DE ARCHIVOS MULTIMEDIA DE VIDEO Y AUDIO.

Tabla 1[10]

[10] Fuente: Departamento de Tecnologías de Información, MediaGurú

Si bien, generalmente es preferible mantener un ambiente homogéneo en tanto en sistemas operativos como en equipos, en el caso de MediaGurú, la heterogeneidad existente está justificada por las características de la información con que laboran y las aplicaciones que se encuentran elaboradas y las que están en vías de desarrollo.

A manera de ejemplo, se cuenta con HP PROLIANT ML350 con un sistema operativo Linux para ejecutar una base de datos Oracle. En este caso, la justificación para seleccionar este sistema operativo radica en el mejor desempeño de la base de datos comparándolo con el desempeño de la misma ejecutándose sobre un sistema operativo Windows.[11]

Por otro lado se cuenta con un servidor HP, PROLIANT ML110G3, con un sistema operativo Windows 2003. La razón para seleccionar este sistema operativo en vez de Linux se debe a que en este equipo se ejecuta la base de datos del sistema principal que está escrito en Visual Fox.

En cuanto a los 25 servidores de vídeo y audio, éstos ejecutan un sistema operativo Windows 98, en este caso, la selección se dio porque el software empleado para la grabación del audio fue diseñado para dicho sistema operativo.

Resumiendo, como se mencionó anteriormente, se cuenta con un ambiente heterogéneo en lo que respecta a sistemas operativos, pero este hecho no es el resultado de soluciones antojadizas.

[11]Se puede consultar http://www.dba-oracle.com/art_builder_linux_oracle.htm al respecto

Capítulo IV: El proceso de auditoría

4.1 Objetivos

Una parte primordial del proceso de auditoría es la definición de los objetivos que se busca cumplir al finalizar la misma. Éstos están expuestos en la introducción de este documento, por lo que se omite el reproducirlos en este punto.

4.2 Alcance

En lo que respecta a área geográfica, se limitará el alcance de esta auditoría a las oficinas de la empresa ubicadas en Curridabat, San José, Costa Rica.

En cuanto al período, el alcance de la presente auditoría se limitará al estado de la empresa en el período que finaliza en diciembre del 2006.

De igual forma, se limita la revisión de seguridad física al acceso al área de servidores de la empresa.

También, la revisión de la seguridad lógica se limitará a los accesos al almacén activo de datos de la empresa.

4.3 Planificación

La etapa de planificación se divide en Planificación Preliminar y Planificación Detallada. La primera tiene la finalidad de permitirle al auditor obtener

una idea de las características de la entidad que se va a auditar. Es en esta etapa donde se busca lograr una manera de obtener la información necesaria para conocer un conocimiento de la entidad, si la misma está sujeta a algún tipo de legislación particular, si se adscribe a alguna normativa de control en particular y otros puntos de interés. Parte del objetivo de esta etapa es descubrir si existen áreas más vulnerables en lo que respecta a aspectos de seguridad, para enfocar el resto de la auditoría hacia esas áreas.

Con el conocimiento obtenido, se puede iniciar la Planificación Detallada, donde se esbozará un programa para indagar el estado de la seguridad de las Tecnologías de Información en la organización. Este programa incluye el diseño de papeles de trabajo[12], así como el diseño y la ejecución de pruebas de cumplimiento, entre otros.

4.4 Comunicación de Resultados

Después de realizadas las pruebas definidas, debe de haberse obtenido la evidencia para elaborar un Informe de Auditoría, que es un documento donde se estipulan los hallazgos encontrados, así como las recomendaciones pertinentes. Sin embargo, antes de la redacción del informe final, se debe dar un proceso de comunicación de resultados donde se le presenta a la administración un borrador del informe donde se detallarán los hallazgos, problemas encontrados en la realización de la auditoría, se incluirán los objetivos de la misma y las conclusiones preliminares.

Posteriormente, se elaborará y se hará entrega del informe final.

[12] los papeles de trabajo, son el conjunto de cédulas en las que el Auditor registra los datos y la información obtenida de la empresa que esta examinando y de esta manera acumula las pruebas encontradas y la descripción de las mismas.
Tomado de
http://www.geocities.com/miguelalatrista/LOSPAPELESDETRABAJOENLAAUDITORIA.htm

4.5 Evaluación del control interno[13] en MediaGurú

Para la evaluación del control interno en la empresa, se preparó un instrumento con una serie de preguntas pertinentes al ámbito de la seguridad.

Dicho instrumento les fue aplicado a funcionarios del departamento de tecnologías de información de Mediagurú.

Después de aplicar el instrumento y apoyado también en observaciones realizadas, se puede afirmar que la empresa tiene una preocupación por los procesos que involucran la seguridad de la información, aunque no se puede garantizar que estos procesos estén siempre bien comunicados

[13] **CONTROL INTERNO**: Es un proceso continuo realizado por la dirección, gerencia y, el personal de la entidad; para proporcionar seguridad razonable, respecto a si están lográndose los objetivos siguientes:
· Promover la efectividad, eficiencia y economía en las operaciones y, la calidad en los servicios que deben brindar cada entidad pública;
· Proteger y conservar los recursos públicos contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal;
· Cumplir las leyes, reglamentos y otras normas gubernamentales; y,
· Elaborar información financiera válida y confiable, presentada con oportunidad.
Tomado de: http://www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indc.htm#84

4.6 Hallazgos encontrados en la auditoría

Después de realizada la auditoría, se llevó a cabo la elaboración de una serie de Hojas de Hallazgos, donde se resume una grupo de condiciones que atentan contra algún criterio o sana práctica de la industria. En estos documentos también se establece el posible efecto de dicha condición y una recomendación para corregir las condiciones.

Como nota aclaratoria se indica que no todas las Hojas de Hallazgos elaboradas son negativas, en algunas se detallan algunos aspectos positivos.

A continuación se listan unos títulos de los hallazgos hallados a lo largo del proceso:

- La empresa carece de una política de seguridad definida
- La empresa carece de un control de acceso adecuado a la sala de servidores
- Cables de red expuestos
- Falta alineación de los objetivos de TI con los de la empresa
- No se cuenta con luces de emergencia
- Se carece de una política de “Escritorio Limpio”
- No existe un monitoreo de la “calidad de los passwords” de los usuarios
- No se cuenta con políticas de tiempo de conexión
- Se cuenta con un procedimiento documentado en caso de fallo de corriente

Debido a que la auditoría se centra en aspectos de seguridad tanto física como lógica, del acceso de los datos e información de la empresa, y tomando en cuenta la importancia de la misma, por razones de confidencialidad no se expone en este documento ni el informe final ni los hallazgos encontrados durante el proceso.

Capítulo V: Conclusiones y Recomendaciones

Una conclusión es una resolución que se ha tomado sobre una materia después de haberla ventilado[14].

En particular, el completar un proceso de auditoría de seguridad permite obtener un mayor conocimiento de la entidad auditada así como tener una visión mucho más clara de la situación en la que se encuentra en lo que se refiere a aspectos de seguridad de información.

Partiendo de lo anterior, es posible esbozar las siguientes conclusiones y recomendaciones:

Conclusiones generales:

- La empresa tiene clara la importancia de la seguridad en las Tecnologías de Información.
- Ha hecho esfuerzos por mantener la información segura en un grado adecuado
- Los controles instituidos hasta el momento han dado resultados adecuados
- Ha fundamentado el diseño de su sistema de seguridad en criterios independientes, no se basa en ninguna norma ya establecida

[14] Definición tomada del Diccionario de la Real Academia Española

- Pese a sus esfuerzos por mantener el acceso a los datos seguros, se han obviado algunos aspectos importantes

Recomendaciones generales[15]:

- Es recomendable no tratar de inventar lo que ya existe. Existen organizaciones (como la ISO y la BSI entre otras), que se encargan de definir normas a seguir para mantener la seguridad de la información. Hay que tratar de alinearse a alguna norma de éstas
- Las auditorías, en especial las que involucran aspectos de seguridad, deben ser procesos cíclicos, repetitivos, para poder, por un lado monitorear los cambios en la empresa y su efecto en los controles establecidos, y por otro lado para poder irse adecuando a los cambios en las mejores prácticas de le industria
- Es importante implantar un esquema de vigilancia constante acerca del cumplimiento y eficacia de los controles existentes
- Es necesario monitorear el cumplimiento de las recomendaciones de la auditoría
- Es necesario definir y comunicar una política de seguridad para la empresa.
- Debe establecerse un sistema de mantenimiento y monitoreo de la red de forma tal que la misma se mantenga protegida y se eviten problemas de seguridad

[15] Algunas de estas recomendaciones están incluidas en las hojas de hallazgos

- Es necesario mejorar los controles de acceso a la sala de servidores, de forma que se restrinja su acceso únicamente al personal que lo requiera
- Es recomendable establecer los medios necesarios para garantizar que cada funcionario pueda acceder a sus aplicaciones sólo en períodos de tiempo definidos

Bibliografía

Brenes Chacón, Albam (1992), **Los trabajos finales de graduación: su elaboración y presentación en ciencias sociales**. San José: Editorial Universidad Estatal a Distancia.

MEDIA GURU SOCIEDAD ANÓNIMA, **Manual de Inducción**, versión 3, 2005

ISA 315 - **Understanding the Entity and its Environment and Assessing the Risks of Material Misstatement**, 2004

ISO/IEC 17799:2005 **Information technology. Security techniques. Information security management systems. Requirements Code of practice for information security**, 2005

ISO/IEC 17799:2005 **Code of practice for information security management** Ed 2, 2005

Ibope Time, http://www.ibopetime.net (2002), Peru

MediaGurú,http://www.mediaGurú.co.cr/ (2003), Costa Rica

http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica

http://library.jid.org/en/mono43/Sanchez%20Soila

http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html

http://www.shellsec.net/articulo/auditoría-empresas/

http://www.segu-info.com.ar/fisica/seguridadfisica.htm

http://es.wikipedia.org/wiki/Seguridad_l%C3%B3gica

http://www.internet-solutions.com.co/ser_fisica_logica.php

http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

http://www.rae.es/

http://www.geocities.com/miguelalatrista/LOSPAPELESDETRABAJOENLAAUDITORIA.htm

http://www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indc.htm#84

http://buscon.rae.es/draeI/SrvltObtenerHtml?LEMA=conclusi%C3%B3n&SUPIND=0&CAREXT=10000&NEDIC=No

http://www.dba-oracle.com/art_builder_linux_oracle.htm

Anexos

Anexo 1: Formato general de la Hoja de Hallazgos

Hoja de Hallazgo

Titulo del Hallazgo

-Aquí se pone un título descriptivo para el hallazgo

Condición:

- Aquí se describe en forma explícita la condición encontrada
-

Criterio

- Aquí se indica el o los criterios contra los que atenta la condición

Causa

- Aquí se detalla la causa que genera la condición expuesta

Efecto:

- Aquí se incluye el posible efecto de continuar con la condición descrita

Recomendación:

- Aquí se formula una recomendación para mejorar la situación

Anexo 2: Instrumento para evaluar el control interno

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por: _____**

Fecha: _____

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
A. SEGURIDAD GENERAL			
1. Administración de la seguridad			
a. Existen y están por escrito las políticas, estándares y procedimientos relacionados con la seguridad en general?			
b. Fueron aprobadas por un funcionario autorizado?			
c. Son del conocimiento de la Alta Dirección?			
d. Están estructurados estos conceptos en manuales? - Se lleva un control de las personas que tienen estos manuales? - Se actualizan cada vez que se presente un cambio? - Se utilizan estos manuales?			
e. Se les ha dado divulgación y se han explicado en detalle a quien corresponda?			
f. Se respetan, acatan, cumplen y aplican sistemáticamente?			
g. Existen sanciones para quienes las incumplan o traten de hacerlo?			
h. Existe una persona encargada de la administración de la seguridad en general? - Cuál es su puesto? - Pertenece a Informática o la Auditoría Interna? - Están establecidas sus labores en la descripción de funciones? - Está claramente establecida su responsabilidad? - Tiene a su cargo todo tipo de seguridad? - Coordina las labores de seguridad con los subalternos encargados?			
i. Existe coordinación entre los guardas de seguridad con el personal de Informática? - Por visitas de "rondas"? - Por timbres desde el salón del computador? - Saben los guardas qué deben hacer en caso de una emergencia?			
j. Se ha realizado una cuantificación de los riesgos por aspectos de seguridad? Refiérase a la sección de "Aspectos Generales"			
k. Están claramente asignados los compromisos y responsabilidades de todos los involucrados, en cuanto a:			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
-aplicación y cumplimiento de políticas y procedimientos? -el conocimiento de todos los conceptos relacionados con la seguridad? -conformación de comités y patrullas de emergencia? -el apoyo de la Alta Dirección? -comunicación con autoridades locales, como: ..el INS ..cuerpos de bomberos ..policía y radiopatrullas ..emergencias (911) ..hospitales y clínicas ..cualquier otra institución relacionada l. Existen planes por escrito con respecto a todos los asuntos de seguridad? - Están por escrito, revisados, aprobados y forman parte de la planificación general? - Están debidamente presupuestados y con contenido económico? - Han sido divulgados a todos los niveles, y se ha dado entrenamiento en aquellos que lo merezcan? m. Tienen en operación un plan de contingencias? - Contiene los aspectos de toda la organización? - Está por escrito, revisado y aprobado? - Se ha probado y se prueba por lo menos una vez al año? - Contiene todos los procedimientos necesarios? - Contiene el plan de recuperación en caso de desastre? n. Existe un organigrama de la función de seguridad? - Incluye los comités y patrullas de emergencia? - Es un organigrama que propicia el control en cuanto a la aplicación de la seguridad? o. Cuentan con las descripciones de funciones de cada uno de los puestos que aparecen en el organigrama? - Se destacan los deberes y responsabilidades de cada quien? -Se anota la coordinación que debe existir entre los diferentes niveles?			

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por:_____**

Fecha: _____

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
B. SEGURIDAD FÍSICA **1. CONSTRUCCIÓN** **1.1 Construcción Especial** a. Es la construcción del centro de cómputo especial? - Qué especialidad tiene? ..Paredes grandes y fuertes? ..Material no inflamable? ..Cielo raso reforzado? ..Antimagnetismo? ..Varias puertas de acceso? Qué función cumplen? b. Cuenta con salidas de emergencia? - De qué tipo son? - A qué lugar llevan? c. Son seguros los accesos y las salidas de emergencia? - Abren sus puertas hacia afuera? - Son puertas corredizas - Son las puertas de vidrio? - Las escaleras son firmes y antideslizantes? - Ha sucedido algún accidente? d. Se han probado las salidas de emergencia? - Fueron los resultados positivos? - Se documentaron los pormenores? e. Llegan las paredes hasta el techo? f. Tienen instalaciones especiales en el cielo raso para instalar dispositivos de seguridad? g. Tienen ventanales grandes de vidrio? - Es vidrio de seguridad? - Cuentan con garantía de esa seguridad? - Están polarizados? - Se pueden abrir esas ventanas? - Las mantienen cerradas constantemente?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
h. Cuántos accesos tiene el centro de cómputo o Informática? -por las escaleras normales? -por el ascensor? -por las escaleras de emergencia? -se llega directamente a él por estos accesos? i. Tienen piso(s) falso(s)? -Está bien instalado? -Es aislante de calor? -Cuentan con rampas de acceso? -Lo revisan y limpian periódicamente? -Están los cables sueltos, o en ductos? j. Los locales internos son amplios y cómodos? - Tienen cubículos separados para salón del computador, cintoteca, bodegas, equipos especiales, programadores, analistas, jefatura? - Tienen una buena disposición, especialmente para la salida en casos de emergencia? - Cuenta el salón del computador con suficiente campo para que los ingenieros puedan dar el mantenimiento? k. La cintoteca está bien protegida? Se guardan en ella otros dispositivos, equipos y suministros, que no sean cintas, diskettes y cartuchos? l. Pasan ductos de agua directamente encima del centro de cómputo, de la cintoteca y de las bodegas de papelería y suministros? m. Existen los planos del centro de cómputo? - Están actualizados y disponibles? **1.2 Instalaciones Eléctricas y de Señal** a. La instalación de la red eléctrica es exclusiva para los equipos de cómputo? - Tiene medidor independiente? - Esta red cubre todo el edificio? - Cumple con los estándares generales y los específicos? - Está conectada a tierra? - Están todos los tomas polarizados? - Están identificados los cables, y los tomas?			

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por:_____**

Fecha: _____

PREGUNTA-ACTIVIDAD	SI	NO	COMENTARIOS
b. Están los cables (de poder y de señal) en ductos? - Son los ductos de material especial? - Están separados de los cables de señal? - Cada uno va en un ducto diferente?			
c. Se revisa la red y se le da mantenimiento constantemente? - Se anotan lo resultados de la revisión? - Se efectúan correcciones? - Existen "pegas" y añadidos en los cables?			
d. Existe una buena disposición de los interruptores y circuitos? - Son de fácil localización? - Están a mano, en caso de emergencia?			
e. Existen y están disponibles los planos de las instalaciones eléctrica y de señal? - Están actualizados? - Tienen copias en lugares protegidos?			
f. Cuentan con personal especializado para las pruebas, revisiones, el mantenimiento y las correcciones de todo lo relacionado con las instalaciones de cables, tendidos y otros?			
g. Están las regletas o tomas múltiples adosadas a las paredes? - Se protegen los cables que están en el piso o que atraviesan oficinas?			
h. Cuentan con protección de UPS´s (baterías) - Cuántas y de qué tipo? (En línea o no) - Existe una para el equipo principal? - Se midieron las potencias para determinar la protección adecuada? - Existe un plan de sustitución para las pequeñas? - Se les da mantenimiento, preventivo, correctivo?			
i. Tienen planta eléctrica propia? - Está coordinada con la UPS? - Se conecta automáticamente? - Se le proporciona mantenimiento, preventivo, correctivo? - Es sólo para emergencias, y para cómputo?			
j. Cuentan con reguladores de voltaje?			
k. Están los aires acondicionados conectados en la misma red que los			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
equipos de cómputo?			
l. Todo el cable de señal es del mismo tipo?			
m. Aplican las medidas de protección, revisión y atención, tanto para los cables de señal, como para los de poder?			
1.3 Ambiente			
a. Cuentan con aire acondicionado en las instalaciones de equipo de cómputo? - Para el equipo de cómputo principal? - Se midió la cantidad de calor a disipar? - Cumplen los aires con la medida?			
b. Tienen detectores de humo? - Funcionan automáticamente? - Accionan alguna alarma? - Llaman la atención del operador?			
c. Pueden detectar y medir la humedad, especialmente en el salón del computador principal, en la cintoteca y en las bodegas de papelería y suministros? - Tienen deshumedecedores? - Funcionan adecuadamente?			
d. Tienen protecciones especiales para los medios magnéticos? - De qué tipo?			
e. Es adecuada la iluminación de todo el centro de cómputo? - Tienen luces especiales? - Tienen luces de emergencia?			
f. Cuentan con extintores bien dispuestos? - Los saben utilizar? - Se les da mantenimiento? - Se han probado?			
g. Están los vidrios de los ventanales polarizados? - Se mantienen cerrados los ventanales?			
h. Utilizan algún tipo de protección contra la contaminación ambiental;			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
especialmente de polvo? - De qué tipo? i. Tienen alarmas? - De qué tipo? - Son automáticas o se activan manualmente? - Están conectadas con los bomberos, la policía? j. Disponen de medidas de seguridad en caso de rayerías, tormentas, temblores, inundaciones? k. Cuentan con protectores de pantalla para los monitores? l. Manejan material inflamable de algún tipo? m. Existen medidas de seguridad efectivas para el personal que trabaja en los turnos de la noche y madrugada? n. Existen medidas de coordinación con los encargados de la seguridad del edificio? - Saben qué tienen que hacer en caso de una emergencia en cómputo? - Se puede comunicar el operador con el guarda? o. Tienen servicio de mantenimiento para todos los equipos y dispositivos especiales, relacionados con la seguridad? p. Tienen recolectores de papel bien dispuestos? - Son especiales? - Qué tipo de material depositan en ellos? - Los vacían en otros recipientes? q. Se prohíbe el consumo de alimentos y bebidas dentro del centro de Cómputo y en los lugares en donde están instalados equipos de cómputo, periféricos y especiales? - Existen rótulos indicadores de esas prohibiciones? r. Cuenta la documentación con medidas de protección efectivas? s. Disponen en cómputo, de una o varias cajas de seguridad o contra Incendio? - Qué almacenan en ellas? **2. <u>UBICACIÓN</u>**			

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por:_____**

Fecha: _____

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
a. Se han presentado problemas por su ubicación de la sala de servidores? De qué tipo? b. Es el espacio físico suficiente? c. Visitan los usuarios el centro de cómputo? - Por qué motivos? - Llevan algún control de estas visitas? - Han tenido problemas con ellos por esta razón? d. Existe aglomeración de equipos y dispositivos? h. Llevan un inventario de todos los equipos de cómputo? - Qué grado de detalle tiene? - Se actualiza regularmente? i. Cuentan con protecciones para las terminales y otros equipos, según la ubicación que tengan? **3. <u>A C C E S O</u>** a. Existen restricciones de acceso físico a la sala de servidores?: b. Permanecen cerradas la puertas de acceso? - Indefinidamente? - Bajo qué condiciones se abren? c. Tienen los profesionales autorizados, identificaciones adecuadas que les permitan el ingreso? d. Utilizan códigos, identificaciones o combinaciones para ingresar? e. Cuentan con bitácoras de visitas? - Al centro de cómputo? - Al salón del computador? f. Existen restricciones de acceso para horas o días no hábiles? - Incluyen al personal autorizado? g. Existe una persona responsable de la custodia de:			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
- la documentación? - los activos del centro o departamento? - los dispositivos de respaldo? - la papelería, especialmente los valores?			
C. MEDIDAS DE PROTECCIÓN ADICIONALES			
1. Contratación de personal			
a. Se consideran los siguientes elementos como factores para la selección, el reclutamiento y la contratación del personal que ejecuta funciones en áreas críticas: - la experiencia? - el conocimiento técnico-teórico? - la habilidad? - el aspecto moral (valores morales y éticos)? - el grado de responsabilidad?			
b. Se investigan las referencias y antecedentes de los solicitantes, mediante estándares establecidos?			
c. Se practican pruebas de admisión, para medir las aptitudes de los solicitantes?			
d. Se practican pruebas psicométricas, para la calificación de actitudes, intereses y conducta de los solicitantes?			
e. Se realizan las pruebas anteriores por personal especializado?			
f. Se detectan y seleccionan fuentes de reclutamiento de prestigio?			
g. Se evita el reclutamiento de personal que no cubra los requisitos mínimos de admisión?			
h. Se comprueban los datos expresados en la solicitud, por medio de visitas socioeconómicas, entrevistas y cartas de recomendación?			
i. Existen casos de violaciones al procedimiento anterior? - Qué medidas se toman para corregirlos?			
j. Existe una descripción de funciones de cada puesto? - Se entrega a la persona contratada, copia de la descripción			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
de sus funciones? - Está de acuerdo y satisfecha con ellas? k. Existe dentro del plan de entrenamiento del personal, un programa de inducción al personal nuevo? l. Se efectúa el entrenamiento del nuevo personal, por medio de un programa estándar? m. Se enfoca el entrenamiento, como una educación permanente y no como un aprendizaje inmediato? n. Se miden y controlan los resultados de la educación, antes y después de la toma del puesto? o. Se fija la remuneración del personal, mediante estudio previo, considerando el mercado laboral? p. Se efectúan evaluaciones periódicas de la eficiencia del personal, por medio de un programa estándar? q. Se emite un informe del resultado de la evaluación del desempeño del personal? - Existe un programa estándar para corregir deficiencias y optimizar los buenos resultados? r. Se acentúa el énfasis de la seguridad, privacidad y confidencialidad de los datos y la información, en todo el proceso de inducción y educación? **2. Seguros** a. Existen pólizas de seguros para la protección de los activos de cómputo? b. Existen coberturas para: - los equipos? - los programas y herramientas de los equipos? - sistemas en operación? - las operaciones del computador? - la documentación? - la recuperación? - los tiempos inactivos?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
c. Son adecuadas las coberturas? - Qué criterios utilizaron para establecerlas? d. Se aseguran los activos en el momento de su compra? - Se aseguran aún cuando estén en el período de garantía? e. Se actualizan las pólizas de seguros cada vez que se incluye o se excluye, algún activo de cómputo? f. Incluyen las pólizas, coberturas por: - Incendio? - Temblor o Terremoto? - Inundaciones? - Sabotaje? - Robo? - Daño? - Tormenta o Huracán? - Disturbios civiles? **3. Garantías** a. Se solicitan garantías por todo activo de cómputo que se adquiera? b. Por cuánto tiempo se otorgan las garantías? c. Son adecuados los tiempos de las garantías? d. Se tiene algún estándar con respecto a equipos que fallen estando bajo garantía? - Por ejemplo, si un equipo falla tres veces en ese período, que lo cambien por uno nuevo. e. Se hacen valer efectivamente las garantías y los tratados sobre ellas? f. Se lleva en el inventario, el control de las garantías? g. Se exige que si un equipo, dispositivo o tarjeta es entregado nuevo, inicia el ciclo de la garantía? h. Se exigen las garantías por escrito, en detalle?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
i. Se archivan y resguardan todas las garantías? - Por quién? - Bajo qué medidas de seguridad? **4. Mantenimiento** a. Se han firmado contratos de mantenimiento preventivo y correctivo, para los equipos principales, dispositivos y equipos especiales? b. Se han negociado favorablemente estos contratos? c. Se les proporciona verdadero mantenimiento preventivo a esos equipos? - o sólo limpieza. d. Incluye el mantenimiento correctivo los repuestos o no? - Si no los incluye, se cotizan de acuerdo con el procedimiento de compras normal? e. Se incluye en el inventario del equipo, lo referente al mantenimiento? - Si está bajo contrato? - Si es mantenimiento preventivo y/o correctivo? - Tiempos de vencimiento? - Empresa o persona que le da el mantenimiento? f. Se tienen planes de mantenimiento por escrito? - Se especifica en ellos los días y las horas, en que a los equipos se les dará mantenimiento? - Es conocido este plan por las personas que tienen equipos a su cargo? - Funciona el plan efectivamente? g. Se lleva una bitácora (diario de anotaciones) para el mantenimiento de cada equipo? - Se anotan en ella los pormenores del mantenimiento? h. Se llena una solicitud de revisión de equipos cuando se detecta una una falla en ellos? - Se cumple con el procedimiento para llamar a la empresa que proporciona el mantenimiento? - Se realiza un diagnóstico previo de las fallas? - Se emite un informe escrito de ese diagnóstico?			

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por:_____**

Fecha: _____

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
i. Si no se tienen contratos, se cumple con el procedimiento establecido para la revisión y reparación de equipos por llamada? j. Exige el procedimiento llenar una solicitud, como se detalla en la pregunta h? - Cuando se repara el equipo se llena un informe de reparación, y firma el responsable del equipo? - Se paga la reparación contra el informe anterior? k. Se exige se devuelvan los dispositivos "malos" una vez realizada la reparación y se hayan comprado repuestos? - Si la empresa que hace la reparación tiene sus propios repuestos, se le exige la presentación de la salida de bodega, o la factura de compra, si es que lo compraron? l. Cuando deban llevarse equipos para reparar, se entrega el mismo bajo un inventario, con anotaciones de números de serie, incluso de los dispositivos y tarjetas internos? m. Cuando regresan los equipos se revisan y cotejan con el inventario con que fueron entregados? n. Se toman las medidas de seguridad pertinentes con respecto a la información que contengan los discos duros de los equipos a reparar? o. Se analizan bien las empresas que ofrecen sus servicios de mantenimiento, con base en: - Prestigio? - Tiempo de estar en el negocio? - Posición financiera? - Número de clientes que atienden? - Grado de satisfacción de sus clientes? - Personal con que cuentan, y su experiencia? p. Se revisan los contratos por parte de los profesionales correspondientes, en cada caso, por ejemplo: - Expertos en cómputo? - Electricistas o electrónicos? - Departamento o asesor legal? - Auditoría Interna?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
D. SEGURIDAD LÓGICA			
1. Procedimientos			
Refiérase a la sección A.1 de este cuestionario.			
2. Esquemas de seguridad			
a. Cuentan con diagramas de los esquemas de seguridad? - Forman parte de la documentación de los sistemas?			
b. Incluyen los esquemas de seguridad: - Los códigos de usuario? -Las claves de acceso? - Las terminales autorizadas? - Los diferentes niveles de seguridad? - Los derechos y privilegios de cada usuario?			
c. Describe el procedimiento correspondiente, los pasos a seguir para establecer los conceptos anteriores?			
d. Se utilizan estándares para la asignación de códigos de usuario y claves de acceso?			
e. Incluyen estos estándares aspectos como: - Caracteres a utilizar? - Tamaños de los conceptos? - Prohibiciones?			
f. Se asignan las claves de acceso mediante la aplicación de un algoritmo complejo? - Puede el usuario cambiar su propia clave de acceso?			
g. Incluye el procedimiento de asignación de claves, aspectos como: - Una solicitud del usuario jefe con indicaciones claras de los accesos autorizados? - Los tiempos vigentes de duración de las claves? - Si vencen automáticamente después de ese tiempo? - Qué hacer en caso que el usuario olvide su clave? - Cómo proceder cuando un usuario deja la organización?			

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por:_____**

Fecha: _____

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
h. Existe algún manual de seguridad lógica?			
i. El encargado de la seguridad coordina todos los aspectos relacionados con la seguridad lógica?			
j. Existen perfiles predefinidos para los usuarios? - Quién genera estos perfiles?			
k. Existe un sistema de encriptamiento para las claves? - Se desarrolló internamente o se compró? - Quién o quiénes lo conocen? - En dónde se custodia?			
l. Existen acceso privilegiados? - De qué tipo?			
m. Son las claves de acceso de los profesionales de cómputo o informática restringidas? - Tienen algún privilegio? - Por qué razón?			
n. Conocen todos los usuarios la responsabilidad que asumen al tener una clave de acceso? - Se les ha comunicado? - Está en la descripción de funciones? - La respetan? - Se aplican sanciones para quien haga uso indebido de su clave, que utilice la clave de otra persona?			
o. Se cuenta con una lista actualizada de los usuarios, con: - Los sistemas, módulos, menús, opciones de menú, a que tienen acceso? - Los códigos de usuario? - Oficina, departamento o área en que trabaja? - Jefe usuario directo? - Funciones que desempeña? - Terminal(es) autorizada(s)?			
p. Están ligadas las claves de acceso a: - Días hábiles de uso?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
- Horas hábiles de uso? - Terminal(es) autorizada(s) **3. Seguridad del Sistema Operativo** a. Se utiliza la seguridad que tienen: - El sistema operativo? - El manejador de la base de datos? - El sistema operativo de redes? - Las herramientas de desarrollo? - Las interfaces inteligentes que se utilicen para conexión de los diferentes equipos? - Los dispositivos de comunicaciones? b. Se integran todas las seguridades? - Cuál de ellas predomina? c. Cuentan con esquemas gráficos de las relaciones de seguridad entre los diferentes programas? d. Existe algún funcionario con acceso irrestricto? - Cuál es su puesto? - Por qué razón tiene ese tipo de acceso? **4. Herramientas adicionales** a. Cuentan con alguna(s) herramienta(s) adicional(es) para seguridad lógica? - De qué tipo es? - Qué nivel de seguridad brinda? - Es complementaria a la seguridad existente o es la principal? - Su adquisición se debió a debilidades en la seguridad principal, o como soporte adicional? - Requiere de mucho almacenamiento y recursos? b. Existen restricciones de acceso a directorios, bibliotecas o espacios para tablas? - De qué tipo? - Se protegen con un programa de seguridad especial? - Es un paquete o un programa hecho a la medida?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
- Se controlan los acceso a estos elementos? c. Tienen bitácoras automatizadas en donde queden registrados todos los eventos relacionados con todos los accesos autorizados y los intentos rechazados? - Están activadas? - Las revisa algún funcionario autorizado? - Se han detectado anomalías en los accesos? - Se ha tomado alguna acción al respecto? d. Proporcionan esas bitácoras, toda la información relacionada con los accesos? e. Se guarda la información de las bitácoras por un tiempo determinado? - Por cuánto tiempo? - Se desecha la información después de ese tiempo? - Se guarda en algún dispositivo magnético por un tiempo adicional? Cuánto? f. Se lista el contenido de las bitácoras en algún momento? - Utiliza algún funcionario estos listados? **5. Segregación de funciones electrónica** a. Existe la segregación electrónica de funciones? b. De qué manera se determina y establece este tipo de segregación de funciones? c. Cuántos tipos de funciones se han determinado? - Se tienen como un estándar? d. Está contenida en un documento oficial? e. Se aplica y se utiliza tal como está establecida y otorgada? f. Se lleva algún control sobre esta segregación? - Quién lo ejerce o ejecuta? - Se verifica que se cumpla a cabalidad? g. Se han detectado anomalías en su aplicación? - Se han corregido?			

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
- Se han aplicado sanciones?			
6. Otros tipos de protecciones			
a. Se utilizan los menús mandatorios u obligatorios para todos los usuarios?			
b. Funciona como un estándar?			
c. Están el código de usuario y la clave de acceso coordinados para que "lleven" al usuario a una biblioteca o directorio específico?			
d. Se cierran para el usuario otros posibles caminos de ingreso a a directorios, bibliotecas, datos o "lugares" a los que no está autorizado, tales como: - Teclas, como por ejemplo la de ayuda? - Comandos? - Salidas al sistema operativo? - Interrupciones?			
e. Se controla este cierre de caminos periódicamente? - Reclama el usuario por este cierre? - Qué explicaciones les han dado?			
f. Reconocen que la seguridad es lo primero en los procesos de cómputo y que debe velarse por la integridad y confidencialidad de la información?			
E. <u>SEGURIDAD EN COMUNICACIONES</u>			
1. Procedimientos Refiérase a la sección A.1 de este cuestionario.			
2. Esquemas de seguridad Refiérase a la sección D-2 de este cuestionario			
3. Cuentan con sistemas de redes?			

REVISIÓN DE LA SEGURIDAD **P.T. No. _____**

CUESTIONARIO DE CONTROL INTERNO **Hecho por:_____**

Fecha: _____

PREGUNTA-ACTIVIDAD	**SI**	**NO**	**COMENTARIOS**
Tiene un administrador físico dedicado? Qué puesto tiene en la organización? Ha recibido entrenamiento formal?			
4. Tiene la red un buen desempeño? Existen fallas frecuentes? Cada cuánto tiempo? Existen quejas de los usuarios?			
5. Tiene un buen equilibrio en todos sus componentes?			
6. Cuentan con comunicaciones remotas? Qué tipo de línea utilizan? Telefónica o de datos? Presenta fallas frecuentes?			
7. Tienen los dispositivos, una buena velocidad? De cuánto?			
8. Son las tarjetas de comunicaciones de marca?			
9. Ofrecen algún tipo de problema?			
10. Es el cableado de la red y de las comunicaciones eficiente?			
11. Tiene el programa (Software) de comunicaciones un buen funcionamiento?			
12. Cuentan con controladores de comunicaciones? Qué tanto es el tráfico de transacciones en la red o enlaces? Lo soporta bien el equipo principal o servidor?			