**Universidad Nacional Autónoma de Nicaragua "UNAN – Managua"**

**Facultad de Ciencias e Ingeniería**

**Departamento de Computación**

# AUDITORÍA DE SEGURIDAD INFORMATICA APLICANDO EL ESTANDAR INTERNACIONAL COBIT 4.1 EVALUANDO LA DIRECCION INFORMATICA, RECURSOS TI, OUTSOURCING Y RIESGO INFORMATICO PARA EL AREA DE INFORMATICA DE MS — AMERICA CENTRAL EN EL AÑO 2010

*Seminario de Graduación*
*Trabajo previo a la obtención del Título de Licenciado en Ciencias de la Computación*

PRESENTADO POR:

*Br. Karla Vanessa Molina Gutiérrez*

*Br. Claudia Regina González Urroz*

*Br. Araceli del Carmen Munguía Alfaro*

TUTOR:

*Lic. Edgard Monge*

19 de Septiembre del 2011

# DEDICATORIA

Dedico esta tesis a Dios por ser parte de mi vida en todo momento, y por ser mi mayor inspiración.

Me gustaría dedicar un apartado muy especial a todos aquellos que son parte de mi familia, por ser mi más grande apoyo y motivación para crecer y superarme profesionalmente y como persona.

Y finalmente a todos aquellos docentes, que dedicaron y mostraron interés por enseñar y trasmitir esos nuevos conocimientos con los que ahora puedo decir: "Aprendí y puedo poner en práctica".

*Karla Vanessa Molina Gutiérrez*

Dedico esta tesis a mi Dios y Padre celestial, por estar conmigo a cada paso que doy en la vida y darme sabiduría, para culminar la licenciatura.

A mis amados padres Reynaldo y Maritza, por ser el principal pilar de mi vida y mis guías, pero en especial a mi madre por sus oraciones, alentarme a continuar y ser mejor cada día.

A mis hermanos por su apoyo y comprensión a lo largo de estos años.

A mis maestros por la noble labor de instruirme en teoría y corregirme en práctica, por todo su poyo aun después de haber culminado las asignaturas.

*Claudia Regina González Urroz*

Dedico esta tesis a Dios que ha sido el pilar más importante en mi vida ya que me ha dado la fuerza y la sabiduría para culminar mis estudios universitarios y no rendirme en el camino.

A mis padres Daniel Munguía y Marina Alfaro que han sido parte importante en esta fase de mi vida ya que el apoyo incondicional que me brindaron me ayudo a luchar por mis ideales y mis sueños.

A mis hermanos que siempre me dieron palabras de aliento.

Y en especial a mi mami Elvira que en paz descanse que con sus consejos me ayudo a formarme como profesional.

*Araceli del Carmen Munguía Alfaro*

## AGRADECIMIENTOS

Agradecemos a Nuestro a Dios y padre amoroso, quien nos da la vida, sabiduría y elementos necesarios en el momento adecuado, para la elaboración del Informe de Auditoría de Seguridad Informática.

Al Staff del Organismo Internacional Asociación Danesa para la Cooperación Internacional "**MS – AMERICA CENTRAL",** ya que sin su colaboración no hubiese sido posible el proceso de Auditoría y la finalización de la investigación, pero en especial de las siguientes personas:

Al Sr. Jan Borsheim-Administrador, por haber aprobado nuestra solicitud y brindarnos la oportunidad de realizar nuestra modalidad de graduación en el área de Informática de MS, a él mil gracias, por permitirnos coronar nuestra licenciatura.

Al Sr. Denis Urbina-Oficial Administrativo Logístico, por el respaldo recibido durante la aplicación de instrumentos de auditoría, por la información proporcionada y su disposición en todo momento.

A la Sra. Luvy Torres-Recepcionista, por haber colaborado y alentado en todo momento en la aplicación de Auditoría de Seguridad Informática en MS.
Al Sr. Christian Korsgaard-Asesor en Comunicaciones, por la colaboración en cuanto a información de página web.
Y la Sra. Antonia Vasconcelos-Oficial Administrativo Financiero, por darnos una reseña de los propósitos organizacionales del Organismo, funciones y módulos del software de contabilidad NAVISION, y sus valiosos consejos en pro de un mejor desarrollo de las actividades a nivel de grupo en el trabajo de Auditoría.
A todos y cada uno del personal que de forma desinteresada se implicaron de forma activa en la facilitación de información que les hemos solicitado.

A nuestras familias por su cariño y confianza, por inculcarnos lo importante que es crecer como profesionales, pero ante todo como personas, por su valioso apoyo y comprensión, y por estar siempre en cada una de las etapas de nuestras vidas.

A nuestro tutor Lic. Edgard Monge por su disponibilidad y asesoramiento continuo, sugerencias y correcciones oportunas con las que hemos elaborado este Informe de Auditoría.

A nuestros compañeros del grupo de investigación, por permitirnos compartir y auto-evaluarnos durante el transcurso de la modalidad de graduación.

Muchas gracias de parte del equipo de Auditoría de Seguridad Informática.

Y ¡Dios les Continúe Bendiciendo!

## RESUMEN

El presente trabajo, detalla el procedimiento de ***" Auditoria de Seguridad Informática",*** implemento el Modelo de Auditoria basado en el Estándar Internacional *Cobit 4.1* donde se evaluaron la dirección Informática, recursos de TI, el Outsourcing, y finalmente el Riesgo Informático", para el área de Informática de MS- América Central en el periodo año 2010.

Considerando que éstos están estrechamente relacionados entre sí y repercuten en gran medida en la administración, mantenimiento y monitoreo de la seguridad del área informática.

La metodología se desarrolló a través del Modelo de Cobit 4.1 como principal instrumento de trabajo de Auditoría, donde se utiliza como base inicial el Detalle de los Objetivos de Control para el análisis de implementación y evaluación de controles relacionados con la seguridad. Posteriormente se describe el proceso tomando como referencia los logros a alcanzar, las directrices gerenciales según los lineamientos que propone el marco normativo Cobit 4.1, como son: Metas y Métricas del objetivo evaluado. Finalmente se hace una valoración del Modelo de Madurez en el cual se ubica a cada uno según el estado actual.

En cuanto al proceso de auditoría, este se divide en tres fases: La Fase de Planeación, Fase de Examen y Evaluación y la Fase Dictamen de Auditoria.

En la *Fase de Planeación* se diseñaron instrumentos, para la recopilación de datos como fuente primaria a fin de alcanzar los objetivos de la investigación. Así mismo, para la Fase I como para la Fase II se utilizaron técnicas como entrevistas, Recopilación y Análisis de Documentos, Encuestas y la Observación como una de las principales técnicas para conocer la situación actual del área de informática. Por otro lado se aplicaron herramientas de auditoría para evaluar la parte lógica y física de los recursos del área de TI, y la Fase III es la emisión de resultados y recomendaciones.

En el desarrollo del proceso de auditoría se utilizaron los Dominios, Procesos y Objetivos de Control de la *Descripción del Proceso* de Cobit retomando en su esencia los Criterios

de Información, Métricas clave y *El Modelo de Madurez* para conocer descripciones de estados posibles y futuros de la Organización en cuanto a la Seguridad Informática, para ellos se diseñó la *Matriz de Prueba y Resultados*.

Una de las principales secciones de este informe, al final del documento detalla los *Hallazgos* basados en el análisis de las pruebas realizadas y la documentación suministrada por la organización, en ellos se describe las debilidades encontradas en el aspecto de la seguridad con sus respectivas recomendaciones y conclusiones.

Anexo al documento se encuentran los papeles de trabajo y anexos los cuales brindan el soporte al documento y la validación del proceso de auditoría.

El Informe propone a la organización la adopción de una metodología para el personal clave del área y la gerencia, para el ambiente de control de TI y la administración apropiada de los riesgos.

# I N D I C E

# INDICE DE FIGURAS

# INDICE DE TABLAS

# INTRODUCCION

La auditora en informática es una técnica que se ha venido implementando, para que las organizaciones estén en constante monitoreo de sus recursos. Esta mejora la calidad institucional desde el punto de vista competitivo y crea un ambiente de trabajo mucho más confiable.

Al hablar de auditoría de seguridad informática se refiere a la revisión técnica y especializada de los centros informáticos, SI, etc. y todo aquello que requiera una revisión exhaustiva, para verificar si cuentan con políticas y controles de seguridad adecuados en la organización, está preocupada tanto por la seguridad de sus instalaciones, como de sus sistemas informáticos ya que éstos son una arteria importante para la empresa y desean verificar la confiabilidad de los mismos y salvaguardar sus activos.

En la organización MS- América Central Action Aid Denmark, se realizó una Auditoría en seguridad informática con el objetivo de analizar si cuenta con políticas y controles de seguridad para la protección de sus recursos, además de revisar si la manera en que distribuyen su trabajo y responsabilidad le ayuda a tener óptimos resultados en la organización.

La finalidad de este informe es de mejorar las áreas donde se encuentren debilidades y de esta manera evitar posibles riesgos informáticos, teniendo en cuenta los componentes que garanticen la confidencialidad, integridad y disponibilidad de sus datos, así como lograr una mayor eficiencia operacional y técnica. El estándar COBIT 4.1 contempla que: “el valor, el riesgo y el control constituyen la esencia del gobierno de TI”.

Se ha organizado la presentación del estudio en seis capítulos y el informe final de auditoría, en este contexto se asocia la teoría con la práctica desarrollada en el proceso de investigación, de tal forma que el lector pueda entender el contenido de cada capítulo con los objetivos de control evaluados. El resultado de la Auditoría permitió visualizar los riesgos a las que está expuesta el área de informática, dando a conocer los hallazgos y recomendaciones que serán de utilidad para corregir las debilidades presentadas en el área de informática.

# JUSTIFICACION

La incorporación de las nuevas tecnologías de información en el ámbito de los sistemas informáticos, ha provocado la aparición de nuevas posibilidades de proceso de la información y de nuevos flujos de información entre las distintas estructuras organizativas. Sin embargo, esto también ha provocado la aparición de nuevos riesgos y amenazas con respecto a la información y a los activos de TI. Por tanto, la organización MS América Central en pro del mejoramiento organizacional ha considerado necesario e importante la evaluación de sus procesos y recursos de TI, a través de la aplicación de criterios de seguridad en procedimientos de auditoría que permita adoptar medidas de *seguridad organizativas y técnicas para el área Informática.*

El propósito de realizar la **Auditoría de Seguridad Informática** en el Área Informática de MS **América Central - Action Aid Denmark."**, es verificar y evaluar la seguridad en los diferentes niveles informáticos desde la planeación hasta el monitoreo de los recursos y aplicaciones, permitiendo a la Administración de TI considerar las recomendaciones para posibles cambios y mejoras a nivel administrativo, técnico y operativo del área y recursos de TI.

Se considera además que **MS América Central - Action Aid Denmark.** No cuenta con ningún tipo de evaluación de las TI, lo cual dificulta identificar los problemas que están afectando el correcto funcionamiento del área informática y los servicios que reciben de sus proveedores.

El resultado de esta auditoría contribuirá a la Organización a visualizar la importancia de implementar políticas de seguridad y control interno eficientemente de manera que minimicen posibles riesgos a los que está expuesta el área informática e incrementar los niveles de seguridad Informática.

La implementación continua del ejercicio de auditoría informática como una de las buenas prácticas de TI ofrecerá a los donantes y usuarios mayor accesibilidad y seguridad de sus aplicaciones, recursos y activos con los que hoy cuentan.

# OBJETIVOS

## Objetivo General

Desarrollar e Implementar un Modelo de Auditoría de Seguridad Informática al Organismo Internacional **MS América Central – Action Aid Denmark** aplicando el Marco normativo denominado COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), en el periodo año 2010

## Objetivos Específicos

1. Visualizar si existen un correcto proceso de organización, planificación y administración por parte de la Dirección Informática de MS- América Central según estrategia de Gobierno de TI de Cobit 4.1.

2. Comprobar la existencia y aplicación de procedimientos, normas, y políticas relativas a la seguridad, requeridas para el desempeño eficiente de cada una de las funciones informáticas.

3. Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos.

4. Analizar el desempeño y proceso del Outsourcing tecnológico entre la organización y proveedoras de servicio tecnológico.

5. Describir los problemas y clasificar el nivel de riesgo en las tecnologías de información del área de informática de MS- América Central.

6. Sugerir recomendaciones que puedan corregir o mejorar los niveles de seguridad de los recursos y activos de TI en el departamento de informática de la Organización.

# DESARROLLO

*Este consta de seis capítulos, los cuales contienen conceptos generales para una mejor comprensión de los términos utilizados en el desarrollo de la tesis de Auditoría de seguridad informática*

# 1

# CAPITULO 1: FUNDAMENTOS GENERALES

## 1.1 Antecedentes de la Auditoría

Los primeros antecedentes formales de la Auditoría se encuentran a partir de 1894 en España a principio del reinado de Sancho VI ¨El Bravo¨, quien ordeno a algunos hombres de confianza llevaran el control de los caudales públicos.

Muñoz[1] menciona que, los inicios de la Auditoría remontan a la *versión y diagnostico* que se practican en los registros de las operaciones contables de las empresas; después se pasó al análisis, verificación y evaluación de sus aspectos financieros.

Hoy en día los registros contables se llevan a cabo en sistemas de cómputos y se ha llegado a las revisiones especializadas de algunas áreas y actividades específicas que se desempeñan en las empresas, entre las cuales se encuentran; *las Auditorías de sistemas computacionales (Auditoría Informática), auditoría del desarrollo de proyectos de mercadotecnia, auditoría de proyectos económicos, y otras muchas ramas de la actividad empresarial.*

En la siguiente tabla se hace mención de algunas referencias internacionales de la Auditoría de sistemas computacionales.

| Nombre | Descripción |
|---|---|
| **En 1988, Echenique** | Publicó su libro *Auditoría de sistemas*, en el cual establece las principales bases para el desarrollo de una auditaría de sistemas computacionales, dando un enfoque teórico-práctico sobre el tema. |
| **En 1992, Lee** | Enuncia los principales aspectos a evaluar en una Auditoría de sistemas… |
| **En 1994, Haffes, F. Holguín y A. Galán** | Un libro sobre auditoría de estados financieros con una parte relacionada a la auditoría de sistemas. |
| **En 1996, Hernández Hernández** | Propone la *Auditoría en Informática*, relacionado con este tema. |
| **En 1998, Mario. G Piattine y Emilio del Peso** | Presentan el libro *Auditoría Informática, un enfoque práctico* con diversos enfoque y aplicaciones de esta disciplina |

***Fuente:*** *Antecedentes de la Auditoría*[2]

[1] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002. p.2.

## 1.2 Conceptos básicos sobre la Auditoría

La definición general que se propone para la auditoría es la siguiente: "S*egún Muñoz*[3], *"Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la racionalidad de sus resultados y el cumplimiento de sus operaciones."*

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican: [4]

| | |
|---|---|
| **1). Contenido:** | Una **opinión** |
| **2). Condición:** | Profesional |
| **3). Justificación:** | Sustentada en determinados **procedimientos** |
| **4). Objeto:** | Una determinada información obtenida en un cierto soporte |
| **5) Finalidad:** | Determinada si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su **fiabilidad**. |

En todo caso es una función que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

***Concepto de Auditor:*** *Muñoz*[5]*, describe al Auditor según en: "En tiempos históricos, auditor era aquella persona a quien le leían lo ingresos y gastos producidos por un establecimiento (de ahí su raíz latina del verbo* ***audire****, oír, escuchar), practica muy utilizada por civilizaciones antiguas".*

*Así mismo* ***Audit:*** *"*Constituye adaptación popular del verbo Inglés **Audit**, el cual significa examinar, revisar cuentas" [6]

---

[2] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002. p.2.

[3] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002. p.11.

[4] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2001. p.4.

[5] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002.p.4.

[6] Ibis .., p.11.

## 1.3 Clasificación de los tipos de Auditoría [7]

Se debe de tener en cuenta que el ámbito de la auditoría es bastante amplia y se han clasificado por:

**1.3.1 Auditoría por su lugar de aplicación**(Auditoría Externa y Auditoría Interna)

**1.3.2 Auditoría por área de aplicación**

**1.3.3 Auditoría especializadas en Aéreas Especificas**

**1.3.4 Auditoría de Sistemas Computacionales**

### 1.3.1 Auditoría por su lugar de aplicación

Con propósitos de una mejor comprensión de los tipos de auditoría que se pueden realizar en empresas e instituciones abordaremos las definiciones de auditoría interna y externa las ventajas, así como las desventajas de cada una de ellas[8].

#### 1.3.1.1 Auditoría Interna

La realización de esta evaluación se lleva a cabo por un especialista de la misma empresa y por tanto está involucrado en la operación de la misma, existiendo cierta dependencia de la gerencia de esta institución, lo que puede llegar a influir en el juicio que emita sobre la evaluación de las áreas de la empresa.

***Definición:*** *¨ Es la revisión que realiza un profesional de la Auditoría, cuya relación de trabajo es directa y subordinada a la institución donde se aplicara la misma, con el propósito de evaluar en forma interna el desempeño y cumplimiento de las actividades, operaciones y funciones que se desarrollan en la empresa y sus áreas administrativas, así como evaluar la razonabilidad en la emisión de sus resultados financieros. El objetivo final es contar con un dictamen interno sobre las actividades de toda la empresa, que permita diagnosticar la actuación administrativa, operacional y funcional de empleados y funcionarios de las áreas que se audita.*

**Ventajas:**

- El auditor conoce integralmente sus actividades, operaciones y área por tal razón su revisión puede ser más profunda en sus actividades, funciones y problemas de la institución.

[7] Ibis . .,p.12.

[8] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002.p.13-15

- El informe que emite el auditor independientemente del resultado, es sólo de carácter interno, por tal razón no sale de la empresa.
- Esta consume sólo recursos internos y es una buena práctica ya que permite detectar el mal uso de los recursos internos a tiempo.
- El programa de evaluaciones es un apoyo a la toma de decisiones de los dirigentes.

**Desventajas:**

- Su veracidad, alcance y confiabilidad pueden ser limitados debido a la intervención por parte de las autoridades de la institución en la evaluación y misión del informe.
- En ocasiones la opinión del auditor tal vez no sea absoluta, debido a que, al laborar en la misma empresa donde realiza la Auditoría, se pueden presentar presiones, compromisos y ciertos intereses al realizar la evaluación.

#### 1.3.1.2 Auditoría Externa

Esta auditoría es realizada por agentes ajenos a la empresa, esto permite que el auditor externo utilice su libre albedrío en la aplicación de los métodos, técnicas y herramientas de auditoría con las que realizara la evaluación de las actividades, y operaciones de la empresa siendo su resultado totalmente independiente de los intereses de la empresa.

***Definición:*** *"Es la revisión independiente que realiza un profesional de la auditoría, con total libertad de criterio y sin ninguna influencia, con el propósito de evaluar el desempeño de las actividades, operaciones y funciones que se realizan en la empresa que lo contrata, así como de la razonabilidad en la emisión de su resultados financieros. La relación de trabajo del auditor es ajena a la institución donde se aplicara la auditoría y esto le permite emitir un dictamen libre e independiente".*

**Ventajas:**

- Al no tener ninguna dependencia, el trabajo del auditor es totalmente independiente y libre de cualquier injerencia por parte de las autoridades de la empresa auditada.

- En su realización, estas auditorías pueden estar apoyadas por una mayor experiencia por parte de los auditores externos, debido a que utilizan técnicas y herramientas que ya fueron probadas en otras empresas con características similares.
- Estas tienen gran aceptación en las empresas para certificar registros contable, impuestos y resultados financieros. Además, sus dictámenes pueden ser válidos para las autoridades impositivas y con ello pueden satisfacer requisitos de carácter legal siempre y cuando sean realizadas por auditores de prestigio y reconocimiento público.

**Desventajas:**

- La principal desventaja es que el auditor conoce poco de la empresa y su evaluación, alcances y resultados depende de la recopilación de información, que puede ser limitada.
- Depende en lo absoluto de la cooperación por parte de los auditados.
- Muchas de las Auditorías de este tipo son resultados de las imposiciones fiscales y legales que pueden crear ambientes contrarios para los auditores dentro de la empresa.
- En algunos casos son sumamente costosas para la empresa, no sólo en el aspecto económico, sino por el tiempo y trabajo adicional que representa.

El realizar auditorías con cierta frecuencia ayuda a asegurar la integridad de los controles de seguridad realizados en los sistemas de información dentro de las instituciones/empresa. Así como las acciones de cambio en las configuraciones, actualización de software, la adquisición de nuevo hardware, entre otros cambios dentro de la institución hacen necesario que los sistemas estén siendo continuamente verificados por una auditoría interna/externa .

# 2

# CAPITULO 2: AUDITORÍA INFORMATICA

## 2.1 Auditoría Informática

Auditoría informática o auditoría de sistemas computacionales (ASC), a continuación mencionaremos las auditorías especializadas de los sistemas computacionales que se aplican en específico a este estudio.

### 2.1.1. Definiciones de Auditoría Informática

*Muñoz[9], define Auditoría Informática como: "…la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y además componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo.*

*El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa."*

Piatinni[10] dice, "La Auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos".

[9] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002. p.19

[10] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.7.

Entonces se puede definir como el conjunto de técnicas, actividades y procedimientos, destinados a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la empresa , por lo que comprende un examen metódico, puntual y discontinuo del servicio informático, con vista a mejorar en rentabilidad, seguridad y eficacia.

Considerando que el Término de Auditoría Informática es muy amplio, en este documento se retoman como parte del estudio los siguientes términos, como lo plantea Muñoz: [11]

- **Auditoría de la seguridad de los sistemas computacionales**
  El aspecto de la *seguridad en el área de la computación* es un campo bastante amplio y ligado a muchas otras tipos de auditorías**.**

**Definición:** "Es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema. Es también la revisión de los planes de contingencia y medidas de protección para la información, los usuarios y los propios sistemas computacionales, y en sí para todos aquellos aspectos que contribuyen a la protección y salvaguarda en el buen funcionamiento del área de sistematización, sistemas de redes o computadoras personales, incluyendo la prevención y erradicación de los virus informáticos"

- **Auditoría a los sistemas de redes**
  Por el crecimiento de los centros de cómputo el sistema de redes, su seguridad y fiabilidad ha tomado vital importancia en las grandes y pequeñas empresas.

**Definición:** "Es la revisión exhaustiva y específica que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, sus protocolos de comunicación, las conexiones accesos, administración,

[11] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002. p.10-28.

funcionamiento y aprovechamiento. Es también la revisión del software institucional, de los recursos informáticos e información de las operaciones, actividades y funciones que permiten compartir las bases de datos, instalaciones, software y hardware de un sistema de red."

- **Auditoría Outsourcing**
  Especialidad adoptada por los sistemas computacionales, relacionada con la prestación de servicios de cómputo a la institución.

**Definición:** "…se realiza para evaluar la calidad en los servicios de asesoría o procedimiento externo de información que proporciona una empresa a otra. Esto se lleva a cabo con el fin de revisar la confiabilidad, oportunidad, suficiencia y asesoría por parte de los prestadores de servicios de procedimientos de datos, así como el cumplimiento de las funciones y actividades que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas."

### 2.1.2 Objetivos de la Auditoría Informática

De manera general señalaremos los objetivos que se pretende alcanzar con una auditoría, para comprensión de las bases de sobre las que descansa el desarrollo de una auditoría:

- *Realizar una revisión independiente de las actividades, áreas o funciones especiales de una institución, a fin de emitir un dictamen profesional sobre la razonabilidad de sus operaciones y resultados.*
- *Hacer una revisión especializada, desde un punto de vista profesional y autónomo, del aspecto contable, financiero y operacional de las áreas de una empresa.*
- *Evaluar el cumplimiento de los planes, programa, políticas, normas y lineamiento que regulan la actuación de los empleados y funcionarios de una institución, así como evaluar las actividades que se desarrollan en sus áreas y unidades administrativas.*

- *Dictaminar de manera profesional e independiente sobre los resultados obtenidos por una empresa y sus áreas, así como sobre el desarrollo de sus funciones y el cumplimiento de sus objetivos y operaciones.* [12]

### 2.1.3 Alcances de la Auditoría Informática

El alcance de la Auditoría Informática es la precisión con que se define el entorno y los límites en que va a desarrollarse, se complementa con los objetivos establecidos para la revisión, este debe definirse de forma clara en el Informe Final, detallando no solamente los temas que fueron examinados, sino también indicando los que no se tomaron en cuenta.

Dentro de los Alcance se mencionan:

- Naturaleza y extensión del trabajo realizado.
- Identificación del área de auditoría y el período cubierto.
- Sistemas de información, aplicaciones o ambiente revisado.
- Limitaciones al alcance.
- Restricciones del auditado.

### 2.1.4 Síntomas de necesidad de la Auditoría Informática [13]

Las empresas acuden a las auditorías externas cuando existen síntomas bien claros y fáciles de percibir de debilidad.

Estos síntomas pueden agruparse en clases:

| Síntomas | Descripción |
|---|---|
| ***Síntomas de descoordinación y desorganización*** | No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía, Pueden ocurrir con una reestructuración fallida de alguna área o en la modificación de alguna Norma importante<br>No se atienden las peticiones de cambios de los usuarios. |
| ***Síntomas de mala imagen e insatisfacción de los usuarios*** | No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables.<br>No se cumplen en todos los casos los plazos de entrega de resultados periódicos. |
| ***Síntomas de debilidades*** | Incremento de los costes. |

[12] Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002. p.29.

[13] Monografías (año). "La Auditoría informática dentro de las etapas de Análisis de Sistemas Administrativos" Disponible en línea en: "http://www.monografias.com/trabajos5/audi/audi.shtml. Ultima Visita 03 de Noviembre del 2010.

| | |
|---|---|
| ***económico-financiero*** | Nace la necesidad de justificación de Inversiones Informáticas (la empresa no está convencida de tal necesidad y decide contrastar opiniones).<br>Desviaciones Presupuestarias significativas. |
| ***Síntomas de integridad*** | Evaluación de nivel de riesgos: Seguridad Lógica, Seguridad Física, Confidencialidad.<br>Continuidad del servicio.<br>Centro de Proceso de Datos fuera de control |

### 2.1.5 Importancia de la Auditoría Informática

A pesar de ser una disciplina cuya práctica ha aumentado en nuestro país durante los últimos años, aun no se tiene claro lo que se podría evitar al adoptar esta práctica para las TI.

- Utilizar resultados o información errónea, abre la posibilidad de que se provoque un efecto dominó y afecte seriamente las operaciones, toma de decisiones e imagen de la empresa.
- Las computadoras, servidores y los Centros de Procesamiento de Datos se han convertido en blancos apetecibles para fraudes, espionaje, delincuencia y terrorismo informático.
- Las bases de datos pueden ser propensas a atentados y accesos de usuarios no autorizados o intrusos.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Mala imagen e insatisfacción de los usuarios porque no reciben el soporte técnico adecuado.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- Los recursos tecnológicos de la empresa incluyendo instalaciones físicas, personal alterno, programas, aplicaciones, servicios de correo, internet, o comunicaciones; son utilizados por el personal sin importar su nivel jerárquico, para asuntos personales, alejados totalmente de las operaciones de la empresa o de las labores para las cuales fue contratado. [14]

[14] Monografías (año). "Auditoría de Sistema y políticas de Seguridad Informática" Disponible en Línea en: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml. Ultima Visita 03 de Noviembre del 2010.

### 2.1.6 Fases de la Auditoría Informática [15]

Las fases de la Auditoría se componen de su definición y formalización. Que siguen el objetivo principal de elaborar un proyecto para ser presentado a la alta dirección, dirigidos al aseguramiento de la calidad y control de los principales elementos relacionados directa o indirectamente con el área de informática.

#### 2.1.6.1 Planeación de la Auditoría Informática.

Para realizar una adecuada planeación de la auditoría, se debe seguir una serie de pasos con anticipación que permitan conocer el tamaño y las características propias del área a auditar dentro de la institución, sus sistemas, organización y equipo de trabajo. Determinar el número del personal participante, características las herramientas necesarias, tiempo y costo, alcance de la Auditoría, para poder elaborar el contrato de la Auditoría.

Esta es una de las fases más importantes de la auditoría ya que una incorrecta planeación podría impedir que se lleve a cabo o no tenga el profesionalismo que se espera por parte del auditor.

***La planeación deberá ser documentada e incluirá:***

- El establecimiento de los objetivos y el alcance del trabajo.
- La obtención de información de apoyo sobre las actividades que se auditarán.
- La determinación de los recursos necesarios para realizar la Auditoría.
- El establecimiento de la comunicación necesaria con todos los que estarán involucrados en la auditoría.
- La realización, en forma más apropiada, de una inspección física para familiarizarse con las actividades y controles a auditar, así como identificación de las áreas en las que se deberá tener énfasis al realizar la Auditoría y promover comentarios y la promoción de los auditados.
- La preparación por escrito del programa de auditoría.
- La determinación de cómo, cuándo y a quien se le comunicaran los resultados de la auditoría.
- La obtención de la aprobación del plan de trabajo de la auditoría. [16]

[15] Echenique G. José A. Auditoría en Informática. Segunda Edición, McRae- Hill/ Interamericana Editores, S.A de C.V, México. 2001. P.30-31

[16] Echenique G. José A. Auditoría en Informática. Segunda Edición, McRae- Hill/ Interamericana Editores, S.A de C.V, México. 2001. p.31.

Para lograr la adecuada planeación es necesario recolectar la información de la organización y de las funciones de informática a evaluar.

**Revisión Preliminar.** El primer paso en el desarrollo de la Auditoría, después de la planeación, es la revisión preliminar del área informática. El objetivo de la revisión preliminar es el de obtener información necesaria, para que el auditor pueda tomar la decisión de cómo proceder en la Auditoría.
Al terminar la revisión preliminar. El auditor puede proceder en uno de los tres caminos siguientes: diseño la auditoría, realizar una revisión detallada de los controles internos o decidir el no confiar en los controles internos del sistema.

La revisión preliminar significa la recolección de evidencia por medio de entrevista con el personal de la instalación, la observación de las actividades en la instalación y la revisión de la documentación, preliminar. Esta es solo una manera de la información inicial que nos permitirá elaborar el plan de trabajo. El auditor externo se enfoca más en las causas de las perdidas y en controles necesario para justificar sus decisiones.

**Revisión Detallada:** El auditor debe decidir si debe de continuar elaborando pruebas de consentimiento y proceder directamente a la revisión con los usuarios. Al terminar la revisión detallada el auditor debe evaluar en qué momento los controles establecidos reduce las perdidas esperadas a un nivel aceptable.

Los métodos de obtención de información de la evaluación detallada son los mismos usados en la investigación preliminar, lo único que difiere es la profundidad con que se obtiene la información y como se evalúa.

**2.1.6.2. Examen y Evaluación de la Información.** El proceso de examen y evaluación de la información es el siguiente:

- Obtención de la información de todos los asuntos relacionados con los objetivos y alcances de la auditoría.
- La información deberá ser suficiente, competente, relevante y útil para que proporcione bases sólidas en relación con los hallazgos y recomendaciones.

- Los procedimientos de auditoría, incluyendo el empleo de las técnicas de pruebas selectivas y el muestreo estadísticos deberán ser elegidos con anterioridad.
- El proceso de recabar, analizar, interpretar y documentar la información para proporcionar una seguridad razonable de que la objetividad del auditor se mantuvo.
- Los procedimientos del trabajo de la Auditoría deberán ser preparados por los auditores y revisados por la gerencia de auditoría.

Los auditores deben reportar los resultados del trabajo de auditoría. Los informes deberán ser objetivos, claros, concisos, constructivos y oportunos, estos deben presentar el propósito, alcance y resultados de la auditoría y, cuando se considere apropiado, contendrá la opinión del auditor.

### 2.1.7 Proceso Metodológico de la Auditoría Informática

El método de trabajo del auditor pasa por las siguientes etapas:

- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Redacción de la Carta de Presentación del Informe final. [17]

### 2.1.8 Personal participante de la Auditoría Informática

El personal participante o llamada también recursos humanos, es una de las partes más importantes de la planeación de la auditoría. El número de persona participante depende de las dimensiones de la empresa/institución, de los sistemas y de los equipos existentes; algo que si hay que considerar son las características y perfiles del personal seleccionado que depende del tipo de auditoría a realizar. Este personal debe estar debidamente capacitado, con alto nivel de moralidad.

[17] Monografías (año). "Auditoría de Sistema y políticas de Seguridad Informática" Disponible en Línea en: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml. Ultima Visita 03 de Noviembre del 2010.

# 3

# CAPITULO 3: POLITICAS Y CRITERIOS DE SEGURIDAD INFORMATICA

## 3.1 Políticas de seguridad informática (PSI)

### 3.1.1. Definiciones de PSI

Las PSI resaltan reglas y procedimientos a seguir en una organización para de esta manera proteger los activos de la empresa. *"Una Política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal en relación con los recursos y servicios informáticos de la organización, además se puede considerar como una descripción de lo que deseamos proteger y el porqué de ello."* [18]

### 3.1.2. Elementos de las PSI.

Para una política de seguridad informática se deben considerar los elementos como:

- Su alcances incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Los objetivos y descripción de los elementos involucrados en su definición.
- Responsabilidad por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización.
- Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política.
- Definición de violaciones y sanciones por no cumplir con las políticas, junto con responsabilidad de los usuarios con la información a la que tiene acceso." [19]

### 3.1.3. Parámetros para establecer PSI

Las PSI se establecen con el objetivo de proteger las áreas y sistemas utilizados en la empresa, para lo cual se debe tomar algunas consideraciones:

[18] ROJAS, X. Et al. Auditoría de seguridad del personal, Física y Ambiental del Auto lote "Club Automotriz Nicaragüense" (CANSA). Managua, 2007, 131 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación. p. 8.

[19] ROJAS, X. Et al. Auditoría de seguridad del personal, Física y Ambiental del Auto lote "Club Automotriz Nicaragüense" (CANSA). Managua, 2007, 131 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación. p. 9.

- Efectuar un análisis de riesgo informático, para valorar los activos y así adecuar las políticas a la realidad de la empresa.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas incluyendo los beneficios y riesgos relacionados con los recursos, bienes y los elementos de seguridad.
- Identificar quien tiene la autoridad para tomar las decisiones en cada departamento pues son ellos los interesados en salvaguardar los activos críticos de su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa de forma tal que ante cambios las políticas puedan actualizarse oportunamente.
- Detallar explícitamente y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas. [20]

### 3.1.4. PSI para Control de Acceso

Estas permiten restringir el acceso a las áreas delicadas de la empresa como también a sus datos. Además ayuda a revisar, preparar y autorizar los datos de entrada y tener control de las personas que acceden a las instalaciones. Toda empresa que cuente con un centro de informática debe tener políticas que permitan la mejor operación de los sistemas y evitar el acceso no autorizado.

**a. Reglas de Control:** [21]

- ***Gestión de Acceso de Usuario*:** Debe establecer un procedimiento forma de registro de altas y bajas de usuarios para garantizar el acceso y la revocación de acceso a todos los sistemas y servicios de información, incluyendo el acceso físico.
- ***Gestión de privilegios:*** Deben restringirse y controlarse la asignación y uso de privilegio de acceso.
- ***Políticas* de limpieza de escritorio y pantalla:** Debe establecerse una política de escritorio limpio de papeles, de medios extraíbles y de pantalla limpia.

[20] Ibíd. ., p. 10.

[21] Piatinni, Et al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p. 293.

- ***Información* móvil y comunicaciones:** Se debe establecer una política de uso y adoptar medidas de seguridad apropiadas contra las amenazas inherentes al uso de equipos informáticos portátiles.

**b. Políticas de Respaldo**

La importancia de tomar en cuentas cada uno de los siguientes puntos de esta política es para que los usuarios y responsables del área tengan claros cómo actuar ante cualquier eventualidad:

- Contar con políticas formales por escrito para efectuar el respaldo mensual, semanal o diarios de la información.
- Todos los medios magnéticos de respaldo no deben estar almacenados en un mismo lugar, ya que si hubiera una contingencia grave (incendio inundación) se tendría el riesgo de perder parte o la totalidad de la información.
- Entre otros.

**c. Políticas y Procedimientos**

Algo importante de estas políticas que no debe pasar por alto es que deben ser actualizadas en todas las áreas que cuenten con ellas y sobre todo tener la documentación necesaria de dichas actualizaciones y ser del conocimiento del personal.

Si la empresa no se preocupa por actualizar las políticas y procedimientos podría tener una administración inadecuada de las operaciones, e incumplimiento de las obligaciones del personal. Estas políticas y procedimientos deben incluir; la seguridad de la información física y lógica, la adquisición de hardware y software, así como la operación del centro.

Es recomendable que se documenten todos los procedimientos de las diversas actividades. Estos, al igual que las normas y políticas, se manifiestan por escrito en manuales de operación. Al proceder de esta manera se obtendrían las siguientes ventajas:

- Se tiene una base uniforme, estable y formal para capacitación, consulta y supervisión y fomentando así la eficiencia del personal en sus funciones.
- Ante la rotación del personal, se evita el desvirtuamiento de las normas y procedimientos originales creados.

- Se precisa la responsabilidad individual de los participantes en una operación, en caso de errores y omisiones. [22]

**d. Políticas de Seguridad Física del Sitio.**

Las políticas deben describir los aspectos de seguridad física mínimos que deben existir dentro del departamento de sistemas, los que se enfocan en el acceso físico a la propiedad, acceso general a sistemas de información y acceso específico a los servicios de esos sistemas. Dentro de estos también el acceso a servicios de red.

Por consiguiente durante las visitas a las instalaciones se deben tomar en cuenta:

- La protección en los servidores para que no puedan ser desconectados accidentalmente o intencionalmente y provocar así serios daños al equipo.
- La existencia de documentos o carteles que indiquen las normas de seguridad mínima que deben observarse al estar en sitio.
- El personal operativo no debe permitir el acceso a personal ajeno al departamento.
- Los equipos electrónicos, interruptores o de comunicación no deben estar al alcance de cualquier persona. [23]

**e. Políticas de Acceso a Servicios de Red**

Algunas características de esta política son:

- Servicios autorizados o explícitamente denegados por la red privada, la forma en la que estos servicios serán usados y las condiciones de las excepciones a esta política.
- La restricción y uso de los servicios de la red interna, esto incluye todos accesos externos a la red, como accesos telefónicos y conexiones SLIP / PPP.
- La política debe ser realista, porque provee un balance entre proteger a la red de riesgos conocidos y proveer al usuario acceso razonable a los recursos de la red.
- La política debe ser sólida para restringir los servicios previendo todos los posibles puntos de acceso a tal servicio. [24]

---

[22] Echenique G. José A. Auditoría en Informática. Segunda Edición, McRae- Hill/ Interamericana Editores, S.A de C.V, México. 2001. Pág. 157.

[23] Echenique G. José A. Auditoría en Informática. Segunda Edición, McRae- Hill/ Interamericana Editores, S.A de C.V, México. 2001. Pág. 159.

[24] Textos científicos. "Políticas de Seguridad", Disponible en Línea en: [http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad], Ultima visita 07 de Agosto del 2010.

**f. Control de Seguridad Física**

Para implementar un control de seguridad se debe efectuar todos los análisis de riesgos necesarios en base a lo que queremos que no sea accedido fácilmente, para no estar expuestos a sabotajes.

- **Control de acceso físico:**
  1. Sistemas de Detección de intrusos centralizado
  2. Control de visitas.
  3. Pases o identificadores
  4. Accesos cerrados fuera de las horas de trabajo.
  5. Control de llaves combinaciones y dispositivos de seguridad.
  6. Se realizan revisiones periódicas del control de llaves. Combinaciones o dispositivos de seguridad. [25]

### 3.1.4.1 Contraseñas:

Las contraseñas son una manera de limitar el acceso a personas no autorizadas y tener protegidos nuestras instalaciones y nuestros sistemas contra el uso indebido de los mismos.

**Identificación, Autenticación y Autorización**

La identificación, autenticación, autorización y control de acceso están estrechamente relacionados. Sabiendo utilizar adecuadamente estos tres principios un administrador del sistema puede controlar que recursos están disponibles, para los usuarios de un sistema.

- **Identificación:** Es la manera como se puede identificar quien son los usuarios del sistemas, estos procesos usualmente se realizar cuando el usuario desea iniciar sesión, o acceder a cualquier instalación.
- **Autenticación:** Responde al procedimiento de asignación, distribución y almacenamiento contenido en el documento de seguridad y que éste procura las garantías suficientes de confidencialidad e integridad de contraseñas. [26]
- **Autorización:** Se produce después de que un usuario del sistema se identifica seguidamente, se autentica y luego es autorizado a utilizar el sistema. Estar

[25] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.301.
[26] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.658-659.

autorizado no significa que puede acceder a todos los sistemas ni a toda la información, sino que sólo está autorizado a usar una porción de los recursos del sistema en función de su papel en la organización.

**Factores de Seguridad:** Un factor perjudicial en la seguridad, es el factor humano que es una de las más grandes amenazas y es con el que se debe tener mayor cuidado, recordando que la seguridad inicia y termina con los usuarios. El administrador debe controlar: los cambios de claves de acceso, desconexión de terminales y los ficheros importantes del sistema (mantenimiento).

#### 3.1.4.2 Virus informático y Software dañino

Otra preocupación y no menos importante con lo que la tecnología se refiere además de la fuga de datos, los virus informáticos son programas que dañan el funcionamiento de una computadora con la intención de eliminar u ocultar cualquier tipo de archivo, al mismo tiempo hacer más lentas las operaciones del equipo, estos archivos se pueden propagar a otras computadoras, a través de Internet y pasando información a través de USB.

**Tipos de virus informáticos:** Los virus nos caen por sorpresa de la manera más inesperada, inclusive a través de archivos que parecieran ser importantes, cada virus se diferencia dependiendo de la infección que transmita y del daño que pueda causar a nuestros sistemas y archivos, algunos de ellos y más conocidos son los caballo de Troya (llamado troyano), gusano, bomba lógica y el virus específicos para redes.

**Software dañino:** Es un tipo de software instalado en el ordenador de un usuario, que se dedica a rastrear la información y el comportamiento del usuario en Internet.

**Tipos de software dañinos:**

**Spyware:** Numerosos programas instalan pequeñas aplicaciones que registran la actividad de los usuarios.

**Malware:** son aquellos que con la excusa de rentabilizar el software que se regala, incluyen aplicaciones para lanzar anuncios. Además registran la actividad del usuario e informan de sus movimientos a unos terceros que modifican el PC a su antojo.[27]

[27] DELGADO, A. Et al. Auditoría en la Administración de la Red del Centro de Operación de Redes (CORE). Managua, 2007, 107 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación. p.31.

# 4

## CAPITULO 4: AUDITORIA DE LA SEGURIDAD INFORMATICA

### 4.1. INTRODUCCION

Pensando en entorno tecnológico, para muchos la seguridad puede ser el área principal a auditar, y es la realidad en muchas entidades, se creó la función de auditoría informática para revisar la seguridad, con el paso del tiempo ha llegado a abarcar controles relacionados con los sistemas de información, calidad, desarrollo de aplicaciones y otras áreas.

La diferencia entre Auditoria de la Seguridad dentro de la Auditoria Informática y la Auditoria de la seguridad dentro de Sistemas de Información[28], es que la primera puede comprender la informática (equipos, sistemas operativos, datos, redes… y su marco de control: normativa, funciones, cumplimiento legal relacionado con la seguridad, centros, continuidad del servicio…), y en el caso de la Auditoria de Sistemas de Información referida a la seguridad, puede abarcar lo anterior, más la evaluación de la protección de sistemas de información no autorizados o sólo parcialmente, de procesos y datos relacionados con esos sistemas, aunque sean procesos y ficheros manuales.

Si buscamos **definiciones[29],** la norma ISO-7498-2 ya indicaba que Auditoria de la Seguridad es: “Una revisión y examen independientes respecto a los registros y actividades de un sistema a fin de verificar si los controles del sistema son adecuados, para garantizar el cumplimiento con la política establecida y con los procedimientos operativos, para detectar problemas de seguridad, y para recomendar posibles cambios en los controles, en la política y en los procedimientos”.

En el caso de auditoría de seguridad, el objetivo y el ámbito se pueden referir a áreas, centros, plataformas, sistemas/aplicaciones, funciones, ficheros/bases de datos… y el

[28] Ranis Miguel.Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.441

[29] Ranis Miguel.Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.443

propósito es evaluar la protección relacionada con la integridad de los datos, con la continuidad (disponibilidad), o bien verificar el grado de cumplimiento de la normativa interna, pudiendo ser la auditoría de seguridad más global o referida a aspectos o sistemas muy concretos.

### 4.2. CONTROL INTERNO Y SEGURIDAD[30]

Al hablar de auditoría y de auditoría de la seguridad, solemos decir que se trata de la evaluación del control interno, y como **Sistemas de Control Interno** podemos considerar el conjunto de proceso, funciones, actividades, dispositivos… cuya misión total o parcial sea garantizar que se alcanzan los objetivos de control, así como que los sucesos no deseados se evitarán, o bien se podrán detectar y se corregirán.

La clasificación clásica de controles abarca tres grupos: preventivos, de detección y de corrección, si bien como algunos autores sugieren se puede añadir dos grupos: el primero y el ultimo de la siguiente relación: Controles de Dirección, Controles preventivos, Controles de detección, Controles de corrección, Controles de recuperación.

COBIT(*Control Objectives for Information and related*), viene a ser un marco de referencia, este se refiere a un conjunto amplio de procesos, y recoge más de 200 objetivos de control relacionados con esos procesos; los objetivos pueden servir de base para implantar controles de una entidad, y específicamente referidos a la seguridad, y también como base para evaluar la seguridad y el control, si bien en todos los casos sirven de orientación pero no son muy precisos ni detallados, por lo que es necesario diseñar los controles a partir de la filosofía que recogen.
Como macroobjetivos de control pueden estar:

- Cumplimiento de los requerimientos legales y de la normativa interna, así como de los requerimientos de las áreas propietarias/usuarias.
- Determinación de funciones y responsabilidades, concienciación y motivación de directivos y usuarios.
- Salvaguarda de los activos relacionados (accesos autorizados), así como respaldo/recuperación: confidencialidad e integridad.
- Fiabilidad de procesos y sistemas y disponibilidad.

[30]Ranis Miguel.Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.445

- Gestión adecuada de incidencias y de cambios.
- Evidentemente, el riesgo será mayor si el sistema de control interno es débil. Cuando hay un sistema de control interno adecuado, los procesos de auditoría, especialmente si son periódicos, pueden ser más ligeros.

### 4.3. PERFIL DEL AUDITOR DE SEGURIDAD[31]

Dentro del perfil y situación podemos encontrar aspectos comunes, como objetividad e independencia, exigibles a todos los auditores, y otros específicos en función de los entornos en los que se va a revisar la seguridad. Es decir, el auditor ha de tener formación y experiencia generales acordes con su función, y en el caso concreto de revisiones técnicas de seguridad de cierta profundidad, serán necesarios conocimientos actualizados relacionados con el entorno o plataforma concretos.

Si queremos definir un perfil del auditor de seguridad más completo, como sería el caso de una selección interna o externa, podemos pensar en características y rasgos como los siguientes:

- Independencia y objetividad.
- Integridad, y conducta según unos principios éticos.
- Formación y experiencia de acorde con el tipo de trabajo
- Una combinación de amabilidad y de firmeza, según se requiera.
- Capacidad de análisis y de síntesis.
- Madurez, que no debemos relacionar con una edad mínima.
- Si el auditor tiene que dirigir equipos de personas, capacidad para ello, así como liderazgo y aceptación.
- Motivación e interés por hacer el trabajo, incluso vocación.

Además, en el caso de los auditores internos ha de existir una relación adecuada con la función de Administración de Seguridad, que puedan existir en la entidad roles de Responsables/s de seguridad, relacionadas con los datos personales o no. Normalmente Administración de Seguridad habrá de implantar las recomendaciones de los auditores, una vez fijada las prioridades por la dirección de la entidad.

[31] Ranis Miguel. Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.447

Otro aspecto relacionado con el perfil: en el caso de contratar auditores externos, también es necesario considerar el perfil de quienes van a realizar el trabajo:

- La entidad auditora ha de ser independiente de la auditada.
- Las personas que vayan a realizar el trabajo han de ser independientes y competentes, según el objetivo.
- No es tan común pedir referencias de otros trabajos similares como en el caso de consultoría pero se puede hacer.
- La auditoría a de encargarse a un nivel suficiente, normalmente Dirección General o incluso Consejero Delegado, y a este mismo nivel recibir los informes.
- Otro aspecto es la confidencialidad.

### 4.4. COBIT Y OTRAS FUENTES DE ISACA[32]

La evaluación se debe hacer *contra* algún patrón o estándar, que puede ser interno como la normativa existente, o el contrario de servicios entre entidades, o bien totalmente externo como la norma **ISO 17799**, COBIT **de ISACA**[152] , o el reglamento en vigor en el caso específico de datos personales , y en todos los casos puede haber interpretaciones o valoraciones diferentes.

Si no hay ninguna norma interna o la normativa es muy parcial y se ha pedido una auditoria general de seguridad, habrá que advertir al cliente que hacer una revisión contra estándares generalizados, que podrían equivaler a los principios generalmente aceptados que dicen auditores de cuentas. El propio COBIT es una referencia excelente, si bien más como filosofía o marco general y para apoyar las recomendaciones que como guía de verificaciones de seguridad en detalle.

Casi todo el COBIT puede servir como base para una auditoria de seguridad, pero si consideramos la última versión: 4.1, de 2007, que ya estamos utilizando en práctica, Objetivos de Control más directamente relacionados pueden los que se presentaran en este contenido.
En cada apartado se indican los puntos más afines, que pueden servir de guion para las revisiones, si bien sugiere consultar el texto completo de cada punto.

[32]Ranis Miguel.Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.453

Objetivos de Control COBIT 4.1 Orientados a la SEGURIDAD INFORMATICA

| | |
|---|---|
| **PO2** Define the informatin architecture | No afecta de forma directa pero sí al integrar la seguridad en el Plan General. |
| **PO3** Define technological direction | influye la arquitectura tecnológica |
| **PO4** Dewfinethe IT processes, organisation and relationships | Influyen los planes, la organización, las funciones y responsabilidades, y sobre todo: Objetivo de Control 4.8 al 4.9, del 4.11 al 4.14 |
| **PO5** Managethe IT investment | Repera en la fiabilidad, inversiones y gastos en seguridad. |
| **PO6** Communicat emanagementaims and direction | Influye las políticas y sobre todo: Objetivo de Control 6.2 al 6.4 |
| **PO9** Assess and mnage IT risks | influye plenamente: Objetivo de Control 9.1 al 9.6 |
| **AI3** Acquire and maintain technology infrastructure | Cierta influencia sobre todo: Objetivo de Control 3.2 al 3.3 |
| **AI4** Enable operation and use | Influyen algunos puntos:Objetivo de Control 4.1 al 4.4 |
| **AI5** Procedure IT resources | Influye en cierto modo: Objetivo de Control 5.1 al 5.4 |
| **DS1** Define and manage service levels | Es calidad, pero influye en seguridad: Objetivo de Control 1.1 al 1.6 |
| **DS2** Managethrid-party service | Influye en cuanto a servicios y seguridad: Objetivo de Control 2.3 al 2.4 |
| **DS5** Ensure systems security | Influencia importante: Objetivo de Control 5.1 al 5.11, excepto el 5.3 |
| **DS7** Educate and trainusers | Influye lo referido a la seguridad. |
| **DS10** Manage problems | Influye: Objetivo de Control 10.1 al 10.4 |
| **DS11** manage data | Influye: Objetivo de Control 11.2 al 11.6 |
| **DS12** Manage the physical environment | Influye: Objetivo de Control 12.1 al 12.5 |
| **DS13** Manage operations | Influye: Objetivo de Control 13.1 al 13.5 |
| **ME1** Monitor and evaluate IT performance | Sobre todo en cuanto a disponibilidad |
| **ME3** Ensure compliance with external requirements | Influye, en función del país: Objetivo de Control del 3.1 al 3.5 |
| **ME4** Provide IT governance | Influye: Objetivo de Control 4.5, 4.7 |

En cuanto a estándares de cómo realizar la auditoria de seguridad, ISACA (*Information Systems and Control Association*) puede ser una de las mejores fuentes, además de los que cada entidad pueda tener.

### 4.5. Áreas a Revisar:[33]

Dependerán de los objetivos del encargado, pero en sentido amplio las áreas y puntos principales relacionados con la seguridad pueden ser los que se indican a continuación, si bien se trata solo de enumerarlos, aunque en relación con muchos de ellos en la práctica se pueden usar listas de verificación muy completas, que en cuánto a aspectos técnicos dependerán de los entornos y de las versiones.

1. El marco normativo interno y nivel de cumplimiento
2. Implicación de la (Alta) Dirección respecto a la protección de la información
3. Cumplimiento de requerimientos externos
4. Cumplimientos de requerimientos internos
5. La organización y la gestión de recursos humanos
6. La protección de Activos
7. Control de accedo lógicos
8. Acceso por terceros a los recursos
9. Explotación u operaciones
10. Seguridad de las comunicaciones y redes
11. Seguridad Física
12. Desarrollo y Mantenimiento de Aplicaciones y paquetes
13. Copias, Recuperación, Planes de Contingencia/ de Continuidad

### 4.6. Fuentes a Utilizar[34]

Cabe señalar que las fuentes a considerar están relacionadas con los objetivos y por tanto deberán ser adecuadas para alcanzar evidencias. Se ha considerado el grado de protección. Entre las posibles fuentes están:

- Políticas, normas, estándares y procedimientos.
- Planes de seguridad y Planes de acción
- Contratos, pólizas de seguros.
- Planos de instalaciones.
- Organigrama y descripción de funciones.
- Documentación de aplicaciones y de paquetes

[33]Ranis Miguel.Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.469

[34]Ranis Miguel.Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.480

- Descripción de dispositivos y especificaciones de algoritmos relacionados con seguridad
- Inventarios
- Topologías de redes. Cortafuegos y sus parámetros, reglas y opciones.
- Registros de problemas, de cambios, de visitas, de accesos lógicos producidos.
- Entrevistas a diferentes niveles, y no solo a técnicos
- Posible acceso a datos en caso necesario, o tal vez visualización supervisada.
- Programas y su documentación e historial de cambios
- Resultados de pruebas realizadas y de las herramientas aplicadas
- Información sobre sistemas operativos y software de bases en general.
- La Observación: no figura en los materiales pero la consideramos importante.
- Actas de reuniones relacionadas
- Documentación de planes de contingencia/continuidad y sus pruebas.
- Informes de suministradores, o de consultores que hayan realizado revisiones.

### 4.7. Técnicas, Métodos y Herramientas.[35]

Entre estos se han determinado los siguientes: Además de las entrevistas y revisiones se podrán realizar muestreos, utilizar cuestionarios, la observación (citada como fuente información), utilizar SQL, u otros lenguajes de *query* o bien para producir informes (tipo CrystalReport), o para tomas/ analizar opciones y parámetros de sistemas, o bien pruebas integradas, *snapshot* para análisis profundo de contenido dinámico de memoria, revisión de programas, o herramientas específicas de análisis de vulnerabilidad de red: puertos y servidores abiertos, o de detección de intrusos, sin descartar hojas de cálculo como Excel como ayuda para estructurar o presentar resultados, y dando por hecho que en todos los casos se utilizaran un procesador de texto para los informes. Parte de lo escrito entra dentro de la categoría de las CAAT (*ComputerAided, AuditingTechniques*), ya que se entiende dentro de este grupo las técnicas, y por extensión las herramientas relacionadas, en que se usan los equipos y la información que recoja, para realizar los análisis, tanto sean de utilidades generales o de análisis de librería/programas.

[35] Ranis Miguel. Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2005. p.482

# 5

## CAPITULO 5: OUTSOURCING Y SEGURIDAD INFORMATICA

Outsourcing va más allá que la mera subcontratación de ciertas actividades o tareas dado que en el proceso de Outsourcing los riesgos, el éxito o el fracaso del propio negocio o actividad se comparten entre el cliente y el tercero[36]

### 5.1 Outsourcing de TI (Tecnología Informática)

Es de mucha ayuda que la tecnología este creciendo a pasos agigantados, aunque esta evolución somete a las empresas a grandes presiones, pero de igual manera les brinda las soluciones. Una de esta es el Outsourcing que se está transformando en un proceso estandarizado con el objetivo de brindar excelentes estrategias de negocios así mismo reducir costos para las empresas, pero no obviando los perfiles de riesgos tolerables.

El Outsourcing se ha ido extendiendo en muchos servicios la cuales se han convertido en parte importantes para las empresas en la actualidad alguna de ellos es la gestión de aplicaciones, gestión y operación de la infraestructura y el aseguramiento de Calidad.

### 5.2 Tipos de Outsourcing

El Outsourcing se ha distribuido en distintas áreas al igual que lo ha hecho la informática brindando de esta manera grandes facilidades para las diferentes áreas que lo soliciten. Este nuevo foco sobre Outsourcing TI [i]es un habilitador clave para lograr una ventaja competitiva y el crecimiento de la empresa.

**Algunos tipos de Outsourcing son**:[37]

- Outsourcing Informático Tradicional
- Outsourcing de Proceso de Negocio
- Outsourcing Total

[36] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.246.
[37] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.251.

### 5.3 Ciclo de vida del Outsourcing

Como todo proceso el Outsourcing tiene un determinado ciclo de vida el cuál debe estar bien estructurado, de esta manera se asegurara que cada una de las fases que se utilizaran en dicho proyecto se ejecute de manera adecuada y consistente y puedan así concluir en tiempo y forma dentro del presupuesto y estándares requeridos.

Existen numerosas metodologías y herramientas para gestionar las diferentes fases y elementos clave algunas de ellas son:

| Fase | ELEMENTOS CLAVE |
|---|---|
| *Planificación Estratégicas* | ✓ Alineamiento con el negocio sus necesidades y direcciones<br>✓ Alineamiento con la estrategia, funcionamiento y arquitectura<br>✓ Opciones: Evaluación de alternativas, Benchmarking<br>✓ Modelo de negocios y de sistemas<br>✓ Plan de proyecto, Gestión de Riesgo.<br>✓ Financiación, Soporte, Stakeholder y Sponsoring |
| *Contratación* | ✓ Proveedores: Ranking, Selección ofertas competitivas.<br>✓ Estudios de Viabilidad.<br>✓ Proceso de Contratación y Adquisición.<br>✓ Aseguramiento de Aspectos Legales y Laborales.<br>✓ Acuerdos y Concreción de Planos. |
| *Transición* | ✓ Gestión del cambio.<br>✓ Relaciones, Comunicaciones y Acoplamientos de las partes.<br>✓ Reingeniería de Procesos y Procedimientos.<br>✓ Organización RRHH y políticas.<br>✓ Controles: Migración, Ajustes, Transferencia de Activos y Procesos / Sistemas. |
| *Gestión y Optimización* | ✓ Métricas, Niveles de servicios, Indicadores, Tendencias.<br>✓ Seguimientos, Feedback y Gobierno del Outsourcing<br>✓ Optimización y Redefinición de Relaciones.<br>✓ Resolución de Problemas y Conflictos.<br>✓ Control Asignación y Gestión de Costes.<br>✓ Optimización de Procesos de TI y de Negocios. |
| *Finalización y Renegociación* | ✓ Reevaluar Opciones y Alternativas.<br>✓ Renegociar o Terminar relaciones y Condiciones.<br>✓ Evaluaciones Generales.<br>✓ Reevaluación del Riesgo. |

***Fuente:*** *Elementos Claves del Outsourcing.* [38]

[38] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.254-255.

### 5.4 Contrato de Outsourcing

Un contrato de Outsourcing no es diferente de otro contrato ya que en ellos plasmamos simplemente lo que esperamos que se cumpla en el periodo de vigencia, contando que durante ese período se cumplan las cláusulas que estipula el mismo, debido a que el mínimo fallo de ellas podrían afectar el control general sobre los servicios que se requieren.

Al realizar un contrato de Outsourcing se debe pensar en un plan de retorno, esto en caso de que la empresa tome la decisión de hacerse cargo ellos de las funciones informáticas o que se tome la decisión de cambiar de proveedor.

Las cláusulas y aspectos a considerar en un contrato de Outsourcing son:

| Cláusulas | ASPECTOS A CONSIDERAR |
|---|---|
| ***Validez del contrato*** | Detalle de las empresas receptoras del servicio. Existencia de refrendos (firmas) por personas con capacidad real. |
| ***Vigencia del contrato*** | Fecha de inicio y fin del contrato. |
| ***Transición*** | Periodo de despliegue del nuevo proveedor. |
| ***Inventario de servicios proporcionados*** | Existencia de un listado de servicios a ser prestados. |
| ***Obligaciones del proveedor y del cliente*** | Compromisos y responsabilidades de las partes. |
| ***Aspectos económicos*** | Tarifas establecidas, Impuestos aplicables, revisión de los precios. |
| ***Control de calidad*** | Capacidad para utilizar el servicio, benchmarking de servicios y precios, satisfacción de cliente (calidad percibida) |
| ***Confidencialidad, seguridad y publicidad de la información*** | Información confidencial y publica |
| ***Derechos de propiedad intelectual e industrial*** | Propiedad de herramientas y software utilizado en el servicio. |
| ***Ley aplicable y resolución de conflictos*** | Legislación aplicable en la prestación del servicio. |
| ***Subcontrataciones*** | El proveedor deberá notificar formalmente al cliente posibles subcontrataciones de servicios prestados y solicitar su aprobación. |
| ***Resolución del contrato*** | Causas que puedan implicar motivos de finalización del contrato con/sin cargo, colaboración en la terminación del contrato. |
| ***Descripción de los servicios*** | Descripción del servicio, actividades detalladas, horario de presentación, responsabilidad y obligaciones de las partes. |
| ***Acuerdo de nivel de servicio*** | Indicadores de nivel de servicio con su procedimiento de cálculo, revisión del cumplimiento del ANS, esquema de |

| | |
|---|---|
| | penalización, obtención de los resultados e informes de gestión. |
| ***Términos económicos*** | Distribución del precio a lo largo de la vida del contrato. Precios de servicios agrupados o individuales por unidad de medida o una banda base acordada. Ejemplos de unidades de medida serían N° de PC y la potencia de cálculo, variación de unidades de medida y revisión del precio. |
| ***Modelo de relación*** | Contacto del proveedor y clientes con sus sometidos. Vías de comunicación entre el proveedor y el cliente y propósito. Comité del seguimiento del contrato, con el detalle de: Funciones, frecuencia de reuniones y generación de actas. |

***Fuente:*** *Clausulas y Aspectos Contractuales* [39]

### 5.5 Ventajas del Outsourcing

Hemos estado hablando de beneficios que tiene las empresas que solicitan el servicio subcontratación (Outsourcing) Y mencionaremos algunas ventajas de utilizar Outsourcing.

a. Flexibilidad en la presentación y en el coste del servicio.
b. Posibles mejoras operativas y beneficios para el negocio
c. Descarga a la dirección de parte de sus actividades.
d. Capacidad de reacción ante los cambios del negocio y del mercado.
e. Capacidad de incorporar nuevas tecnologías en el momento de su aparición.
f. Eliminación de las contingencias laborales( absentismo, enfermedades y vacaciones)
g. Permite liberar recursos e invertirlos en la actividad principal de la empresa.[40]

### 5.6 Inconvenientes del Outsourcing

Al igual que ventajas, tenemos inconvenientes de subcontratación y algunas son:

a. La estrategia de Outsourcing puede entrar en conflicto con los objetivos o la estrategia de la organización.
b. Pérdida de control de los activos: obsolescencia del software, hardware.
c. Un mantenimiento incorrecto afecta a la capacidad de proceso.
d. Si los tiempos de respuesta no son aceptables, el trabajo se deteriora.
e. El nivel de servicio se puede ir deteriorando en el transcurso de la relación.

[39] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.261-263.
[40] Piatinni, Mario. Et. al. Auditoría de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008. p.256.

f. Impacto cultural en la organización [41]

### 5.7 Acuerdos de nivel de servicio (ANS)

Este debe ser un documento vivo, el cual se debe adaptar a las necesidades, expectativas y responsabilidades del servicios así mismo las modificación son parte de esta. El ANS debe ser revisado a petición de cualquieras de las parte de la esto si la situación lo requiere.

Un ANS es una herramienta con diferentes objetivos:

| | |
|---|---|
| **Comunicación.** | La comunicación que se desarrolla entre las partes durante la elaboración del Acuerdo Nivel de Servicio (ANS) contribuye al intercambio de opiniones y necesidades. |
| **Gestionar las expectativas.** | Este proceso de un ANS implica la identificación y discusión sobre las expectativas sobre los servicios y su entrega. |
| **Reducción de Conflictos.** | Este se da ante la ausencia de entendimiento entre las necesidades y prioridades y ayuda a la minimizar los conflictos contribuye a una solución. |
| **Control.** | Recoge los servicios a ser prestados y los valores mínimos de servicios establecido. |

***Fuente:*** *Acuerdo de Nivel de Servicio* [42]

[41] Ibis. ., p.256.

[42] Ibis. ., p.267.

# 6

## CAPITULO 6: EVALUACION DEL RIESGO EN LA SEGURIDAD INFORMATICA

La mayoría de las empresas e instituciones desconocen la magnitud del problema con el que se enfrentan, considerando la seguridad informática como algo secundario y prestando poca atención a los riesgos que en la actualidad existen, como las amenazas internas, una de ellas, los errores humanos y las amenazas externas dentro de las cuales podemos nombrar a los virus.

A medida que los niveles de inversión incrementan, las pérdidas materiales se multiplican, efecto de esto es que no se anticipa una estimación de la representación del riesgo desde la adquisición de nuevas tecnologías hasta su implementación, mantenimiento y seguimiento de las mismas.[43]

### 6.1 Definición de Riesgo

Riesgo se puede definir como aquella eventualidad que imposibilita el cumplimiento de un objetivo. De manera cuantitativa el riesgo es una medida de las posibilidades de incumplimiento o exceso del objetivo planteado. Así definido, un riesgo conlleva dos tipos de consecuencias: ganancia o pérdidas.

En lo relacionado con tecnologías, generalmente el riesgo se plantea como amenaza, determinando el grado de exposición a la ocurrencia de una perdida (por ejemplo el riesgo de perder datos debido a rotura de disco, virus informático, etc.). [44]

En la versión 4.1 de Cobit [45] define el Riesgo como: “El potencial de una amenaza específica explore las debilidades de un acto o grupo de activos para ocasionar perdidas y/o dalos a los activos. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia”. En este sentido se identifican elementos claves que conceptualizan e integran el concepto de riesgo. Estos elementos son: Probabilidad, Amenazas, Vulnerabilidad, activo e impacto.

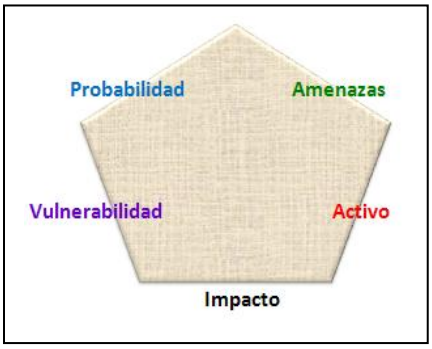
---

[43] Sena Leonardo, Tenzer Simón. Introducción al Riesgo. 2004.p.2.

[44] SENA Leonardo, Tenzer Simón. Introducción al Riesgo. Agosto 2004. p.2.

[45] Cobit and IT Governance Institute (2007),”COBIT 4.1”, 4ta Edición, Internet Document unloaded, 07 de Agosto 2010. http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf.p.191.

***Grafico 6.1:*** *Elementos que integran el Riesgo*




***Fuente:*** *Introducción al Riesgo* [46]

**A continuación se definen estos elementos:** [47]

- **Probabilidad:** Establecer la probabilidad de ocurrencia puede realizarse de manera cuantitativa o cualitativa, pero siempre considerando que la medida no debe contemplar la existencia de ninguna acción paliativa, o sea, debe considerarse en cada caso que posibilidades existen que la amenaza se presente independientemente del hecho que sea no contrarrestada.
- **Amenaza:** Las amenazas siembre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa de la empresa. Comúnmente se indican como amenazas a las fallas, a los ingresos no autorizados, a los virus, uso inadecuado de software, los desastres ambientales como terremotos o inundaciones, accesos no autorizados, facilidad de acceso a las instalaciones, etc.

**GRAFICO 6.2:** Posibles Amenazas


***Figura:*** *Introducción al Riesgo*

[46] SENA Leonardo, Tenzer Simón. Introducción al Riesgo. 2004.p.2

[47] SENA, Ibid.,p.3

Las amenazas pueden ser de carácter físico o lógico, como una inundación en el primer caso, o un acceso no autorizado a una base de datos en el segundo caso.

- **Vulnerabilidad:** Posibilidad de ejercer de forma accidental o intencional una vulnerabilidad.

  Es así que las vulnerabilidades en cualquiera de los contextos pueden desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad, entre ambas existe una estrecha relación: sin vulnerabilidad no hay amenaza y sin amenaza no hay vulnerabilidades.
- **Activo:** Los activos a reconocer son aquellos relacionados con sistemas de información. Ejemplos típicos son los datos, el hardware, el software, servicios, documentos, edificios y recursos humanos.
- **Impacto:** Las consecuencias de la ocurrencia de las distintas amenazas son siempre negativas. Las pérdidas generadas pueden ser financieras, no financieras, de corto plazo o de largo plazo.

Se pueden establecer que las más comunes son: la pérdida directa de dinero, la pérdida de confianza, la reducción de la eficacia y la pérdida de oportunidades de negocio. Otras no tan comunes, felizmente, son la pérdida de vidas humanas, afectaciones del medio ambiente, etc.

## 6.2 Administración y análisis de riesgo [48]

Como herramienta de diagnóstico para poder establecer la exposición real a los riesgos por parte de una organización se recurre a lo que se llama ***Análisis de Riesgo***. Este análisis tiene como objetivo identificar los riesgos (mediante la identificación de sus elementos) y lograr establecer el riesgo total (o exposición bruta al riesgo) y luego el riesgo residual, tanto sea en términos cuantitativos o cualitativos.

Cuando se refiere al riesgo total, se trata de la combinación de los elementos que lo conforman. Comúnmente se calcula el valor del impacto promedio de ocurrencia para cada amenaza y activo.

De esta manera tendremos, para cada combinación valida de activos y amenazas:

**RT *(Riesgo Total)*** = **Probabilidad x Impacto promedio.**

[48] SENA Leonardo, Tenzer Simón. Introducción al Riesgo. 2004. p..4.

Por ejemplo, si la probabilidad de incidentes en el año es 0.0001 y el impacto promedio en términos monetarios de los activos amenazados por un incendio es $600.000. La exposición al riesgo anual es de 60 (ver explicación más adelante).

A este cálculo se debe agregar el efecto de medidas mitigantes de las amenazas, generándolas el riesgo residual. El riesgo residual es el riesgo permanente luego de la aplicación de medidas destinadas a mitigar los riesgos existentes.

Las medidas mencionadas son aquellas que generalmente se conocer como controles.
De hecho, el riesgo residual es una medida del riesgo total permanente luego de contemplar la efectividad de las acciones mitigantes existentes. De esta manera, siguiendo con el ejemplo planteado, si el riesgo total de la amenaza incendio es 60, luego de contratar un segundo sobre la totalidad de los activos, el riesgo residual resultante sería igual a cero. Por otra parte si se asegurara por la mitad del capital, el riesgo residual sería igual a 30.

Obviamente, este ejemplo esta simplificado, con el único objetivo de ayudar a comprender los conceptos vertidos. En la realidad no es nada sencillo cuantificar adecuadamente los riesgos. Por lo anterior es que usualmente se utiliza un enfoque cualitativo, expresando los riesgos en altos, medios y bajos, o en niveles similares.

El proceso de análisis descriptivo genera habitualmente un documento que se conoce como matriz de riesgo. En este documento se ilustran todos los elementos identificados, sus relaciones y los cálculos realizados. La sumatoria de los riesgos residuales calculados es la exposición neta total de la organización a los riesgos.
La afirmación anterior fue efectuada con el supuesto de que el resultado obtenido es positivo. En caso que el resultado sea negativo se establece que la organización se encuentra cubierta de todos los riesgos analizados, pero, sin embargo, es ineficiente porque tiene más controles que los necesarios. Realizar el análisis de riesgo es indispensable para lograr administrar adecuadamente los mismos.

El ciclo de administración de riesgo se cierra (luego de efectuar las tareas referentes al análisis) con la determinación de las acciones a seguir respecto los riesgos residuales identificados.

***Estas acciones pueden ser:***

1. **Controlar el riesgo**: Se fortalecen los controles existentes o se agregan nuevos.
2. **Eliminar el riesgo**: Se elimina el activo relacionado y por ende el riesgo.
3. **Compartir el riesgo**: Mediante acuerdos contractuales se traspasa parte del riesgo (o Su totalidad) a un tercero (un ejemplo son los seguros.)
4. **Aceptar el riesgo**: Determinar que el nivel de exposición es adecuado.

La opción elegida deberá ser adecuada, fundamentada y autorizada por el nivel jerárquico correspondiente sobre la base del riesgo asociado.

**Proceso de Administración del Riesgo:** El proceso de administración de riesgo es un proceso continuo, dado que es necesario evaluar periódicamente si los riesgos identificados y la exposición a los mismos calculada en etapas anteriores se mantienen vigentes. La dinámica en la cual se ven inmersa las organizaciones actualmente demanda este esfuerzo día a día. Es por eso que en cada inicio de las etapas tempranas, se debe realizar el análisis de riesgo referido al proyecto, así como su impacto futuro en la estructura de riesgo de la Organización.

***GRAFICO 6.3:*** *Proceso de Administración del Riesgo*


***Figura:*** *Introducción al Riesgo*

**Ejemplo de Matriz del Riesgo**

En la siguiente hoja se presenta una matriz, donde:

- En cada fila se presenta una amenaza identificada
- En la columna de probabilidad se indica cuan probable es que esa amenaza actué, con independencia de los controles que existan o que se establezcan. La certeza es el 100% y la imposibilidad es 0%. Cada porcentaje de cada fila es manejado en forma independiente.
- En las columnas siguientes se indica para cada uno de los activos a proteger cuan importe es la perdida media estimada que ocasionaría esa amenaza en ese activo.

Por ejemplo, por servidores se entiende computadores centrales que soportan las bases de datos, la gestión del correo electrónico, la red internet y otros servicios. Las terminales son los puestos de trabajo computarizados. Los datos son la información de la Organización. Las instalaciones se refiere a toda la parte física, incluyendo edificio, mobiliario, componentes de red (cableado, "routers", "bridges", "switches"), etc. Personal son los recursos humanos.

- Los datos precedentes permiten calcular la columna siguiente, riesgo total, el cual suma los productos de la probabilidad de la amenaza por el impacto, de toda la fila.
- A continuación se presenta la efectividad del control actuante, o sea que nivel de riesgo total se puede mitigar. Por ejemplo. La amenaza de inundación puede ser mitigada ubicando el Centro de Cómputos en un piso elevado. Por otra parte, también suele estar bajo tierra, por razones de seguridad. Otro ejemplo: los accesos no autorizados vía internet pueden ser mitigados con un "firewall" (barrera de control de acceso desde fuera y hacia afuera) correctamente configurado.
- Finalmente, en la última columna, se indica cual es el riesgo residual, que resulta de aplicar la efectividad del control al riesgo total. [49]

**TABLA 6.1: MATRIZ DEL RIESGO**

| | | Grado de impacto (US$miles) | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Amenazas | Proba-bilidad | Servi-dores | Termi-nales | Datos | Instala-ciones | Per-sonal | Riesgo Total | Efec-tividad del control | Riesgo Residual |
| *Incendio* | 1% | 10 | 5 | 8 | 62 | 41 | 1,26 | 100% | 0 |
| *Inundación* | 1% | 10 | 1 | 8 | 22 | 8 | 0,245 | 90% | 0.0245 |
| *Accesos no autorizados* | 20% | 1 | 0 | 12 | 0 | 0 | 2,6 | 50% | 1.3 |
| *Fallas* | 25% | 0,5 | 0,5 | 2 | 0 | 0 | 0,75 | 50% | 0.375 |
| *Virus* | 30% | 2 | 3 | 1 | 0 | 0 | 1,8 | 80% | 0.36 |

***Fuente:*** *Introducción al Riesgo*

Esta matriz ha sido presentada para ejemplificar y no deben ser consideradas como un único instrumento de este tipo de herramientas. Existen abundantes metodologías que abordan el tema de distintas manera como por ejemplo la Tabla NIST, ente otras.

[49] SENA Leonardo, Tenzer Simón. Introducción al Riesgo. 2004. p.5-6

# 7

## CAPITULO 7: ASPECTOS INTITUCIONALES

### DESCRIPCIÓN SITUACION ACTUAL DE MS-AMERICA CENTRAL

MS América Central - ActionAid Denmark forma parte de una gran familia global.

MS América Central Action Aid es un organismo Internacional que trabaja sin fines de lucro Tiene su origen en Dinamarca, pero desde su creación inicial en 1944 se ha extendido por el mundo. Hoy en día se consideramos una organización global y formamos parte de una de las redes de ONGs de desarrollo más grandes del mundo - ActionAid International.

El trabajo de MS América Central – ActionAid Denmark está marcado por la visión de un mundo en paz, con mejores condiciones para los pobres y marginalizados. Un mundo en donde la gente trabaja en conjunto para lograr la justicia global.

Junto con miles de organizaciones asociados en África, Centroamérica, Asia, el Medio Oriente y en los Balcanes, apoyan a los pobres del mundo en su lucha por una vida mejor. Entre las organizaciones asociadas existen desde grandes organizaciones nacionales hasta pequeñas asociaciones a nivel local, trabajando con educación, desarrollo comunal, medio ambiente, vih/sida, derechos humanos y otros temas.

Cuando otros proveen medicina, carreteras o fondos, MS América Central apuesta a capacitaciones, entrenamientos, organización propia por parte de los actores, e intercambio de experiencias. Apuesta a inversiones en humanos, porque el ser humano es el recurso más importante en el proceso de desarrollo. Desarrollo participativo basado en apoyo a socios locales es lo que llaman ‘ayuda a la autoayuda’ – y es la base que necesitan para asegurar el desarrollo que los pobres..

Incidencia a nivel local y global da a los pobres la oportunidad de presentar sus casos, y a través de una política de desarrollo más solidaria en el Norte, el trabajo en el Sur tiene una relación directa con las decisiones que se toman en Dinamarca y otros países ricos.

A principios de los noventas, se inició un programa regional en Nicaragua, Guatemala, Honduras y El Salvador.
MS América Central Action Aid provee mantenimiento y servicio tecnológico nos solo al personal de MS, sino también otras Organizaciones no gubernamentales que trabajan similarmente bajo los mismo lineamientos estratégicos en el ámbito social.

Dicha organización se encuentra ubicada en Bolonia, óptica Nicaragüense 1c. Arriba, 1½c. Sur, Managua. Actualmente MS cuenta con un personal de 20 Personas tanto del área de administración, como de Proyectos, contabilidad, comunicación, etc.
Con el objetivo de mantener la seguridad y el efectivo funcionamiento tecnológico de los recursos de TI con los que cuenta la Organización, se recurre al servicio de Outsourcing con diferentes empresas proveedoras de este servicio. A continuación se detalla información específica del Área.

## I. PERSONAL MS

Se cuenta con 20 miembros que laboran para diferentes áreas, de estas 16 personas hacen uso del servicio de Internet, de Equipos PC de Escritorio y algunos Portátiles, servicio de impresión, correo electrónico y acceso al Servidor de Red.

Las tareas con respecto a la administración del área informática están divididas bajo las responsabilidades de tres personas: El Administrador Regional- Administración de la Red, Contratación Externa, Recursos Humano, el Oficial Administrativo Financiero– Software de Navision, Infraestructura, Capacitación y Oficial Administrativo Logístico- Mantenimiento, distribución y Adquisición de nuevos Equipos, Proveedores, Inventarios.

Actualmente una persona es la responsable de mantener la seguridad lógica de los sistemas informáticos pero no del área en sí.
Otros Organismos: Refiriéndonos al área Informática los servicios de TI son prestados a los Organismo HABTAT, Solidaridad infantil y Asociación Danesa de Discapacitados.

## II. SERVIDOR – BACKUP, E- mail, Net User

Usualmente se crean nuevos usuarios dentro de la red que coinciden con el nombre de sesión de equipo, que tendrá el usuario creando la misma contraseña. Además se crean

los permisos en la carpeta a las que tendrá acceso en el directorio F: DATOS y el respectivo archivo script que crea la conexión entre el equipo y el servidor.

***Arquitectura de la Información:***

La arquitectura de la información no está claramente definida desde los sistemas de información. En cuanto a los usuarios finales conocen poco sobre cómo está estructurada y almacenada la información en las unidades del servidor de red.

## III. Cuenta de Correo.

Las cuentas de correo electrónico se crean en MDaemon, que es el programa administrador de correos en el servidor. Este programa tiene una carpeta especial que guarda los correos basura, con más de un mes de antigüedad, se conserva un mes de correos basura porque algunos correos buenos son retenidos como correos basura y que se pueden liberar y ubicar en la lista de correos seguros. Además el Outlook express Versión 2007 del servidor, debe estar abierto porque este recibe todos los correos equivocados que deben ser borrados periódicamente.

## IV. Respaldo de la información.

El respaldo en el disco duro externo se elabora de manera semanal los lunes: se copian las carpetas de correos, datos y Navision del directorio H: Respaldo al disco duro externo. El servidor realiza semanalmente y automáticamente copias de las carpetas ubicadas en otros directorios hacia el directorio respaldo.

**Copias de seguridad:** Información almacenada en el Servidor.

- Respaldo del Sistema de Datos
- Respaldo del Sistema de Correo Outlook 2007
- Respaldo del Sistema de Contabilidad Navision
- Respaldo del Sistema

## V. CONTRATACIÓN EXTERNA

- **SEQUINSA***:* Brinda los servicios de técnicos de mantenimiento en computación y redes, con aproximadamente una relación de servicio de 5 años con MS-AMERICA CENTRAL.
- **AMNET:** Es la proveedora del servicio de internet Platinium 1mbps (con capacidad de 1024 Kbps) y maneja el dominio cam.org.ni. Con aproximadamente de 2 años

de servicio, con este se sostiene un contrato de servicio formal el cual contiene Procedimientos de atención a fallos, políticas de uso aceptables de productos y servicios, Acuerdos de nivel de servicio. Hasta la fecha AMNET ha brindado soporte técnico al usuario de acuerdo al procedimiento y tiempos establecidos de manera satisfactoria. Además brinda el mantenimiento adecuado a la red externa y los equipos de su propiedad, así como repararlos o restituirlos en casos necesarios.

- **UNI:** Es el proveedor del **dominio cam.org.ni** a quien se le paga anual.

## VI. ACCESS POINT

Existen 5 equipos de acceso a internet "Access Point" ubicados en: 1 - en el servidor, 2- Oficina de asesor de información, 3- Oficina del coordinador del proyecto de jóvenes, 4- en la sala de espera del segundo piso y 5 – Guardado en bodega. Los códigos de administración y navegación de todos estos equipos están en la lista de contraseñas que ese encuentra en manos del Administrador.

## VII. PASSWORD

La lista de contraseñas de todos los programas y equipos los maneja el Administrador y el Oficial logístico administrativo – Administración MS. Cada usuario de equipo maneja su contraseña de e- mail y de usuario en el servidor que es el mismo usuario de Windows de cada equipo, además cada usuario maneja la contraseña de candado de laptops. Se recomienda a todos los usuarios de equipo cambiar la contraseña del Windows y e- mail mensualmente de ser posible, el momento de este cambio también se debe cambiar en el servidor.

## VIII. ANTIVIRUS

Dar mantenimiento y seguimiento a Symantec Antivirus ™ Versión 10.1, mantener la seguridad de la red libre de Virus, intrusos, etc.

## IX. CONTROLES

Los controles definidos para el área de TI son definidos, evaluados y aprobados por la alta gerencia, esta se encarga de valorar que controles se necesitan para una mejor administración, tanto de los recursos, como del desarrollo de las diferentes actividades de TI, en la práctica aun hacen falta controles específicamente para el área informática.

Es importante recalcar que MS- AMERICA CENTRAL en sus años de trabajo en Nicaragua no se le ha realizado ningún tipo de Auditoria, estudio e investigación que les permita tener una visión sobre la administración de la actividades y de la plataforma de TI en general

## HIPOTESIS

"La gerencia que evalúa continuamente la efectividad de los controles y procedimientos informáticos tienen menor riesgo ante pérdidas económicas, humanas y físicas de sus activos."

# DISEÑO METODOLOGICO

## Metodología de Cobit

Toda investigación sin ser esta una excepción tiene grandes fases: *elección del tema, planteamiento del problema, marco teórico y diseño metodológico.* Las dos primeras responden al qué investigar, la tercera constituye el sustento teórico de la investigación. Finalmente se encuentra el diseño metodológico, que se refiere al *cómo* se lleva a cabo el mencionado proceso. Es en este diseño donde se describen las decisiones metodológicas tanto para la recolección de datos como para el análisis de los mismos. Específicamente, en este trabajo se presentan aspectos relacionados con el proceso de análisis evaluación del entorno informático con énfasis en la seguridad informática.

Para el abordaje de este se definió los aspectos metodológicos u operacionales del proyecto de investigación, el cual se especifican a continuación.

**Tipo de Estudio:** Según el análisis y alcance de resultados el tipo de estudio se definió como Analítico, Explicativo.
El método analítico permitió hacer uso del conocimiento para la identificación de cada una de las partes que caracterizan el área de informática de MS- América Central estableciendo de esta manera la relación causa- efecto entre los elementos que componen el objeto de investigación.

Es un Estudio Explicativo porque va más allá de la descripción de conceptos o fenómenos o del establecimiento de relaciones entre conceptos; este estudio se dirigió a fin de responder a las causas de los fenómenos estudiados. Su interés se centró en explicar por qué ocurre un fenómeno y bajo qué condiciones éste se da.

**Universo y Muestra:** El universo está constituido por el área Administración, Contabilidad, Comunicación, Proyectos todas correlacionadas con el Área de Informática del Organismo Internacional MS – América Central, ubicada sus instalaciones en la Ciudad de Managua, así mismo se delimito el tamaño de la muestra escogiendo los elementos al azar para garantizar la representatividad de cada una de las unidades de análisis del universo.

La metodología para el desarrollo e implementación de la Auditoría en Informática se describe su intervención a través de:

**PROCESO METODOLOGICO**

- **DESARROLLO DEL MODELO**

La presente metodología es una propuesta de evaluación de la seguridad informática para el área informática del Organismo internacional MS América Central, utilizando una de las mejores prácticas en la administración de la tecnología de información como lo es Cobit 4.1.

Una de las motivaciones que llevaron al desarrollo de este proyecto fue la de proveer al Organismo de una herramienta para realizar un auto-diagnóstico de su plataforma de tecnología de información, a fin de darle continuo seguimiento y cumplimiento a lo dispuesto en el Marco Normativo de Cobit como una estrategia. El periodo auditado comprende de Enero a Diciembre del 2010.

Por ello, la metodología de evaluación planteada entre sus actividades la evaluación de los procesos de tecnología de información de acuerdo a los objetivos de control de Cobit 4.1, adicionalmente se utilizan los modelos de madurez, los conductores de valor, los conductores de riesgo, las pruebas de diseño de controles de Cobit 4.1, y la valoración del impacto en el negocio a partir del análisis de los resultados obtenidos durante la fase 2.

Con las calificaciones obtenidas se elaboran mapas, gráficos estadísticos y matrices concentradoras de resultados, lo que permitirá a la Organización ir madurando progresivamente sus procesos de Tecnología de información hacia la obtención de un buen gobierno de TI.

**Introducción al Marco Normativo de Cobit**

La misión de Cobit es Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.

La orientación al negocio que enfoca COBIT consiste en alinear las metas de negocio con las metas de TI, brindando métricas y modelos de madurez para medir sus logros, e

identificando las responsabilidades asociadas de los dueños de los procesos de negocio y de TI.

El enfoque COBIT se ilustra con un modelo de procesos, el cual subdivide TI en 34 procesos de acuerdo a las áreas de responsabilidad de planear, construir, ejecutar y monitorear, ofreciendo una visión de punta a punta de las TI. Los conceptos de arquitectura empresarial ayudan a identificar aquellos recursos esenciales para el éxito de los procesos, es decir, aplicaciones, información, infraestructura y personas.

En resumen, para proporcionar la información que la empresa necesita para lograr sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos agrupados de forma natural.

Los objetivos de control se han desarrollado para su aplicación en el amplio aspecto de sistemas de información en la empresa. Estos tienen en cuenta lo siguiente:

- Adecuación a los estándares y normativas legislativas
- Revisión crítica de las diferentes actividades y tareas bajo los dominios de control.
- Establecimiento de directrices y fundamentos para proporcionar investigación consistente sobre los temas de auditoría y control de TI.

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

**CRITERIOS DE INFORMACIÓN DE COBIT**

Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

- *La efectividad:* tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
- *La eficiencia:* consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos.
- *La confidencialidad:* se refiere a la protección de información sensitiva contra revelación no autorizada.
- *La integridad:* está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

- *La disponibilidad:* se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- *El cumplimiento:* tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
- *La confiabilidad:* se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

El sistema consiste en objetivos de control de TI de alto nivel y una estructura global para su clasificación y funcionamiento. La teoría para la clasificación elegida, en línea con las experiencias de Re-Ingeniería, en esencia hay tres niveles de esfuerzos en TI cuando se considera la gestión de los recursos de TI:

- **Actividades:** las actividades, junto con las tareas están en el nivel inferior. Las actividades tienen el concepto de ciclo de vida mientras que las tareas se consideran discretas en el tiempo.
- **Procesos:** se definen en un nivel superior como series de actividades unidas con puntos de control naturales.
- **Dominios:** correspondientes al nivel superior, son agrupaciones de procesos. COBIT distingue cuatro dominios en línea con el ciclo de gestión o el ciclo de vida aplicables a los procesos de TI.

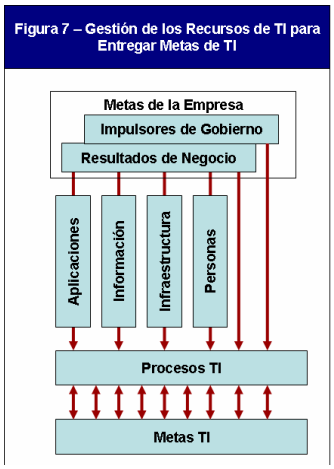
**Los recursos de TI identificados en COBIT se pueden definir como sigue:**

- *Aplicaciones:* incluyen tanto sistemas de usuarios automatizados, como procedimientos manuales que procesan información.
- I*nformación:* son los datos en todas sus formas, de entradas, procesados y generados por los sistemas de información, en cualquiera de sus formas en que sean utilizados por el negocio.
- *Infraestructura*: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc.,

así como el sitio donde se encuentras y el ambiente que lo soporta) que permiten el proceso de aplicaciones.

- *Personas*: son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los Sistemas y los servicios de información. Estas pueden ser internas, por Outsourcing o contratadas, de acuerdo a como se requieran.

**Grafico 1:** Gestión de los Recursos de TI para Entregar metas de TI

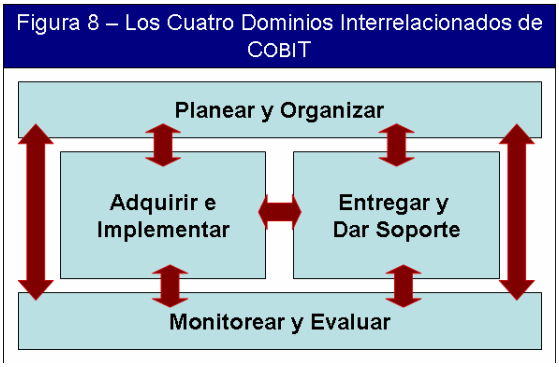



COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se facilitaran a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados.

Dentro del marco de COBIT, estos dominios, como se muestra en la Figura 8, se llaman: *Planear y Organizar (PO)* – Proporciona dirección para la entrega de soluciones (AI) *y la entrega de servicio (DS)*, *Adquirir e Implementar (AI)* – Proporciona las soluciones y las pasa para convertirlas en servicio, *Entregar y Dar Soporte (DS)* – Recibe las soluciones y las hace utilizables por los usuarios finales, *Monitorear y Evaluar (ME)* -Monitorear todos los procesos para asegurar que se sigue la dirección provista.

**Grafico 2:** Los Cuatro Dominios Interrelacionados de COBIT




**Fuente:** Cobit 4.1

El marco conceptual se enfoca desde tres puntos de vista distintos: criterios de gestión para la información, recursos de TI y procesos de TI. Estos tres puntos de vista se ensamblan en un formato cúbico y permiten que se obtengan referencias cruzadas en dicho marco y se pueda acceder a él eficientemente.

Los objetivos de control de TI están organizados inicialmente por proceso/actividad, pero las ayudas para la navegación que se aportan, facilitan la entrada desde cualquier punto estratégico. También facilitan la adopción de enfoques combinados o globales, tal como la instalación/implementación de un proceso, responsabilidades de gestión global para un proceso, y el uso de los recursos de TI por un proceso. La información que los procesos de gestión necesitan está proporcionada por el uso de los recursos de TI.

Para asegurar que los requisitos de gestión para la información se aplican, se tienen que definir medidas de control adecuadas, para implementar y monitorear estos recursos. Está claro que no todas las medidas de control satisfacen los requisitos de gestión en el mismo grado, así que se hace una distinción en COBIT contemplando el cumplimiento:

- **Primario (P):** grado en que el objetivo de control satisface completamente el requisito de información correspondiente.
- **Secundario (S):** grado en que el objetivo de control satisface solamente en menor extensión o indirectamente el requisito de información correspondiente.

Muchos estudios han identificado que la falta de transparencia en los costos, valor y riesgos de TI, es uno de los más importantes impulsores para que exista el gobierno de TI.

COBIT se enfoca en qué se requiere para lograr una administración y un control adecuado de TI, y se posiciona en un nivel alto. COBIT ha sido alineado y armonizado con otros estándares y mejores prácticas más detallados de TI, (vea Apéndice IV). COBIT actúa como un integrador de todos estos materiales guía, resumiendo los objetivos clave bajo un mismo marco de trabajo integral que también se alinea con los requerimientos de gobierno y de negocios.

- **FASES DE LA METODOLOGA**

La metodología utilizada contempla 3 fases para el desarrollo del Modelo de Auditoria basado en la aplicación del Marco Normativo de Cobit 4.1.

**Fase 1:** ***Planeación de la Auditoria***

Con el propósito de interpretar adecuadamente la aplicación de esta fase se especifican los procedimientos secuenciales que la componen.

**P.1. Identificar el origen de la Auditoria**

Se plantea el origen de la auditoria a partir de la solicitud expresa de procedencia externa, esta surge de una petición formal de alguien ajeno a la organización, a quien por alguna causa le interesa que sean auditados los sistemas computacionales del área informática. En el caso concreto es solicitado y desarrollado por el grupo de estudiantes de la Universidad Nacional Autónoma de Nicaragua con el tema de Auditoria en Seguridad informática para la culminación del seminario de grado 2010 impulsado y respaldado por la UNAN- Managua.

**P.2. Realizar una vista preliminar al área que será evaluada**

En este sentido la Visita preliminar juega un papel importante para la definición consecutiva del proceso metodológico, ya que esta permitió mejorar los objetivos de auditoría presentados durante la visita preliminar, iniciando a través de un documento formal, así mismo se delimito el alcance de la Auditoria y se logró establecer una relación formal de cooperación por parte del personal para el desarrollo de la auditoria, lo que facilito identificación de la problemática central.

Como resultado de este inciso se calculan los recursos y el personal necesario para la realización y la implementación del procedimiento de auditoría (Ver Anexo. Presupuesto de Auditoria) y se describen los objetivos planteados para el caso de estudio.

**P.3. Establecer los objetivos de la Auditoria**

En este particular se logra establecer el alcance del estudio a través de la definición del Objetivo General y 6 Objetivos específicos los cuales contienen en síntesis:

1. El análisis de la administración de Dirección Informática de MS- América Central según estrategia de Gobierno de TI de Cobit 4.1.
2. Evaluar la existencia normas, y políticas relativas a la seguridad.

3. Revisar el nivel de seguridad de los recursos de TI.
4. Proceso del Outsourcing tecnológico en la organización.
5. El nivel de riesgo en las TI.
6. Emisión de resultados de auditoría.

**P.4. Determinar los puntos que serán evaluados en la Auditoria**

Una vez que se determinó el origen, objetivos concretos que se pretenden alcanzar, es de suma importancia destacar los puntos que fueron evaluados durante el periodo auditado.

**ELEMENTOS AUDITADOS EN EL CONTEXTO DEL OBJETIVO EN ESTUDIO "SEGURIDAD INFORMATICA"**

Los elementos fueron identificados a través del estudio de sitio como punto de partida para la delimitación del proceso de Auditoria, evaluó exhaustivamente cada uno de los elementos que componen el centro de cómputo en estudio, que se resumen en la Tabla 1. En la investigación se ha tenido en cuenta todos aquellos elementos o recursos que pueden interactuar con los diferentes sistemas de información alineados con el alcance de la Auditoria, esto incluye a usuarios, personal interno y externo (Recursos humanos y activos).

A continuación se describe la Escala de Evaluación aplicados a los elementos y Criterios de Información considerados en el proceso de auditoria

**TABLA1: Escala de Evaluación de los Elementos Auditados**

| Escala de Evaluación Tablas de COBIT | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| | No existe | Muy deficiente | Deficiente | Regular | Bueno | Excelente |

**TABLA 2: Aplicación Escala en Elementos del Área de Informática de Ms- América Central**

| ELEMENTOS | Planificación | Adquisición | Mantenimiento | Seguridad | Servicio |
|---|---|---|---|---|---|
| **Gerencia** | 4 | | | | |
| **Responsable Informática** | 3 | 4 | | | |
| **Técnicos Informática** | | | 4 | 3 | 4 |
| **Webmaster** | 4 | 4 | 4 | 4 | 4 |
| **Administrador Seguridad** | | 4 | | 4 | |
| **Personal MS** | | | | | 4 |

| | | | | | |
|---|---|---|---|---|---|
| **(proyectos, administración y finanzas, comunicación.)** | | | | | |
| **Infraestructura** | | | | | 4 |
| **Usuarios** | | | | | 4 |
| **Tecnologías** | | 4 | 4 | 4 | |
| **Marco Legal** | 4 | 4 | 4 | 4 | 4 |
| **Marco Normativo Estándares** | 4 | 4 | 4 | 4 | 4 |
| **Proveedores (Servicios y licencias,)** | | 4 | 4 | 3 | |
| **HW Base: Servidores** | | | 4 | 3 | 4 |
| **HW Redes** | | | 4 | 4 | 4 |
| **SW Base: Sistemas Operativos y Servicios Web** | | | 4 | 5 | 4 |
| **SW Redes** | | | 4 | 4 | 4 |
| **SW BD** | | | 4 | 4 | 4 |
| **SW Aplicación** | | | 4 | 4 | 4 |
| **Datos e información** | | | | 4 | |

**CRITERIOS DE INFORMACION DE COBIT**

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio.

Con base en los requerimientos más amplios de calidad, fiduciarios y de seguridad, se definieron los siguientes siete criterios de información:

**TABLA 3: Descripción de los Criterios de Información**

| Código de Asignación | Criterio de Información | DESCRIPCION DEL CRITERIO |
|---|---|---|
| **01** | **Efectividad** | Tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable. |
| **02** | **Eficiencia** | Consiste en que la información sea generada con el óptimo (más productivo y económico) uso de los recursos. |
| **03** | **Confidencialidad** | Se refiere a la protección de información sensitiva contra revelación no autorizada. |

| | | |
|---|---|---|
| **04** | **Integridad** | Está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio. |
| **05** | **Disponibilidad** | Se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas. |
| **06** | **Cumplimiento** | Tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas. |
| **07** | **Confiabilidad** | Se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno. |

**TABLA 4: Evaluación de los Criterios de Información**

| Elementos | 01 | 02 | 03 | 04 | 05 | 06 | 07 |
|---|---|---|---|---|---|---|---|
| Gerencia | 4 | | | | | 4 | |
| Responsable Informática | 4 | | | | | 4 | |
| Técnicos Informática | 4 | | | 4 | | 4 | |
| Webmaster | 4 | | | 4 | 4 | 4 | |
| Administrador Seguridad | 4 | | 4 | 4 | 4 | 4 | 4 |
| Personal MS (proyectos, administración y finanzas, comunicación.) | | | | | | | |
| Infraestructura | | | | 4 | | 4 | 4 |
| Usuarios | | | | 4 | | | |
| Tecnologías | 4 | | 4 | 4 | 4 | | 4 |
| Marco Legal | | | | | | | |
| Marco Normativo Estándares | 4 | | 4 | 4 | 4 | 4 | 4 |
| Proveedores | 4 | | 4 | 4 | 4 | 4 | |
| HW Base: Servidores | | | | 4 | 4 | | 4 |
| HW Redes | | | | 4 | 4 | | 4 |
| SW Base: Sistemas Operativos, Servidor de Red | | | | 4 | 4 | 4 | 4 |
| SW Redes | | | | 4 | 4 | | 4 |
| SW BD | | | | 4 | 4 | 4 | 4 |
| SW Aplicación | | | | 4 | 4 | 4 | 4 |
| Datos e Información | | | 4 | 4 | 4 | | 4 |

**MAPEO OBJETIVOS DE CONTROL, PROCESOS DE TI Y AREAS FOCALES**

Inicialmente se identifican lo Objetivos de Control aplicables al caso de estudio, así como los dominios y procesos determinados por la Metodología de COBIT, para la incorporación de la Seguridad Informática en las actividades desarrolladas por el Área

Informática como son: Planificación, Adquisición, Mantenimiento, Administración y Servicio y por último la Evaluación y Monitoreo. Para ellos se determina el nivel de cumplimiento de los Objetivos, se utilizan los términos de relación es decir la P, en COBIT se utiliza cuando hay una relación primaria y la S cuando solamente existe una relación secundaria.

A continuación, para cada uno de los procesos que se relacionan con las funciones identificadas, con un grado de cumplimiento P o S, el hecho que no exista una P o S no significa que no exista una relación, solo que es menos importante o marginal. Por ejemplo, para el proceso P01, Definir un plan estratégico de TI, la función de Planificación debe auditarse, el auditor debe comprobar si existen planes a largo corto plazo desarrollados por la alta gerencia para contar a nivel de todos los recursos con la seguridad informática requerida para el ejercicio efectivo de las actividades de TI.
La siguiente tabla está apoyada por la utilización de la herramienta metodológica del Marco Normativo de COBIT 4.1

**TABLA 5:** Dominios y Procesos de COBIT que intervienen sobre las funciones del Área en Estudio

| ESTRUCTURA DE COBIT | | INCORPORACIÓN DE LA SEGURIDAD INFORMATICA | | | | |
|---|---|---|---|---|---|---|
| **PROCESO** | **DENOMINACIÓN PROCESO** | **Planificación** | **Adquisición** | **Mantenimiento** | **Admon y Servicios** | **Monitoreo y Evaluación** |
| **DOMINIO: Planear y Organizar** | | | | | | |
| **PO2** | Definir la Arquitectura de la Información | **P** | | | **S** | |
| **PO3** | Determinar la Dirección Tecnológica | **S** | **P** | | **P** | |
| **PO4** | Definir los Procesos, Organización y Relaciones de TI | **S** | | | **P** | **P** |
| **PO5** | Administrar la Inversión en TI | **P** | **P** | **S** | **P** | **S** |
| **PO6** | Comunicar las Aspiraciones y la Dirección de las Gerencia | **S** | | | **S** | **S** |
| **PO9** | Evaluar y Administrar los Riesgos de TI | **p** | | | **P** | |
| **DOMINIO: Adquirir e Implementar** | | | | | | |
| **AI3** | Adquirir y Mantener Infraestructura Tecnológica | | | | **P** | |
| **AI4** | Facilitar la Operación y el uso | **S** | | | **P** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **AI5** | Adquirir recursos de TI | | | | **P** | |
| **DOMINIO: Entregar y Dar Soporte** | | | | | | |
| **DS1** | Definir y administrar los Niveles de Servicio | **P** | **P** | | **P** | **P** |
| **DS2** | Administrar los Servicios de Tercero | | | | **P** | **S** |
| **DS5** | Garantizar la Seguridad de los Sistema | | | | **P** | |
| **DS7** | Educar y Entrenar a los Usuarios | **P** | **P** | | | **S** |
| **DS10** | Administrar los Problemas | | | | **P** | **S** |
| **DS11** | Administrar los Datos | | | | **P** | |
| **DS12** | Administrar el Ambiente Físico | | | | **P** | |
| **DS13** | Administrar las Operaciones | | | | **P** | **P** |
| **DOMINIO: Monitorear y Evaluar** | | | | | | |
| **M1** | Monitorear y evaluar el Desempeño de TI | **S** | **S** | **S** | **S** | **P** |
| **M3** | Garantizar el Cumplimiento de Requisitos Externos | **P** | | | **P** | **P** |
| **M4** | Proporcionar Gobierno de TI | **P** | **P** | **P** | **P** | **P** |

**P.5. Elaborar planes, programas y presupuestos para realizar la auditoria, para ello se realizó el siguiente análisis:**

Planeación del Plan de Auditoria: se elaboró un instrumento de apoyo, para el equipo auditor denominado Plan de Auditoria.

El formato consiste que para cada objetivo de auditoría existen varios objetivos de control, para cada uno de ellos se elaboró el Plan de Auditoria de tal manera que de acuerdo a la descripción del Objetivo de Control Cobit 4.1 se definen los criterios de seguridad que serán en este caso el determinante a considerar durante la investigación, así mismo se define una numeración y la fecha de aplicación del instrumento.

En sí este instrumento apoyó a orientar y a desarrollar el proceso de evaluación al equipo auditor, en la secuencia del alcance según objetivos específicos de Auditoria, los cuales apuntan a objetivos de control de Cobit 4.1.

**Presupuesto de Auditoria.**

Se realiza una estimación de los costos tanto de los recursos humanos como materiales e informáticos. (Ver detalle del Presupuesto en Anexo. Presupuesto de Auditoria). En términos generales se detallan los gastos incurridos antes, durante y después del proceso de Auditoria.

**P.6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoria.**

**Técnicas e instrumentos:** Los métodos para recolección de datos utilizados durante la auditoria fueron la encuesta, para obtener información sobre la base de preguntas escritas, la observación, para confirmar o constatar la información obtenida en las diferentes áreas visitadas utilizando como instrumento las listas de verificación o Check List.

Las técnicas utilizadas en la recolección de datos es la entrevista, ya que permite orientar a los sujetos de estudio sobre la información solicitada, ficha bibliográfica; para obtener datos de diferentes libros que respaldan el marco teórico, esta como fuente primaria y como fuente secundaria trabajos monográficos y web grafía; las visitas de campo, para llegar a los sujetos de estudio en el lugar de trabajo, en cada una de las áreas correlacionadas con las actividades de TI; el instrumento utilizado para la recolección de datos es: el cuestionario, que está diseñado con preguntas, cerradas, abiertas y categorizadas, dirigidas a los sujetos de estudio.

El análisis de acuerdo con el enfoque cuantitativo o cualitativo, se hace al final de cada fase para facilitar la emisión de resultados o durante toda la investigación como es el caso de los diseños cualitativos.

El análisis de los datos y evaluación de procesos del presente proyecto se ha llevado a cabo a través de matrices descriptivas denominadas Diseño de Pruebas y Resultado (Ver Anexo Matrices de Pruebas y resultados), que recuperan la información desde diferentes técnicas y fuentes, tales como: la observación, el análisis documental, entrevistas, cuestionarios, etc.

Finalmente la Obtención de Información para dicho efecto se solicitó las siguientes fuentes:

- ✓ Políticas, normas, estándares y procedimientos.
- ✓ Planes de seguridad y Planes de acción
- ✓ Contratos
- ✓ Organigrama y descripción de funciones.
- ✓ Documentación de aplicaciones y de paquetes
- ✓ Inventarios: de soporte, de aplicaciones. de datos (diccionario de datos) y clasificación.
- ✓ Topologías de redes. Cortafuegos y sus parámetros, reglas y opciones.
- ✓ Registros: de problemas, de cambios, de visitas, de accesos lógicos producidos.
- ✓ Documentación de planes de contingencia/continuidad y sus pruebas.
- ✓ Programas y su documentación e historial de cambios, incluyendo versiones fuente en su caso.
- ✓ Resultados de pruebas realizadas y de las herramientas aplicadas: a programas, en cuanto a vulnerabilidad de redes.
- ✓ Información sobre sistemas operativos y software de bases en general, incluidos gestores de bases de datos: versiones, parches, opciones y parámetros; parte de la documentación general puede resultar accesible a través del fabricante y su Web, o la tendremos de otros proyectos.

**Herramientas:** Para el análisis profundo y desarrollo de pruebas se utilizaron herramientas específicas de acuerdo a los requerimientos de aplicación.

**1. Herramientas de Auditoria según su función:**

Herramientas de Software de Sistema: Estas se refieren a las herramientas básicas integradas. En el sistema Operativo en este caso Windows, como son copias de seguridad, Firewall, etc.

**2. Herramientas de Auditoria Informática:**

NESSUS 4.4 para el análisis de la vulnerabilidad de la Red: conocido también como “El escáner de vulnerabilidades Nessus” tiene una alta velocidad de descubrimientos, auditoria de configuración, perfilado de activos, descubrimiento de información sensible y análisis de vulnerabilidades del punto de vista de la seguridad de la organización.

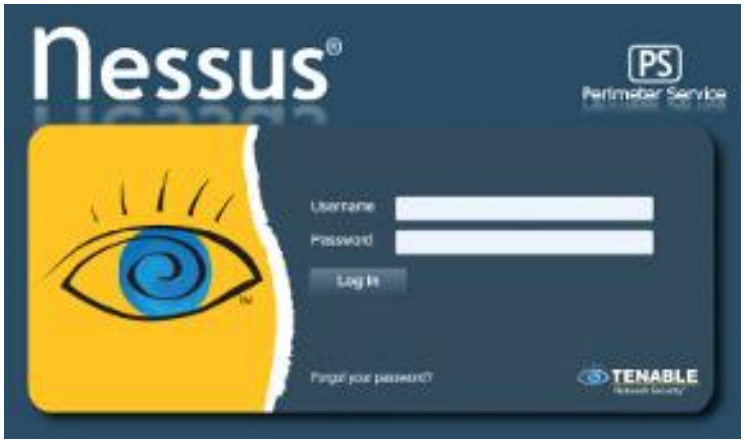
El Nessus Perimeter Service es un servicio de escaneo remoto de vulnerabilidades de categoría empresarial que puede ser usado para auditar las direcciones IP conectadas a Internet en busca tanto de vulnerabilidades de aplicaciones web como de red.

Desarrollado por Tenable está en la actualidad ofrece esa misma tecnología como un SaaS o modelo alojado para un despliegue más sencillo y rápido, provee auditorias de terceros de las infraestructuras conectadas a Internet. Realiza un barrido básico, pero eficiente de los sistemas de nuestra red, buscando fallos en la configuración de la red y vulnerabilidades de aplicaciones. Nessus se considera como una aplicación cliente/servidor.

Tiene su propia base de datos de usuario y un método de autentificación segura, por lo que los usuarios remotos que utilicen el cliente Nessus (ya sea para Unix o Windows) pueden iniciar una sesión, configurar un rastreo de vulnerabilidades y dejarlo preparado.

Los creadores de Nessus hicieron un lenguaje de series de comandos denominados Lenguaje de creación de series de comando de ataque para Nessus (NASL) para ser usado con su producto. En Nessus cada rastreo de vulnerabilidades es en realidad una serie de comandos o complemento diferente, escrito en NASL. Esta arquitectura modular permite añadir fácilmente rastreos (y posibles pruebas de ataque) a medida que se descubre nuevas vulnerabilidades.

**Grafico 3:** Herramienta NESSUS



Algunos beneficios que se reciben de esta herramienta es que:

- Los escaneos puede iniciarse inmediatamente o de forma programada mediante un sencillo navegador web o con la aplicación Nessus.
- Capacidad para preparar evaluaciones de seguridad para los estándares PCI actuales.
- Acceso a la base de conocimientos más confiable de la industria que detecta más de 40.000 verificaciones únicas de seguridad.
- Auditoría segura y confiable de terceros con cifrado punta a punta.

Para su implementación se desarrolla herramienta en la segunda fase de Auditoría

**3. Herramientas de Diseño:**

**Visio 2007:** Para el diseño de Sitio Web conceptual de la página web de MS- AMERICA CENTRAL, Diagrama de Gantt para el diseño del Cronograma de Actividades del proceso de Auditoria y Seminario de Graduación, Mapas y diseños de Planos de Acceso y Seguridad y Distribución de Plantas. Y finalmente el Diagrama de Auditoria y Organigramas. Para su aplicación

**4. Herramientas para la Emisión de Resultados y Análisis estadísticos:**

Word 2007 para elaboración del Informe de Auditoría y Trabajo de Seminario.
Excel 2007: Para la elaboración de algunos papeles de trabajo y presupuestos
PowerPoint 2007: Presentación dinámica de los resultados del informe de Auditoría en Pre defensas y defensa final.

**P.7. Asignar los recursos y sistemas a evaluar para la auditoria.**

Para finalizar la fase 1 se especifican los sistemas a evaluar, en cuanto a los recursos se asignan de acuerdo a las necesidades ya sean estas: Monetarios, recursos humanos, etc.

Aplicaciones: Software Navision
Información: Datos
Infraestructura: Sistema de Red, Sistema de control de acceso a los sistemas, seguridad física, seguridad lógica. Local.
Personas: Capacitación, seguridad, Roles, etc.

## Fase 2: *Ejecución de la Auditoria*

**E.1.** Realizar las acciones programadas para la auditoria

Para ello se echa andar el Cronograma de Auditoria *(Ver anexo: Cronograma de Auditoria)*

**E.2.** Aplicar los instrumentos y herramientas para la Auditoria

Haciendo uso y aplicación del estándar para Auditoria se describe su inducción al mismo.

**Navegación en el Marco de Trabajo COBIT**

Para cada uno de los procesos TI de COBIT, se proporciona un objetivo de control de alto nivel, junto con las metas y métricas clave en forma de cascada Introducción a los Componentes Esenciales de COBIT.

El marco de trabajo de COBIT está compuesto de los siguientes componentes esenciales, incluidos en el resto de esta publicación y organizados en los 34 procesos de TI, brindando así una visión completa de cómo controlar, administrar y medir cada proceso. Cada proceso está cubierto en cuatro secciones, y cada sección constituye aproximadamente una página, de la manera siguiente:

• La sección 1 contiene una descripción del proceso que resume los objetivos del proceso, con el objetivo de control de alto nivel representado en formada de cascada.

Esta página también muestra el mapeo de este proceso con los criterios de información, con los recursos de TI y con las áreas de enfoque de gobierno de TI, indicando con una P la relación primaria y con una S la secundaria.

La sección 2 contiene los objetivos de control detallados para este proceso.

La sección 3 contiene las entradas y salidas del proceso, la matriz RACI, las metas y las métricas.

La sección 4 contiene el modelo de madurez para el proceso.

**Grafico 4:** Aplicación de Descripción del Proceso Usando Cobit 4.1

MS América Central
actionaid denmark

## AUDITORIA DE SEGURIDAD INFORMATICA

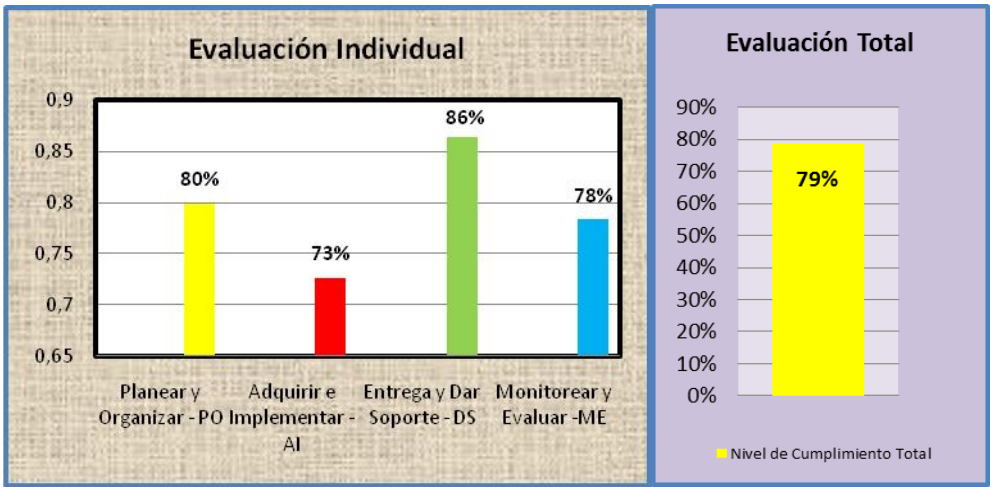
RESUMEN EVALUACIÓN CRITERIOS
INSTRUMENTO DE EVALUACION DEL NIVEL DE CUMPLIMIENTO
PROCESOS DE TI COBIT 4.1

### RESUMEN EVALUACIÓN CRITERIOS

| Rangos de clasificación del Cumplimientos de los procesos de TI: | Completado | Moderado | No alcanzado |
|---|---|---|---|
| | 100% - 81% | 80% - 60% | 59% - 0% |

| Criterios de Evaluación | | Total | Evaluación |
|---|---|---|---|
| Dominio: | Planear y Organizar – PO | 80% | Moderado |
| Dominio: | Adquirir e Implementar – AI | 73% | No Alcanzado |
| Dominio: | Entrega y Dar Soporte – DS | 86% | Completado |
| Dominio: | Monitorear y Evaluar –ME | 78% | Moderado |
| **Nivel de Cumplimiento de los Procesos de TI** | | **79%** | **Moderado** |

### GRAFICA DE EVALUACION DEL NIVEL DE CUMPLIMIENTO DE LOS PROCESOS DE TI




### CONCLUSION

En términos generales se evaluaron los Objetivos de Cobit en base a indicadores de Desempeño, este análisis de datos es obtenido a través de la recopilación de información suministrada durante la FASE I y II de Auditoria, lo que ubica al sistema de administración, planeación, control y monitoreo de las actividades de TI de MS- AMERICA CENTRAL en una clasificación de Moderado

**TABLA 6:** Aplicación de Descripción del Proceso- PO

# PLANEAR Y ORGANIZAR – PO

| Objetivo de Control | Control sobre el proceso de TI | Que satisface el requerimiento del negocio de TI | Enfocándose en | Se logra con | Y se mide con | Evaluación % de Cumplimiento |
|---|---|---|---|---|---|---|
| **PO2** | finir la arquitectura de la información | Agilizar la respuesta a los requerimientos, proporcionar información confiable y consistente, para integrar de forma transparente las aplicaciones dentro de los procesos del negocio | El establecimiento de un modelo de datos empresarial que incluya un esquema de clasificación de información que garantice la integridad y consistencia de todos los datos | La asignación de propiedad de datos | El porcentaje de aplicaciones que no cumplen con la metodología de arquitectura de la información usada por la empresa | 70% |
| **PO3** | Determinar la dirección tecnológica | Contar con sistemas aplicativos estándares, bien integrados, rentables y estables, así como recursos y capacidades que satisfagan requerimientos de negocio, actuales y futuros | La definición e implementación de un plan de infraestructura tecnológica, una arquitectura y estándares que tomen en cuenta y aprovechen las oportunidades tecnológicas | El establecimiento de un plan de infraestructura tecnológica equilibrado versus costo, riesgo y requerimientos. | Frecuencia de las revisiones/actualizaciones del plan de infraestructura tecnológica. | 60% |
| **PO4** | Definir los procesos, organización y relaciones de TI | Agilizar la respuesta a las estrategias del negocio mientras se cumplen los requerimientos de gobierno y se establecen puntos de contacto definidos competentes | El establecimiento de estructuras organizacionales de TI Transparentes, flexibles y responsables, en la definición e implementación de procesos de TI con dueños, la integración de roles y responsabilidades en procesos de negocio y de decisión | La definición de un marco de trabajo de procesos de TI | El porcentaje de roles con descripción de puestos y autoridad documentados | 70% |
| **PO5** | Administrar la Inversión en TI | Mejorar de forma continua y demostrable la rentabilidad de TI y su contribución a la rentabilidad del negocio con servicios integrados y estandarizados que satisfagan al usuario. | Decisiones de portafolio e inversión en TI efectivas y eficientes, y el establecimiento y seguimiento de presupuestos de TI de acuerdo a la estrategia de TI y a las decisiones de inversión. | El pronóstico y la asignación de presupuestos | El porcentaje de reducción en el costo unitario del servicio de TI | 85% |

| | | | | | | |
|---|---|---|---|---|---|---|
| **PO6** | Comunicar las Aspiraciones y la Dirección de la Gerencia | Una información precisa y oportuna sobre los servicios de TI actuales y futuros, los riesgos asociados y las responsabilidades | Proporcionar políticas, procedimientos, directrices y otra documentación aprobada, de forma precisa y entendible y que se encuentre dentro del marco de trabajo de control de TI a los interesados | La elaboración e implantación de políticas para TI | Porcentaje de interesados que entienden el marco de trabajo de control de TI de la empresa | 75% |
| **PO9** | Evaluar y administrar los riesgos de TI | Analizar y comunicar los riesgos de TI y su impacto potencial sobre los procesos y metas de negocio | La elaboración de un marco de trabajo de administración de riesgos el cual está integrado en los marcos gerenciales de riesgo operacional, evaluación de riesgos, mitigación del riesgo y comunicación de riesgos residuales | La garantía de que la administración de riesgos está incluida completamente en los procesos administrativos, tanto interna como externamente, y se aplica de forma consistente (1) | Porcentaje de objetivos críticos de TI cubiertos por la evaluación de riesgos | 50% |

| | |
|---|---|
| **Suma Total %** | **470%** |
| **Distribución del %** | **17** |
| **Cumplimiento Dominio PO %** | **80%** |

**TABLA 7:** Aplicación de Descripción del Proceso- AI

# ADQUIRIR E IMPLEMENTAR AI

| Objetivo de Control | Control sobre el proceso de TI | Que satisface el requerimiento del negocio de TI | Enfocándose en | Se logra con | Y se mide con | Evaluación % de Cumplimiento |
|---|---|---|---|---|---|---|
| **AI3** | Adquirir y dar mantenimiento a la infraestructura tecnológica | Adquirir y dar mantenimiento a una infraestructura integrada y estándar de TI | Proporcionar plataformas adecuadas para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología | La planeación de mantenimiento de la infraestructura | El número de procesos de negocio críticos soportados por infraestructura obsoleta (o que pronto lo será) | 75% |
| **AI4** | Facilitar la operación y el uso | Garantizar la satisfacción de los usuarios finales mediante ofrecimientos de servicios y niveles de servicio, y de forma transparente integrar las soluciones de aplicación y tecnología dentro de los procesos del negocio | Proporcionar manuales efectivos de usuario y de operación y materiales de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitosos del sistema. | La generación de materiales de entrenamiento | El número de aplicaciones que cuentan con un adecuado entrenamiento de apoyo al usuario y a la operación | 70% |
| **AI5** | Adquirir recursos de TI | Mejorar la rentabilidad de TI y su contribución a la utilidad del negocio | Adquirir y mantener las habilidades de TI que respondan a la estrategia de entrega, en una infraestructura TI integrada y estandarizada, y reducir el riesgo de adquisición de TI | La adquisición de hardware, software y servicios requeridos de acuerdo con los procedimientos definidos | El porcentaje de interesados clave satisfechos con los proveedores | 75% |

| | |
|---|---|
| **Suma Total %** | **220%** |
| **Distribución del %** | **33** |
| **Cumplimiento Dominio AI %** | **73%** |

**TABLA 8:** Aplicación de Descripción del Proceso- DS

# ENTREGAR Y DAR SOPORTE – DS

| Objetivo de Control | Control sobre el proceso de TI | Que satisface el requerimiento del negocio de TI | Enfocándose en | Se logra con | Y se mide con | Evaluación % de Cumplimiento |
|---|---|---|---|---|---|---|
| **DS1** | Definir y Administrar los niveles de servicio | Asegurar la alineación de los servicios claves de TI con la estrategia del negocio | La identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio | La formalización de acuerdos internos y externos en línea con los requerimientos y las capacidades de entrega | El porcentaje de Interesados satisfechos de que la entrega del servicio cumple con los niveles previamente acordados. | 90% |
| **DS2** | Administrar Servicios de Terceros | Brindar servicios satisfactorios de terceros con transparencia acerca de los beneficios, riesgos y costos | El establecimientos de relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados y el monitoreo de la presentación del servicio para verifica y asegurar la adherencia a los convenios | La identificación y mitigación de riesgo del proveedor | El porcentaje de los principales proveedores que cumplen claramente los requerimientos definidos y los niveles de servicios. | 90% |
| **DS5** | Garantizar la seguridad de los sistemas | Mantener la integridad de la información y de la infraestructura de procesamiento y minimizar el impacto de las vulnerabilidades e incidentes de seguridad | La definición de políticas, procedimientos y estándares de seguridad de TI y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad | El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad. Probando la seguridad de forma regular | El número de sistemas donde no se cumplen los requerimientos de seguridad<br>El número de de violaciones en la segregación de tareas | 65% |
| **DS7** | Educar y entrenar a los usuarios | El uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos | Un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados | Establecer un programa de entrenamiento | Lapso de tiempo entre la identificación de la necesidad de entrenamiento y la impartición del mismo | 80% |
| **DS10** | Administración de problemas | Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir | Registrar, rastrear y resolver problemas operativos; investigación de las causas raíz de todos los problemas | Analizando las tendencias | Porcentaje de problemas resueltos dentro del período de tiempo solicitado | 70% |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | el retrabajo y los defectos en la prestación de los servicios y de las soluciones | relevantes y definir soluciones para los problemas operativos identificados | | | |
| **DS11** | Administración de datos | Optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera. | Mantener la integridad, exactitud, disponibilidad y protección de los datos | Respaldando los datos y probando la restauración Administrando almacenamiento de datos en sitio y fuera de sitio. | Satisfacción del usuario con la disponibilidad de los datos. Porcentaje de restauraciones exitosas de datos. | 90% |
| **DS12** | Administración del ambiente físico | Proteger los activos de cómputo y la información del negocio minimizando el riesgo de una interrupción del servicio | Proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo | Implementando medidas de seguridad físicas. | Tiempo sin servicio ocasionado por incidentes relacionados con el ambiente físico | 85% |
| **DS13** | Administrar operaciones | Mantener la integridad de los datos y garantizar que la infraestructura de TI puede resistir y recuperase de errores y fallas | Cumplir con los niveles operativos de servicio para procesamiento de datos programado, protección de datos de salida sensitivos y monitoreo y mantenimiento de la infraestructura | Operando el ambiente de TI en línea con los niveles de servicio acordados y con las instrucciones definidas. Manteniendo la infraestructura de TI | Número de niveles de servicio afectados a causa de incidentes en la operación. Porcentaje de activos de hardware incluidos en los programas de mantenimiento. | 95% |

| | |
|---|---|
| **Suma Total %** | **665%** |
| **Distribución del %** | **13** |
| **Cumplimiento Dominio DS %** | **86%** |

**TABLA 9:** Aplicación de Descripción del Proceso- ME

# MONITOREAR Y EVALUAR- ME

| Objetivo de Control | Control sobre el proceso de TI | Que satisface el requerimiento del negocio de TI | Enfocándose en | Se logra con | Y se mide con | Evaluación % de Cumplimiento |
|---|---|---|---|---|---|---|
| **ME1** | Monitorear y evaluar el desempeño de TI | Transparencia y entendimiento de los costos, beneficios, estrategia, políticas y niveles de servicio de TI de acuerdo con los requisitos de gobierno | Monitorear y reportar las métricas del proceso e identificar e implementar acciones de mejoramiento del desempeño | Comparar el desempeño contra las metas acordadas e iniciar las medidas correctivas necesarias | Porcentaje de procesos críticos monitoreados | 60% |
| **ME3** | Garantizar el cumplimiento regulatorio | Cumplir las leyes y regulaciones | La identificación de todas las leyes y regulaciones aplicables y el nivel correspondiente de cumplimiento de TI y la optimización de los procesos de TI para reducir el riesgo de no cumplimiento | El monitoreo y reporte del cumplimiento de los requisitos regulatorios | Frecuencia de revisiones de cumplimiento | 90% |
| **ME4** | Proporcionar gobierno de TI | La integración de un gobierno de TI con objetivos de gobierno corporativo y el cumplimiento con las leyes y regulaciones | La elaboración de informes para el consejo directivo sobre la estrategia, el desempeño y los riesgos de TI y responder a los requerimientos de gobierno de acuerdo a las directrices del consejo directivo | El establecimiento de un marco de trabajo para el gobierno de TI, integrado al gobierno corporativo | La frecuencia de informes del consejo directivo sobre TI a los interesados | 85% |

| | |
|---|---|
| **Suma Total %** | **235%** |
| **Distribución del %** | **33,33** |
| **Cumplimiento Dominio ME %** | **78%** |

**Modelo de Madurez**

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar, como respuesta a esto, se debe desarrollar un plan de negocio para mejorar y alcanzar el nivel apropiado de administración y control sobre la infraestructura de información.

La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora.

El Modelo de Madurez o también llamado Perfiles de Procesos de TI, es una herramienta presentada en el estándar COBIT 4.1 para medir el nivel en que se encuentra la Organización, y la identificación de las mejoras necesarias, el cual se aplicó en el presente estudio.
Para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0), inicial (1), repetible pero intuitivo (2), definido (3), administrado (4), hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software.

Los niveles de madurez están diseñados como perfiles de procesos de TI que una empresa reconocería como descripciones de estados posibles actuales y futuros. No están diseñados para ser usados como un modelo limitante, donde no se puede pasar al siguiente nivel superior sin haber cumplido todas las condiciones del nivel inferior. Con los modelos de madurez de COBIT, a diferencia de la aproximación del CMM original de SEI, no hay intención de medir los niveles de forma precisa o probar a certificar que un nivel se ha conseguido con exactitud.

La ventaja de un modelo de madurez es que es relativamente fácil para la dirección ubicarse a sí misma en la escala y evaluar qué se debe hacer si se requiere desarrollar una mejora. Las escalas del modelo de madurez ayudarán a los profesionales a explicarle a la gerencia dónde se encuentran los defectos en la administración de procesos de TI y a establecer objetivos donde se requieran.

Los gráficos presentados a continuación representan el estado actual con relación al modelo de madurez, en el que se encuentra la organización usando como referencia los dominios utilizados durante la auditoria. Cabe señalar que si este se encuentra en diferentes niveles de madurez se debe que en algunos objetivos de control se realizan algunas acciones en menor nivel de requerimiento.

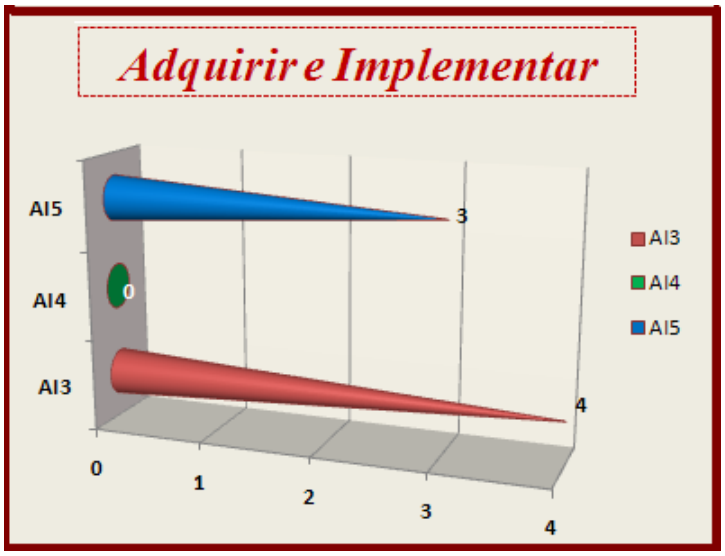
**DOMINIO: PLANEAR Y ORGANIZAR**


El grafico de nivel de madurez para el dominio planear organizar indica que se encontró a el objetivo de control (PO9) Evaluar y administrar riesgos de TI en un nivel Inicial (1), ya que los riesgos de TI se toman en cuenta de manera inicial, no cuentan con evaluaciones de riesgos en un plan de proyectos, ni la asignación a gerentes específicos.

Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente en los proyectos.

**DOMINIO: ADQUIRIR E IMPLEMENTAR**

El grafico de nivel de madurez para el dominio Adquirir Implementar indica que se encontró a el objetivo de control (AI4) Facilitar la operación y el uso, en un nivel no existente (0), ya que no existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento.

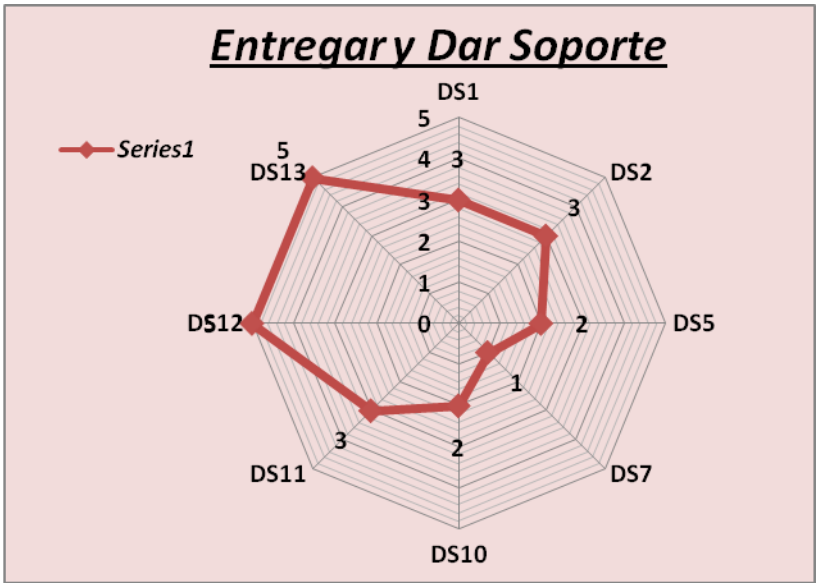



Los únicos materiales existentes son aquellos que se suministran con los productos que se adquieren. El conocimiento sobre los nuevos sistemas debe estar disponible, y

proporcionar entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.

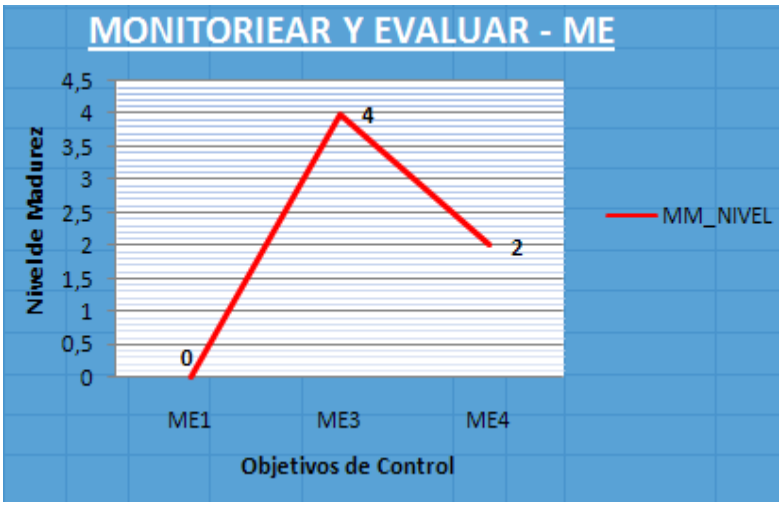
**DOMINIO: ENTREGAR Y DAR SOPORTE**

En el nivel de madurez para el dominio Entregar y dar Soporte se constató que en el objetivo de control (DS5) Garantizar la seguridad de sistemas, la organización sí reconoce la necesidad de seguridad para TI, sin embargo la conciencia de esta necesidad de seguridad depende principalmente del individuo.




No se mide la seguridad de TI, ya que no se realiza un monitoreo de seguridad y pruebas periódicas para prever acciones correctivas sobre las debilidades o incidentes de seguridad identificados. La efectiva administración de la seguridad debe proteger todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

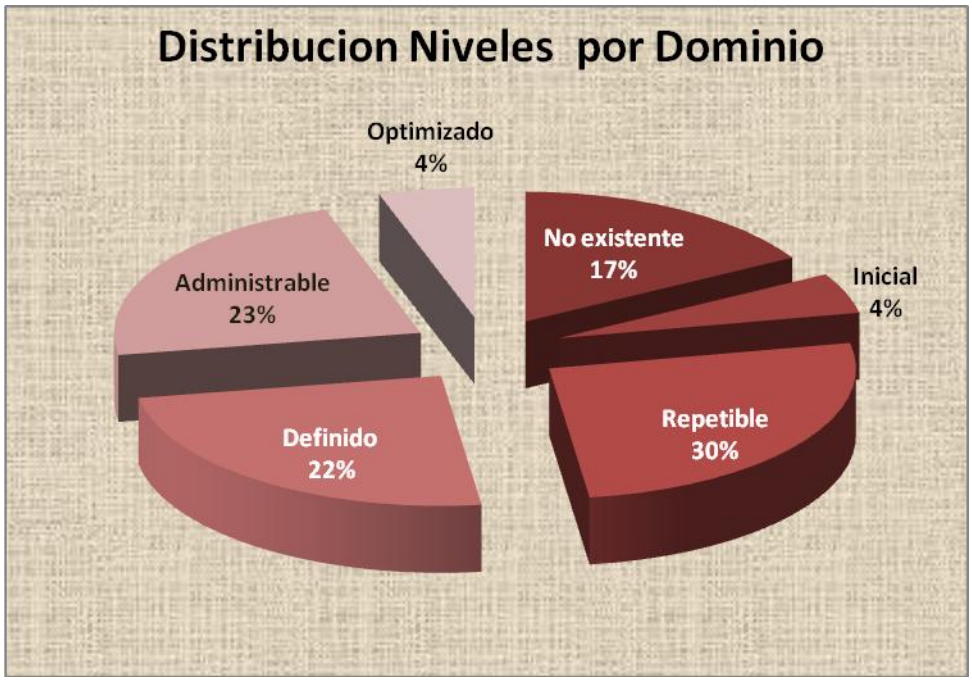
Así también en el objetivo de control (DS7) Educar y Entrenar a los Usuarios Se encontró evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no hay procedimientos estandarizados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios.




**DOMINIO: MONITOREAR Y EVALUAR**

En el nivel de madurez para el dominio Monitorear y evaluar se constató que en el objetivo de control

(ME1) Monitorear y evaluar el desempeño de TI, No se encontró la existencia de un medio de información a la alta dirección, ni de portafolios relevantes, ni programas de desempeños de TI, con soportes como informes, para permitir a la alta dirección revisar el progreso de la empresa hacia las metas identificadas. Por tanto se considera que no se trabaja en conjunto con el consejo directivo para definir el nivel de riesgo de TI aceptable por la empresa y obtener garantía razonable. Las prácticas de administración de riesgos de TI son apropiadas para asegurar que el riesgo actual de TI no excede el riesgo aceptable de dirección.




El incremento de madurez reduce el riesgo y mejora la eficiencia generando menos errores, más procesos predecibles y un uso rentable, para la organización que decide utilizar el MM como indicador.

**E.3.** Identificar y elaborar los documentos que contengas las pistas de auditoría y hallazgos
**E.4.** Elaborar el dictamen preliminar y presentarlo a discusión
**E.5.** Integrar el legado de papeles de trabajo de auditoria

**Fase 3:** ***Dictamen de la Auditoria*** (Ver Informe de Auditoria)
**D.1** Analizar la información y elaborar un informe de situaciones detectadas
**D.2** Elaborar el dictamen de la Auditoria
**D.3** Presentar el informe de la Auditoria

# GUIAS DE AUDITORIA

*Las guías de Auditoria contienen los alineamientos con los que se debe dirigir el proceso de Auditoria, en ella se emplean los Objetivos de COBIT 4.1 y los criterios de seguridad.*

### 10.1 Guías de Objetivo de Auditoria 1

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de los Procesos de Organización, Planificación y Admón. de TI*

| AREA DE INFORMÁTICA *(Organización, Planificación, Admón.)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 1 de 5 |
| DOMINIO: PLANEAR Y ORGANIZAR | 02 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Analizar los procesos de organización, planificación y administración como principal estrategia de Seguridad de TI en el Organismo Internacional MS- América Central. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **PO3** | **Determinación de la dirección tecnológica**<br><br>La función de servicios de información debe determinar la dirección tecnológica para dar soporte al negocio. Esto requiere de la creación de un plan de infraestructura tecnológica y de un comité de arquitectura que establezca y administre expectativas realistas y claras de lo que la tecnología puede ofrecer en términos de productos, servicios y mecanismos de aplicación. El plan se debe actualizar de forma regular y abarca aspectos tales como arquitectura de sistemas, dirección tecnológica, planes de adquisición, estándares, estrategias de migración y contingencias. Esto permite contar con respuestas oportunas a cambios en el ambiente competitivo, economías de escala para consecución de personal de sistemas de información e inversiones, así como una interoperabilidad mejorada de las plataformas y de las aplicaciones. | *Influye la arquitectura tecnológica.*<br><br>PO3.1 Planeación de la dirección tecnológica<br>PO3.2 Plan de infraestructura tecnológica<br>PO3.3 Monitoreo de tendencias y regulaciones futuras<br>PO3.4 Estándares tecnológicos<br>PO3.5 Consejo de arquitectura de TI | • Se debe identificar el papel de los diversos actores en relación con los activos a proteger.<br>• Se deben definir con claridad las responsabilidades.<br>• Se deben definir y documentar las funciones y obligaciones del personal<br>• Se deben definir y documentar procedimientos de seguridad.<br>• Dependiendo de los requisitos de la aplicación, se deben tener en cuenta los aspectos de seguridad en el proceso de asignación de puestos. | |

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de los Procesos de Organización, Planificación y Admón. de TI*

| AREA DE INFORMÁTICA *(Organización, Planificación, Admón.)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 2 de 5 |
| DOMINIO: PLANEAR Y ORGANIZAR | 02 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Analizar los procesos de organización, planificación y administración como principal estrategia de Seguridad de TI en el Organismo Internacional MS- América Central. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **PO4** | **Definir los procesos, organización y relaciones de TI**<br>Una organización de TI se debe definir tomando en cuenta los requerimientos de personal, funciones, rendición de cuentas, autoridad, roles, responsabilidades y supervisión. La organización está embebida en un marco de trabajo de procesos de TI que asegure la transparencia y el control, así como el involucramiento de los altos ejecutivos y de la gerencia del negocio. Un comité estratégico debe garantizar la vigilancia del consejo directivo sobre TI, y uno ó más comités de dirección, en los cuales participen tanto el negocio como TI, deben determinar las prioridades de los recursos de TI alineados con las necesidades del negocio. Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones. Para garantizar el soporte oportuno de los requerimientos del negocio, TI se debe involucrar en los procesos importantes de decisión. | *Influyen los planes, la organización, las funciones y responsabilidades y sobre todo:*<br><br>PO4.8 Responsabilidad sobre el riesgo, la seguridad y el cumplimiento<br>PO4.9 Propiedad de datos de sistemas<br><br>PO4.11 Segregación de funciones<br>PO4.12 Personal de TI<br>PO4.13 Personal Clave de TI<br>PO4.14 Políticas y procedimientos para personal contratado | • Se debe identificar el papel de los diversos actores en relación con los activos a proteger.<br>• Se deben definir con claridad las responsabilidades.<br>• Se deben definir y documentar las funciones y obligaciones del personal<br>• Se deben definir y documentar procedimientos de seguridad.<br>• Dependiendo de los requisitos de la aplicación, se deben tener en cuenta los aspectos de seguridad en el proceso de asignación de puestos. | |

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de los Procesos de Organización, Planificación y Admón. de TI*

| AREA DE INFORMÁTICA *(Organización, Planificación, Admón.)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 3 de 5 |
| DOMINIO: PLANEAR Y ORGANIZAR | 03 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Analizar los procesos de organización, planificación y administración como principal estrategia de Seguridad de TI en el Organismo Internacional MS- América Central. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **PO5** | **Administrar la inversión en TI**<br><br>Establecer y mantener un marco de trabajo para administrar los programas de inversión en TI que abarquen costos, beneficios, prioridades dentro del presupuesto, un proceso presupuestal formal y administración contra ese presupuesto. Los interesados (stakeholders) son consultados para identificar y controlar los costos y beneficios totales dentro del contexto de los planes estratégicos y tácticos de TI, y tomar medidas correctivas según sean necesarias. El proceso fomenta la asociación entre TI y los interesados del negocio, facilita el uso efectivo y eficiente de recursos de TI, y brinda transparencia y responsabilidad dentro del costo total de la propiedad, la materialización de los beneficios del negocio y el retorno sobre las inversiones en TI. | *Repercute en la fiabilidad y por las inversiones y gastos en seguridad.*<br><br>PO5.1 Marco de Trabajo para la administración financiera<br>PO5.2 Prioridades dentro del presupuesto de TI<br>PO5.3 Proceso presupuestal<br>PO5.4 Administración de costos de TI<br>PO5.5 Administración de beneficios | • Para cada activo se debe identificar a su propietario, así como su valor e importancia en términos cuantitativos o cualitativos, en función de los requisitos de autenticidad, integridad, confidencialidad y disponibilidad que le son aplicables. Esta información es crucial, pues facilita el análisis y gestión de riesgos y, por tanto sirve, para determinar las medidas de seguridad proporcionadas | |

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de los Procesos de Organización, Planificación y Admón. de TI*

| AREA DE INFORMÁTICA *(Organización, Planificación, Admón.)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 4 de 5 |
| DOMINIO: PLANEAR Y ORGANIZAR | 04 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Analizar los procesos de organización, planificación y administración como principal estrategia de Seguridad de TI en el Organismo Internacional MS- América Central. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **ME1** | **Monitorear y evaluar el desempeño de TI**<br><br>Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y Políticas. | *Sobre todo en cuanto a disponibilidad*<br><br>ME1.1 Enfoque del monitoreo<br>ME1.2 Definición y recolección de datos de monitoreo<br>ME1.3 Método de monitoreo<br>ME1.4 Evaluación del desempeño<br>ME1.5 Reportes al consejo directivo y a ejecutivos<br>ME1.6 Acciones correctivas | • La situación y actividades de seguridad se deben revisar de forma independiente (auditoria) y periódicamente para asegurar que las prácticas de la organización siguen estas normas y que además son efectivas.<br>• La determinación de objetivos, estrategia y política de seguridad se alimenta de la anterior para definir que hay que proteger y por qué, y sirven de guía y respaldo para la implementación de las medidas necesarias de protección. | |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA

## *Evaluación de los Procesos de Organización, Planificación y Admón. de TI*

| AREA DE INFORMÁTICA *(Organización, Planificación, Admón.)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 5 de 5 |
| DOMINIO: MONITOREAR Y EVALUAR | 04 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Analizar los procesos de organización, planificación y administración como principal estrategia de Seguridad de TI en el Organismo Internacional MS- América Central. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **ME4** | **Proporcionar gobierno de TI**<br><br>El establecimiento de un marco de trabajo de gobierno efectivo, incluye la definición de estructuras, procesos, liderazgo, roles y responsabilidades organizacionales para garantizar así que las inversiones empresariales en TI estén alineadas y de acuerdo con las estrategias y objetivos empresariales. | *Influye:*<br><br>ME4.4 Administración de recursos<br>ME4.5 Administración de riesgos | • Se debe identificar el papel de los diversos actores en relación con los activos a proteger. (Criterio 1)<br><br>• Se debe realizar el análisis y la gestión de riesgos aplicando, Metodología de análisis y gestión de riesgos de los sistemas de información, para determinar las medidas organizativas y técnicas adecuadas que salvaguardan la autenticidad, confidencialidad, integridad y disponibilidad de acuerdo con la naturaleza de los datos y los tratamientos, los riesgos a que están expuestos y el estado de la tecnología.<br>• Los riesgos y las salvaguardas de la aplicación se deben revisar periódicamente, así como siempre que las circunstancias lo aconsejen, como una parte más de la gestión de la seguridad. | |

### 10.2 Guías de Objetivo de Auditoria 2

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de Políticas, Normas y Estándares de Seguridad*

| AREA DE INFORMÁTICA *(Políticas, Normas y Estándares de Seguridad)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 1 de 1 |
| DOMINIO: PLANEAR Y ORGANIZAR | 05 | 11 | 10 | |

| | |
|---|---|
| **Objetivo:** | Evaluar la existencia y aplicación de normas, políticas y estándares de seguridad, requeridas para el desempeño eficiente de cada una de las funciones informáticas. |
| **Usuarios** | Oficial Administrativo Logístico |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que eran evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **PO6** | **Comunicar las aspiraciones y la dirección de la gerencia**<br>La dirección debe elaborar un marco de trabajo de control empresarial para TI, y definir y comunicar las políticas. Un programa de comunicación continua se debe implementar para articular la misión, los objetivos de servicio, las políticas y procedimientos, etc., aprobados y apoyados por la dirección. La comunicación apoya el logro de los objetivos de TI y asegura la concienciación y el Entendimiento de los riesgos de negocio y de TI. El proceso debe garantizar el cumplimiento de las leyes y reglamentos relevantes. | *Influyen las políticas y sobre todo:*<br>PO6.2 Riesgo corporativo y marco de referencia de control interno de TI<br>PO6.3 Administración de políticas para TI<br>PO6.4 Implantación de políticas de TI | • La concienciación y formación tiene un papel fundamental para el éxito de la política de seguridad.<br>• La determinación de objetivos, estrategia y política de seguridad se alimenta de la anterior para definir que hay que proteger y por qué, y sirven de guía y respaldo para la implementación de las medidas necesarias de protección. | |
| **ME3** | **Garantizar el cumplimiento con requisitos externos**<br>Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales. Este proceso incluye la identificación de requerimientos de cumplimiento, optimizando y evaluando la respuesta, obteniendo aseguramiento que los requerimientos se han cumplido y, finalmente integrando los reportes de cumplimiento de TI con el resto del negocio. | *Influye en función del País.*<br>ME3.5 Identificar los requerimientos de las leyes, regulaciones y cumplimiento contractuales<br>ME3.6 Optimizar la respuesta a requerimientos externos<br>ME3.7 Evaluación del cumplimiento con requerimientos externos<br>ME3.8 Aseguramiento positivo del cumplimiento | • Las copias de documentos originales almacenados por medios o en soportes electrónicos, informáticos o telemáticos, expedidas por los órganos de la Administración General del Estado o por sus entidades vinculadas o dependientes, tendrán la misma validez y eficacia del documento original siempre que quede garantizada su autenticidad, integridad y conservación. | |

### 10.3 Guías de Objetivo de Auditoria 3

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMATICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 1 de 9 |
| DOMINIO: PLANEAR Y ORGANIZAR | 18 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **PO2** | **Definir la Arquitectura de Información**<br><br>La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto incluye el desarrollo de un diccionario corporativo de datos que contiene las reglas de sintaxis de los datos de la organización, el esquema de clasificación de datos y los niveles de seguridad. Este proceso mejora la calidad de la toma de decisiones gerenciales asegurándose que se proporciona información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades. | *Influyen el diccionario de datos, el esquema de clasificación de datos y la integridad de los datos.*<br><br>PO2.1 Modelo de arquitectura de la información<br>PO2.2 Diccionario de datos empresarial y reglas de sintaxis de datos<br>PO2.3 Esquema de clasificación de datos<br>PO2.4 Administración de la integridad | • Se deben definir y documentar los requisitos y los objetivos de seguridad.<br>• Se deben definir y documentar las estrategias, normas, pautas y procedimientos para satisfacer los requisitos de seguridad y alcanzar los mencionados objetivos.<br>• Seguridad que la información, o los datos, están protegidos contra modificación o destrucción no autorizada, y certidumbre de que los datos no han cambiado de la creación a la recepción. | ***Información*** |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 2 de 9 |
| DOMINIO: ADQUIRIR E IMPLEMENTAR | 18 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **AI3** | **Adquirir y mantener infraestructura tecnológica**<br><br>Las organizaciones deben contar con procesos para adquirir, Implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio. | *Cierta influencia, sobre todo:*<br><br>AI3.2 Protección y disponibilidad del recurso de infraestructura<br>AI3.3 Mantenimiento de la infraestructura | • Se debe construir barreras físicas del suelo al techo para prevenir entradas no autorizadas o contaminación del entorno. Las ventanas y puertas de las áreas seguras deben estar cerradas y controlarse periódicamente. Las ventanas deben protegerse externamente. Se pueden necesitar barreras adicionales y perimetrales entre áreas con diferentes requisitos de seguridad dentro del perímetro global de seguridad.<br>• Se debe construir las instalaciones de forma discreta y minimizar las indicaciones sobre su propósito, evitando signos obvios (fuera o dentro del edificio) que identifiquen la presencia de las actividades cuya seguridad se desea. No informar al personal que no esté directamente implicado de las actividades que se hacen dentro de las áreas seguras. | ***Infraestructura*** |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 3 de 9 |
| DOMINIO: ADQUIRIR E IMPLEMENTAR | 09 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **AI4** | **Facilitar la operación y el uso**<br><br>El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la Infraestructura. | *Influyen algunos puntos:*<br><br>AI4.1 Plan para soluciones de operación<br>AI4.2 Transferencia de conocimientos a la gerencia del negocio<br>AI4.3 Transferencia de conocimientos a usuarios finales<br>AI4.4 Transferencia de conocimientos personal de operaciones y soporte. | • Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.<br>• Se debe formar y concienciar a los usuarios en relación con los procedimientos de comunicación, consulta y reacción ante incidencias. Se deben establecer canales para informar lo más rápidamente posible de las incidencias y el mal funcionamiento de los sistemas. | ***Aplicación*** |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 4 de 9 |
| DOMINIO: ADQUIRIR E IMPLEMENTAR | 10 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **AI5** | **Adquirir recursos de TI (Persona, HW, SW, Servicios)**<br><br>Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable. | *Influyen en cierto modo:*<br><br>AI5.1 Control de Adquisición<br>AI5.2 Administración de Contratos con proveedores<br>AI5.3 Selección de proveedor<br>AI5.4 Adquisición de recursos de TI | • En relación con los activos de tipo información, se debe documentar a qué usuarios se autoriza el acceso y los atributos relacionados con el referido acceso. | ***Aplicación*** |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 5 de 9 |
| DOMINIO: ENTREGAR Y DAR SOPORTE | 11 | 11 | 10 | Ref. DS5 |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Observaciones: |
|---|---|---|
| **Garantizar la seguridad de los sistemas**<br><br>La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI.<br>La administración de la seguridad también incluye realizar monitoreo de seguridad y pruebas periódicas así como realizar acciones correctivas sobre las debilidades o incidentes de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad. | DS5.1 Administración de la seguridad de TI<br>DS5.2 Plan de seguridad de TI<br>DS5.3 Administración de Identidad<br>DS5.4 Administración de Cuentas de Usuario<br>DS5.5 Pruebas, vigilancia y monitoreo de la seguridad<br>DS5.6 Definición de incidentes de seguridad<br>DS5.7 Protección de la tecnología de seguridad<br>DS5.8 Administración del llaves criptográficas<br>DS5.9 Prevención, detección y corrección de software malicioso<br>DS5.10 Seguridad de la Red<br>DS5.11 Intercambio de datos sensitivos | ***Aplicación*** |

### Criterio de Seguridad

- El análisis y gestión de riesgos se encarga de estudiar los activos, amenazas, vulnerabilidades, impactos, y riesgos que una seguridad insuficiente que puede tener para la organización, así como de las salvaguardas necesarias.
- La fase de reacción a cada evento, registro de incidencias y recuperación de estados de seguridad tiene un carácter básicamente operacional.
- El sistema debe exigir que cada usuario se identifique y autentifique su identidad, antes de que se le permita realizar cualquier acción, para acceder a la aplicación y a otros recursos (también al puesto local, al servidor, al dominio de red, etc.).
- Se debe verificar que el nivel de acceso asignado al usuario corresponde a necesidades de funcionamiento de la Organización y es consistente con la normativa de seguridad de la Organización y que no se contradice con el principio de segregación de funciones (según grupos de usuarios, servicios y sistemas de información).
- Se debe eliminar de forma inmediata las autorizaciones de acceso a los usuarios que dejen la Organización o cambien su función dentro de ella y comprobar que los identificadores eliminados no sean reasignados a otros usuarios.

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 6 de 9 |
| DOMINIO: ENTREGAR Y DAR SOPORTE | 22 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **DS7** | **Educar y entrenar a los usuarios**<br>Para una educación efectiva de todos los usuarios de sistemas de TI, incluyendo aquellos dentro de TI, se requieren identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo de la tecnología al disminuir los errores, incrementando la productividad y el cumplimiento de los controles clave tales como las medidas de seguridad de los usuarios. | *Influye lo referido a seguridad:*<br><br>DS7.1 Identificación de necesidades de entrenamiento y educación<br>DS7.2 Impartición de entrenamiento y educación<br>DS7.3 Evaluación del entrenamiento recibido | • Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.<br>• Se debe formar y concienciar a los usuarios en relación con los procedimientos de comunicación, consulta y reacción ante incidencias. Se deben establecer canales para informar lo más rápidamente posible de las incidencias y el mal funcionamiento de los sistemas.<br>• Se debe formar al personal en el funcionamiento de todos los sistemas instalados, realizando simulaciones de contingencias. | ***Personas*** |

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 7 de 9 |
| DOMINIO: ADQUIRIR E IMPLEMENTAR | 19 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **DS11** | **Administrar los datos**<br><br>Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio. | *Influye:*<br><br>DS11.2 Acuerdos de almacenamiento y conservación<br>DS11.3 Sistemas de administración de librerías de medios<br>DS11.4 Eliminación<br>DS11.5 Respaldo y restauración<br>DS11.6 Requerimientos de seguridad para la administración de datos | Se deben:<br>• Implantar procedimientos de explotación de la aplicación y de los sistemas adecuados a la protección de la integridad.<br>• Implantar procedimientos de copias de respaldo de ficheros y bases de datos, y de protección y conservación de soportes de información.<br>• Generar copias de los doc emitidos en soportes no re escribibles de tipo 'múltiple lectura única escritura' (WORM), como CD-ROM o DVD<br>• Realizar un análisis periódico de los accesos y de los recursos utilizados.<br>• Adoptar medidas de protección frente a código dañino en los servidores de aplicación, en los equipos de los usuarios y en los soportes circulantes (disquetes, CD's, otros): asi como instalar exploradores del SW, con actualización periódica. | ***Información*** |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 8 de 9 |
| DOMINIO: ENTREGAR Y DAR SOPORTE | 19 | 11 | 10 | Ref. **DS12** |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Observaciones |
|---|---|---|
| **Administrar el ambiente físico**<br><br>Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio. | *Influye:*<br><br>DS12.1 Selección y diseño del centro de datos<br>DS12.2 Medidas de seguridad física<br>DS12.3 Acceso físico<br>DS12.4 Protección contra factores ambientales<br>DS12.5 Administración de las instalaciones físicas. | ***Infraestructura*** |

## Criterio de Seguridad

- Se debe situar el equipamiento que soporta a la aplicación así como los soportes de información en áreas seguras y protegidas adecuadamente.
- Se debe proteger los locales de amenazas potenciales: Eléctricas, incendios, clima, agua, interferencias, Otros: elegir la ubicación evitando excesivas vibraciones. Control del polvo mediante limpieza regular y pinturas especiales para el suelo de la sala que evite su acumulación
- Se debe documentar debidamente los procedimientos de emergencia y revisar esta documentación de forma regular.
- Los equipos que soporten la aplicación y cuya interrupción accidental pueda provocar alteración o pérdida de datos o documentos administrativos, deben estar protegidos contra fallos de suministro eléctrico mediante sistemas de alimentación ininterrumpida.
- Se deberá preparar y mantener operativo un plan de contingencias.
- Se deben adoptar las medidas apropiadas de seguridad física en el entorno donde se encuentren los equipos que den soporte a la aplicación.

MS América Central
actionaid denmark

# GUIA DE AUDITORIA
## *Evaluación de los Recursos de TI*

| AREA DE INFORMÁTICA – *(Aplicación, información, Infraestructura y Personas)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 9 de 9 |
| DOMINIO: ENTREGAR Y DAR SOPORTE | 22 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos. |
| **Usuarios** | Oficial Administrativo Logístico/ Oficial Administrativo Financiero/ Usuarios Primarios y Secundarios |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **DS13** | **Administrar las operaciones**<br><br>La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (sitio), la selección de Instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal. | *Influye:*<br><br>DS13.1 Procedimientos e instrucciones de operación<br>DS13.2 Programación de tareas<br>DS13.3 Monitoreo de la infraestructura de TI<br>DS13.4 Documentos sensitivos y dispositivos de salida<br>DS13.5 Mantenimiento preventivo del hardware | • Se deben definir procedimientos para el paso de aplicaciones a explotación, ya sean nuevas o actualizaciones de las existentes, que recojan los requisitos que estas deben cumplir y las pruebas a realizar antes de su aceptación.<br>• Se deben tener en cuenta los aspectos de seguridad de la aplicación en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y el mantenimiento e incorporando las funciones de salvaguarda antes de su puesta en explotación. | ***Infraestructura*** |

### 10.4 Guías de Objetivo de Auditoria 4

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de la Contratación Externa - Outsourcing*

| AREA DE INFORMÁTICA *(Outsourcing)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 1 de 2 |
| DOMINIO: ENTREGAR Y DAR SOPORTE | 23 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Evaluar el desempeño y proceso de contratación externa entre la Organización y las proveedoras de servicio tecnológico |
| **Usuarios** | Oficial Administrativo Logístico |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **DS1** | **Definir y administrar los niveles de servicio**<br><br>Contar con una definición documentada y un acuerdo de servicios de TI y de niveles de servicio, hace posible una comunicación Efectiva entre la gerencia de TI y los clientes de negocio respecto de los servicios requeridos. Este proceso también incluye el monitoreo y la notificación oportuna a los Interesados (Stakeholders) sobre el cumplimiento de los niveles de servicio. Este proceso permite la alineación entre los servicios de TI y los requerimientos de negocio relacionados. | *Es calidad, pero influye en seguridad:*<br><br>DS1.1 Marco de Trabajo de la Administración de los niveles de servicio<br>DS1.2 Definición de servicios<br>DS1.3 SLA – Acuerdos de los niveles de servicio<br>DS1.4 OLA- Acuerdos de niveles de operación<br>DS1.5 Monitoreo y reporte del nivel de cumplimiento de los niveles de servicio<br>DS1.6 Revisión de la SLA y de los contratos | • Se deben aplicar técnicas de comprobación de la integridad de la información: funciones resumen o hash, firma electrónica, etc. (en particular a documentos y mensajes) para verificar la integridad de la misma.<br>• En las aplicaciones que ejecuten transacciones o procesos donde se produzcan múltiples actualizaciones de datos que se encuentren relacionados entre sí, se deben adoptar herramientas o procedimientos que aseguren la integridad de estos datos en el caso de que se produzca un fallo de proceso y no se pueda completar la transacción. | |

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación de la Contratación Externa – Outsourcing*

| AREA DE INFORMÁTICA *(Outsourcing)*<br>DOMINIO: ENTREGAR Y DAR SOPORTE | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 2 de 2 |
| | 24 | 11 | 10 | |

| | |
|---|---|
| **Objetivo** | Evaluar el desempeño y proceso de contratación externa entre la Organización y las proveedoras de servicio tecnológico |
| **Usuarios** | Oficial Administrativo Logístico |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que serán Evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **DS2** | **Administrar los servicios de terceros**<br><br>La necesidad de asegurar que los servicios provistos por terceros cumplan con los requerimientos del negocio, requiere de un proceso efectivo de administración de terceros. Este proceso se logra por medio de una clara definición de roles, Responsabilidades y expectativas en los acuerdos con los terceros, así como con la revisión y monitoreo de la efectividad y cumplimiento de dichos acuerdos. Una efectiva administración de los servicios de terceros minimiza los riesgos del negocio asociados con proveedores que no se desempeñan de forma adecuada. | *Influye en cuanto a servicios y seguridad* .<br>DS2.3 Administración de Riesgos del proveedor<br>DS2.4 Monitoreo del desempeño del proveedor | • Dar a conocer al personal interno como externo las medidas de seguridad que afecten al desarrollo de sus funciones y que en su caso deban aplicar, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.<br>• Establecer obligaciones de confidencialidad en los casos de personal con contratos temporales o personal perteneciente a empresas subcontratadas, cuando la información que puedan manejar en el desempeño de sus obligaciones temporales sean datos de carácter personal, u otra información sensible. El personal temporal o subcontratado deberá aceptar expresamente las prescripciones de confidencialidad.<br>• Se deben adoptar medidas adicionales específicas para el control de acceso de terceras partes | |

### 10.5 Guías de Objetivo de Auditoria 5

MS América Central
actionaid denmark

# G U I A  D E  A U D I T O R I A

## *Evaluación del Riesgo, Problemas e incidentes*

| AREA DE INFORMÁTICA *(Riesgo, Problemas e incidentes)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 1 de 2 |
| DOMINIO: PLANEAR Y ORGANIZAR | 29 | 11 | 10 | |

| | |
|---|---|
| **Objetivo:** | Evaluar el grado de exposición al riesgo en la seguridad informática en base a las deficiencias o ausencias de controles informáticos |
| **Usuarios** | Oficial Administrativo Logístico - **Administrador de Red** |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que eran evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **PO9** | **Evaluar y administrar los riesgos de TI**<br><br>Crear y dar mantenimiento a un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible para los Interesados (Stakeholders) y se debe expresar en términos financieros, para permitirles alinear los riesgos a un nivel aceptable de tolerancia. | *Influye plenamente:*<br><br>PO9.1 Alineación de administración del Riesgo de TI y del negocio<br>PO9.2 Establecimiento del contexto del riesgo<br>PO9.3 Identificación de eventos<br>PO9.4 Evaluación de Riesgos de TI<br>PO9.5 Respuesta a los riesgos<br>PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgo | • Se debe informar al propietario de la aplicación y de los ficheros de los riesgos detectados al objeto de que pueda tomar decisiones sobre la política de seguridad a seguir. | |

MS América Central
actionaid denmark

# GUIA DE AUDITORIA

## *Evaluación del Riesgo, Problemas e incidentes*

| AREA DE INFORMÁTICA *(Riesgo, Problemas e incidentes)* | Fecha | | | Hoja No. |
|---|---|---|---|---|
| | DD | MM | AA | 2 de 2 |
| DOMINIO: ENTREGAR Y DAR SOPORTE | 30 | 11 | 10 | |

| | |
|---|---|
| **Objetivo:** | Evaluar el grado de exposición al riesgo en la seguridad informática en base a las deficiencias o ausencias de controles informáticos |
| **Usuarios** | Oficial Administrativo Logístico - **Administrador de Red** |

| Referencia | Objetivo de Control Detallado | Objetivos de Control que eran evaluados | Criterio de Seguridad | Observaciones |
|---|---|---|---|---|
| **DS10** | **Administrar los problemas**<br><br>Una efectiva administración de problemas requiere la identificación y clasificación de problemas, el análisis de las causas desde su raíz, y la resolución de problemas. El proceso de administración de problemas también incluye la identificación de recomendaciones para la mejora, el mantenimiento de registros de problemas y la revisión del estatus de las acciones correctivas. Un efectivo proceso de administración de problemas mejora los niveles de servicio, reduce costos y mejora la conveniencia y satisfacción del usuario | *Influye:*<br><br>DS10.1 Identificación y clasificación de los problemas de hardware<br>DS10.2 Rastreo y resolución de problemas<br>DS10.3 Cierre de problemas<br>DS10.4 Integración de las administraciones de cambio, configuración y problemas | • Se debe realizar el análisis y la gestión de riesgos aplicando la Metodología de análisis y gestión de riesgos más adecuado a los sistemas de información, para determinar las medidas organizativas y técnicas adecuadas que salvaguardan la autenticidad, confidencialidad, integridad y disponibilidad de acuerdo con la proporcionalidad entre la naturaleza de los datos y los tratamientos, los riesgos a que están expuestos y el estado de la tecnología.<br>• Se debe formar a los usuarios en el uso adecuado de la aplicación y en los procedimientos de reacción ante incidentes.<br>• Se debe implantar un registro incidencias acorde al procedimiento y a los datos manejados con el tipo de incidencia, momento, persona que realiza la notificación, a quién lo notifica y los efectos de la misma. Esta información junto con otra relativa a la seguridad se debe conservar para aprender de estas experiencias, con objeto de minimizar los posibles daños y consecuencias, para investigaciones futuras y para el control de los accesos. | |

2010

# INFORME DE AUDITORIA

## Área de Informática MS- América Central

AUDITORIA DE SEGURIDAD INFORMATICA APLICANDO EL ESTANDAR INTERNACIONAL COBIT 4.1 EVALUANDO LA DIRECCION INFORMATICA, RECURSOS TI, OUTSORCING Y RIESGO INFORMATICO PARA EL AREA DE INFORMATICA DE MS – AMERICA CENTRAL EN PERIODO AÑO 2010


PRESENTADO POR:

*Br. Karla Vanessa Molina Gutiérrez*

*Br. Claudia Regina González Urroz*

*Br. Araceli del Carmen Munguía Alfaro*


**Managua, 24 de Agosto del 2011**

**Jan Borsheim**
Administrador Regional
MS- América Central
Sus manos

Reciba cordiales saludos.

Por medio de la presente le remitimos los resultados de Auditoría aplicada en el área Informática del Organismo Internacional Asociación Danesa para la Cooperación Internacional al que representa legalmente.

Los procedimientos de evaluación van acorde al periodo del **01 de Enero a Diciembre del 2010**, el objetivo de aplicar un Modelo de Auditoria basada en la Normativa de COBIT, es porque propone un marco de acción donde se evalúan y analizan los criterios de información, los recursos de TI y la gestión del Riesgo informático.

El proceso de auditoría tuvo como alcance:

1. Evaluar los procesos de Organización, planificación, y administración de la dirección y del área de informática
2. Normas, Procedimientos y Políticas de Auditoria
3. Evaluar los recursos de TI
4. Outsourcing
5. Riesgo informático

El contenido del informe ha sido dividió en 4 secciones por cada una de las áreas auditadas, estas son:

- **Situación Actual:** Es el estado en que se encuentra la área informática antes y durante del proceso de investigación.
- **Tendencias:** Son las percepciones del equipo auditor en cuanto a la visión futura del personal de TI, en lo que respecta a tecnologías modernas y mejoras al sistema de control actual.
- **Puntos débiles y amenazas por orden de importancia:** Son en síntesis las falencias y debilidades encontradas en los diferentes niveles organizacionales desde el gobierno de TI hasta los usuarios finales.

- **Recomendaciones y Plan de Acción:** Son mejoras que sugiere el equipo auditoria para los elementos que requieren atención.

Escala de calificación establecida según el nivel crítico: Es el nivel o estado en el que se encuentran los elementos auditados a fin de que se puedan orientar acciones correctivas o preventivas en tiempos de cortos o largos plazos según sea el caso.

0 **= Alto** grado critico- acción correctiva inmediata
1 **= Alto** grado critico – acción preventiva inmediata
2 = **Medio** grado moderado- acción correctiva extendida
3 = **Bajo** grado mínimo – acción preventiva extendida.

A criterio del equipo auditor se señala que durante el proceso de examen y evaluación se encontró transparencia en la gestión y administración por parte de la gerencia de TI, sin embargo existen falencias y debilidades en el monitoreo y seguimiento a las actividades de TI. Este se remarca aún más en la falta de un Plan estratégico de TI que oriente de manera lógica y continua los objetivos y metas de TI establecidos por el organismo a fin de garantizar la seguridad, efectividad y eficiencia en todos los niveles institucionales.

Por otro lado es importante recalcar que el área informática se encuentra vulnerable a intentos fraudulentos y expuestos a perdidas de información sensitiva, así como daños a los recursos materiales ya que no se cuenta con un plan de contingencia que dé respuesta rápida u oportuna de problemas e incidentes que ponen en riesgo la seguridad de los sistemas.
La información contenida en este informe es de carácter confidencial y de uso exclusivo para la organización. Dado en la ciudad de Managua a los 24 días del mes de Agosto del 2011.
Sin más a que referir y agradeciendo su atención y cooperación de saluda.

Atentamente.



Br. Karla Molina G. Br. Claudia González U. Br. Araceli Munguía A.

**DICTAMEN DEL ANALISIS POR AREAS DE EVALUACION.**

**1.Evaluar los procesos de Organización, planificación, y administración de la dirección y del área de informática**

**Situación Actual:** Los procesos de Organización, planificación, y administración de la dirección y del área de informática son dirigidos por tres personas Administrador regional, Oficial Administrativo logístico y el oficial administrativo financiero, asa mismo son ellos los que se encargan de tomar decisiones sobre las diferentes áreas de trabajo.

- **Determinar la Dirección Tecnológica.**

No existe documentación sobre el plan de infraestructura tecnológica de la organización.
Se recomienda formular la documentación del plan de dirección tecnológica con el fin de dar a conocer la arquitectura de la información.

*Escala crítica: **1***

- **Definir los Procesos, Organización y Relaciones de TI.** Se encontraron debilidades en cuanto a la delegación de responsabilidades en la atención de vigilancia y monitoreo de los controles de seguridad.

*Escala crítica: **0***

- **Administrar la Inversión de TI:** A nivel de adquisición de hardware y software no existen informes y detalle presupuestario sobre la inversión de TI en el área informática, a nivel de servicios no se detalla el gasto invertido para la seguridad del sistema solo a nivel administrativo. Es importante señalar que tanto los ciclos de vida del HW como del SW tiene su vida útil y vencimiento de sus licencias por tanto se deberá tener detalle y estimaciones de inversiones realizadas, así como las proyecciones futuras. Para ello se deberá trabajar conjuntamente en una planificación anual sobre un portafolio de proyecto a fin de llevar el control y manejo de este objetivo.

*Escala crítica: 2*

- **Monitorear y Evaluar el Desempeño de TI:** No existe un modelo de evaluación donde se mida y reporte el desempeño de TI a través de indicadores específicos, por tanto no cuentan con reportes útiles, oportunos y precisos. A fin de madurar los procesos esto corresponde a una enorme debilidad por parte de la dirección o gerencia ya que todo proceso de TI se debe de evaluar y dar un continuo seguimiento de las mejorar y buena s practicas.

*Escala crítica: **1***

• **Proporcionar Gobierno de TI:** No se realizan revisiones independientes del cumplimiento de TI, el cumplimiento del objetivo de control es satisfactorio únicamente a través del área administrativa para el cumplimiento de los requerimientos legales, pero no se revisa y administra el nivel de riesgo tanto para los activos como para los recursos de TI. La asignación de responsabilidades es clave para el objetivo ya asura que la organización y en especifico el área de TI evalúen y reporten riesgos relacionados al buen funcionamiento y aseguramiento de la seguridad

*Escala crítica:* ***1***

**Recomendaciones y plan de acción:**

Es necesario que el área de informática cuente con documentos que respalden obligaciones y responsabilidades del personal de TI y que estos a su vez describan procedimientos predefinidos.

Se recomienda realizar revisiones del cumplimiento de TI y analizar si alcanzan sus objetivos.

Definir e implantar un Plan de Monitoreo que contemple indicadores de desempeño para evaluar periódicamente los procesos de la organización con el objetivo de alcanzar las metas de TI de la organización.

Se sugiere realizar anualmente una estimación de inversiones costo beneficios tanto para adquisición del hardware y software, así como a nivel de servicios de manera que pueda visualizar el impacto en cuanto a calidad vs seguridad, considerando que actualmente el hardware y software evaluado se encuentran defesados y con licencias vencidas.

**2.Normas, Procedimientos y políticas relativas a la seguridad**

**Situación actual:** Las Normas, procedimientos y políticas relativas a la seguridad son definidos y aprobados en consenso por la alta gerencia para todas la areas, son participantes claves la directora regional, el Administrador regional, Oficial Administrativo logístico y el oficial administrativo financiero. El cumplimiento de los procedimientos son vigilados por la persona relacionada a las actividades de para el cual fueron diseñados los procedimientos y normas.

Por otro lado las políticas son dadas a conocer al personal desde el momento que son contratadas sin embargo no hay por parte de la gerencia una revisión de estas de manera evaluativas en cuanto al nivel de cumplimiento sobre todo para el área de TI.

- **Comunicar las aspiraciones y la dirección de la gerencia:** No poseen documento físico, que establezcan políticas de TI tanto para el personal de TI, como a usuarios. Estas son trasmitidas al personal de manera verbal.

*Escala crítica: **1***

**Recomendaciones y plan de Acción:**

Es necesario elaborar un documento de administración de políticas de TI y control interno en el cual de contemplen multas y acciones disciplinarias asociadas con la falta de cumplimiento de esta políticas.

### 3. Seguridad en los Recursos de TI

**Situación actual:** El área informática lleva un control de inventario actualizado anualmente, por otro lado no se monitorean continuamente los recursos y sistemas de TI lo que ubica al área vulnerable ante ataques de seguridad.

- **Operación y el uso:** No existe proceso de elaboración y desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento.

*Escala crítica: 2*

- **Seguridad de los Sistemas:** El acceso lógico se encuentra bien definido pero no documentado los usuarios desconocen los procedimientos formales.

No se han establecidos medidas de control preventivas, detectivas y correctivas ante amenazas y virus formalmente documentada.

Desarrollar documento que describan los procedimientos de requisición, establecimiento, emisión, y suspensión de cuentas de usuario siendo estas informadas a los usuarios formalmente

*Back-up:* El almacenamiento de los Backups debe realizarse en locales diferentes de donde reside la información primaria. De este modo se evita la pérdida si el desastre alcanza todo el edificio o local.

Se debe verificar, periódicamente, la integridad de los respaldos que se están almacenando. No hay que esperar hasta el momento en que se necesitan para darse cuenta de que están incompletos, dañados, mal almacenado, etc.

Se debe de contar con un procedimiento para garantizar la integridad física de los respaldos, en previsión de robo o destrucción.

*Seguridad en la Red:* No existen reportes de detección de virus al servidor de red LAN y a usuarios del sistema, no se monitoria el ataque de seguridad e intrusos de manera continua.

*Identificación, Autenticación y Acceso:* El acceso a los recursos de TI está limitado al personal que cuenta con un usuario y password claramente definido, pero no existe un control estricto sobre el manejo de cuentas. Los cambios de password están obligados para todos los sistemas, incluyendo para el sistema de contabilidad NAVISION, para el acceso a servidores los nombres de usuario y clave no pueden ser cambiados por los usuarios únicamente por el administrador del área de TI.

El procedimiento actual de creación de usuarios, establece su ejecución en el servidor es el administrador el encargado de crear en el servidor de dominio las cuentas de usuarios con sus debidos permisos, estos con relación a su perfil se define a que unidades y carpetas tendrá acceso y que derechos, sin embargo este procedimiento no está documentado, las contraseñas de usuarios no se modifican en un debido tiempo y no cumplen con una regla estricta para la asignación de la contraseña. Por otro lado las cuentas de usuarios y contraseñas son conocidas únicamente por el administrador regional y el oficial administrativo logístico, así como personas terceras en este caso el equipo de Sequinsa el cual da mantenimiento correctivo y preventivo a los equipos.

*Escala crítica: 0*

- **Educar y Entrenar a los Usuarios.:** No se realizan programas de entrenamiento y educación para el personal con respecto a temas de TI y los posibles riesgos informáticos.

*Escala crítica: 2*

- **Administración de Datos:** No Existe Manual instructivo acerca de los procedimientos de almacenamiento y conservación de datos para conocimiento de usuario. Se encuentra un único respaldo de información en medio de almacenamiento físico.

*Escala crítica: 2*

- **Administración del Ambiente Físico:** No se realizan las debidas rotulaciones para cada medida de seguridad establecidas por el Área de TI. Las instalaciones no cuentan con detectores de humo e incendio.

Es Factible tomar en cuenta la instalación de detectores de humo e incendio, para un mejor resguardo de los activos.

*Escala crítica: **3***

**Recomendaciones y plan de acción:**

Se recomienda contar con Manuales de operación, procedimientos de usuarios y controles, de manera que los mismos estén en permanente actualización para el mejor desempeño y control de los usuarios.

Elaborar documento que contenga descripción y políticas definida para el acceso lógico por usuarios y cargos.

Retomar como punto de agenda en encuentros, reuniones y capacitación en temas tecnológicos el aspecto del uso de tecnologías a fin de que se adopte una conducta concientizada y responsable.

Realizar pruebas de ataques simulados a los sistemas que permiten evaluar los lugares en los que hay puntos vulnerables y ajustar las directivas y los controles de seguridad en consecuencia.

Elaborar o diseñar un manual instructivo para usuarios.

Realizar un segundo respaldo de los datos fuera de las instalaciones.

Es necesario que el personal pueda visualizar los rótulos que ayuden a minimizar el riesgo de pérdida humana o material.

## 4. Contrato Outsourcing

**Situación Actual:**

Actualmente MS – AMERICA CENTRAL mantiene contacto con SEQUINSA pero no cuentan con un contrato formal donde definan políticas de uso y criterios de seguridad al prestar el servicio de mantenimiento de Equipos del área informática, esto pone en riesgo la seguridad al sistema de información de MS, ya que cualquier persona tercero puede hacer unos de la información sin ninguna precaución.

- **Definir y manejar los niveles de servicio:** No se monitorea continuamente la entrega de servicio por parte de la organización hacia el proveedor, hasta que surgen fallas en los servicios.

No existen reportes de fallas de seguridad ni procedimientos formales para dar soluciones a problemas.

**Recomendaciones y plan de acción:**

Es necesario que con los proveedores se establezca ACUERDOS DE SERVICIOS FORMALES que sustenten los términos de calidad, disponibilidad y seguridad en el acceso y administración de los recursos de TI.

Se recomienda valorar el desempeño del proveedor durante las actividades de evaluación del comité directivo, seguridad de TI, a fin de asegurar el cumplimiento de los acuerdos del contrato

*Escala:* ***0***

## 5. Riesgo Informático

**Situación Actual:**

No poseen documentos donde se contemplen, acuerdos de riesgos de TI, estrategia de mitigación y riesgos residuales, que ayuden a minimizar los posibles riesgos en términos financieros aceptables.

- **Evaluar y administrar los riesgos de TI:** La metodología de evaluación de riesgo es manejada administrativamente, ya que la descripción de trabajo realizado se deja como soporte para la administración y no para el área de TI.

No es documentada la debida identificación y clasificación del sistema, no las acciones correctivas para cada incidente.

Se debe tener en cuenta la probabilidad que sucedan los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

*Escala:* ***0***

**Recomendaciones y plan de acción:**

Definir y elaborar un plan de contingencia que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Elaborar el documento en donde se establezca la evaluación y mitigación de los posibles riesgos para TI.

Es factible manejar copia de los trabajos realizados como un soporte para el área de informática, para un mejor control de la metodología utilizada en los riesgos y para la adopción de las buenas prácticas.

Se recomienda que exista un registro de manejo de problemas, para resolver de manera eficiente los incidentes identificados

# DISEÑO DE PRUEBAS Y RESULTADOS

*El Diseño de Pruebas representan el instrumento donde se especifican las técnicas y procedimientos que se utilizaron para la obtención de evidencias comprobatorias para cada uno de los Objetivos de COBIT 4.1*

*Los resultados de la Evaluación emite de manera específica los resultados obtenidos para cada uno de los Objetivos de COBIT 4.1. Así mismo en su contenido detalla el Modelo de Madures actual y los hallazgos encontrados durante la Auditoria, se proponen Además recomendaciones y conclusiones que serán retomadas en el Dictamen Final.*

## *12.1 Objetivo 1 de Auditoria*

Analizar los procesos de organización, planificación y administración de la Dirección Informática de MS- América Central según estrategia de Gobierno de TI de Cobit 4.1.

*Cuadro 1.1:* ***Diseño de Prueba y resultado P03***

| MS América Central actionaid denmark — **MATRIZ DE PRUEBA Y RESULTADO** | |
|---|---|
| **DOMINIO PLANEAR Y ORGANIZAR** *Determinar la Dirección de Tecnología* | **PO3** |
| **Sub Objetivo 1.1:** Analizar de qué manera se aprovecha la tecnología disponible a través de la creación de un plan de infraestructura y seguridad tecnológica. | |
| ***Diseño de Prueba PO3*** | Verificar que la organización cuenta con un plan de infraestructura y seguridad tecnológica. |
| ***Alcance:*** Plan de infraestructura tecnológica, Estándares tecnológicos, Consejo de arquitectura tecnológica de TI<br>***Instrumento:*** Entrevista Oficial logístico Administrativo | |
| ***Descripción de la Prueba:***<br>Se realiza visitas a la organización con el fin de analizar la infraestructura tecnológica y seguridad de los sistemas de la organización.<br>Se solicita el plan de contingencia para evaluar la seguridad en la infraestructura tecnológica.<br>***Se toma en cuenta:***<br>✓ La capacidad de adecuación y evolución de la infraestructura actual.<br>✓ El monitoreo de desarrollos tecnológicos que serán tomados en consideración durante el desarrollo y mantenimiento del plan de infraestructura tecnológica.<br>✓ Las contingencias, con lo que se evaluará sistemáticamente el plan de infraestructura tecnológica.<br>✓ Planes de adquisición. | |
| ***Evaluación – Resultado P03*** | |
| En la Entrevista y el proceso de planificación y ejecución de actividades se constatan la buena práctica de evaluar el desempeño y capacidad de las TI una vez por semana a través de reuniones formales.<br>La alta gerencia no desarrolla planes estratégicos a largo ni a corto plazo para el área de informática.<br><br>**MM_NIVEL 2. (Repetible)**<br>Se difunde la necesidad e importancia de la planeación tecnológica<br>La planeación es táctica y se enfoca en generar soluciones técnicas a problemas técnicos.<br>Las personas obtienen sus habilidades sobre la planeación tecnológica a través de un aprendizaje práctico y de una aplicación repetida de las técnicas. | |
| **Hallazgos** | No existe documentación sobre el plan de infraestructura tecnológica de la organización. |
| **Recomendaciones** | Formular un plan de Dirección Tecnológica con el fin de dar a conocer la arquitectura tecnológica. |
| **Conclusiones** | Es necesario que se implemente un adecuado plan de infraestructura tecnológica tomando en cuenta los planes a largo y a corto plazo apropiado para la organización. |
| **Anexo** | Ninguno |

*Cuadro 1.2: Diseño de Prueba y resultado P04*

MS América Central actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO PLANEAR Y ORGANIZAR<br>*Definir los Procesos, Organización y Relación de TI* | PO4 |
|---|---|

**Sub Objetivo 1.2:** Evaluar cómo se distribuye las funciones y responsabilidades del personal de TI en la organización de MS.

| | |
|---|---|
| ***Diseño de Prueba PO4*** | Verificar una adecuada segregación de funciones para el personal de MS con el fin de evitar riesgos de TI. |

***Alcance:*** Responsabilidad sobre el riesgo, la seguridad, y el cumplimiento, Propiedad de datos de sistemas, Segregación de funciones, Personal de TI y las Políticas y Procedimientos para personal de contrato.

***Instrumento:*** Entrevista Oficial Administrativo Logístico

***Descripción de la Prueba***

Se realiza entrevista al personal clave de MS y administrador logístico. Con el fin de conocer de que manera está distribuida las responsabilidades en la organización.
Se revisa contratos de trabajo y matriz de distribución de funciones.

***Se toma en cuenta para la evaluación:***

- ✓ El comité de dirección, encargado de vigilar la función de servicios de información y sus actividades.
- ✓ La Gerencia deberá crear una estructura para designar formalmente a los propietarios y custodios de los datos. Sus funciones y responsabilidades deberán estar claramente definidas.
- ✓ Supervisión, para asegurar que las funciones y responsabilidades sean llevadas a cabo apropiadamente
- ✓ Segregación de funciones,
- ✓ Los roles y responsabilidades
- ✓ La descripción de puestos
- ✓ Los niveles de asignación de personal
- ✓ El personal clave

***Evaluación - Resultados de PO4***

En la entrevista realizada al Oficial Administrativo Logístico se constata que la segregación de funciones las decide la alta gerencia de MS, de acuerdo al contrato de trabajo formal que se establece con cada persona empleada, para el caso del área informática la mayoría de las responsabilidades la asume el Oficial Administrativo Logístico (*Ver anexo: Tabla distribución de tarea a personal MS*).

**MM_NIVEL 3. (Definido)**

- ✓ Existen roles y responsabilidades definidos para la organización de TI y para terceros.
- ✓ Se define el ambiente de control interno
- ✓ Se formulan las relaciones con terceros, incluyendo los comités de dirección, auditoría interna y administración de proveedores
- ✓ Existen definiciones de las funciones a ser realizadas por parte del personal de TI y las que deben realizar los usuarios.
- ✓ Los requerimientos del personal de TI y experiencia están definidos y satisfechos.
- ✓ Existe una definición formal de las
- ✓ relaciones con los usuarios y con terceros.

| | |
|---|---|
| **Hallazgos** | Se encontraron debilidades en cuanto a la delegación de responsabilidades en la |

| | |
|---|---|
| | vigilancia y monitoreo en los controles de seguridad. |
| **Recomendaciones** | Es necesario que el área de informática cuente con documentos que respalden obligaciones y responsabilidades del personal de TI. |
| **Conclusiones** | La alta gerencia deberá realizar la documentación adecuada para la segregación de funciones y responsabilidades de manera formal y detallada del personal de TI, con el objetivo de que el personal asuma y realice el trabajo asignado de manera eficiente. |
| **Anexos** | Organigrama institucional.<br>Política de distribución de tareas por puesto de trabajo. |

*Cuadro 1.3:* ***Diseño de Prueba y resultado P05***

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| **DOMINIO PLANEAR Y ORGANIZAR** *Administrar la Inversión en TI* | **PO5** |
|---|---|

**Sub Objetivo 1.3:** Evaluar los recursos financieros aplicables para los requerimientos de TI y las prioridades dentro del presupuesto.

| ***Diseño de Prueba PO5*** | Verificar que los recursos financieros de TI y el proceso presupuestal incorporan la seguridad como una prioridad de TI. |
|---|---|

***Alcance:*** Prioridades dentro del presupuesto de TI, Proceso presupuestal, Administración de costos de TI y la Administración de beneficios de TI.

***Instrumento:*** Formato de Adquisición de compras, Formato de entrevista área informática

***Descripción de la Prueba:***
Se realiza entrevista a la alta gerencia que facilitó la información necesaria de la distribución de recursos financieros para el área de informática.

***Se toma en cuenta para la evaluación:*** Las alternativas de financiamiento, El control del gasto real y la justificación de costos y beneficios

***Evaluación - Resultados de PO5***

1. En la revisión de documentos detalle de gastos, se observo que existe consistencia en la distribución de presupuesto para la obtención de recursos de TI.
2. A nivel de Software y Hardware se sigue formalmente un procedimiento para la adquisición de Recursos de TI *(Ver Tabla de Formato de adquisición de compras)*, donde se evalúan a través de tres proformas facilitados por proveedores *(Ver Tabla Lista de Proveedores)* de equipos tecnológicos la opción más factible donde se retoman el aspecto de costos beneficios. De acuerdo a la selección que es consultada por la alta gerencia se procede a la compra.
3. A nivel de servicio se procede a entrevistar a la persona contacto de la empresa y de acuerdo a los beneficios que ofrecen es seleccionado el proveedor, términos prioritarios que se evalúan son costo, beneficio, calidad, experiencia y prestigio.

**MM_NIVEL 3. (Definido)**

- ✓ Las políticas y los procesos para inversiones y presupuestos están definidas y comunicadas y cubren temas clave de tecnología y negocio.
- ✓ Los procesos de selección de inversiones en TI y de presupuestos están formalizados, documentados y comunicados.

| | |
|---|---|
| **Hallazgos** | A nivel de adquisición de hardware existen informes y detalle presupuestarios, a nivel de servicios no se detalla el gasto invertido para la seguridad del sistema solo a nivel administrativo. |
| **Recomendaciones** | Se sugiere realizar anualmente una estimación de inversiones costo beneficios para adquisición del hardware y software, así como a nivel de servicios de manera que pueda visualizar el impacto en cuanto a calidad vs seguridad. |
| **Conclusiones** | El detalle de gastos de los recursos financieros satisface los requerimientos del negocio. |
| **Anexos** | Inversiones de TI, Política procedimiento Orden de compra. |

*Cuadro 1.4:* ***Diseño de Prueba y resultado ME1***

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO MONITOREAR Y EVALUAR<br>*Monitorear y Evaluar el desempeño de TI* | ME1 |
|---|---|

**Sub Objetivo 1.6:** Evaluar el monitoreo y desempeño en los procesos de TI tomando en cuenta la satisfacción del cliente con los servicios prestados.

| | |
|---|---|
| ***Diseño de Prueba ME1*** | Analizar que el Proceso de monitoreo realizado por la gerencia garantiza el funcionamiento correcto y el buen desempeño de los procesos de TI. |

***Alcance:*** Definición y recolección de datos de monitoreo, Enfoque y Método de Monitoreo, Evaluación del Desempeño, Reportes y Acciones correctivas

**Instrumento:** Formato de Entrevista al Administrador Regional

***Descripción de la Prueba:***
Se solicita a la gerencia reportes de indicadores de desempeño
Plan estratégico de TI para evaluar la comparación de Metas.

***Se toma en cuenta para la evaluación:***

- ✓ Definición por parte de la gerencia reportes e indicadores de desempeño gerenciales y la implementación de sistemas de soporte así como la atención regular a los reportes emitidos.
- ✓ Indicadores claves de desempeño y/o factores críticos de éxito y compararlos con los niveles objetivos propuestos para evaluar el desempeño de los procesos de la organización.
- ✓ El grado de satisfacción de los clientes con respecto a los servicios de información

***Evaluación - Resultados de ME1***

El monitoreo se realiza de manera informal, no existe una formato de recolección y evaluación.
El monitoreo por lo general se desarrolla eventualmente cuando surge un incidente, a pesar de eso no ha surgido la iniciativa por parte del Oficial Administrativo Logístico en desarrollar un Plan de Monitoreo formal, continuo y definido, donde se proyecten evaluación y aplicación de métricas de desempeño para este caso en los proceso de TI.

**MM_NIVEL 0. (No existe)**
La organización no cuenta con procesos implantados de monitoreo.
TI no lleva acabo monitoreo de proyectos o procesos de forma independiente.
No se cuenta con reportes útiles, oportunos y precisos.

| | |
|---|---|
| **Hallazgos** | No existe un modelo de evaluación donde se mida y reporte el desempeño de TI a través de indicadores específicos, por tanto no cuentan con reportes útiles, oportunos y precisos. |
| **Recomendaciones** | Definir e implantar un Plan de Monitoreo que contemple indicadores de desempeño, para evaluar periódicamente los procesos de la organización con el objetivo de alcanzar las metas de TI de la organización. |
| **Conclusiones** | Se concluye que es necesario que la gerencia se reúna para la planificación y definición de un plan de Monitoreo, así como su efectiva implementación en los proceso de TI. |
| **Anexos** | Ninguno |

*Cuadro 1.5:* ***Diseño de Prueba y resultado ME4***

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO MONITOREAR Y EVALUAR<br>*Proporcionar Gobierno de TI* | ME4 |
|---|---|

**Sub Objetivo 1.7**: Verificar que existe un gobierno de ti que contemple un marco de trabajo con leyes y regulaciones para una optima administración de los riesgos y recursos de TI.

| | |
|---|---|
| ***Diseño de Prueba ME4*** | Constatar la existencia de la administración de riesgos y recursos de TI. |

***Alcance:*** Administración de recursos y Administración de riesgos.
***Instrumento:*** Formato de Entrevista Responsable del Área Informática- Oficial Administrativo Logístico

***Descripción de la Prueba:***
Se llevó a cabo la entrevista al responsable de área informática.
Se indago la existencia de reporte e incidentes informáticos

***Se toma en cuenta para la evaluación:***

- ✓ Revisar inversión, uso y asignación de los activos de TI
- ✓ Definición del nivel de riesgo aceptable por la empresa y de prácticas usadas para la administración de riesgos de TI.
- ✓ Asignación de responsabilidades para la administración de riesgos en la organización, asegurando que el negocio y TI regularmente evalúan y reportan riesgos relacionado

***Evaluación - Resultados de ME4***

Se comprobó que la organización cuenta con gobierno de TI.

**MM_NIVEL 2. (Repetible pero Intuitivo)**
**L**a gerencia ha identificado mediciones básicas para el gobierno de TI, así como métodos de evaluación y técnicas; sin embargo, el proceso no ha sido adoptado a lo largo de la organización.
Los procesos, herramientas y métricas para medir el gobierno de TI están limitadas y pueden no usarse a toda su capacidad debido a la falta de experiencia en su funcionalidad.

| | |
|---|---|
| **Hallazgos** | No se realizan revisiones independientes del cumplimiento de TI |
| **Recomendaciones** | Se recomienda realizar revisiones del cumplimiento de TI y analizar si alcanzan sus objetivos |
| **Conclusiones** | Es necesario que el gobierno de TI implemente en su marco de trabajo el manejo de reportes de tal manera que exista un control sobre los riesgos presentados. |
| **Anexos** | Contrato AMNET |

## *12.2 Objetivo 2 de Auditoria*

Evaluar la existencia de procedimientos, normas, y políticas relativas a la seguridad, requeridas para el desempeño eficiente de cada una de las funciones informáticas.

*Cuadro 2.1:* ***Diseño de Prueba y resultado P06***

MS América Central
actionaid denmark

**MATRIZ DE PRUEBA Y RESULTADO**

| **DOMINIO PLANEAR Y ORGANIZAR**<br>***Comunicar las Aspiraciones y la Dirección de Gerencia*** | **PO6** |
|---|---|

**Sub Objetivo 2.1:** Evaluar que exista una correcta distribución a los usuarios de políticas y procedimientos de TI.

| | |
|---|---|
| ***Diseño de Prueba PO6*** | Verificar la distribución y conocimiento en los usuarios sobre las políticas y procedimientos de TI existentes en el área de informática. |

***Alcance:*** Riesgo corporativo y marco de referencia de control interno TI, Administración de políticas de TI y la Implantación de políticas para TI.

***Instrumento:*** Formato de Entrevista para el Oficial Administrativo Logístico, C -01: Políticas y Medidas de Seguridad Informática

***Descripción de la Prueba***

Se realiza encuesta a usuarios con el objetivo de comprobar el grado de conocimiento que tienen sobre las políticas de seguridad de TI y aplicación de control interno.

Se entrevista al Oficial Administrativo Logístico con el fin de evaluar cuáles son los parámetros para establecer las PSI y el aseguramiento de su implantación en el área informática.

***Se toma en cuenta para la evaluación:***

- ✓ Los código de ética / conducta, el cumplimiento de las reglas de ética, conducta, seguridad y estándares de control interno debe ser establecido por la Alta Gerencia y promoverse
- ✓ Las directrices tecnológicas, El cumplimiento, aseguramiento y monitoreo durante la implementación de sus políticas y Las políticas de seguridad y control interno

***Evaluación- Resultados de PO6***

La alta gerencia comunica al personal las políticas de seguridad y control interno.

**MM_NIVEL 2. (Repetible pero intuitivo)**

- ✓ La gerencia tiene un entendimiento implícito de las necesidades y de los requerimientos de un ambiente de control de información efectivo, aunque las prácticas son en su mayoría informales.
- ✓ La gerencia ha comunicado la necesidad de políticas, procedimientos y estándares de control, pero la elaboración se delega a la discreción del gerente y áreas de negocios individuales.

| | |
|---|---|
| **Hallazgos** | No poseen documento físico, que establezcan políticas de TI tanto para el personal de TI, como a usuarios. Estas son trasmitidas al personal de manera verbal. |
| **Recomendaciones** | Es necesario elaborar un documento para la administración de políticas de TI y control interno en el cual de contemplen multas y acciones disciplinarias asociadas con la falta de cumplimiento de esta políticas. |
| **Conclusiones** | Los usuarios tienen poco conocimiento de las políticas que se deben de poner en práctica, dejando expuestos a posibles riesgos que afecten la seguridad de MS. |
| **Anexos** | Ninguno |

*Cuadro 2.2:* ***Diseño de Prueba y resultado ME3***

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| **DOMINIO MONITOREAR Y EVALUAR**<br>***Garantizar el Cumplimiento con requerimientos externos*** | **ME3** |
|---|---|

**Sub Objetivo 2.2**: Evaluar el cumplimiento del área informática con respecto a los requerimientos externos.

| | |
|---|---|
| ***Diseño de Prueba ME3*** | Constatar que las obligaciones legales y contractuales se rigen por una base continua de leyes locales e internacionales. |

***Alcance:*** Identificar los requerimientos de las leyes, regulaciones y cumplimientos contractuales y la evaluación del cumplimiento con requerimientos externos.

***Instrumentos:*** Formato de Entrevista 05: SEQUINSA – Gerente de Operaciones

***Descripción de la Prueba***
Se retoma, Contrato de Servicios con AMNET
Se realiza Entrevista a Gerente de Operaciones de SEQUINSA
Se investigaron lo servicios ofrecidos por AMNET y cual cumplía con las Políticas Locales

***Se toma en cuenta para la evaluación:***

- ✓ Definición y mantenimiento de procedimientos para la revisión de requerimientos externos, para la coordinación de estas actividades y para el cumplimiento continúo de los mismos.
- ✓ Leyes, regulaciones y contratos
- ✓ Seguridad y ergonomía con respecto al ambiente de trabajo de los usuarios y el personal de la función de servicios de información.
- ✓ Privacidad
- ✓ Propiedad intelectual

***Evaluación- Resultados de ME3***

Se constató que el servicio brindado por AMNET está debidamente respaldado por medio de cláusulas que garantizan el cumplimiento de ellas.
La forma de trabajo implementado por SEQUINSA es por medio de servicios realizados.
**MM_NIVEL 4. (Administrado y medible)**
Existe un entendimiento completo de los eventos y de las exposiciones a requerimientos externos y la necesidad de asegurar el cumplimiento de todos los niveles.
Las responsabilidades son claras y se entiende el empoderamiento de los procesos.
Buenas prácticas internas estandarizadas se usan para necesidades específicas tales como reglamentos vigentes y contratos recurrentes de servicio.

| | |
|---|---|
| **Hallazgos** | No aplica |
| **Recomendaciones** | No aplica |
| **Conclusiones** | La organización MS lleva a cabo una identificación y análisis de requerimientos previos para adquirir un servicio, contando con documentos legales que lo respalden, obteniendo así, un óptimo resultado en los servicios prestados por terceros. |
| **Anexos** | Ninguno |

## *12.3 Objetivo 3 de Auditoria*

Revisar el nivel de seguridad de los recursos de TI para garantizar la protección de activos y el resguardo e integridad de los datos.

*Cuadro 3.1:* ***Diseño de Prueba y resultado PO2***

MS América Central actionaid denmark

**MATRIZ DE PRUEBA Y RESULTADO**

| **DOMINIO PLANEAR Y ORGANIZAR** *Definirla Arquitectura de la Información* | **PO2** |
|---|---|

**Sub Objetivo 3.1:** Revisar el modelo de creación y Mantenimiento de los Sistema de Información (SI)

| ***Diseño de Prueba PO2*** | Revisar la definición de los Modelos y arquitectura de los SI |
|---|---|

***Alcance:*** Requerimientos de negocio, organización de los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio, asegurándose que se definan los sistemas apropiados para optimizar la utilización de esta información
***Instrumento:*** Formato de Entrevista Oficial Administrativo Logístico, Listas de Verificación. Revisión Documental de los Sistemas.

***Descripción de la Prueba***

Se aplica entrevista a Oficial Administrativo Logístico para revisar el modelo de creación y mantenimiento que se definan los sistemas apropiados para optimizar la utilización de esta información, se aplican instrumentos como listas de verificación

***Se toma en cuenta para la evaluación:***

- ✓ La documentación deberá conservar consistencia con las necesidades permitiendo a los responsables llevar a cabo sus tareas eficiente y oportunamente.
- ✓ El diccionario de datos, el cual incorporara las reglas de sintaxis de datos de la organización y deberá ser continuamente actualizado.
- ✓ La propiedad de la información y la clasificación de severidad con el que se establecerá un marco de referencia de clasificación general relativo a la ubicación de datos en clases de información.

***Evaluación - Resultados de PO2***

Se verifico en el servidor la arquitectura de la información y se solicito documentación sobre la arquitectural el cual no se encontró documentada por el responsable del área.

**MM_NIVEL 2. (Repetible)**
Surge un proceso de arquitectura de información y existen procedimientos similares, aunque intuitivos e informales, que se siguen por distintos individuos dentro de la organización. Las personas obtienen sus habilidades al construir la arquitectura de la información por medio de experiencia práctica y aplicación repetida de técnicas.

| | |
|---|---|
| **Hallazgos** | No Existe documentado el marco de referencia de clasificación general de datos en clase de información. |
| **Recomendaciones** | Elaborar o diseñar un manual que defina la arquitectura y distribución de información. |
| **Conclusiones** | Un 70 % de los trabajadores conocen como está estructurada la información a nivel operativo. La Información es transmitida verbalmente. |
| **Anexos** | Imágenes Arquitectura de la Información |

*Cuadro 3.2: Diseño de Prueba y resultado AI3*

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ADQUIRIR E IMPLEMENTAR<br>*Adquirir y mantener infraestructura tecnológica* | AI3 |
|---|---|

**Sub Objetivo 3.1: Evaluar y analizar la plataforma tecnología para aplicaciones**

| ***Diseño de Prueba AI3*** | Evaluar el Desempeño de Hardware y Software |
|---|---|

***Alcance:*** *Cierta influencia, sobre todo en la* Protección y disponibilidad del recurso de infraestructura y el Mantenimiento de la infraestructura
***Instrumento:*** Formato de Entrevista Oficial Administrativo Logístico

***Descripción de la Prueba***
Se aplica entrevista a Oficial Administrativo Logístico para evaluar la protección y disponibilidad de los recursos, así como la administración de la seguridad en el sistema de Red.
Se realiza chequeo y verificación de visitas por parte de SEQUINSA para el mantenimiento preventivo de Hardware.

***Se toma en cuenta para la evaluación:***

Para ello se realizara una evaluación del desempeño del hardware y software, la provisión de mantenimiento preventivo de hardware y la instalación, seguridad y control del software del sistema y toma en consideración:

- ✓ Evaluación de tecnología para identificar el impacto del nuevo hardware o software sobre el rendimiento del sistema general, Mantenimiento preventivo del hardware.
- ✓ Seguridad del software de sistema, instalación y mantenimiento para no arriesgar la seguridad de los datos y programas ya almacenados en el mismo.

***Evaluación - Resultados de AI3***

Se procedió a evaluar el desempeño del hardware y software. Encontrando lo siguiente:
Se evalúa previamente la compatibilidad del HW y SW de manera que no afecte y mejore el rendimiento del sistema general. Mantenimiento preventivo del hardware se realiza trimestralmente según reportes de SEQUINSA y Programación de Actividades del Oficial Administrativo Logístico. Cada equipo cuenta con los Drivers del Sistema y respaldo de información, en casos de que la instalación y mantenimiento inadecuado por personal inexperto falle.

**MM_NIVEL 4. (Administrado y definido)**
Se desarrolla el proceso de adquisición y mantenimiento de la infraestructura de tecnología a tal punto que funciona bien para la mayoría de las situaciones, se le da un seguimiento consistente y un enfoque hacia la reutilización. La infraestructura de TI soporta adecuadamente las aplicaciones del negocio.

| | |
|---|---|
| **Hallazgos** | No Aplica |
| **Recomendaciones** | No Aplica |
| **Conclusiones** | Los usuarios de MS son eficientes y autónomos sin dificultad de migración de software ejemplo (profesional – Vista), el objetivo está desarrollado eficientemente según Sequinsa. |
| **Anexos** | Contrato AMNET |

**Cuadro 3.3: Diseño de Prueba y resultado AI4**

| MS América Central actionaid denmark — MATRIZ DE PRUEBA Y RESULTADO | |
|---|---|
| **DOMINIO ADQUIRIR E IMPLEMENTAR** *Facilitar la operación y el uso* | **AI4** |
| **Sub Objetivo 3.2: Evaluar el nivel de operación y uso de Aplicaciones por parte del personal involucrado.** | |
| ***Diseño de Prueba AI4*** | Revisar técnica y operativamente el nivel de transferencia y conocimiento del personal con respecto a las operaciones y uso de aplicaciones. |
| ***Alcance:*** *Influyen algunos puntos en el* Plan para soluciones de operación, la Transferencia de conocimientos a la gerencia del negocio, Transferencia de conocimientos a usuarios finales y la Transferencia de conocimientos a personal de operaciones y soporte<br>***Instrumento:*** Formato de Entrevista Oficial Administrativo Logístico y Oficial Administrativo financiero. C-03: Contingencia de aplicaciones | |
| ***Descripción de la Prueba***<br>Se realiza encuesta a Usuarios de Manera Aleatoria sobre aplicaciones en operación y uso<br>Se realiza entrevista a Oficial Administrativo Logístico y Oficial Administrativo financiero.<br>Se revisa documentación de aplicaciones.<br><br>***Se toma en cuenta para la evaluación:***<br>Para ello se realiza un enfoque estructurado del desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento y toma en consideración:<br>✓Manuales de procedimientos de usuarios y controles, de manera que los mismos permanezcan en permanente actualización para el mejor desempeño y control de los usuarios.<br>✓Manuales de Operaciones y controles, de manera que estén en permanente actualización.<br>✓Materiales de entrenamiento enfocados al uso del sistema en la práctica diaria. | |
| ***Evaluación - Resultados de AI4*** | |
| Se procede a evaluar a usuarios y responsable de la capacitación a través de entrevistas y metodología de observación.<br>La Oficial Administrativo financiero es la responsable de brindar capacitación y entrenamiento a usuarios nuevos del sistema de una manera práctica.<br>Así mismo el Oficial Administrativo Financiero es el que solicita nuevas actualizaciones y un Plan de capacitación anual para el personal.<br>El personal cuenta con un nivel de conocimiento básico sobre el uso de aplicaciones.<br><br>**MM_NIVEL 0. (No existe)**<br>No existe el proceso con respecto a la producción de documentación de usuario, manuales de operación y material de entrenamiento, los únicos materiales que existentes son aquellos que se suministran con los productos que se adquieren. | |
| **Hallazgos** | No existe proceso de elaboración y desarrollo de manuales de procedimientos de operaciones para usuarios, requerimientos de servicio y material de entrenamiento. |
| **Recomendaciones** | Se recomienda contar con Manuales de operación, procedimientos de usuarios y controles, de manera que los mismos estén en permanente actualización para el mejor desempeño y control de los usuarios. |
| **Conclusiones** | Es importante que todo usuario reconozca el nivel de conocimiento en base a |

| | |
|---|---|
| | documentos formales, la complemento del conocimiento se basa en el aprendizaje practico como teórico y desarrollando u nivel de conciencia en los usuarios sobre el manejo y uso de las aplicaciones. |
| **Anexos** | Ninguno |

*Cuadro 3.4:* ***Diseño de Prueba y resultado AI5***

MS América Central actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ADQUIRIR E IMPLEMENTAR<br>*Adquirir recursos de TI (Persona, HW, SW, Servicios)* | **AI5** |
|---|---|

**Sub Objetivo 3.3: Evaluar la rentabilidad y utilidad de los recursos de TI**

| | |
|---|---|
| ***Diseño de Prueba AI5*** | Revisar la existencia y aplicación de procedimientos estándares para la adquisición de recursos de TI |

***Alcance:*** *Influyen en cierto modo el* Control de Adquisición, Administración de Contratos con proveedores, Selección de proveedor y la Adquisición de recursos de TI
***Instrumento:*** Formato de Entrevista a Oficial Administrativo Logístico

***Descripción de la Prueba:***
Se aplica Entrevista a Oficial Administrativo Logístico, Se evalúa el procedimiento de adquisición de Hardware y Software, Se solicita Documentación de Procedimientos y estándares de aplicación
Se solicita lista de Proveedores

***Se toma en cuenta para la evaluación:*** de los procedimientos de adquisición, selección de proveedores y se toma en consideración la Asesoría profesional legal y estructural, La definición de procedimientos y estándares de adquisición y la adquisición de Hardware, Software y Servicios requeridos de acuerdo a los procedimientos definidos

***Evaluación- Resultados de AI5***

Se procede a realizar entrevista al Oficial Administrativo logístico y revisión documental, teniendo como resultado que existe un procedimiento de adquisición de recursos de TI, el cual consiste en elaborar un estudio de factibilidad por parte del Oficial administrativo Logístico.
Este se pasa al Oficial Administrativo Financiero, Una vez aprobado se pasa al Administrador regional para su revisión y autorización final.
Luego se procede a realizar 3 cotizaciones como mínimo sobre oferta de venta, estas se evalúan y se aprueba la que cumple con las políticas de requerimientos y adquisición de recursos de TI de la institución.
En cuanto a la elección de proveedores se cuenta con una BD que se actualiza de manera trimestral, manteniendo en primera prioridad aquellos proveedores que en su momento demostraron en el servicio: calidad, eficacia, eficiencia y confidencialidad y seguridad. La definición de procedimientos y estándares de adquisición son definidas por los responsables de área.

**MM_NIVEL 3. (Definido)**
La administración establece políticas y procedimientos para la adquisición de TI.
Los proveedores de recursos de TI se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.
La administración de TI comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de TI.

| | |
|---|---|
| **Hallazgos** | No Aplica |
| **Recomendaciones** | No Aplica |
| **Conclusiones** | Existe una lista de proveedores, con sus respectivo contrato y hay un control sobre las adquisiciones de TI |
| **Anexos** | Contrato AMNET. Inversiones de TI, Política de Procedimiento de Orden de Compra |

*Cuadro 3.5: Diseño de Prueba y resultado DS5*

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ENTREGAR Y DAR SOPORTE<br>*Garantizar la seguridad de los sistemas* | DS5 |
|---|---|

**Sub Objetivo 3.4: Evaluar la administración y el nivel de seguridad de los sistemas**

| | |
|---|---|
| ***Diseño de Prueba DS5*** | Evaluar procedimientos para mantener un satisfactorio y eficiente nivel de seguridad lógico de los sistemas por parte del personal involucrado. |

***Alcance:*** *Influencia importante en la* Administración de la seguridad de TI, Plan de seguridad de TI, Administración de Identidad, Administración de Cuentas de Usuario, Pruebas, vigilancia y monitoreo de la seguridad, Definición de incidentes de seguridad, Protección de la tecnología de seguridad, Prevención, detección y corrección de software malicioso, Seguridad de la Red y el Intercambio de datos sensitivos.

**Instrumentos:**

C-05: Administración de la Seguridad de la Aplicaciones
C-06: Administración de la Seguridad informática
C-09: Sistema de Red y Comunicación
LV- AC 07: Evaluación de la Administración de Acceso

***Descripción de la Prueba:***

Se aplica herramientas de Auditoria como NESSUS, para evaluar la vulnerabilidad de la red de MS, Symantec Antivirus Corporativo contra intrusos, amenazas, virus y software malicioso

Revisión de Cortafuego Corporativo SONICWALL
Seguridad mínima de los sistemas, pruebas de control de acceso, revisión de cuentas y perfiles de usuarios, Documentación y reportes de incidentes

***Se toma en cuenta para la evaluación:***

Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración:

- ✓ Autenticación y Autorización, el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso
- ✓ Perfiles e identificación de usuarios estableciendo procedimientos para asegurar acciones oportunas relacionadas con la requisición, establecimiento, emisión, suspensión de cuentas de usuario
- ✓ Manejo, reporte y seguimiento de incidentes implementado capacidad para la atención de los mismos
- ✓ Prevención y detección de virus tales como Caballos de Troya, estableciendo adecuadas medidas de control preventivas, detectives y correctivas.
- ✓ Firewalls si de Utilización existe una conexión con Internet u otras redes públicas en la organización

***Evaluación - Resultados de DS5***

En la evaluación a través de los mecanismos de prueba se logró verificar los siguiente:

1. Autenticación y Autorización: Existe un mecanismo el acceso lógico para el uso de los recursos de TI se restringen a través políticas formales. El mecanismo de autenticación lo realiza el Oficial Administrativo logístico se encarga de la creación de usuarios, considerando el perfil, el cargo y las responsabilidades, tomando en cuenta esto se le dan los permisos de acceso.
2. Perfiles e identificación de usuarios: Cuentan con procedimientos para la requisición, establecimiento, emisión y suspensión de cuentas de usuario, pero estos procedimientos no están documentados
3. No hay reporte de los incidente afrontados por el área de informática
4. Para la Prevención y detección de virus como Caballos de Troya, están establecidas medidas de

control preventivas, detectives y correctivas. Se hace uso del Software Symantec Antivirus instalado en el servidor de red y en los Cliente, este software cuenta con licencia de uso y es administrado por el Oficial Administrativo logístico. Como no existe una política para el uso adecuado de Internet, se encontró que usuarios hacen descarga de SW y otros archivos que incrementa la exposición de virus en los equipos.

5. Se realizaron pruebas de descarga de instalación de SW que aparentemente parecen ser seguros verificando que SYMANTEC ANTIVIRUS detecto Troyanos, enviando a cuarentena el archivo y deteniendo la instalación.
6. Se encontró además que en algunos equipos el SW no estaba actualizado y estos equipos estaban con virus, en los reportes emitíos por SEQUINSA, no detallan actualización del SW.
7. Como seguridad mínima en todos los equipos se encuentra activado el Firewalls
8. En el servidor se encuentra instalado SONICWALL, este defiende la seguridad de las redes inalámbricas móviles y tradicionales, usuarios y aplicaciones (y sus dispositivos de punto final), a la vez que analiza y desinfecta todo el flujo de datos a través de las plataformas y perímetros.

SONICWALL, provee protección antivirus, Antispyware y prevención de intrusos a nivel de puertas de enlace. En la actualidad el sistema ha detectado intrusos bloqueándolos automáticamente.

**MM_NIVEL 2 (Repetible pero Intuitivo)**
Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI.
Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza.

Los reportes de la seguridad de TI son incompletos, engañosos o no aplicables.

| | |
|---|---|
| **Hallazgos** | El acceso lógico se encuentra bien definido pero no documentado los usuarios desconocen los procedimientos formales. No existen reportes de detección de virus al servidor de red LAN y a clientes del sistema.<br>No existen reportes de detección de virus al servidor de red LAN y a clientes del sistema.<br>No se han establecidos medidas de control preventivas, detectives y correctivas ante amenazas y virus formalmente documentada. |
| **Recomendaciones** | Elaborar documento que contenga descripción y políticas definida para el acceso lógico por usuarios y cargos.<br>Contar con un manual de procedimiento ante amenazas y virus tanto para usuarios como para el administrador del área y sistemas.<br>Desarrollar documento que describan los procedimientos de requisición, establecimiento, emisión, y suspensión de cuentas de usuario siendo estas informadas a los usuarios formalmente. |
| **Conclusiones** | Técnicamente se dan todas las acciones pero sin fundamento formal.<br>Actualmente el área de informática tiene implantado el SW de auditoría Symantec 10.1 para monitorear el sistema de red ante intrusos, amenazas y virus pero a pesar de que se cuenta con esta herramienta no se emiten reportes desde el servidor como de los clientes de la red. |
| **Anexos** | Vulnerabilidad de la Red NESSUS 4.4, Captura de imágenes. |

*Cuadro 3.6:* ***Diseño de Prueba y resultado DS7***

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| **DOMINIO ENTREGAR Y DAR SOPORTE**<br>***Educar y entrenar a los usuarios*** | **DS7** |
|---|---|

**Sub Objetivo 3.5: Evaluar el nivel de conocimiento y capacitación del personal MS con respecto a tecnologías informáticas.**

| | |
|---|---|
| ***Diseño de Prueba DS7*** | Revisar el nivel de responsabilidad y conciencia acerca del uso de las TI |

***Alcance:*** *Influye lo referido a seguridad en la* Identificación de necesidades de entrenamiento y educación, impartición de entrenamiento y educación y en la Evaluación del entrenamiento recibido.

***Instrumento:*** Cuestionario de Seguridad Informática- Usuario1 y Usuario 2, Formato de Entrevista al Oficial Administrativo Logístico, Formato de Entrevista al Oficial Administrativo Financiero.

***Descripción de la Prueba:***
Se realiza entrevista a dos usuarios seleccionados de manera aleatoria para medir el nivel de conocimiento en TI
Se aplica entrevista al Oficial administrativo logístico y al Oficial Administrativo financiero para evaluar el plan de entrenamiento y desarrollo de conocimientos en temas Informáticos.
Se solicitan procedimientos de identificación de necesidades de capacitación

***Se toma en cuenta para la evaluación:***
Para ello se realiza un plan completo de entrenamiento, desarrollo y se toma en consideración:

- ✓Curriculum de entrenamiento estableciendo y manteniendo procedimientos para identificar y documentar las necesidades de entrenamiento de todo el personal que haga uso de los servicios de información
- ✓Campañas de concientización, Técnicas de concientización proporcionando un programa de educación y entrenamiento que incluya conducta ética de la función de servicios de información.

***Evaluación- Resultados de DS7***

Cada personal presenta al Oficial Administrativo Logístico en los primeros meses del Año un plan de Capacitación personal sobre las necesidades de formación.
El nivel de conocimiento de los usuarios en TI, es básico, el del personal responsables de áreas de TI es medio – alto. No se realiza técnicas ni campañas de concientización

**MM_NIVEL 1 (Inicial)**
Hay evidencia de que la organización ha reconocido la necesidad de contar con un programa de entrenamiento y educación, pero no
hay procedimientos estandarizados

| | |
|---|---|
| **Hallazgos** | No se realizan programas de entrenamiento y educación para el personal con respecto a temas de TI y los posibles riesgos informáticos. |
| **Recomendaciones** | Retomar como punto de agenda en encuentros, reuniones y capacitación en temas tecnológicos a fin de que se adopte una conducta concientizada y responsable. |
| **Conclusiones** | El programa de capacitación, no es asignado por la alta gerencia, según las necesidades del área Informática, sino que son elegidas según las necesidades que se plantean por parte del trabajador. |
| **Anexos** | Ninguno |

*Cuadro 3.7:* ***Diseño de Prueba y resultado DS11***

MS América Central actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ENTREGAR Y DAR SOPORTE<br>*Administrar los datos* | DS11 |
|---|---|

**Sub Objetivo 3.6: Analizar los controles generales y de operación de la administración de datos**

| | |
|---|---|
| ***Diseño de Prueba DS11*** | Revisar y analizar procedimientos de validación, almacenamiento, respaldo y recuperación de los datos. |

***Alcance:*** *Influye en los* Acuerdos de almacenamiento y conservación, en los Sistemas de administración de librerías de medios, Eliminación, Respaldo y restauración y Requerimientos de seguridad para la administración de datos

**Instrumentos:** Formato de Entrevista al Oficial Administrativo Financiero y Asistente Administrativo.

***Descripción de la Prueba:*** Revisión de Documentos Fuentes, Revisión de documentos de controles generales y de aplicación sobre las operaciones de TI y acuerdos de almacenamiento, Revisión de Registros Físicos de datos y Pruebas de validación y Entrada de datos.

***Se toma en cuenta para la evaluación:*** Una combinación efectiva de controles generales y de aplicación sobre las operaciones de TI. Para tal fin, la gerencia deberá diseñar formatos de entrada de datos para los usuarios de manera que se minimicen lo errores y las omisiones durante la creación de los datos.

- ✓Este proceso deberá controlar los documentos fuentes, de manera que estén completos, sean precisos y se registren apropiadamente. Cabe destacar la importancia de crear procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas) de todas las transacciones y datos manejados por la organización, albergados tanto dentro como fuera de la empresa.
- ✓La gerencia deberá asegurar también la integridad, autenticidad y confidencialidad de los datos almacenados, definiendo e implementando procedimientos para tal fin.

***Evaluación- Resultados de DS11***

Existen procedimientos para el almacenamiento, respaldo y recuperación de datos, teniendo un registro físico (discos, disquetes, CDs y cintas magnéticas), este se encuentra dentro de las instalaciones como única copia.

La gerencia con el proveedor de Mantenimiento de equipos no asegura a través de un documento formal la confidencialidad de los datos y almacenados.

Los procedimientos de respaldo se realizan, una vez por semana

**MM_NIVEL 3.Definido**

Se entiende y acepta la necesidad de la administración de datos tanto de dentro de TI como dentro de la organización. Se establece la responsabilidad sobre la administración de los datos.

Los procedimientos de administración de datos se formalizan dentro de TI y se utilizan algunas herramientas de respaldo, recuperación y desecho de equipos.

| | |
|---|---|
| **Hallazgos** | No Existe Manual instructivo acerca de los procedimientos de almacenamiento y conservación de datos para conocimiento de usuario.<br>Se encuentra un único respaldo de información en medio de almacenamiento físico. |
| **Recomendaciones** | Elaborar o diseñar un manual instructivo para usuarios.<br>Realizar un segundo respaldo de los datos y almacenar fuera de las instalaciones. |
| **Conclusiones** | Se concluye que es necesario tomar en cuenta el Riesgo de tener un único respaldo físico de información dentro de las instalaciones, por lo cual se debe tener otro respaldo fuera para minimizar la posible pérdida de información. |
| **Anexos** | Captura de imágenes. |

**Cuadro 3.8:** *Diseño de Prueba y resultado DS12*

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ENTREGAR Y DAR SOPORTE<br>*Administrar el ambiente físico* | DS12 |
|---|---|

**Sub Objetivo 3.7: Inspeccionar el ambiente físico de las instalaciones de MS**

| | |
|---|---|
| ***Diseño de Prueba DS12*** | Evaluar los procedimientos y controles físicos y ambientales de las instalaciones. |

***Alcance:*** Selección y diseño del centro de datos, Medidas de seguridad física, Acceso físico, Protección contra factores ambientales y la Administración de las instalaciones físicas.
**Instrumento:** C- 08: Control de Acceso Físico

***Descripción de la Prueba:*** Se realiza visita a las diferentes áreas de MS para evaluar las condiciones y medidas de seguridad, Se aplica Lista de verificación de Administración de controles, Se aplica Lista de verificación de Administración de Acceso, Se aplica Cheklist Acceso Físico.

***Se toma en cuenta para la evaluación:*** La instalación de controles físicos y ambientales adecuados que sean revisados regularmente para su funcionamiento apropiado definiendo procedimientos que provean control de acceso del personal a las instalaciones y contemplen su seguridad física.

***Evaluación - Resultados de DS12***

De acuerdo a la verificación: Existen procedimientos de control para la instalación de controles físicos y ambientales. Existe un documento de seguridad interno donde se describen algunas normas de control y cuido del local. El ambiente físico cuenta con cámaras de seguridad, personal de seguridad día y noche, cuadernos de control de equipos que entran y salen en horarios de trabajo y fuera de horario.

Existe un Sistema de Alarma, extintores en 4 puntos clave y planta eléctrica manual.
Los aires acondicionados permanecen a una temperatura adecuada para evitar el recalentamiento de los equipos, y existen extractores de humedad. El área de banco de datos se encuentra restringida solo con acceso a persona autorizado.

**MM_NIVEL 5 (Optimizado)**
Hay un plan acordado a largo plazo para las instalaciones requeridas para soportar el ambiente cómputo de la organización.
Los estándares están definidos para todas las instalaciones, incluyendo la selección del centro de cómputo, construcción, vigilancia, seguridad personal, sistemas eléctricos y mecánicos, protección contra factores ambientales (por ejemplo, fuego, rayos, inundaciones, etc.).
Se clasifican y se hacen inventarios de todas las instalaciones de acuerdo con el proceso continuo de administración de riesgos de la organización.

| | |
|---|---|
| **Hallazgos** | No se realizan las debidas rotulaciones para cada medida de seguridad establecidas por el Área de TI.<br>Las instalaciones no cuentan con detectores de humo e incendio. |
| **Recomendaciones** | Es necesario que el personal pueda visualizar los rótulos que ayuden a minimizar el riesgo de pérdida humana o material.<br>Es Factible tomar en cuenta la instalación de detectores de humo e incendio, para un mejor resguardo de los activos. |
| **Conclusiones** | Se debe definir e implementar procedimientos de seguridad física, que salvaguarden al personal, activos y recursos de TI. Previendo, el riesgo de una interrupción de servicio. |
| **Anexos** | Plano de Control de Acceso y Seguridad, Captura de Imágenes. |

*Cuadro 3.9:* ***Diseño de Prueba y resultado DS13***

MS América Central
actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ENTREGAR Y DAR SOPORTE<br>*Administrar las operaciones* | DS13 |
|---|---|

**Sub Objetivo 3.8: Evaluar los procedimientos e instrucciones para la administración de Operaciones de TI**

| | |
|---|---|
| ***Diseño de Prueba DS13*** | Revisar y evaluar la calendarización, cumplimiento y monitoreo de actividades de soporte de TI. |

***Alcance:*** Procedimientos e instrucciones de operación, Programación de tareas, Monitoreo de la infraestructura de TI, Documentos sensitivos y dispositivos de salida y Mantenimiento preventivo del hardware.

Instrumento: Formato de Entrevista al Oficial administrativo logístico

***Descripción de la Prueba***

Se realiza entrevista al Oficial administrativo logístico para evaluar procedimientos y funciones importantes llevada a cabo para el soporte de TI.
Se revisa la emisión de informe.

***Se toma en cuenta para la evaluación:*** se logra a través de una calendarización de actividades de soporte que sea registrada y completada en cuanto al logro de todas las actividades. Para ello, la gerencia deberá establecer y documentar procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales deberán ser revisados periódicamente para garantizar su eficiencia y cumplimiento.

***Evaluación - Resultados de DS13***

Se realiza entrevista al Oficial Administrativo Logístico para evaluar procedimientos:
Todas las actividades de TI se calendarizan.
La gerencia establece procedimientos para las operaciones de tecnología de información (incluyendo operaciones de red), los cuales son revisadas y evaluadas periódicamente por el personal involucrado de TI, para garantizar su eficiencia y cumplimiento.

**MM_NIVEL 5. (Optimizado)**
Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio con una pérdida de productividad mínima.
Los procesos automatizados que soportan los sistemas contribuyen a un ambiente estable.
Todos los problemas y fallas se analizan para identificar la causa que los originó

| | |
|---|---|
| **Hallazgos** | No Aplica |
| **Recomendaciones** | No Aplica |
| **Conclusiones** | El Objetivo se desarrolla eficientemente.<br>Se planifican y monitoreas las actividades del área con el personal involucrado. |
| **Anexos** | Reporte de Mantenimiento de equipos SEQUINSA<br>Captura de Imágenes |

## *12.4 Objetivo 4 de Auditoria*

Evaluar el desempeño y proceso del Outsourcing tecnológico entre la organización y proveedoras de servicio tecnológico.

*Cuadro 4.1:* ***Diseño de Prueba y resultado DS1***

MS América Central
actionaid denmark

**MATRIZ DE PRUEBA Y RESULTADO**

| **DOMINIO ENTREGAR Y DAR SOPORTE**<br>***Definir y Administrar los Niveles de Servicios*** | **DS1** |
|---|---|

**Sub Objetivo 4.1:** Verificar la administración de los niveles servicio tomando en cuenta la calidad, disponibilidad y seguridad

| | |
|---|---|
| ***Diseño de Prueba DS1*** | Comprobar que la administración de los niveles de servicio tiene contenidas SLA y OLA. |

***Alcance:*** Marco de trabajo de la administración de los niveles de Riesgo, SLA acuerdos de niveles de servicio, OLA acuerdos de niveles de operación, Monitoreo y reporte del nivel de cumplimiento de los niveles de servicio.

***Instrumentos:*** Formato de Entrevista 05: SEQUINSA – Gerente de Operaciones, Formato de Entrevista al Oficial Administrativo Logístico

***Descripción de la Prueba:*** Se realiza la revisión de procedimientos de desempeño y responsabilidades en las diferentes áreas. Se solicita el organigrama para observar dependencias, se revisa el contrato de servicio con AMNET y se revisan los acuerdos de servicios con SEQUINSA.

***Se toma en cuenta para la evaluación:***

- ✓ Convenios formales que determinen la disponibilidad, confiabilidad, desempeño, capacidad de crecimiento, niveles de soporte proporcionados al usuario, plan de contingencia / recuperación, nivel mínimo aceptable de funcionalidad del sistema satisfactoriamente liberado, restricciones (límites en la cantidad de trabajo), cargos por servicio, instalaciones de impresión central (disponibilidad), distribución de impresión central y procedimientos de cambio.
- ✓ Definición de las responsabilidades de los usuarios y de la función de servicios de información
- ✓ Procedimientos de desempeño
- ✓ Definición de dependencias asignando un Gerente de nivel de Servicio que sea responsable de monitorear y reportar los alcances de los criterios de desempeño del servicio especificado y todos los problemas encontrados durante el procesamiento.
- ✓ Provisiones para elementos sujetos a cargos en los acuerdos de niveles de servicio.
- ✓ Garantías de integridad
- ✓ Convenios de confidencialidad
- ✓ Implementación de un programa de mejoramiento del servicio.

***Evaluación- Resultados de DS1***

Se pudo comprobar que las responsabilidades están definidas, coordinadas y comunicadas a las áreas afectadas.

**MM_NIVEL 3. (Definido)**

- ✓ Los servicios y los niveles de servicio están definidos, documentados y se ha acordado utilizar un proceso estándar.
- ✓ Hay un claro vínculo entre el cumplimiento del nivel de servicio esperado y el presupuesto contemplado.

| | |
|---|---|
| **Hallazgos** | La falta de un contrato formal con SEQUINSA pone en riesgo la seguridad al |

| | |
|---|---|
| | sistema de información de MS. |
| **Recomendaciones** | Es necesario que con los proveedores se establezca ACUERDOS DE SERVICIOS FORMALES que sustenten los términos de calidad, disponibilidad y seguridad en el acceso y administración de los recursos de TI. |
| **Conclusiones** | Se ha comprobado que MS cuenta con niveles de servicios óptimos para alcanzar los objetivos de la organización, ya que toman en cuenta los SLA y OLA, únicamente cuando se establece una RELACION DE CONTRATO DE SERVICIO. |
| **Anexos** | Contrato AMNET |

*Cuadro 4.2:* ***Diseño de Prueba y resultado DS2***

MS América Central actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| **DOMINIO ENTREGAR Y DAR SOPORTE**<br>***Administrar los Servicios de Terceros*** | **DS2** |
|---|---|

**Sub objetivo 4.2:** Verificar que el servicio administrado por terceros sea claramente definido.

| ***Diseño de Prueba DS2*** | Analizar si se establecen acuerdos de confidencialidad por parte de terceros evitando riesgos a la organización. |
|---|---|

***Alcance:*** Administración de Riesgos del Proveedor, Monitoreo del Desempeño del Proveedor
Instrumentos: Formato de Entrevista 05: SEQUINSA – Gerente de Operaciones

***Descripción de la Prueba:*** Revisión y análisis de contrato AMNET y servicios que prestan SEQUINSA a la Organización.
Se realizó entrevista a proveedores de reparación y mantenimiento.
***Se toma en cuenta para la evaluación:***

- ✓ Acuerdos de servicios con terceras partes a través de contratos entre la organización y el proveedor de la administración de instalaciones
- ✓ Acuerdos de confidencialidad, Requerimientos legales regulatorios de manera de asegurar que estos concuerde con los acuerdos de seguridad identificados, declarados y acordados.
- ✓ Monitoreo de la entrega de servicio con el fin de asegurar el cumplimiento de los acuerdos del contrato.

***Evaluación - Resultados de DS2***

No existe una supervisión, ni seguimiento por parte de la organización en los trabajos realizados por SEQUINSA ya que consideran no es necesario.
Por medio de trabajo realizado se comprobó que existen acuerdos de seguridad y confidencialidad estipulados en el contrato adquirido con AMNET.
**MM_NIVEL 3. (Definido)**
Hay procedimientos bien documentados para controlar los servicios de terceros con procesos claros para tratar y negociar con los Proveedores.
Cuando se hace un acuerdo de prestación de servicios, la relación con el tercero es meramente contractual.
La naturaleza de los servicios a prestar se detalla en el contrato e incluye requerimientos legales, operativos y de control.
Se asigna la responsabilidad de supervisar los servicios de terceros. Los términos contractuales se basan en formatos estandarizados.
El riesgo del negocio asociado con los servicios del tercero está valorado y reportado.

| | |
|---|---|
| **Hallazgos** | No se monitorea continuamente la entrega de servicio por parte de la organización hacia el proveedor, hasta que surgen fallas en los servicios, de AMNET y SEQUINSA |
| **Recomendaciones** | Se recomienda valorar el desempeño del proveedor durante las actividades de evaluación, a fin de asegurar el cumplimiento de los acuerdos del contrato |
| **Conclusiones** | En la evaluación de servicios por terceros concluimos que está debidamente tomado en cuenta el criterio de confidencialidad en los servicios que se proveen por AMNET. |
| **Anexos** | Contrato AMNET |

## *12.5 Objetivo 5 de Auditoria*

Evaluar problemas y clasificar el nivel de riesgo en las tecnologías de información del área de informática de MS- América.

*Cuadro 5.1:* ***Diseño de Prueba y resultado PO9***

MS América Central
actionaid denmark

### MATRIZ DE PRUEBA Y RESULTADO

| **DOMINIO PLANEAR Y ORGANIZAR**<br>***Evaluar y Administrar los Riesgos de TI*** | **PO9** |
|---|---|

**Sub objetivo 5.1:** Verificar que existe un marco de trabajo de administración de riesgo, que garantice el alcance de los objetivos de la organización.

| | |
|---|---|
| ***Diseño de Prueba PO9*** | Evaluar y analizar los criterios de construcción, ejecución y Monitoreo del Plan de Acción de Riesgo en el Área Informática de MS. |

***Alcance:*** Alineación de administración del riesgo de TI y del negocio, Establecimiento del contexto del riesgo, Identificación de eventos, Evaluación de Riesgo de TI, Respuesta a los Riesgos de TI y el Mantenimiento y monitoreo de un Plan de Acción de riesgo.

***Instrumento:*** Formato de Entrevista Oficial Administrativo Logístico – Evaluación del Riesgo.

***Descripción de la Prueba:*** Se Aplica entrevista al Oficial Administrativo Logístico.
***Se toma en cuenta para la evaluación:***

- ✓ Identificación, definición y actualización regular de los diferentes tipos de riesgos de TI
- ✓ Definición de alcances, límites de los riesgos y la metodología para las evaluaciones de los riesgos, Actualización de evaluación de riesgos, Metodología de evaluación de riesgos
- ✓ Medición de riesgos cualitativos y/o cuantitativos
- ✓ Definición de un plan de acción contra los riesgos para asegurar que existan controles y medidas de seguridad económicas que mitiguen los riesgos en forma continúa.
- ✓ Aceptación de riesgos dependiendo de la identificación y la medición del riesgo, de la política organizacional, de la incertidumbre incorporada al enfoque de evaluación de riesgos y de que tan económico resulte implementar protecciones y controles.

***Evaluación- Resultados de PO9***

De acuerdo a trabajos realizados se constata que no poseen registro de incidentes ocurridos.
**MM_NIVEL 1 (Inicial)**
Los riesgos de TI se toman en cuenta de manera inicial. Se realizan evaluaciones informales de riesgos según lo determine cada Proyecto.
Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto.
Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas en reuniones gerenciales.

| | |
|---|---|
| **Hallazgos** | No poseen documentos donde se contemplen, acuerdos de riesgos de TI, estrategia de mitigación y riesgos residuales, que ayuden a minimizar los posibles riesgos en términos financieros aceptables.<br><br>La metodología de evaluación de riesgo es manejada administrativamente, ya que la descripción de trabajo realizado se deja como soporte de factura. |
| **Recomendaciones** | Elaborar el documento en donde se establezca la evaluación y mitigación de los posibles riesgos para TI. |

| | |
|---|---|
| | Es factible manejar copia de los trabajos realizados como un soporte para el área de informática, para un mejor control de la metodología utilizada en los riesgos y para la adopción de las buenas prácticas. |
| **Conclusiones** | Al no poseer registro de incidentes ocurrido, se considera que no hay un adecuado monitoreo ni conciencia del impacto de riesgo. |
| **Anexos** | Evaluación del Riesgo |

*Cuadro 5.2: **Diseño de Prueba y resultado DS10***

MS América Central actionaid denmark

## MATRIZ DE PRUEBA Y RESULTADO

| DOMINIO ENTREGA Y DAR SOPORTE<br>*Administración de problemas* | DS10 |
|---|---|

**Sub objetivo 5.2:** Verificar si se da un seguimiento adecuado a las problemas e incidentes que se presentan y que garantizan la satisfacción de los usuarios.

| | |
|---|---|
| ***Diseño de Prueba DS10*** | Revisar la existencia de reportes de problemas de tal manera que se pueda asignar el valor que indique el grado de daño. |

***Alcance:*** Identificación y clasificación de los problemas de Hardware, Rastreo y solución de problemas, Cierre de Problemas, Integración de la Administración de cambio, configuración y problemas.

**Instrumento:** Formato de Entrevista al Oficial Administrativo Logístico

***Descripción de la Prueba:*** Se realizó entrevista al Oficial Administrativo Logístico
***Se toma en cuenta para la evaluación:***

- ✓ Para ello se necesita un sistema de manejo de problemas que registre y dé seguimiento a todos los incidentes, además de un conjunto de procedimientos de escalamiento de problemas para resolver de la manera más eficiente los problemas identificados. Este sistema de administración de problemas deberá también realizar un seguimiento de las causas a partir de un incidente dado de prueba, entrenamiento, revisión post-implementación.

***Evaluación- Resultados de DS10***

En la entrevista al oficial administrativo logístico se verifico que existe una adecuada administración de problemas e incidentes que afecten la seguridad de la información almacenada.

**MM_NIVEL 3 (Definido)**
La revisión de incidentes y los análisis de identificación y resolución de problemas son limitados e informales.

| | |
|---|---|
| **Hallazgos** | No se realiza la debida documentación, identificación y clasificación del sistema, ni las acciones correctivas para cada incidente. |
| **Recomendaciones** | Se recomienda que exista un registro de manejo de problemas, para resolver de manera eficiente los incidentes identificados |
| **Conclusiones** | Podemos concluir que no se realizan seguimientos a los incidentes presentados ya que no han persistido, por tal razón no se mantiene registro de estos. |
| **Anexos** | Evaluación del Riesgo |

# CONCLUSIONES Y RECOMENDACIONES

*Las Conclusiones y Recomendaciones están orientadas a la mejora de los Niveles de Seguridad de los recursos y Activos de TI a partir de los Objetivos de Control Críticos Identificados durante la Auditoria.*

## 13.1 CONCLUSIONES

La Auditoria se realizó aplicando el marco metodológico denominado Cobit 4.1, enfocándose en la dirección Informática, recursos de TI, Outsourcing y Riesgo Informático para el área de Informática de la organización MS América Central, en base a este análisis exhaustivo de los aspectos mencionados se tienen las siguientes conclusiones:

En primera instancia la dirección informática no cuentan con un Plan Estratégico incorporado.

1. No se realizan revisiones independientes del cumplimiento de TI
2. La organización no contempla en sus planes de evaluación la auditoría interna informática.

El segundo aspectos, es el relativo a las *políticas de seguridad.*

3. No tienen descrita una política de seguridad, en la que se indiquen los derechos y obligaciones, o las sanciones en las que pueden incurrir los usuarios. En ese sentido la Organización deberá considerar los aspectos que debería contemplar una política de seguridad.

4. Los procedimientos se desarrollan de manera informal estos a su vez no son evaluados por la gerencia continuamente.

5. Los controles existentes, se consideran con un bajo nivel criterio de seguridad, por tanto la gerencia deberá de considerar la asesoría de un especialista en el área de computación para el diseño y plan de implantación y seguimiento de estos.

*En lo relativo a la seguridad de los recursos y activos de TI:*

6. No existe documentación sobre el plan de infraestructura tecnológica de la organización.

7. Los usuarios de TI no cuentan con un documento físico de políticas de uso y explotación adecuado de los recursos de TI.

8. No cuenta con un plan de capacitación con el cual se desarrollen las habilidades del personal de la organización orientado al manejo de sistemas o temas relacionados de informática.

9. No se encontró documento formal del Plan de Contingencia, los incidentes y respuestas a estos se realizan de manera intuitiva y no siguiendo un procedimiento formal. El no tener determinados correctamente los recursos críticos de TI, puede acarrear el no contar con planes de continuidad adecuados y por lo tanto propensos a sufrir un ataque de seguridad, perdida de información, etc. De los cuales será casi imposible recuperarse sin causar pérdidas económicas a la organización.

*Con relación al tema de Outsourcing*

10. Se verifico que no existen con todos sus proveedores un contrato formal lo que no permite evaluar de manera crítica y bajo indicadores contundentes el servicio prestado por estos.

Y finalmente en base a los objetivos propuestos el último aspecto evaluado es *Riesgo Informático* sobre este se concluye que:

11. Los sistemas informáticos tienen un alto nivel de riesgo y no son percibidos por qué no se le da un seguimiento continuo a los problemas e incidentes identificados por los mismos sistemas.

De la discusión del informe final de la auditoria se concluye que no existe una conciencia formal por parte de la gerencia de TI para asegurar la correcta gestión de la seguridad, por tanto se afirma la hipótesis y se reafirma a través de los datos obtenidos a través del análisis de matriz de riesgo.

Así mismo la hipótesis que afirman una relación esperada inicial se logra a través de la evaluación de indicadores propuestos en la Descripción de los procesos de Cobit y los criterios de seguridad fundamentan la teoría.

Tomando en cuenta los aspectos anteriores se concluye que la documentación es un componente de máxima importancia para la operación y el buen funcionamiento de los sistemas en el área de Informática, así también para los procedimientos, normas y políticas relativas a la seguridad.

Es importante poder disponer de documentación actualizada, para garantizar la protección activos y el resguardo e integridad de los datos en la organización.

El área informática debido a su objetivo primordial, que es el de prestar los mejores servicios y obtener los mayores réditos financieros por estas actividades a enfocado sus esfuerzos y preocupación en alcanzar la satisfacción total del cliente bajo cualquier circunstancias. Esto ha hecho que ciertas áreas de seguridad informática sean descuidadas y las actividades de ejecución sean trasladadas a empresas que prestan el servicio de Outsourcing en el peor de los casos se han convertido en un problema critico ya que no cubren las recomendaciones y estándares de seguridad requeridos.

Cobit está diseñado para ofrecer a los niveles de la gerencia de la organización una visión general de la situación actual de las tecnologías de información, para conocer sus mayores debilidades y fortalezas; y de cómo estas pueden afectar al cumplimiento de los objetivos gerenciales, mas no puede ser considerado como una respuesta netamente tecnológica y de información para el área de informática de la organización.

El estudio y conocimiento de los documentos COBIT es necesario para lograr un enfoque adecuado de la auditoria y por ende resultados reales y que ayuden al cumplimiento de los objetivos de la organización.

Cobit no proporciona una estructura formal y especifica de cómo desarrollar un plan de auditoría y su ejecución posterior, en su lugar, ofrece una serie de guías de cómo realizar el análisis y evaluación de los controles existentes de la organización, en el área informática y que están relacionados con el alcance de los objetivos de la organización.

## 13.2 RECOMENDACIONES

Una vez presentadas las conclusiones se emiten las recomendaciones necesarias para establecer y aplicar los procesos recomendados como resultado de la auditoria para que la Organización cubra todas sus debilidades en cuanto a la seguridad, evaluando cuál de ellas son las más urgentes. En base a lo anterior mencionamos las más relevantes.

1. Definir procedimientos específicos para el establecimiento de controles efectivos dentro de la gestión de seguridad, como la implementación de revisiones de posibles violaciones a la seguridad y acceso no autorizados.

2. Implementar Planes Estratégicos a corto o largo plazo.

3. Es necesario diseñar manuales de infraestructura tecnológica a los que puedan recurrir los usuarios para conocer claramente las funciones o atributos que puedan realizar en el sistema.

4. El Organismo MS – América Central debe contemplar las autoevaluaciones en el área de informática para un mejor aprovechamiento de los Recursos de TI

5. Establecer conjuntamente con la participación de la gerencia general el nivel de participación y de importancia del área tecnológica dentro de la organización, no solo tomando el papel que se cumpla dentro del cumplimiento de las labores de los demás colaboradores, sino también considerando su grado critico en lo referente al servicio brindado a usuarios no solo en cuanto a navegación y otros servicios de internet, sino en cuanto al nivel de seguridad que se le debe ofrecer para la realización de sus actividades que tiene que ver con tecnologías dentro de MS- América Central.

6. La gerencia de deberá plasmar las políticas de TI en un documento formal, donde estén las sanciones incurridas por el incumplimiento de las mismas.

7. Se debe tomar en cuenta un plan de capacitación para mantener un nivel satisfacción de los interesados y así contar con un clara asignación de roles que correspondan a sus habilidades.

8. Definir e implementar un plan de contingencia.

9. El riesgo con respecto al manejo de cuentas de usuarios y contraseñas de parte de terceras personas es que si no existe un documento o acuerdo de nivel de servicio formal, estos cuando ya no sean prescindible sus servicios para la organización podrían causar daños al sistema, eso por eso que se recomienda en estos casos establecer acuerdos de nivel de servicio con sumo cuidado y con toda la debida formalidad que se requiera.

10. Así mismo se recomienda mejorar el procedimiento de gestión de cuentas y password para estar acorde a los estándares de seguridad y políticas de password.

11. Se recomienda tomar en cuenta los reportes generados por SONICWALL, detector de vulnerabilidades y de intrusos y tomar acciones correctivas, si es necesario revisar reglas de Firewall existentes y de ser necesario modificarlas.

12. Realizar una redistribución de funciones que defina la responsabilidad de realizar una correcta seguridad de la red, y en caso de ser necesario contemplar una posible consultoría técnica de una persona adicional para ayudar a mejorar la gestión de la seguridad en la organización.

13. En la evaluación del Modelo de Madurez de Cobit, parte clave de la implementación del gobierno de TI, haciendo referencia a algunas dificultades encontradas en el uso responsable de los recursos y la administración apropiada de los riesgo de TI, ubican en ciertos aspectos al área de informática en un distribución no equilibrada del Modelo de madurez, lo que dificulta una visión entendible para la gerencia, de lo que hace TI, se recomienda considerar en el perfil del administrador del área informática para incorporar como actividad prioritaria la evaluación y monitoreo del riesgo informático.

14. Se recomienda Cobit como una herramienta para realizar el análisis y evaluación de los puntos críticos de la organización, tomando como base las guías de auditoría, documento bastante específico en donde se detallan todas evaluaciones a los controles existentes.

Si bien Cobit brinda en sus documentos las herramientas necesarias para el proceso de auditoría, es conveniente tener conocimiento básico de cómo desarrollar una auditoria informática y de esta manera explotar mejor todas las Pistas de auditoría que brinda Cobit.

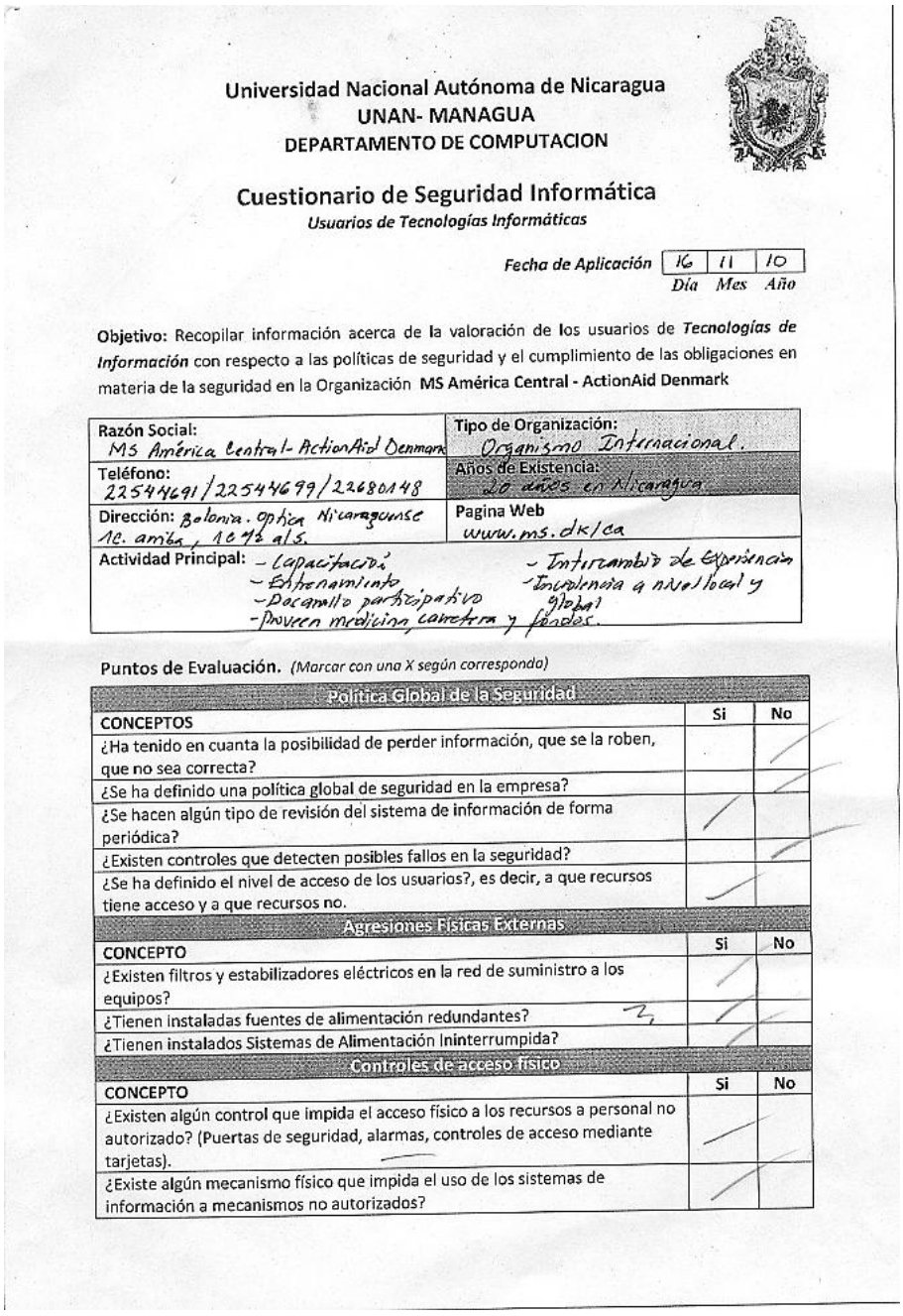
Se espera que las recomendaciones aquí expuestas sean consideradas y lleven a la organización a tomar iniciativas que garanticen el alcancen de los objetivos mediante un óptimo desempeño del área de informática.

# PAPELES DE TRABAJO

*Los Papeles de Trabajo son los archivos o legados que maneja el Equipo auditor y que contienen todos los documentos que sustentan el trabajo efectuado durante la auditoria, así mismo constituyen la principal evidencia de la tarea de auditoría realizada y de las conclusiones alcanzadas que se reportan en el informe de auditoria*

## 14.1. ENCUESTAS

**EU: Encuesta Usuario** Secretaria de Oficina y Recepcionista - Cuestionario de Seguridad Informática



Universidad Nacional Autónoma de Nicaragua
UNAN- MANAGUA
DEPARTAMENTO DE COMPUTACION

**Cuestionario de Seguridad Informática**
*Usuarios de Tecnologías Informáticas*

*Fecha de Aplicación* 16 (Día) 11 (Mes) 10 (Año)

**Objetivo:** Recopilar información acerca de la valoración de los usuarios de ***Tecnologías de Información*** con respecto a las políticas de seguridad y el cumplimiento de las obligaciones en materia de la seguridad en la Organización **MS América Central - ActionAid Denmark**

| | |
|---|---|
| **Razón Social:** MS América Central- ActionAid Denmark | **Tipo de Organización:** Organismo Internacional. |
| **Teléfono:** 22544691/22544699/22680148 | **Años de Existencia:** 20 años en Nicaragua |
| **Dirección:** Bolonia. Optica Nicaragüense 1c. arriba, 1c 1/2 als. | **Pagina Web** www.ms.dk/ca |
| **Actividad Principal:** - Capacitación - Entrenamiento - Pacamito participativo - Proveen medicina, carretra y fondos. | - Intercambio de Experiencia - Incidencia a nivel local y global |

**Puntos de Evaluación.** *(Marcar con una X según corresponda)*

| Política Global de la Seguridad | | |
|---|---|---|
| **CONCEPTOS** | **Si** | **No** |
| ¿Ha tenido en cuanta la posibilidad de perder información, que se la roben, que no sea correcta? | | X |
| ¿Se ha definido una política global de seguridad en la empresa? | | X |
| ¿Se hacen algún tipo de revisión del sistema de información de forma periódica? | X | |
| ¿Existen controles que detecten posibles fallos en la seguridad? | | X |
| ¿Se ha definido el nivel de acceso de los usuarios?, es decir, a que recursos tiene acceso y a que recursos no. | X | |
| **Agresiones Físicas Externas** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Existen filtros y estabilizadores eléctricos en la red de suministro a los equipos? | X | |
| ¿Tienen instaladas fuentes de alimentación redundantes? | X | |
| ¿Tienen instalados Sistemas de Alimentación Ininterrumpida? | X | |
| **Controles de acceso físico** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Existen algún control que impida el acceso físico a los recursos a personal no autorizado? (Puertas de seguridad, alarmas, controles de acceso mediante tarjetas). | X | |
| ¿Existe algún mecanismo físico que impida el uso de los sistemas de información a mecanismos no autorizados? | X | |

| Servidores | | |
|---|---|---|
| **CONCEPTO** | **Si** | **No** |
| ¿Existen sistemas operativos, que impiden el acceso a los datos, a los usuarios no autorizados? | ✓ | |
| ¿Están los servidores protegidos en cuanto a inicio de sesión y acceso a través de la red? | ✓ | |
| ¿Tienen instaladas fuentes de alimentación redundantes? | | |
| ¿Tienen instaladas Sistemas de alimentación Ininterrumpida? | ✓ | |
| ¿Tienen discos RAID? | | |
| **Copias de seguridad** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Se realizan copias de los datos? ¿Con que periodicidad? | | ✓ |
| ¿Existe un procedimiento de copia de seguridad? ¿Esta automatizado? | ✓ | |
| ¿Se almacenan las copias de seguridad en un lugar de acceso restringido? | ✓ | |
| ¿Se almacena alguna copia fuera de los locales de trabajo? | | ✓ |
| ¿Ha probado a restaurar alguna copia de seguridad? | | ✓ |
| **Mecanismos de Identificación y Autenticación** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Existe un procedimiento de Identificación y Autenticación? | ✓ | |
| ¿Esta basado en contraseñas? | ✓ | |
| ¿Las contraseñas se asignan de forma automática por el servidor? | | ✓ |
| ¿Existe un procedimiento de cambio de contraseña? | ✓ | |
| **Controles de Acceso** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Existen controles para el acceso a los recursos? | ✓ | |
| ¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de accesos ilícitos? | | |
| Una vez pasados los filtros de identificación, ¿Se han separados los recursos a los que tienen acceso cada usuario? | ✓ | |
| **Virus** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Tienen cuentas de correo electrónico en Internet? | ✓ | |
| ¿Tienen antivirus corporativo? | ✓ | |
| ¿Protege su antivirus los correos electrónicos y la descarga de archivos vía Web? | ✓ | |
| ¿Actualizan regularmente el antivirus? | ✓ | |
| ¿Ha tenido alguna vez problema con algún virus en su sistema? | | ✓ |
| **Planes de Seguridad y Contingencia** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Se ha elaborado algún plan de seguridad? | | ✓ |
| ¿Existe un responsable o responsables que coordinen las medidas de seguridad aplicables? | ✓ | |
| ¿Existe un Plan de contingencia? | | ✓ |
| ¿Existe un presupuesto asignado para la seguridad de la Organización? | | ✓ |
| ¿Se ha elaborado un plan de seguridad? | | ✓ |
| ¿Se han incluido en el mismo los aspectos relacionado con las comunicaciones? | | ✓ |
| ¿Realiza el seguimiento del plan de seguridad personal de la Empresa? | | ✓ |
| ¿Existe un contrato de mantenimiento en el que se priorice la seguridad y el | | ✓ |

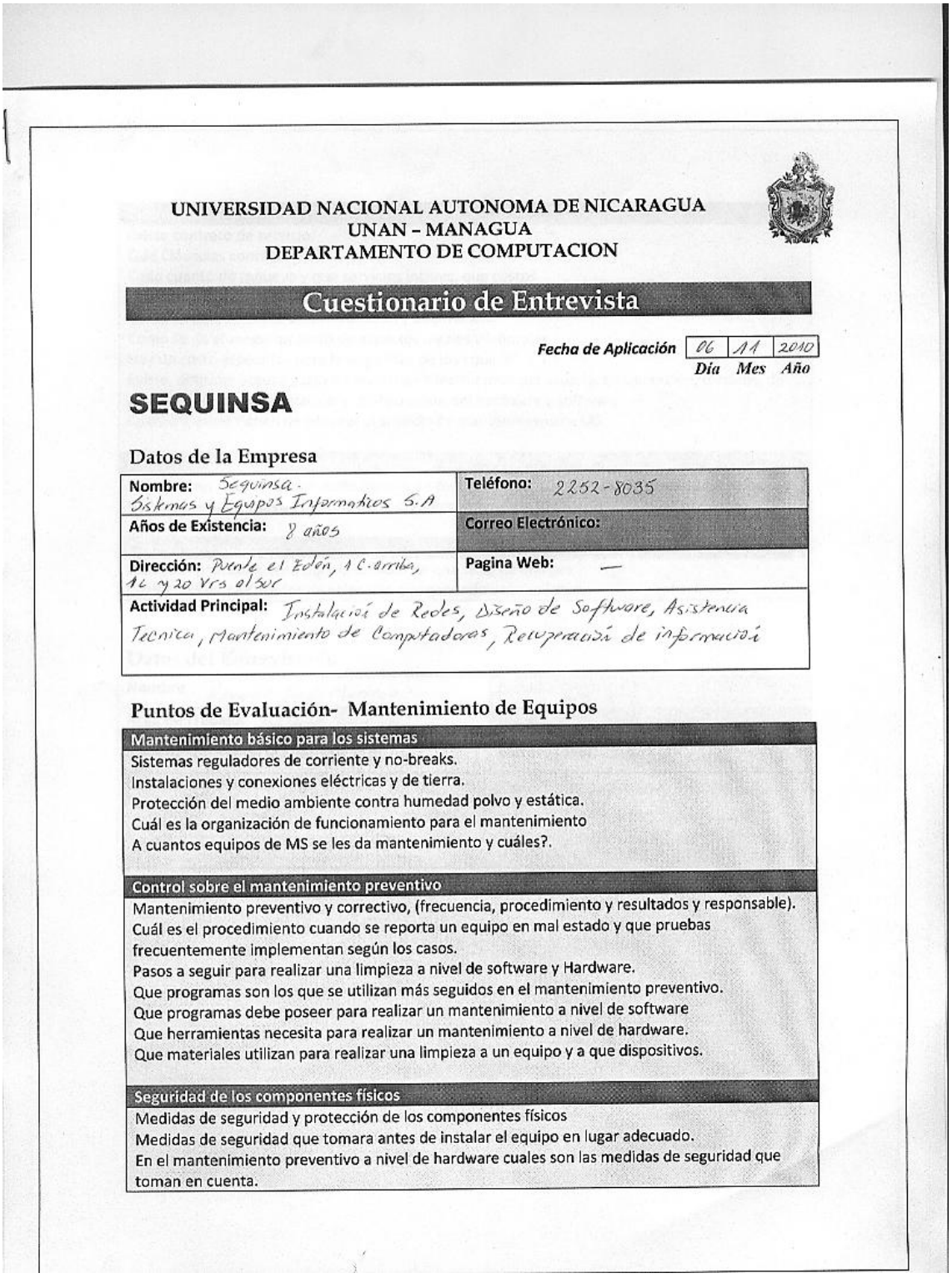
| | | |
|---|---|---|
| plan de contingencias? | | |
| ¿Dispone del personal informático involucrado directamente con la seguridad del sistema? | | ✓ |
| **Cifrado de las comunicaciones** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Existe un procedimiento de cifrado de las comunicaciones? | | ✓ |
| **Correo Electrónico** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Disponen de correo electrónico todos los usuarios? | ✓ | |
| De aquellos que disponen, ¿Se les ha informado de las políticas de la Organización en cuanto a su uso? | ✓ | |
| ¿Existe algún control sobre los mensajes que se envían y/o reciben? | | ✓ |
| **Acceso a Internet** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Existe alguna política definida para los accesos a internet? | | ✓ |
| ¿Se ha explicado claramente a los trabajadores de la Organización? | | ✓ |
| ¿Existe un acceso a Internet corporativo? | | ✓ |
| ¿Esta limitado el acceso por puesto? | | ✓ |
| ¿Esta limitado el acceso por usuario? | | ✓ |
| ¿Existe control sobre las páginas accedidas por cada puesto o usuario? | | ✓ |
| ¿Se revisan las páginas accedida para tomar medidas contra el usuario que no cumpla sus funciones? | | ✓ |
| ¿Existen controles sobre instrucciones externas en su sistema de información? | | ✓ |
| **Web Site** | | |
| **CONCEPTO** | **Si** | **No** |
| ¿Dispone de Web Site Empresarial? | ✓ | |
| ¿Se ha contratado el Hosting a una empresa externa? | | ✓ |
| ¿Se ha realizado el mantenimiento por el personal de la propia empresa? | | ✓ |
| ¿Esta alojado el la red empresarial del servidor web? | | ✓ |
| ¿Se ha contratado personal informático para que diseñe la protección? | ✓ | |
| ¿Dispone de cortafuego? | ✓ | |
| ¿Dispone de herramientas que auditen intentos de accesos externos? | | ✓ |

**Datos del Informante:**

| | |
|---|---|
| **Nombre del Informante:** Luoy Torres Villalta | **E- mail:** luoy.ms@cam.org.ni |
| **Área:** Administrativa - Logísticas. | **Cargo:** Secretaria - Recepción |
| **Funciones:** Recepción - Secretaria. | |
| **Firma** | |
| **Encuestador:** Claudia Regina González Urroz. | |

## 14.2 Entrevistas

### ET: Entrevista SEQUINSA



UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA
UNAN – MANAGUA
DEPARTAMENTO DE COMPUTACION

**Cuestionario de Entrevista**

*Fecha de Aplicación* 06 (Día) 11 (Mes) 2010 (Año)

**SEQUINSA**

Datos de la Empresa

| | |
|---|---|
| **Nombre:** Sequinsa - Sistemas y Equipos Informaticos S.A | **Teléfono:** 2252-8035 |
| **Años de Existencia:** 8 años | **Correo Electrónico:** |
| **Dirección:** Puente el Edén, 1 C. arriba, 1c y 20 Vrs al Sur | **Pagina Web:** — |
| **Actividad Principal:** Instalación de Redes, Diseño de Software, Asistencia Tecnica, Mantenimiento de Computadoras, Recuperación de información | |

Puntos de Evaluación- Mantenimiento de Equipos

| |
|---|
| **Mantenimiento básico para los sistemas** |
| Sistemas reguladores de corriente y no-breaks.<br>Instalaciones y conexiones eléctricas y de tierra.<br>Protección del medio ambiente contra humedad polvo y estática.<br>Cuál es la organización de funcionamiento para el mantenimiento<br>A cuantos equipos de MS se les da mantenimiento y cuáles?. |
| **Control sobre el mantenimiento preventivo** |
| Mantenimiento preventivo y correctivo, (frecuencia, procedimiento y resultados y responsable).<br>Cuál es el procedimiento cuando se reporta un equipo en mal estado y que pruebas frecuentemente implementan según los casos.<br>Pasos a seguir para realizar una limpieza a nivel de software y Hardware.<br>Que programas son los que se utilizan más seguidos en el mantenimiento preventivo.<br>Que programas debe poseer para realizar un mantenimiento a nivel de software<br>Que herramientas necesita para realizar un mantenimiento a nivel de hardware.<br>Que materiales utilizan para realizar una limpieza a un equipo y a que dispositivos. |
| **Seguridad de los componentes físicos** |
| Medidas de seguridad y protección de los componentes físicos<br>Medidas de seguridad que tomara antes de instalar el equipo en lugar adecuado.<br>En el mantenimiento preventivo a nivel de hardware cuales son las medidas de seguridad que toman en cuenta. |

| Contratos |
| --- |
| Existe contrato de servicio,<br>Que Cláusulas contiene<br>Cada cuanto de renueva y que servicios incluye, que costos.<br>Realizan Estudios de viabilidad y a quien le compete (Proveedor - Cliente).<br>Como se da el Proceso de contratación y adquisición.<br>Como se da el aseguramiento de aspectos legales y laborales.<br>Hay un costo específico para la seguridad de los equipos<br>Existe, difusión, acceso y uso de manuales e instructivos del usuario, de operación, técnicos, de procedimientos de instalación y configuración del hardware y software.<br>Cuanto tiempo tienen de proveer el servicio de mantenimiento a MS |
| **Madurez para la función de Mantenimiento** |
| Hay un nivel de cultura por parte del cliente para enfrentar cambios según avances tecnológicos<br>Hay un grado de apoyo continuo de la organización para la innovación del mantenimiento |
| **Compra de Equipo** |
| Cuál es el procedimiento para la compra de una serie de equipos<br>Cuales serian los criterios de selección que generalmente solicitan. |

**Datos del Entrevistado**

| | |
| --- | --- |
| **Nombre** Ricardo José Marenco | **E-mail:** ricardo.marenco@segosa.com rjmmarenco@yahoo.com |
| **Área de Trabajo:** Soporte Tecnico | **Cargo:** Gerente Operaciones |
| **Años de laborar en la Empresa** 8 años | **Entrevistador:** Karla Molina G. |
| **Funciones laborales:** Instalación de Redes, Diseño de Software, Asistencia Tecnica, Mantenimiento de Computadoras, Recuperación de Información. | |
| **Firma** | |

## 14.3. CUESTIONARIOS

**C -01:** Políticas y Medidas de Seguridad Informática

### Cuestionario
**POLITICAS Y MEDIDAS DE SEGURIDAD INFORMATICA**

Doc. No C-01

Aplicado en Obj 2 de Auditoria - POO6 Fecha: 05/11/10

1. ¿La política de seguridad esta detallada y completamente documentada?
   *Si* ☐ *No* ☑

2. La política de seguridad y los programas para conocerla concierne al personal de TI y de Oficina
   *Si* ☑ *Solo Usuarios* ☐ *Solo IT Staff* ☐ *Ni usuarios ni el IT Staff* ☐

3. ¿Algunas de las siguientes áreas no están cubiertas por la política de seguridad?
   *Software de Aplicación* ☐ *Procedimientos de oficina* ☑
   *Software de Sistema* ☐ *Datos* ☐
   *Redes (si aplica)* ☐ *Hardware/ Equipo de oficina* ☐

4. ¿La política de seguridad deberá cubrir disponibilidad, autenticidad, confidencialidad, correcto funcionamiento e integridad. Todos estos están cubiertos?
   *Si* ☑ *No* ☐

5. ¿Las autoridades de seguridad son detalladas y conducidas en periodos regulares?
   *No* ☑ *Si, por un departamento independiente* ☐
   *Si, por este departamento* ☐ *Si, por consultores externos* ☐

6. ¿Qué aspectos/ partes de un sistema son normalmente incluidos en la Auditoria?
   *Desarrollo/ Operación de Software* ☐ *Ambos* ☑
   *Solo procedimientos de oficina* ☐ *Ninguno de ellos* ☐

7. ¿Las políticas y medidas de seguridad son estrictamente forzadas?
   *Si* ☐ *No* ☐ *Algunas veces* ☐

8. ¿Existe una clara delimitación entre las responsabilidades del Staff en lo referente a operaciones, desarrollo e ingreso de datos?
   *Si- Todos ellos* ☑ *Algunos de ellos* ☐ *Ninguno de ellos* ☐

9. ¿Existe un especialista a cargo de la tarea de coordinar la seguridad y asegurar que las políticas sean comunicadas apropiadamente?
   *No* ☑ *Solo coordinación* ☐
   *Solo Comunicación* ☐ *Ambos* ☐

10. ¿Los gerentes saben de su responsabilidad sobre la seguridad dentro de sus dominios?
    *Si* ☑ *No* ☐

11. ¿El nuevo personal está informado de las políticas/ estándares de seguridad y de su responsabilidad de ellas?
    *Si* ☑ *No* ☐

12. ¿Existe un programa en proceso para incrementar la conciencia de seguridad (posiblemente incluya carta y seminarios/cursos)?
    *Si* ☐ *No* ☑

13. Existen reglas en el lugar para la elección de password? Longitud mínima de 5 caracteres, la elección obvia debe ser eliminada, etc.
*Si* [✓] *No* [ ] *No Aplica* [ ]

14. ¿El mal uso de recursos esta estrictamente definido y prohibido (no juegos, desarrollos "privados", etc.) y existe software para restringirlo?
*Si, con software de control* [ ] *No* [✓]
*Si, No con software control* [ ]

15. ¿Contratos con cualquiera de lo siguiente no incluye una clausula directamente relacionada con responsabilidades de seguridad?
*Agencia/ Contratante de Staff* [ ] *Ingenieros/ Personal mantenimiento* [ ]
*Vendedores/ Proveedores* [ ] *Personal Permanente* [ ]

16. ¿Hay un nivel de seguridad asignado a todos los usuarios?
*Si* [✓] *No* [ ]

17. Se realiza chequeos específicos para asegurar que el sistema cumpla con la legislación local/ internacional (servicios financieros, etc.).
*Si* [✓] *No* [ ] *No Aplica* [ ]

18. ¿La seguridad u otra política estipulada convenciones de nombre para user-ids, transacciones, programas, archivos de datos? Indique cualquiera aplicable pero no cubierto:
*User- ids* [ ] *Programas/ Módulos* [ ]
*Transacciones* [ ] *Archivo de Datos.* [ ]

***Observaciones Generales del Punto evaluado***
Aplicado al dominio planear y organizar.
Se evalua la existencia de politicas y procedimientos de TI y la comunicación de estas al personal de la organización.

Dirección de Gerencia.

**Aplicado Por** Araceli Mingucci P.

**C -02:** Contingencia y Back-up

## Cuestionario
### CONTINGENCIA Y BACK-UP

Doc. No C-02

Aplicado en Obj 4 de Auditoria - DS11 | Fecha: 11/11/2010

1. ¿Se realizan copias de back-up regularmente y donde se mantienen?
   *No* ☐ *Si, en el Sitio* ☑ *Si, Fuera del Sitio* ☐ *Si dentro y fuera del Sitio* ☐

2. ¿Están las copias especiales (si existen) fuera del sitio?
   *Si* ☐ *No* ☑

3. ¿Se mantienen copias de la documentación e instrucciones de operación?
   *No* ☑ *Si, en el Sitio* ☐
   *Si, Fuera del Sitio* ☐ *Si, dentro y fuera del Sitio* ☐
   *No aplica* ☐

4. Los Back-up en el sitio, de archivos, programas, documentación e instrucciones de operación están almacenados para prevenir el acceso no autorizado y riesgo de daño (fuego, etc.).
   *Solo acceso no autorizado* ☐ *Solo riesgo de daño* ☐
   *Ambos acceso y daños* ☑ *Ni acceso ni daño* ☐

5. ¿Se han asignado responsabilidades individuales para la implementación de cada componente del plan de recuperación y se han nombrado un coordinador de la recuperación?
   *Si* ☐ *No* ☑

6. El plan de recuperación debería incluir detalles de todos los requerimientos administrativos y acuerdos. ¿Cuáles de los siguientes, si existe, son omitidos?
   *Procedimientos Obtenidos* ☑ *Planes financieros* ☐ *Detalles del seguro* ☐

7. ¿Existe un plan de recuperación en un lugar fuera del sitio?
   *Si* ☐ *No* ☑

8. Los detalles para el reemplazo de equipos han sido formulados, incluyendo costos (unitario y total) y el tiempo de reemplazo de la unidad?
   *Si* ☐ *No* ☑ *No incluye costos* ☐ *No incluye tiempo* ☐

9. Los acuerdos legales obligatorios en el sitio con vendedores incluye soporte de hardware para equipos critico (incluyendo garantías en tiempo de respuesta)?
   *Si* ☑ *No* ☐

***Observaciones Generales del Punto evaluado***

- Aplicado en el Dominio Entregar y Dar soporte
- Se evaluan los planes, Responsabilidades, Acuerdos y documentación de procedimientos.

Aplicado Por Karla Molina G.

**C -03:** Contingencia de Aplicaciones

## Cuestionario
### CONTINGENCIA DE APLICACIONES

Doc. No C-03

**Aplicado en** Obj y de Auditoria - DS11 **Fecha:** 11/11/2011

1. ¿Está la frecuencia de la copia de datos (Por Back-up) parcial o completamente determinada por las capacidades de recuperación de la aplicación?
   *No* ☐ *Parcial* ☐ *Completa* ☑ *No Back-up de datos* ☐

2. ¿Existe un mecanismo en el lugar, como un punto de chequeo y restart, para ayuda en caso de fallas del sistema durante un proceso de datos?
   *Si* ☑ *No* ☐

3. Son los procedimientos de contingencia de aplicaciones y salvaguardas probados y satisfechos:
   *Periódicamente* ☐ *Rara vez* ☑ *Nunca* ☐ *No aplica* ☐

***Observaciones Generales del Punto evaluado***

. Aplicado en el Dominio Entregar y Dar Soporte
. Se evalua frecuencia, mecanismos y procedimientos para la aplicación y monitoreo de los planes de contingencia, copias de datos, etc.

**Aplicado Por** Karla Molina G.

**C -04:** Auditoria del Sistema

## Cuestionario
### AUDITORIA DEL SISTEMA

Doc. No C-04

Aplicado en Obj 4 de Auditoría – DSS | Fecha: 11/11/10

1. ¿El acceso a los registros/ archivos está restringido al personal necesario por sus funciones (por defecto seria sin acceso)?
   *Si* [✓] *No* [ ]

2. ¿Qué tipo de acceso tiene el auditor para auditar los registros/ archivos? Seleccione la opción más aplicable.
   *Ninguno* [ ] *Lectura* [✓] *Actualización* [ ] *Borrado* [ ] *Otro* [ ]

3. ¿El sistema mantiene un log de los accesos e intentos de acceso a este (incluye terminales-ids, etc.)?
   *Si* [✓] *No* [ ] *Solo Violaciones* [ ]

4. ¿Qué tan a menudo se producen y son revisados los logs por violaciones? Seleccione la opción más apropiada

| | | | |
|---|---|---|---|
| *Diario o más frecuente* | [ ] | *Cuando se sospecha violaciones* | [ ] |
| *Un día si otro no* | [✓] | *Nunca* | [ ] |
| *Semanalmente* | [ ] | *No aplica* | [ ] |

5. ¿Es posible auditar y monitorear la actividad de un usuario específico?
   *Si* [✓] *No* [ ]

6. ¿Son los programas más sensitivos auditados individualmente cuando se ejecutan?
   *Si* [ ] *No* [✓]

7. ¿La fecha y hora del último logos es desplegado cuando un usuario ingresa? ¿Están todos los usuarios instruidos para chequear esto y reportar cualquier discrepancia?
   *Si* [ ] *No* [✓]

***Observaciones Generales del Punto evaluado***

Aplicado al dominio entregar y Dar soporte. se evalua la administracion y seguridad de los sistemas

**Aplicado Por** Araceli Murguia A.

**C -05:** Administración de la Seguridad de las Aplicaciones

## Cuestionario
### ADMINISTRACION DE LA SEGURIDAD EN LAS APLICACIONES

Doc. No C-05

Aplicado en: obj 4 de Auditoría – DSS | Fecha: 12/11/10

1. ¿La auditoria incluye un intento controlado de romper los controles de seguridad del sistema por una persona ajena a este?
   *Si* [✓] *No* [ ]

2. ¿Las medidas y políticas de seguridad de la organización están estrictamente aplicadas en los sistemas?
   *Si en todos ellos* [✓] *Algunos de ellos* [ ] *Ninguno de ellos* [ ]

3. ¿Existe una definición clara de las responsabilidades operacionales, de desarrollo y de entrada de datos entre el Staff?
   *Si* [ ] *No* [ ]

4. ¿Están todos los recursos asignados a un usuario específico y es responsabilidad especificar el nivel de protección de los mismos?
   *Si, con especificación* [ ] *Si, sin especificación* [✓] *No* [ ]

5. ¿El nuevo personal es informado de las políticas/ estándares de seguridad y de su responsabilidad en relación a estas?
   *Si* [✓] *No* [ ]

6. ¿Están los usuarios conscientes de la importancia de mantener sus Password confidenciales y que será el responsable de cualquier divulgación?
   *No* [ ] *Solo Confidencial* [ ] *Confidencial y Responsable* [✓] *No aplica* [ ]

7. ¿Los usuarios saben que no deben dejar una terminal ingresada (login) y desatendida?
   *Si* [✓] *No* [ ]

8. ¿Están los usuarios conscientes que no deben almacenar password en teclas de función de terminales o en discos con programas de auto logon?
   *Si* [✓] *No* [ ]

9. ¿Están los datos fuentes diseñados a un nivel de seguridad o debidamente identificado (para restringir el acceso y/o identificar su sensibilidad?
   *No* [ ] *Algunos Datos* [ ] *Todos los datos* [✓]

10. ¿Si existe un software producido fuera de la compañía, se han realizado chequeos para asegurar que la Organización es confiable? ¿Los contratos han sido cambiados para asegurar la integridad del software?
    *Chequeos no realizados* [ ] *Contratos cambiados* [ ]
    *Chequeos y contratos* [✓] *Ni chequeos ni contratos* [ ]

11. ¿Está el sistema completa y adecuadamente asegurados?

| | | | |
|---|---|---|---|
| *Solo reemplazo físico* | ☐ | *Solo pérdidas funcionales* | ☐ |
| *Perdida física y funcional* | ☐ | *Ningún tipo de pérdida.* | ☑ |

***Observaciones Generales del Punto evaluado***

Aplicado al dominio Entregar y Dar soporte y se evalua el nivel de seguridad de las aplicaciones

**Aplicado Por** Araceli Mendoza. A.

**C -06:** Administración de la Seguridad Informática

## Cuestionario
### ADMINISTRACION DE LA SEGURIDAD INFORMATICA

Doc. No C-06

**Aplicado en** Obj 4 de Auditoria - PSM **Fecha:** 04/11/10

1. ¿El rol y función de la administración del sistema de seguridad está definido y separado de otras?
   *Si* ☐ *No* ☐ *Diferente pero no definido* ☑ *Definido pero no diferente* ☐

2. ¿Existe un control dual/ mecanismo de validación en el lugar para cambios en las reglas de acceso a recursos?
   *Si* ☑ *No* ☐ *No Aplica* ☐

3. ¿Puede el administrador de la seguridad tener acceso a password activas (si un usuario olvida su clave)?
   *Si* ☑ *No* ☐ *No Aplica* ☐

4. ¿El acceso al sistema está controlado por el uso de user-ids?
   *Si* ☑ *No* ☐

5. ¿Cada acceso individual al sistema tiene un user-ids único, o hay user-ids compartidos?
   *User-ids son individuales* ☑ *Algunos user-ids son compartidos* ☐

6. ¿Cuando un user-ids es creado o su password es reseteada, como se comunica el nuevo password al usuario?
   *Este es estándar y conocido* ☐ *Por teléfono* ☐
   *En persona* ☑ *Por carta* ☐
   *Otro/ Combinación de estos* ☐

7. ¿Cuando un nuevo password es emitido por el administrador de seguridad o del sistema, ésta expira automáticamente cuando se usa por primera vez (forza al usuario a cambiarla)?
   *Si* ☐ *No* ☑ *No Aplica* ☐

8. ¿Los user-ids y password son removidos cuando un miembro del Staff es transferido o deja la organización?
   *Si* ☑ *Solo en terminación laboral* ☐
   *No deshabilitado* ☐ *Solo en trasferencia* ☐
   *Desconoce* ☐

9. ¿Es necesario una solicitud formal por escrito de la administración antes que un nuevo usuario sea configurado?
   *Si* ☐ *No* ☑

10. ¿Existe un "Súper usuario" o "Especial" y está limitado al mínimo número de usuarios que lo requieren para su función?
    *Si* ☐ *No* ☑ *No con tales atributos* ☐

11. ¿El acceso al sistema está controlado por password?
    *Si* ☑ *No* ☐

12. ¿Cómo se escogen los password?

| | | | |
|---|---|---|---|
| *Por el usuario* | ☐ | *Generada por el sistema* | ☐ |
| *Por el gerente* | ☐ | *Por el administrador de seguridad* | ☑ |
| *Otro* | ☐ | | |

13. ¿Se requiere una autorización formal para el cambio/ creación de password?

*Si* ☑ *No* ☐ *Solo creación* ☐ *Solo cambio* ☐

***Observaciones Generales del Punto evaluado***

Aplicado en el Dominio Entregar y Dar Soporte.
Se evaluan los diferentes mecanismos para la administración de la seguridad informatica desde el acceso hasta el control de la seguridad.

**Aplicado Por** Karla Molina G.

**C -07:** Hardware

## Cuestionario
### HARDWARE

Doc. No C-07

Aplicado en Obj 4 de Auditoría - DSI3 | Fecha: 22/11/10

1. ¿Cuánto tiempo de servicio fue perdido el último año por fallas de hardware?
   *0% - 1%* [x] *1%-3%* [ ] *4%-5%* [ ] *Mas de 5%* [ ]

2. ¿Las siguientes actividades son permitidas en el cuarto de equipos o en las proximidades de dispositivos de hardware?
   *Fumar* [ ] *Comer* [ ] *Beber* [x]

3. ¿Existen procedimientos en el sitio para un seguro download (y eventual restart) después de una falla de hardware crítica detectada?
   *Si* [ ] *No* [x]

4. ¿Cuántos Proveedores están involucrados en contratos de mantenimiento?
   *1-2* [x] *3-5* [ ] *Más de 5* [ ]

5. ¿El mantenimiento preventivo se lleva a cabo regularmente y en fechas predeterminadas?
   *Si* [x] *No* [ ]

6. ¿Todo el trabajo de mantenimiento es documentado y supervisado?
   *Si* [ ] *No* [ ] *No, Siempre* [x]

7. ¿El trabajo de mantenimiento por los Proveedores se lleva a cabo en presencia de una o más miembros del personal permanente?
   *Si* [ ] *No* [x] *No, Siempre* [ ]

8. ¿Que practica es adoptada cuando el hardware de almacenamiento tiene que ser removido del sitio por mantenimiento o reparación?
   *Vaciado de datos sensitivos* [ ] *Ninguno* [ ]
   *Acompañamiento del personal* [ ] *No aplica* [x]
   *Ambos* [ ]

***Observaciones Generales del Punto evaluado***
Se evalua procedimientos de mantenimiento con Segelinsa aplicado en el dominio Entregar y Dar Soporte
Se evalua la documentacion existente

Aplicado Por Claudia González

**C -08:** Control de Acceso Físico

## Cuestionario
### CONTROL DE ACCESO FISICO

Doc. No C-08

Aplicado en Obj. 4 de Auditoria – 0512 Fecha: 19/11/10

1. ¿Qué tan cercano es el acceso del público a las instalaciones?
   - *Muy cerca del edificio* ☐
   - *Acceso al edificio* ☐
   - *Acceso al sitio pero no al edificio* ☑
   - *No cercano al edificio* ☐

2. ¿Existe un parqueadero de autos sobre, al lado o bajo las instalaciones del edificio?
   *Si* ☑ *No* ☐

3. El sitio/ locación ha sido sujeto a manifestaciones, desordenes civiles, piquetes, etc.
   *Si* ☐ *No* ☑

4. ¿Cuál es la percepción en general del público sobre la instalación?
   - *Combinación de ambos* ☐
   - *Indeseable* ☐
   - *Apreciada por la comunidad* ☑
   - *Publico no conoce sobre su función* ☐

5. ¿Ubicación exacta de la instalación?
   - *Base/ Sótano del edificio* ☐
   - *Planta baja* ☐
   - *1ro/ 2do piso* ☑
   - *Otro* ☐
   - *3er piso o sobre el edifico* ☐
   - *Construcción del centro de cómputo* ☐
   - *Adecuada* ☐

6. ¿Cuántas entradas/ salidas existen para el ingreso y salida de la instalación (además de las de emergencias)?
   *Ninguna* ☐ *Una* ☑ *Dos* ☐ *Tres* ☐ *Más de Una* ☐

7. ¿Qué sistema de acceso mecánico/ eléctrico existe en el lugar durante las horas laborable?
   - *Dispositivo Biométrico* ☐
   - *Sistema de Tarjeta/ Tacto* ☐
   - *Ninguno* ☑
   - *Seguro con combinaciones* ☐
   - *Seguro y Llave del sistema* ☐

8. ¿Todas las puertas y ventanas externas están alarmadas?
   *Si* ☐ *No* ☑

9. ¿Los controles de acceso físico son probados e inspeccionados regularmente (incluyendo test de intento de acceso no autorizado).
   *Si* ☐ *No* ☑

10. ¿Quién debe de llevar identificación para el acceso a las Instalaciones?
    - *Nadie* ☑
    - *Empleados* ☐
    - *No empleados* ☐
    - *Empleados y No- Empleados* ☐

11. ¿Cuando una persona relevante con autorizaciones deja la organización, que de los siguiente no se realiza. Selecciones lo aplicable a la instalación?
*Cambio de seguros* [x] *Eliminación de Tarjeta* [ ]
*Cambio de combinaciones* [ ] *Recuperación de la identificación* [ ]

12. Los controles de acceso también aplican al personal de servicio (limpieza, proveedores, etc.).
*Si* [ ] *No* [ ] *No Aplica* [x]

13. Para terminales que desplieguen datos altamente sensitivos, estas son:
*Standard* [ ] *LCD* [ ] *Plasma* [ ] *No aplica* [x]

14. ¿El movimiento de medios (magnéticos, reportes sensitivos, etc.)hacia y desde la instalación es estrictamente controlado y registrado?.
*Si* [x] *No* [ ]

15. Los chequeos de inventarios se realizan para:
*Medios magnéticos* [ ] *Salidas y Entradas/ documentación* [ ]
*Ambos* [x] *Ninguno* [ ]

***Observaciones Generales del Punto evaluado***
Aplicado al dominio Entregar y Dar Soporte
Se inspecciona el ambiente físico de las instalaciones
y Se evalua el procedimiento y Controles Físicos
de las Instalaciones.

**Aplicado Por** Claudia González

**C -09:** Sistema de Red y Comunicación

## Cuestionario
### SISTEMA DE RED Y COMUNICACION

Doc. No C_09

Aplicado en Obj 4 de Auditoria - DS12 | Fecha: 19/11/10

1. La red es:
   - Interna a un edificio [x]
   - Interna a un sitio [ ]
   - En una región geográfica [ ]
   - En un país [ ]
   - En más de un país [ ]

2. ¿Cuál es el tipo de conexión a líneas púbicas?
   - Interna PABX o PBX [x]
   - Línea directa [ ]
   - Compartida PABX o PBX [ ]
   - Otro [ ]
   - No aplica [ ]

3. ¿Cuántos nodos hay en la Red?
   - 2 [ ]
   - 3-5 [ ]
   - 6-10 [ ]
   - 11-20 [ ]
   - Más de 20 [x]

4. ¿Qué protocolos son usados?
   - X25/ Packet Switched [ ]
   - SDLC/HDLC [ ]
   - Binary Synchronous/9030 [ ]
   - Asynchronous [ ]
   - LAN/ETHERNET/DECNET/TCP/IP [x]
   - Otros [ ]

5. ¿Cuántos usuarios tienen acceso al sistema?
   - Menos de 50 [x]
   - 51 a 250 [ ]
   - 251 a 1000 [ ]
   - 2001 a 10,000 [ ]
   - Más de 10,000 [ ]

6. ¿Han sido definidos los requerimientos mínimos en términos de disponibilidad y rendimiento?
   - Si [x]
   - No [ ]

7. ¿Que de los siguiente elementos no han sido definidos en la red?
   - Enlaces críticos [ ]
   - Equipo Crítico [ ]
   - Software Crítico [x]

8. ¿Qué facilidades de recuperación de la red existen en el lugar?
   - Líneas de reservas/ adicionales [ ]
   - Rutas Alternadas [ ]
   - Ninguna de estas [ ]
   - No aplica [x]

9. ¿Puede una sesión pendiente, ser cancelada fácilmente si una violación de seguridad ha ocurridos o existe la sospecha?
   - Si [x]
   - No [ ]

10. ¿Para tener acceso a la red/sistema, todos los usuarios deben ingresar al menos un usuario y password, un password junto con tarjeta, una representación con un dispositivo biométrico u otro valor similar único?
    - Si [x]
    - No [ ]

11. ¿El ID del terminal es siempre transmitido al acceder al sistema?
*Si* ☐ *No* ☑

12. ¿Se usa un mensaje técnico de autenticación?
*Si* ☑ *No* ☐

13. ¿El sistema previene la transmisión de mensajes/ datos sensitivos o nodos y terminales indefinidos o inválidos?
*Si* ☑ *No* ☐

14. ¿En términos de promedio que tan viejo es el equipo de comunicaciones?
*Menos de 2 años* ☐ *5 a 8 años* ☐
*Menos de 5 años* ☑ *Más de 8 años* ☐

15. ¿Cuál es el porcentaje de tiempo fuera debido a fallas de red/ comunicación se dio durante los últimos 12 meses?
Menos de 1% ☑ 1-3% ☐ Más de 3% ☐

16. ¿Está el equipo de prueba y diagnostico para unidades de líneas/ comunicaciones lista y disponibles?
*Si* ☑ *No* ☐ *No aplica* ☐

17. ¿Existe una transmisión de datos sensitiva o confidencial?
*Si* ☐ *No* ☐ *No aplica* ☑

18. ¿Los datos transmitidos son encriptados?
*Todos* ☐ *Solo datos seleccionados* ☑ *No* ☐

19. ¿Cuál es el primer medio usado para transmisión?
*Cobre/ Par trenzado* ☐ *Fibra Óptica* ☑
*Coaxial Cable* ☐ *Otro* ☐
*Satélite/ Microonda* ☐

20. ¿El acceso al circuito de red y sus diagramas de configuración es estrictamente controlado y limitado a aquellos que lo requieren?
*Si* ☑ *No* ☐ *No aplica* ☐

21. ¿En lo posible los multiplexores, switches y otros equipos de comunicación sensitivos están localizados en áreas seguras?
*Si* ☑ *No* ☐ *No aplica* ☐

22. ¿Qué tan frecuente se reasignan puertos en la instalación?
*Muy frecuente* ☐ *Frecuentemente* ☐
*Algunas veces* ☐ *Raramente* ☑
*Nunca* ☐ *No aplica* ☐

23. ¿Las asignaciones y reasignaciones de puertos están correctamente registradas y documentadas?
*Si* ☐ *No* ☐ *No aplica* ☑

24. ¿El nivel de tráfico de la red es monitoreado?
*Si* [x] *No* [ ] *No aplica* [ ]

25. ¿Se transmiten mensajes de registro de ingreso?
*Si* [x] *No* [ ] *Depende de la Aplicación* [ ]

***Observaciones Generales del Punto evaluado***

Se. Aplica en el Dominio Entregar y Dar Soporte.
Se evalua el sistema de Red, Arquitectura, Accesos, Configuraciones Perfiles de Usuarios, Permisos y sobre todo la seguridad en el sistema como los equipos que la integran.

**Aplicado Por** Karla Molina.

**C -10:** Riesgo Informático

## Cuestionario
### RIESGO INFORMATICO

Doc. No C-10

Aplicado en Obj 6. de Auditoria-PDG | Fecha: 29/11/10

1. ¿Qué restricciones de humo existen en el sitio?
   *Ninguna* ☐ *No se permite fumar en absoluto* ☑

2. ¿Qué tan frecuente se realizan trabajos en el edificio o se dan alteraciones en él?
   *A menudo* ☐ *Algunas veces* ☐
   *Rara vez* ☑ *Nunca* ☐

3. ¿Cuántos incendios han existido dentro de la instalación en los últimos 5 años? Si son más de 5 ingrese 5. *Número de incendios =>* Ninguno.

3. ¿El Equipo eléctrico es apagado cuando no se usa?
   *Si* ☑ *No* ☐

4. ¿Qué tan a menudo son las áreas de computadoras limpiadas a profundidad?
   *Diariamente* ☐ *Semanalmente* ☑
   *Un día sí, otro no* ☐ *Mensualmente* ☐

5. ¿Están los detectores de humo presentes a lo largo de las instalaciones?
   *Si* ☐ *No* ☑

6. ¿Están los detectores de calor/fuego presentes a lo largo de las instalaciones?
   *Si* ☐ *No* ☑

7. ¿Qué tan a menudo son probados los sistemas de detección de humo/calor/fuego?
   *Regularmente* ☐ *Periódicamente* ☐
   *Rara vez* ☐ *Nunca* ☑

8. Son los extintores manuales suficientes para el rango de potenciales incendios (eléctricos, químicos, etc.)
   *Si* ☑ *No* ☐

9. ¿Están los extintores adecuadamente ubicados y marcados claramente?
   *Si* ☐ *No* ☑

10. ¿Están todos los empleados instruidos en el uso de extintores y conocen de los procedimientos y políticas de incendios?
    *Si* ☑ *No* ☐

11. ¿Las paredes alrededor de áreas críticas van desde el sub piso hasta el súper- techo (sobre el techo falso)?
    *Solo desde el sub – piso* ☐ *Ambos* ☑
    *Solo hasta el Súper- Techo* ☐ *Ninguno* ☐
    *No aplica* ☐

12. ¿Existen puertas de incendio en el lugar para diseminar el fuego?
    *Si* ☐ *No* ☑

13. ¿Hay salidas y rutas de evacuación claramente marcadas e identificadas?
*Si* [✓] *No* [ ]

14. Han ocurrido inundaciones o daños por agua en la instalación:
*En los últimos 3 años* [ ] *3 a 5 años* [ ]
*5 a 8 años* [ ] *Más de 8 años* [ ]
*No en absoluto* [✓]

15. ¿Ha habido una falla de energía en la instalación en los últimos 3 años?
*Si* [✓] *No* [ ]

16. ¿Existe un regulador de energía y un sistema de monitoreo instalado?
*Si* [✓] *No* [ ]

17. ¿Qué tan a menudo se realiza un mantenimiento preventivo al equipo de UPS y soporte?
*Regularmente/ a la Marcha* [ ] *Rara vez* [ ]
*Periódicamente* [✓] *Nunca* [ ]

18. ¿Puede una falla en la unidad de aire acondicionado causar daño al hardware o resultar en pérdida del servicio?
*Si* [ ] *No* [✓]

19. ¿Cuántas veces el sistema de cómputo ha sido interrumpido en los últimos dos años debido a una falla en el aire acondicionado?
*Número de interrupciones =>* Ninguna Vez.

20. ¿Existe un plan de Standy/back-up en caso de una falla prolongada del aire acondicionado?
*Si* [✓] *No* [ ]

21. ¿Cuál de las siguientes, si existe, podría afectar más seriamente a la instalación o el área en general?
*Hundimiento* [ ] *Huracanes/ Vientos extremos* [ ]
*Inundaciones* [ ] *Nieve pesada/ Daño de hielo* [ ]
*Tormentas electicas* [ ] *Terremotos* [✓]

22. ¿Es el edificio estructuralmente más fuerte y construido con materiales no combustibles?
*Si* [ ] *No* [✓]

23. ¿Cuántos pisos tiene el edificio? Número de pisos=> 2

24. ¿Han sido examinados y probados los pisos que contiene equipos de computación y eléctrico para soportar su peso?
*Si* [✓] *No* [ ]

***Observaciones Generales del Punto evaluado***
Aplicado al dominio planear Organizar.
Se evalua la administracion de los Riesgos de TI

**Aplicado Por** Claudia González

## 14.4. LISTAS DE VERIFICACION

**LV- ASA 01:** Evaluación de la Administración del Software para Aplicaciones

MS América Central

**Lista de Verificación**

*Software*

*Evaluación de la Administración del Software para Aplicaciones*

Doc. No LV-ASA 01

*Fecha de Aplicación:* 09 de Noviembre del 2010 *Responsable:* Claudia González

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Paqueterías y programas integrados (Office y Smartsuite) | | ✓ | | |
| Programas y paqueterías para aplicación de escritorio (Hoja de cálculo, Base de Datos, procesadores de texto, agenda y presentaciones) | | ✓ | | |
| Programas y paqueterías para gráficos, diseños, presentaciones, publicaciones, autoedición y multimedia | | ✓ | | |
| Programas y paquetería para comunicación y red. | | ✓ | | |
| Aplicaciones y utilerías para internet. | | ✓ | | |
| Aplicaciones para la administración de redes, cliente/servidor y sistemas mayores. | | ✓ | | |
| Manuales e instructivos de instalación, operación, técnico de programación y demás documentación para el funcionamiento y uso del programa | | ✓ | | |
| Otro software para aplicaciones y productividad. | | ✓ | | |

**LV – ACSSC 02:** Evaluación de las Administración de los controles de Seguridad del Sistema Computacional

MS América Central

## Lista de Verificación

*Evaluación de la Administración de los Controles de Seguridad del Sistema Computacional.*

Doc. No LV. ACSSC02

*Fecha de Aplicación:* 11 de Noviembre 2010 *Responsable:* Karla Molina

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Métodos, procedimientos y medidas de seguridad y protección de los Sistemas Operativos, programas, paquetes, utilería y demás software del sistema computacional. | | ✓ | | |
| Métodos, rutinas de programación, procedimiento y medidas de seguridad y protección de los componentes físicos (interno y externo) del sistema computacional, como son los periféricos, dispositivos asociados y demás componentes físicos. | | | ✓ | |
| Evaluación de los procedimientos, medidas de seguridad y protección de la información que se procesa en los sistemas computacionales | | | ✓ | |
| Métodos, procedimientos y sistemas de administración y control para los accesos (lógicos y físicos) uso consulta, captura de datos y modificación de información del sistema computacional del área de sistema | | ✓ | | |
| Evaluación de la administración y control de los niveles de acceso, privilegios, permisos y contraseñas para los diferentes usuarios (administrador, operadores, personal ajeno al área de sistemas como los proveedores). | | ✓ | | |
| Evaluación de los métodos, procedimientos y sistemas de administración y control para los accesos remotos al sistema computacional, procesador, terminales y a los programas e información del área de sistemas por medio de redes, internet, fax-modem, redes virtuales y comunicación externa. | | ✓ | | |
| Evaluación de los métodos, procedimientos y sistemas de administración y control para la protección contra virus informáticos, hackers y personas ajenas al sistema computacional de la empresa. | | | ✓ | |
| Evaluación de la existencia, difusión, acceso y uso de manuales e instructivos de usuario, de operación, técnico, de procedimientos, de elaboración de proyectos informáticos, de programación y de los | | | ✓ | |
| demás manuales e instructivos para el manejo de los sistemas de la organización. | | | | |
| Listas de verificación para la administración de los controles de seguridad de los diferentes sistemas computacional. | | | ✓ | |
| Evaluación de la existencia, difusión y uso de estándares de seguridad para la administración de los sistemas computacionales y del área en general. | | ✓ | | |

**LV- SO 03:** Evaluación del Sistema Operativo

MS América Central

**Lista de Verificación**

*Software*

*Evaluación el Sistema Operativo*

Doc. No LV – SO 03

*Fecha de Aplicación:* 18 de noviembre de 2010 *Responsable:* Claudia Argüello

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Fabricante, características y Operabilidad. | | ✓ | | |
| Plataforma y ambiente de aplicación. | | ✓ | | |
| Licencias y permisos. | ✓ | | | |
| Versión, actualizaciones, cambios e innovaciones. | | ✓ | | |
| Manuales e instructivos técnicos, de operación de programación y demás documentación relacionados con el funcionamiento del lenguaje | | ✓ | | |
| Facilidad para administración del sistema operativo. | | ✓ | | |
| Sistemas, rutinas y programas para la seguridad y protección de los datos y del sistema operativo | | | ✓ | |
| Tecnología de aprovechamiento. | | | ✓ | |
| Compatibilidad y escalabilidad con otros sistemas operativos | | | ✓ | |

**LV- PPA 04:** Evaluación de los Programas y Paqueterías de Aplicación

MS América Central

**Lista de Verificación**

*Software*

*Evaluación de los Programas y Paqueterías de Aplicación*

Doc. No LV - PPA 04

*Fecha de Aplicación:* 18 de Noviembre 2010 *Responsable:* Araceli M

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Fabricante, características y Operabilidad del programa. | | ✓ | | |
| Ambiente de aplicación y uso. | | ✓ | | |
| Versión, actualización y utilidad para el usuario. | | ✓ | | |
| Licencias y permisos. | ✓ | | | |
| Biblioteca y utilerías de apoyo. | | ✓ | | |
| Compatibilidad, exportabilidad y escalabilidad con otros y paquetería de aplicación de desarrollo o con el sistema operativo | | ✓ | | |
| Requerimientos de capacitación y especialización. | | | ✓ | |
| Paqueterías y programas desarrollados internamente. | | | | ✓ |
| Manuales e instructivos de instalación, operación, técnico de programación y demás documentación para el funcionamiento del programa | | | ✓ | |

**LV - UFS 05:** Evaluación de las Utilerías para el funcionamiento del Sistema

MS América Central

**Lista de Verificación**

*Software*

*Evaluación de las Utilerías para el Funcionamiento del Sistema*

Doc. No LV- UFS 05

*Fecha de Aplicación:* 18 de Noviembre 2010 *Responsable:* Araceli y f.

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Utilería para el archivo de información. | | | ✓ | |
| Utilería para la comprensión de datos. | | | ✓ | |
| Utilería para la administración del sistema. | | | ✓ | |
| Utilería para la administración del sistema Windows. | | | ✓ | |
| Utilerías y bibliotecas para el manejo de redes. | | | ✓ | |
| Utilerías para internet y telecomunicaciones. | | ✓ | | |
| Otras utilerías para el manejo del sistema. | | ✓ | | |

**LV – DLS 06:** Evaluación del Diseño lógico del Sistema

MS América Central

**Lista de Verificación**

*Evaluación del Diseño Lógico del Sistema*

Doc. No LV- DLS 06

*Fecha de Aplicación:* 18 de Noviembre 2010 *Responsable:* Karla Molina

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Componentes lógicos del Sistema operativo, desarrollo, comunicaciones, base de datos y de los programas de aplicación. | ✓ | | | |
| Características lógicas del funcionamiento del hardware, Software, periféricos, instaladores y componentes asociados al sistema. | | | ✓ | |
| Procesos lógicos para la captura y procesamientos de datos y elaboración de informe. | ✓ | | | |
| Arquitectura y configuración lógicas (internas y externas) del sistema, así como sus periféricos y archivos. | | | ✓ | |
| Aplicaciones lógicas para los métodos de acceso, consulta y operación del sistema. | ✓ | | | |
| Administración y controles de los niveles lógicos de acceso para los administradores, operadores y usuarios del sistema, así como su uso y explotación. | ✓ | | | |
| Métodos y sistemas lógicos para la seguridad y protección de lenguajes, programas, paqueterías, utilería y demás software institucional. | | ✓ | | |
| Aplicaciones de los esquemas de seguridad lógica para protección de acceso, privilegios y manejo de las base de datos y respaldo de información. | | ✓ | | |

**LV- AC 07:** Evaluación de la Administración de Accesos

MS América Central

## Lista de Verificación

*Evaluación de la Administración de Accesos*

Doc. No LV - AA 07

*Fecha de Aplicación:* 18 de Noviembre 2010 *Responsable:* Karla Molina

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Evaluación de los estándares e instructivos de operación y manipulación para el procesamiento de datos, de acuerdo con el propio sistema y su software. | | ✓ | | |
| Evaluación de la estandarización del uso de sistemas operativos, lenguajes, programas, y paqueterías para el procesamiento de información en el sistema. | | ✓ | | |
| Evaluación de los proceso lógicos y físicos para el procesamiento de datos | | ✓ | | |
| Evaluación de la administración y control de la frecuencia, volumen, repetitividad e incidencias en los procesamientos de datos y operaciones lógico- matemáticas de las actividades que se realizan en el sistema. | ✓ | | | |
| Lista de verificación para la administración y los controles de almacenamiento. | ✓ | | | |
| Evaluación del diseño de archivos, bases de datos y medios establecidos para el almacenamiento de información de la Organización. | | ✓ | | |
| Evaluación de la administración y control de archivos de información del área de sistemas de la Organización | | ✓ | | |
| Evaluación de los planes y programas de prevención de contingencias relacionadas con el manejo de la información en el área de sistemas | | | | ✓ |
| Evaluación de la administración y control de la seguridad y protección de respaldos de información y de datos. | | ✓ | | |
| Evaluación de las normas, políticas y procedimientos para el almacenamiento, custodia, protección y seguridad de la información de las áreas de sistemas y de las demás áreas que cuenten con sistemas computacionales. | | | ✓ | |

**LV – DFS 08:** Evaluación del Diseño Físico del Sistema

MS América Central

## Lista de Verificación

*Evaluación del Diseño Físico del Sistema*

Doc. No LV-DFS08

*Fecha de Aplicación:* 19 de Noviembre 2010 *Responsable:* Karla Molina

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Arquitectura interna y configuración física del sistema computacional, equipos periféricos, componentes e instalaciones. | | ✓ | | |
| Arquitectura externa del área de sistema de la configuración física del sistema computacional, mobiliarios, equipos, e instalaciones. | | ✓ | | |
| Componentes físicos del sistema, periféricos, equipos complementarios, que permite su funcionamiento adecuado. | | ✓ | | |
| Diseño físico de los circuitos, compuertas y cableado interno y externo del sistema computacional. | ✓ | | | |
| Instalaciones eléctricas, de comunicación de datos y de comunicación telefónica del sistema computacional. | ✓ | | | |
| Administración y control de los métodos de acceso, seguridad y protección física del área informática, así como de la seguridad de los administradores, operadores y usuarios de los diferentes sistemas, de la información y del propio sistema computacional. | | ✓ | | |
| Evaluación de la distribución física del mobiliario, equipos y sistemas | ✓ | | | |

**LV – PCS 09:** Evaluación de los Periféricos más Comunes del Sistema

MS América Central

## Lista de Verificación

*Parte Física del Sistema*

*Evaluación de los Periféricos más Comunes del Sistema*

LV – PCS 09

Doc. No

**Fecha de Aplicación:** 22 de noviembre del 2010 **Responsable:** Claudia Gonzalez

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| *Teclado y Ratón del sistema:* marca, modelo, ergonomía, utilidad, durabilidad. | | ✓ | | |
| *Monitores:* marca, modelo, características, aceleradores de gráficos, tarjetas de expansión y funcionamiento. | | ✓ | | |
| *Impresoras:* marca, modelo, características, velocidad de impresión, buffers, compatibilidad, manejo de papel y tamaño/peso. | | ✓ | | |
| *CD-ROM:* velocidad de lectura/acceso, velocidad de transferencia de datos e información, capacidad de almacenamiento, compatibilidad de sonido, imágenes y datos, soporte multimedia, interfaz IDE/SCSI y software para respaldo. | | ✓ | | |
| *CD-RW:* velocidad de lectura/grabación, velocidad de lectura/grabación, velocidad de transferencia de datos e información, capacidad de almacenamiento compatibilidad con sonido, imágenes y datos, soporte multimedia, interfaz IDE/SCSI, tecnología para grabación de copia, software para funcionamiento, compatibilidad y multimedia. | | ✓ | | |
| *Fax-módem:* velocidad de acceso (Mbps) software de soporte, compatibilidad y protocolos de comunicación. | | ✓ | | |
| *Otros Periféricos* | | ✓ | | |

**LV – MBS 10:** Evaluación del Mantenimiento Básico de los Sistemas

MS América Central

**Lista de Verificación**

*Hardware de la computadora*

*Evaluación del Mantenimiento Básico de los Sistemas*

Doc. No LV-MBS 10

*Fecha de Aplicación:* 22 de Noviembre 2010 *Responsable:* Karla Molina

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Mantenimiento preventivo y correctivo (frecuencia y resultado) | | | ✓ | |
| Sistemas reguladores de corrientes y no-breaks. | ✓ | | | |
| Instalaciones y conexiones eléctricas y de tierra | ✓ | | | |
| Protección de medio ambiente contra humedad, polvo y estática. | ✓ | | | |

**LV - AUSC 11:** Evaluación del Aprovechamiento y Utilidad del Sistema Computacional

MS América Central

**Lista de Verificación**

*Hardware de la computadora*

*Evaluación del Aprovechamiento y utilidad del Sistema Computacional*

Doc. No LV-AUSC 11

*Fecha de Aplicación:* 22 de Noviembre 2010 *Responsable:* Araceli M

| EVALUAR Y CALIFICAR LOS SIGUIENTES ASPECTOS: | Excelente | Bueno | Regular | No Cumple |
|---|---|---|---|---|
| Capacidad para el crecimiento del Sistema. | | ✓ | | |
| Calidad de los componentes del sistema. | | ✓ | | |
| Obsolencia y durabilidad del equipo | | | ✓ | |
| Garantía y soporte del fabricante | | ✓ | | |

# ANEXOS

**ANEXO No. 1.** Contrato AMNET

amnet

Managua, 25 de Noviembre del 2009.-

**Lic. Jan Borsheim.**
**Apoderado General de Administración.**
**Asociación Danesa para la Cooperación internacional (MS) .**

Estimado Licenciado: Borsheim.

Mediante la presente le remito la documentación que detallo a continuación, con el fin de que la misma sea firma por su persona, para normar las relaciones contractuales entre su administrada y mi asesorada.

Le remito tres juegos en originales consistentes en:

1 Contratos de Servicios Números: **777640113**
2 Orden de Servicio: **777640113**
3 Procedimiento de Atención a Fallos
4 Políticas de Uso Aceptable de Productos y Servicios;
5 Acuerdo de Nivel de Servicio;

Uno de estos juegos es para recibir conforme, siendo copia fiel de sus originales.

Dichos documentos forman parte integral de un todo, siendo indivisibles al presente Contrato. Por lo que le solicito que rubrique y firme todas y cada una de las hojas que componen los referidos documentos en señal de aceptación.

Agradezco de ante mano la confianza depositada, en nuestra empresa.

Atentamente,

**Lic. César Ernesto Rodríguez Cajina**
**Asesor Legal.**
**Newcom Nicaragua, S.A.**

C.c. Archivo.-

Ofiplaza El Retiro, Edificio N° 5
Segundo Piso, Suite 5. 2-3
PBX: (505) 2276-8100 • (505) 8887-6196
FAX: (505) 2270-1596

**ANEXO No. 2.** Reporte de Mantenimiento de Equipos SEQUINSA

Managua 19 de Marzo de 2010

**Lic. Denis Urbina**
Oficial Administrativo Logístico
**MS-Asociacón Danesa**

Recibido por Mesoamérica Central Asociación Danesa para la Cooperación Internacional
Cia. MS
Ck. No. 1216

**Ref:** Reporte de Mantenimiento

Estimado Lic. Urbina,

El presente documento es un resumen de las activadades realizadas en el mantenimiento preventivo realizado en las Oficina de Casa Otro Mundo (MS), de igual forma presentamos un reporte de mantenimiento por equipo

| Item | Usuario | Estado Actual | Comentarios |
|---|---|---|---|
| 01 | Antonia:<br>Equipo marca HP DX2000, Procesador Intel Pentium IV de 2.8 Ghz<br>Disco Duro de 80 GB<br>Memoria RAM de 1 GB 4x256 | El equipo se encuentra en buen estado; se realiza mantenimiento preventivo. | El equipo se encuentra en buen estado. |
| 02<br><br>03 | Antonia:<br>Impresora Hp Laser Jet 1300.<br>HP Officejet Pro K550 Series | Limpieza y Mantenimiento de impresoras | Las impresoras se encuentran en Buen estado. |
| 04 | Bayardo:<br>HP DX2000, Win XP SP3<br>Intel Pentium IV de 2.8Ghz<br>1x 1 GB RAM | Se realiza Mantenimiento Preventivo, limpieza de temporales y chequeo general se sistema operative. | El equipo presentaba un error que decir no se había encontrado un archivo de flash, este error era ocasionado por el protector de pantalla; se cambio el protector y el problema se resolvió. |
| 05 | Impresora HP Laser Jet 1200. | Se realiza Mantenimiento preventivo. | La impresora está funcionando correctamente. |
| 06 | Bayardo –Portatil DELL | Mantenimiento Preventivo | El equipo funciona correctamente<br>La batería no esta mantenimiento la carga, se debe reemplazar. |
| 07 | Revisión de computadora de escritorio HP MS | Este equipo proviene de Honduras, el mismo no enciende ya que no tiene | El equipo se encuentra en buen estado, se prueba y se enciende con la memoria del |

*Dirección: puente el eden 1c. al sur 1 1/2c. arriba* *Cel. : 854-3926 & 854-9572 & 252-8035*
*e-Mail :* ricardo.marenco@sequinsa.com

Honararios

| Cant | Descripcion | Costo | Sub-Total |
|---|---|---|---|
| 5 | Computadoras Portátiles | 30.00 | 150.00 |
| 5 | Computadoras de escritorio | 30.00 | 150.00 |
| 7 | Impresoras | 10 | 70.00 |
| 1 | Servidor | 35 | 35.00 |
| | | Total USD: | $405.00 |

Se realiza Mantenimiento preventivo y correctivo, los equipos quedaron funcionando correctamente y sin fallas, se reinstalaron dos computadoras Conferencia y Portátil – Denis, Se instaló el antivirus en dos de los equipos.

Favor de Emitir cheque a Nombre de: *Ricardo Jose Marenco Ortiz*

Por su preferencia, les estamos entregando una Licencia de Panda Antivirus Pro 2010, la cual puede ser instalada en el equipo que ustedes nos indiquen sin costo.

Sin otro particular me suscribo,

Ante cualquier duda o consulta estamos siempre a disposición.

Resporte realizado:
Ricardo Jose Marenco Ortiz
Distribuidores de Panda Security
IT Support.
+505 8854-3926
+505 2252-8035


*Dirección: puente el eden 1c. al sur 1 1/2c. arriba* *Cel. : 854-3926 & 854-9572 & 252-8035*
*e-Mail :* ricardo.marenco@sequinsa.com

**ANEXO No. 3.** Inversiones de TI – Gastos Área Informática

MS América Central
actionaid denmark

**GASTOS HW - AREA DE INFORMATICA MS**

**De Enero a Diciembre 2010**

| Posting Date | Document No. | Description | Amount US$ |
|---|---|---|---|
| 29/01/2010 | 83 | MS Director Jan10 Toshiba Notebook | 1.005,00 |
| 16/04/2010 | 472 | Ergonomic Mouse (3) 50% adv | 555,00 |
| 16/04/2010 | 473 | Adv.Ch.Korsgaard laptop Toshiba | 913,99 |
| 07/05/2010 | 600 | MS May 3 ergonomic roller mouses 50% paid | 555,00 |
| 01/06/2010 | 762 | P4C APRIL Computer Toshiba 2909R | 762,50 |
| 03/08/2010 | 1171 | B.Rocha Aug. Toshiba Notebook | 1.208,00 |
| 01/06/2010 | 734 | MS ES May HP printer C4680 | 115,00 |
| 24/06/2010 | 852 | MS June HP printer+USB cable | 477,00 |
| 11/08/2010 | 1186 | MS Hond. July Pixma MX870 printer | 177,29 |
| 23/09/2010 | 1361 | Inspir.UCA S.Ramon Sept. Toshiba laptop | 435,00 |
| 23/09/2010 | 1361 | Inspir.Red Comal Sept. Toshiba laptop | 435,00 |
| 23/09/2010 | 1361 | Inspir. Fumdec Sept. Toshiba laptop | 975,00 |
| 30/09/2010 | 1416 | MS Hond. Sept. Toshiba laptop | 975,00 |
| 30/09/2010 | 1429 | Gender Adv. Sept. Toshiba laptop | 975,00 |
| 25/10/2010 | 1538 | Inspirat.Comucap Oct. laptop | 975,00 |
| 25/10/2010 | 1538 | Inspirat.RDDL Oct. laptop | 536,00 |
| 25/10/2010 | 1538 | Inspirat.UTC Oct. laptop | 536,00 |
| 25/10/2010 | 1538 | Inspirat. Adroh Oct. laptop | 536,00 |
| 25/10/2010 | 1538 | Activist. Hond. Oct. laptop | 536,00 |
| 04/11/2010 | 1635 | MS Admon. Nov. Docking Station Targus | 149,00 |
| | | **Total** | 12.831,78 |

**GASTOS POR SERVICIO FIJOS - AREA DE INFORMATICA MS**
**De Enero a Diciembre 2010**

| Posting Date | Document No. | Description | Amount US$ |
|---|---|---|---|
| 25/11/2010 | 2010112510E | Pago del Dominio cam.org.ni - Año 2010 UNI | 50,00 |
| 05/01/2010 | 0045527 | Servicios Integrales de Seguridad - Enero 2010 Wackenhut de Nicaragua, S.A | 40,00 |
| 22/03/2010 | 370 | 1er Trimestre de Mantenimiento General a Equipos Staff MS/SEQUINSA | 405,00 |
| 01/01/2010 | 17138 | Servicio de Internet platinum 1024 Kbps – Enero 2010/AMNET | 290,00 |
| 09/02/2010 | 23178 | Sistema de Copiado Analógico, digitales y Color – Fotocopiadora LANIER – Febrero 2010 COPINSA | 200,00 |

**ANEXO No. 4.** Política Procedimiento Orden de Compra

## FORMATO DE DECISION DE COMPRA

**MSAA-CA**

**Fecha:** 14 de Noviembre del 2010

**Fondos:** MSAA-CA

**Destino de la Compra:** LESBIA MORALES

| Cantidad | Artículos | COMTECH | DATATEX | J ICAZA |
|---|---|---|---|---|
| 1 | TECLADO Y RATON INALAMBRICO | C$ 1,078.98 | C$ 551.00 | C$ 1,038.70 |
| 1 | MONITOR PLANO 17" | C$ 3,853.50 | C$ 2,622.76 | |
| | COSTO TOTAL | C$ 4,932.48 | C$ 3,173.76 | C$ 1,038.70 |

***Decisión de Compra***

| | |
|---|---|
| Tienda: | DATATEX |
| Precio Unit: | |
| Precio Total: C$ | 3,173.76 |

***Motivo de la Decisión***

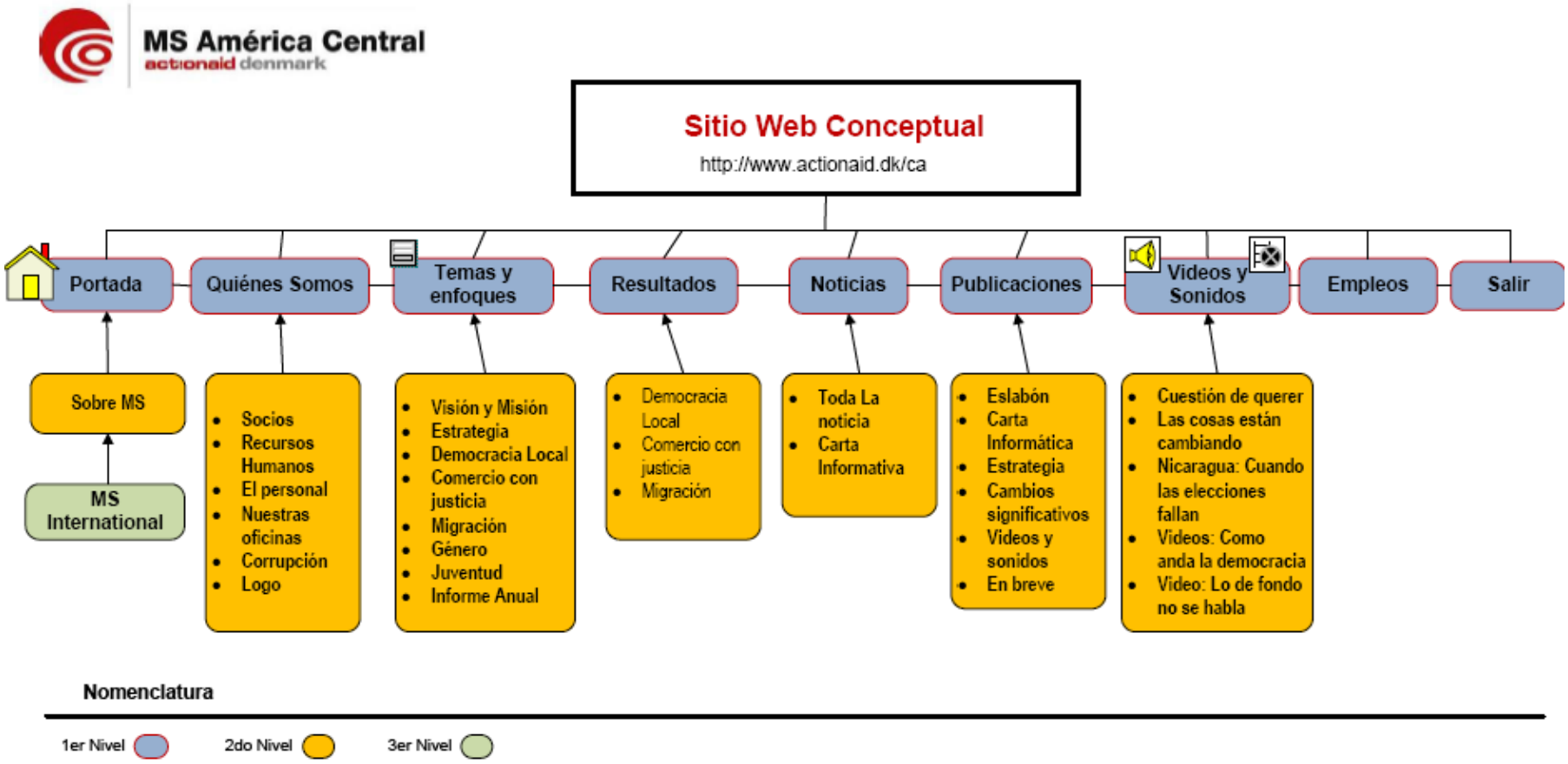
ES EL MEJOR PRECIO DE LAS 3 COTIZACIONES
APLICAR DEDUCCIONES QUE CORRESPONDEN
2 Cotizaciones de monitor porque en las otras tiendas el tamaño era diferente y hubiese variado el precio.

Cotizado Por: Autorizado Por:

**Observación:** La política estable que para la compra de cualquier equipo e inmueble deberá presentarse 3 proformas de proveedores, según criterios se selecciona el proveedor que brinda mejor imagen, prestigio y seguridad, así como mejor oferta. Otro criterio de selección es la integración de garantía, y en raros casos se solicita visita técnica para instalaciones.

El procedimiento de compra es realizado por el Oficial Administrativo logístico y autorizado por el Oficial Administrativo financiero y Administrador Regional.

**ANEXO No. 5.** Sitio Web Conceptual



**ANEXO No.6.** Organigrama Institucional

**ANEXO No. 7.** Política Distribución de Tareas por Puesto de Trabajo

MS América Central
actionaid denmark

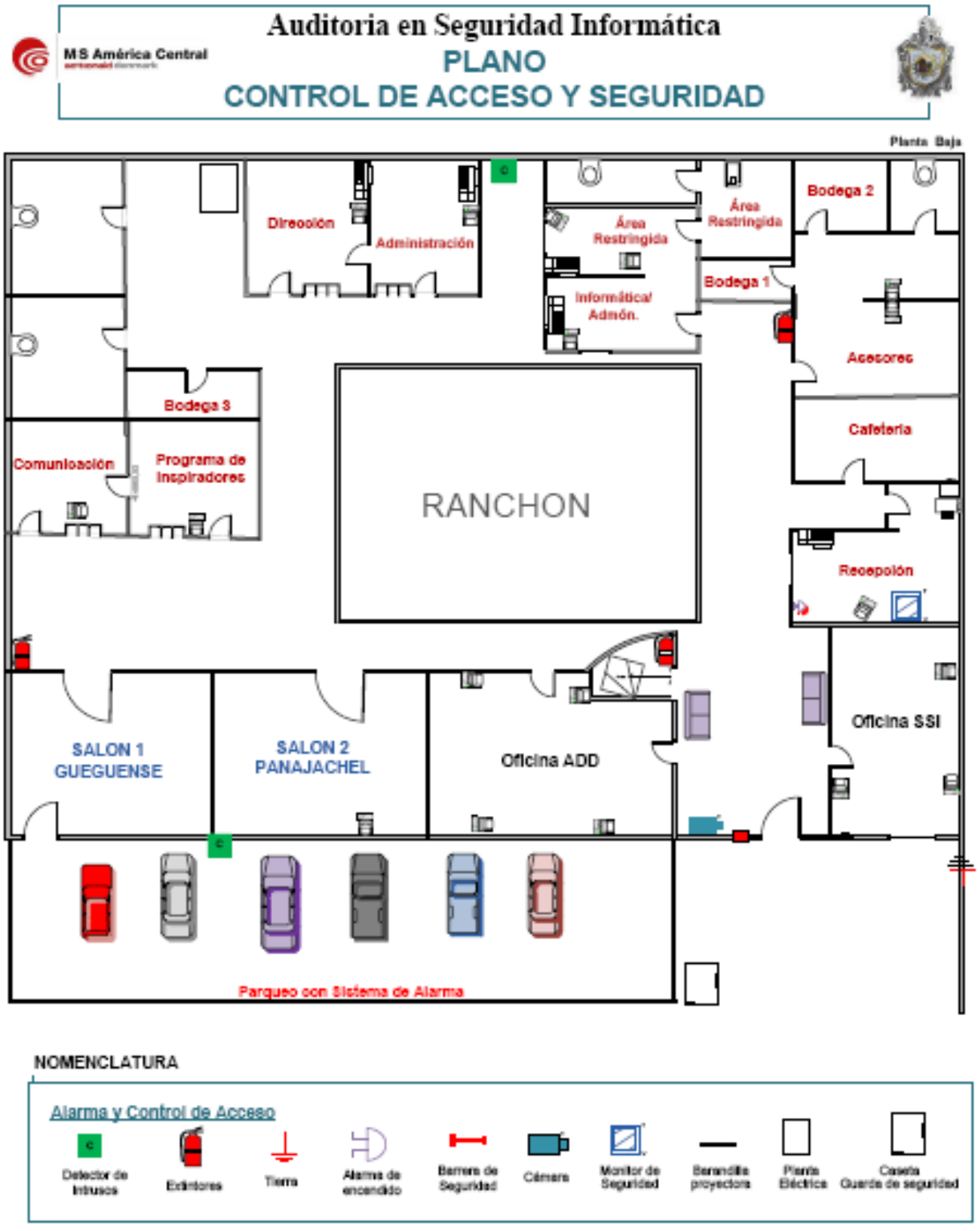
## CUADRO DE DISTRIBUCION DE TAREAS DEL AREA ADMNISTRATIVA

**por perfil laboral**

| Administrador | Oficial de Administracion | Oficial de Logistica | Secretaria Oficina | Secr.Reg/Asist Prog |
|---|---|---|---|---|
| **Area de Administracion** | **Contabilidad** | **Administracion** | **Comunicaciones** | **Eventos** |
| Presupuesto General MS | Levantam. Información Contable | Compras - Cotizaciones | Control Correspondencia (papel+elect) | |
| Contratos | Acreedores control y pago | Ventas | Biblioteca | Formulario Solicitud |
| Manejo de personal | Proveedores control y pago | Inventario | Correo físico | Local / Hotel |
| Vacaciones,permisos,asuetos | Planilla de pago/salarios/honor | | Capacitación del Personal en equipos | Alimentación |
| Ajustes | Informe Contable DK | **Contabilidad** | | Documentos distrib |
| Manuales y reglamentos | Facturacion a Dk y otros | Caja chica | **CASA Oficina** | Equipos |
| Staff manual | Elaboracion de cheques | | Cuadro utilización Salas de reunión | Honorarios/Reemb. |
| Guías de seguridad | Relaciones bancarias | **Transporte** | | Boletería |
| Procedimientos Financieros y Admtivos | | Tramite compra veh. | | Convivios |
| Auditorias | **Proyectos** | Tramites ventas veh. | | |
| Transferencias Bancarias | Anticipos / transferencias Rendiciones | Seguros / Local-DK Mtto./ Chequeo | | |
| **Administracion DW** | Asesorias Contables | Doc.legal / Permisos | | |
| Vacaciones | Auditoria | Control de kilometraje TMS Ruta diaria del conductor | | |
| **CASA Oficina** | | **Casa-Oficina** | | |
| Reglamento de casa | | Reparaciones Mantenimiento | | |
| **IT** | | Control y cobro de servicios | | |
| Servidor diseño del sistema | | Fumigación | | |
| Personal de Administración | | Jardines+ADD-SI-CD | | |
| Administrador Regional | | Alarmas y seguridad | | |
| Asistente | | | | |

| Administrador | Oficial de Administracion | Oficial de Logistica | Secretaria Oficina | Secr.Reg/Asist Prog |
|---|---|---|---|---|
| Asistente<br>Secretaria Oficina<br>Conductor<br>Vigilantes (2)<br>Conserje<br>Jardinero (temporal)<br>Apoyo administrativo del<br>Oficial de Guatemala<br>Consultor de El Salvador | | Parqueos<br>Vigilancias- roles<br>Cafetería e insumos<br>Limpieza e insumos<br>Papeleria y utiles de oficina<br>**IT**<br>Servidor- Mtto.<br>Antivirus - licencias<br>Navision<br>Software<br>Técnicos contratac.<br>Internet - Email<br>Intranet<br>**Eventos**<br>Coordinacion con Programas<br>**Administracion DW**<br>Casas/Mantenimiento<br>Inventarios<br>Rend/ Gastos Reemb<br>Introducciones<br>Doc legales Visa Tecnica Otros<br>Documentacion Nacional<br>Seguros<br>Cursos: idioma,driving,<br>First Aids, etc | | |

**ANEXO No. 8.** Plano de Acceso y Seguridad

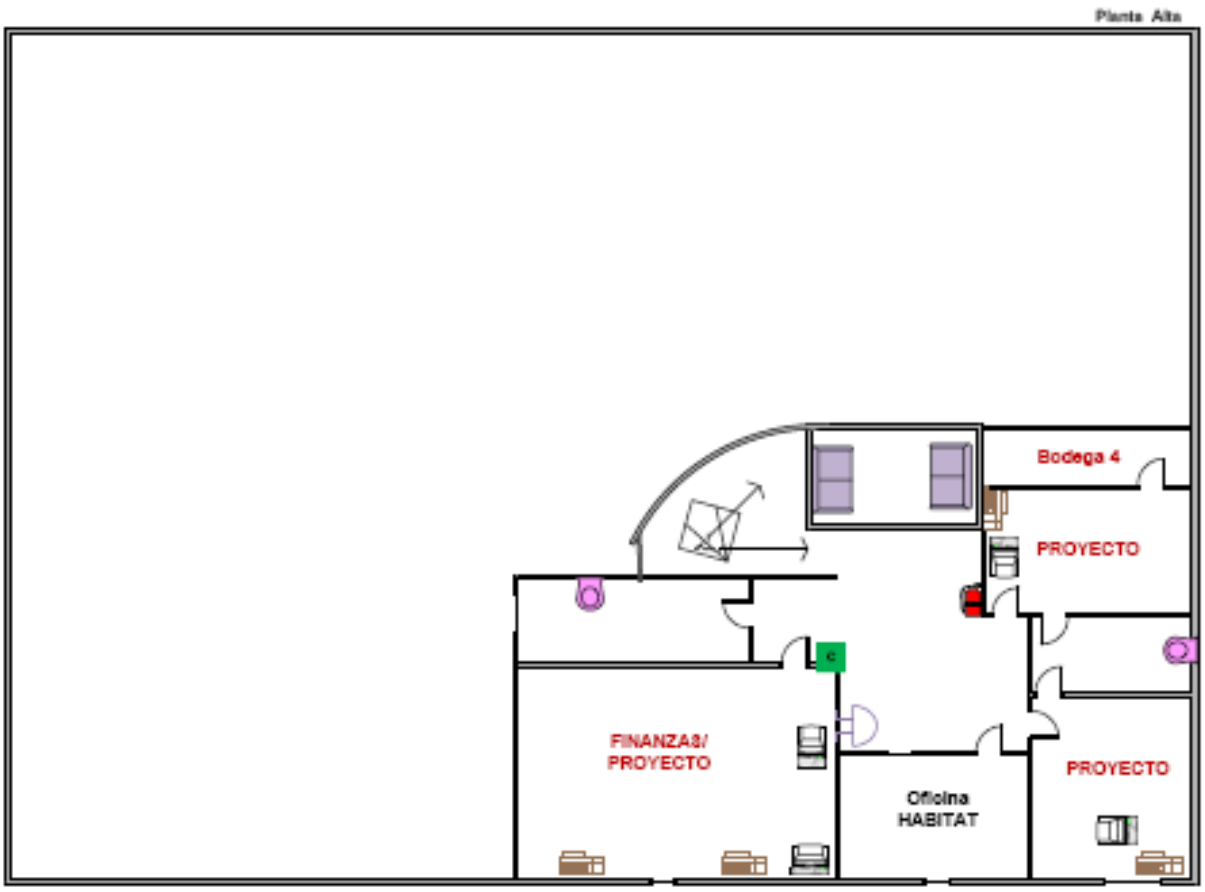


MS América Central

# Auditoria en Seguridad Informática

## PLANO

## CONTROL DE ACCESO Y SEGURIDAD




NOMENCLATURA

Alarma y Control de Acceso

Detector de Intrusos

Extintores

Alarma de encendido

**ANEXO No. 9.** Presupuesto de Auditoria

MS América Central
actionaid denmark

## AUDITORIA EN SEGURIDAD INFORMATICA

### PRESUPUESTO GENERAL

**Empresa Auditada:** Organismo Internacional MS América Central - Action Aid Denmark
**Periodo:** Enero - Diciembre 2010

| Descripción de Costos por Fases | Costo de Inversión | Valor Total en US$ |
|---|---|---|
| | | |
| **Fase I: Planeación de Auditoria** | | |
| ***Actividades*** | | |
| 1.1: Revisión Preliminar | $ 237,35 | |
| 1.2: Revisión Detallada | $ 39,84 | |
| 1.3: Elaboración informe FASE I | $ 40,24 | |
| 1.4: Reunión Equipo Técnico y Personal de la Institución | $ 15,30 | |
| | **Total Fase I** | **$ 2.732,73** |
| | | |
| **Fase II: Examen y Evaluación** | | |
| ***Actividades*** | | |
| 2.1: 2da Reunión Equipo Técnico Auditor. | $ 17,56 | |
| 2.2: Evaluación de la Dirección informática | | |
| 2.3: Evaluación del Control Interno | | |
| 2.4: Evaluación de los Procedimientos, Normas y Políticas de Seguridad | $ 58,36 | |
| 2.5: Evaluación de los Recursos de TI: Aplicación, Información, Infraestructura y Personas | $ 74,09 | |
| 2.6: Evaluación de la Contratación Externa | $ 52,83 | |
| 2.7: Evaluación del Riesgo Informático | $ 28,37 | |
| 2.8: Elaboración Diseño Grafico | $ 10,24 | |
| 2.9: Elaboración de Informe FASE II | $ 33,87 | |
| 2.10: Reunión con Equipo Técnico de Auditoria y Personal Institucional | $ 13,80 | |
| | **Total Fase II** | **$ 289,12** |
| | | |
| **Fase III: Dictamen de la Auditoria** | | |
| ***Actividades*** | | |
| 3.1: Elaborar informe Final de Proceso de Auditoria | $ 81,51 | |
| 3.2: Presentación y discusión del Informe Final | $ 88,47 | |
| 3.3: Revisión y correcciones Finales | $ 29,92 | |
| 3.4:Emisión de Documento a la dirección de MS- América Central | $ 149,28 | |
| | **Total Fase III** | **$ 2.743,43** |
| | Sub Total Presupuesto General | 5765,28 |
| | Imprevistos **5%** | 288,26 |
| | | |
| | ***Total Presupuesto General*** | ***$ 6.053,54*** |

MS América Central
actionaid denmark

# AUDITORIA EN SEGURIDAD INFORMATICA

## PRESUPUESTO
### FASE I: Planeación de la Auditoria

**Empresa Auditada:** Organismo Internacional MS América Central - Action Aid Denmark
**Periodo:** Enero - Diciembre 2010

**T/C US$ → C$ 21,90**

| RUBROS | Actividades | 1.1 Revisión Preliminar | | | 1.2 Revisión Detallada | | | 1.3. Elaboración de Informe | | | 1.4 Reunión E Auditor y Personal Institucional | | | TOTAL RUBROS FASE I |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Unidad de Medida | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | |
| ***Suministro Recursos Materiales*** | | | | | | | | | | | | | | |
| Folders | Unidad | 3 | $ 0,14 | $ 0,42 | 3 | $ 0,14 | $ 0,42 | 3 | $ 0,14 | $ 0,42 | 4 | $ 0,14 | $ 0,56 | $ 1,82 |
| Lapiceros | Caja | 1 | $ 4,20 | $ 4,20 | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 4,20 |
| Cuaderno de notas | Unidad | 2 | $ 0,91 | $ 1,82 | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 1,82 |
| Papel Bond | Resma | 1 | $ 5,48 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| Resaltadores | Caja | 1 | $ 8,28 | $ 8,28 | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 8,28 |
| Casset en blanco | Unidad | 2 | $ 1,37 | $ 2,74 | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 2,74 |
| USB | Unidad | 3 | $ 13,00 | $ 39,00 | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 39,00 |
| ***Suministro de Scanner, Copias e impresión*** | | | | | | | | | | | | | | |
| Copias | Hoja | 820 | $ 0,05 | $ 6,90 | 50 | $ 0,05 | $ 2,50 | 30 | $ 0,05 | $ 1,50 | 30 | $ 0,05 | $ 1,50 | $ 42,40 |
| Impresiones | Hoja | 410 | $ 0,14 | $ 57,40 | 100 | $ 0,14 | $ 14,00 | 60 | $ 0,14 | $ 8,40 | 15 | $ 0,14 | $ 2,10 | $ 81,90 |
| Escaneo | Hoja | 0 | $ 0,22 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| Encolochado | Hoja | 3 | $ 1,37 | $ 4,11 | 0 | $ 1,37 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 4,11 |
| ***Trasporte y Viatico*** | | | | | | | | | | | | | | |
| Transporte | Persona | 3 | $ 0,50 | $ 1,50 | 3 | $ 0,50 | $ 1,50 | 3 | $ 0,50 | $ 1,50 | 3 | $ 0,50 | $ 1,50 | $ 6,00 |
| Alimentación | Persona | 3 | $ 3,00 | $ 9,00 | 3 | $ 3,00 | $ 9,00 | 3 | $ 3,00 | $ 9,00 | 3 | $ 3,00 | $ 9,00 | $ 36,00 |
| ***Servicios y Alquiler de Equipos*** | | | | | | | | | | | | | | |
| Internet | Hora | 10 | $ 0,64 | $ 6,40 | 8 | $ 0,64 | $ 5,12 | 6 | $ 0,64 | $ 3,84 | 1 | $ 0,64 | $ 0,64 | $ 16,00 |
| Comunicaciones y Telefonía | Recarga | 3 | $ 2,30 | $ 6,90 | 0 | $ - | $ - | 3 | $ 2,30 | $ 6,90 | 0 | $ - | $ - | $ 13,80 |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Grabadora | día | 1 | $ 5,00 | $ 5,00 | 1 | $ 5,00 | $ 5,00 | 1 | $ 5,00 | $ 5,00 | 0 | $ - | $ - | $ 15,00 |
| Equipo (PC) | Hora | 4 | $ 0,46 | $ 1,84 | 5 | $ 0,46 | $ 2,30 | 8 | $ 0,46 | $ 3,68 | 0 | $ - | $ - | $ 7,82 |
| ***Recursos Humanos (Anticipo 50% )*** | | | | | | | | | | | | | | |
| Honorarios Personal Técnico $400 x Mes / c/u 240 Horas * Mes | Personas 3 Personas * 2 Meses | 3 | $ 800,00 | $ .400,00 | 0 | $ - | $ - | 0 | $ - | $ - | | $ - | $ - | $ 2.400,00 |
| **TOTAL Por Actividad** | | | | **$ 237,35** | | | **$ 39,84** | | | **$ 40,24** | | | **$ 15,30** | **$ 2.732,73** |

## PRESUPUESTO
## FASE II: EXAMEN Y EVALUACION (PARTE 1)

**Empresa Auditada:** Organismo Internacional MS América Central - Action Aid Denmark
**Periodo:** Enero - Diciembre 2010

**T/C US$ → C$ 21,90**

| RUBROS | Actividades | *2.1 2da Reunión Equipo Técnico Auditor* | | | *2.2 Evaluación de la dirección informática* | | | *2.3 Evaluación de los Recursos de TI* | | | *2.4 Evaluación de la Contratación Externa* | | | TOTAL RUBROS FASE II - PARTE 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Unidad de Medida** | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | |
| ***Suministro Recursos Materiales*** | | | | | | | | | | | | | | |
| Folders | Unidad | 0 | $ - | $ - | 3 | $ 0,14 | $ 0,42 | 3 | $ 0,14 | $ 0,42 | 3 | $ 0,14 | $ 0,42 | $ 1,26 |
| Casset en blanco | Unidad | 0 | $ - | $ - | 1 | $ 1,37 | $ 1,37 | 0 | $ - | $ - | 1 | $ 1,37 | $ 1,37 | $ 2,74 |
| ***Suministro de Scanner, Copias e impresión*** | | | | | | | | | | | | | | |
| Copias | Hoja | 15 | $ 0,05 | $ 0,68 | 60 | $ 0,05 | $ 3,00 | 69 | $ 0,05 | $ 3,45 | 39 | $ 0,05 | $ 1,95 | $ 9,08 |
| Impresiones | Hoja | 5 | $ 0,14 | $ 0,70 | 20 | $ 0,14 | $ 2,80 | 23 | $ 0,14 | $ 3,22 | 13 | $ 0,14 | $ 1,82 | $ 8,54 |
| Escaneo | Hoja | 0 | $ - | $ - | 30 | $ 0,22 | $ 6,60 | 30 | $ 0,22 | $ 6,60 | 30 | $ 0,22 | $ 6,60 | $ 19,80 |
| Encolochado | Hoja | 0 | $ - | $ - | 0 | $ 1,37 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| ***Trasporte y Viatico*** | | | | | | | | | | | | | | |
| Transporte | Persona | 3 | $ 0,50 | $ 1,50 | 6 | $ 0,50 | $ 3,00 | 13 | $ 0,50 | $ 6,50 | 5 | $ 0,50 | $ 2,50 | $ 13,50 |
| Alimentación | Persona | 3 | $ 3,00 | $ 9,00 | 6 | $ 3,00 | $ 18,00 | 13 | $ 3,00 | $ 39,00 | 5 | $ 3,00 | $ 15,00 | $ 81,00 |
| ***Servicios y Alquiler de Equipos*** | | | | | | | | | | | | | | |
| Internet | Hora | 6 | $ 0,64 | $ 3,84 | 9 | $ 0,64 | $ 5,76 | 9 | $ 0,64 | $ 5,76 | 9 | $ 0,64 | $ 5,76 | $ 21,12 |
| Comunicaciones y Telefonía | Recarga | 0 | $ - | $ - | 3 | $ 2,30 | $ 6,90 | 0 | $ 2,30 | $ - | 3 | $ 2,30 | $ 6,90 | $ 13,80 |
| Grabadora | día | 0 | $ - | $ - | 1 | $ 5,00 | $ 5,00 | 1 | $ 5,00 | $ 5,00 | 1 | $ 5,00 | $ 5,00 | $ 15,00 |
| Equipo (PC) | Hora | 4 | $ 0,46 | $ 1,84 | 9 | $ 0,46 | $ 4,14 | 9 | $ 0,46 | $ 4,14 | 9 | $ 0,46 | $ 4,14 | $ 14,26 |
| **TOTAL por Actividad** | | | | **$ 17,56** | | | **$ 58,36** | | | **$ 74,09** | | | **$ 52,83** | **$ 202,84** |

# PRESUPUESTO
## FASE II: EXAMEN Y EVALUACION (PARTE 2)

**Empresa Auditada:** Organismo Internacional MS América Central - Action Aid Denmark
**Periodo:** Enero - Diciembre 2010

**T/C US$ → C$ 21,90**

| RUBROS | Actividades | 2.5 Evaluación del Riesgo Informático | | | 2.6 Elaboración de Diseños Gráficos | | | 2.7 Elaboración de Informe | | | 2.8 Reunión Eq Auditor y Personal Institucional | | | TOTAL RUBROS FASE II - PARTE 2 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Unidad de Medida | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | |
| ***Suministro Recursos Materiales*** | | | | | | | | | | | | | | |
| Folders | Unidad | 3 | $ 0,14 | $ 0,42 | 0 | $ 0,14 | $ - | 3 | $ 0,14 | $ 0,42 | 4 | $ 0,14 | $ 0,56 | $ 1,40 |
| Lapiceros | Caja | 0 | $ 4,20 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| Cuaderno de notas | Unidad | 0 | $ 0,91 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| Papel Bond | Resma | 0 | $ 5,48 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| Resaltadores | Caja | 0 | $ 8,28 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| Casset en blanco | Unidad | 0 | $ 1,37 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| USB | Unidad | 0 | $ 13,00 | $ - | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ - |
| ***Suministro de Scanner, Copias e impresión*** | | | | | | | | | | | | | | |
| Copias | Hoja | 30 | $ 0,05 | $ 1,35 | 0 | $ 0,05 | $ - | 30 | $ 0,05 | $ 1,50 | 0 | $ - | $ - | $ 2,85 |
| Impresiones | Hoja | 10 | $ 0,14 | $ 1,40 | 10 | $ 0,14 | $ 1,40 | 60 | $ 0,14 | $ 8,40 | 15 | $ 0,14 | $ 2,10 | $ 13,30 |
| Escaneo | Hoja | 30 | $ 0,22 | $ 6,60 | 3 | $ 0,22 | $ 0,66 | 0 | $ - | $ - | 0 | $ - | $ - | $ 7,26 |
| Encolochado | Hoja | 0 | $ 1,37 | $ - | 0 | $ 1,37 | $ - | 1 | $ 1,37 | $ 1,37 | 0 | $ - | $ - | $ 1,37 |
| ***Trasporte y Viatico*** | | | | | | | | | | | | | | |
| Transporte | Persona | 2 | $ 0,50 | $ 1,00 | 1 | $ 0,50 | $ 0,50 | 3 | $ 0,50 | $ 1,50 | 3 | $ 0,50 | $ 1,50 | $ 4,50 |
| Alimentación | Persona | 2 | $ 3,00 | $ 6,00 | 1 | $ 3,00 | $ 3,00 | 3 | $ 3,00 | $ 9,00 | 3 | $ 3,00 | $ 9,00 | $ 27,00 |
| ***Servicios y Alquiler de Equipos*** | | | | | | | | | | | | | | |
| Internet | Hora | 6 | $ 0,64 | $ 3,84 | 3 | $ 0,64 | $ 1,92 | 1 | $ 0,64 | $ 0,64 | 1 | $ 0,64 | $ 0,64 | $ 7,04 |
| Comunicaciones y Telefonía | Recarga | 0 | $ - | $ - | 0 | $ - | $ - | 3 | $ 2,30 | $ 6,90 | 0 | $ - | $ - | $ 6,90 |
| Grabadora | día | 1 | $ 5,00 | $ 5,00 | 0 | $ - | $ - | 0 | $ - | $ - | 0 | $ - | $ - | $ 5,00 |
| Equipo (PC) | Hora | 6 | $ 0,46 | $ 2,76 | 6 | $ ,46 | $ 2,76 | 9 | $ 0,46 | $ 4,14 | 0 | $ - | $ - | $ 9,66 |
| **TOTAL Por Actividad** | | | | **$ 28,37** | | | **$ 10,24** | | | **$ 33,87** | | | **$ 13,80** | **$ 86,28** |
| | | | | | | | | | | | | | **Total Fase II** | **$ 289,12** |

# PRESUPUESTO
## FASE III: DICTAMEN Y RESULTADO

**Empresa Auditada:** Organismo Internacional MS América Central - Action Aid Denmark
**Periodo:** Enero - Diciembre 2010

**T/C US$ → C$ 21,90**

| RUBROS | Actividades | 3.1 Elaborar informe final de proceso de auditoria | | | 3.2 Presentación y discusión Informe final | | | 3.3 Revisión y correcciones Finales | | | 3.4: Emisión de Documento a la dirección de MS A.C | | | TOTAL RUBROS FASE III |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Unidad de Medida | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | Cant | Costo Unitario | Total | |
| ***Suministro Recursos Materiales*** | | | | | | | | | | | | | | |
| Folders | Unidad | 0 | $ - | **$ -** | **5** | $ 0,14 | **$ 0,70** | 0 | $ - | **$ -** | 0 | $ - | **$ -** | **$ 0,70** |
| DVD | Unidad | 0 | $ - | **$ -** | **0** | $ - | **$ -** | 1 | $ - | **$ -** | 5 | $ 1,15 | **$ 5,75** | **$ 5,75** |
| ***Suministro de Scanner, Copias e impresión*** | | | | | | | | | | | | | | |
| Copias | Hoja | 540 | $ 0,05 | **$ 24,30** | 600 | $ 0,05 | **$ 30,00** | 0 | $ - | **$ -** | 600 | $ 0,05 | **$ 30,00** | **$ 84,30** |
| Impresiones: Act 3.4 a color, 2 juegos de 225 pg c/u | Hoja | 180 | $ 0,14 | **$ 25,20** | 200 | $ 0,14 | **$ 28,00** | 0 | $ - | **$ -** | 200 | $ 0,36 | **$ 72,00** | **$ 125,20** |
| Empastado | Documento | 0 | $ - | **$ -** | 0 | $ - | **$ -** | 0 | $ - | **$ -** | 2 | $ 11,41 | **$ 22,82** | **$ 22,82** |
| Quemado CD | Documento | 0 | $ - | **$ -** | 0 | $ - | **$ -** | 0 | $ - | **$ -** | 2 | $ 0,91 | **$ 1,82** | **$ 1,82** |
| Encolochado | Hoja | 1 | $ 1,37 | **$ 1,37** | 5 | $ 1,37 | **$ 6,85** | 0 | $ - | **$ -** | 0 | $ 1,82 | **$ -** | **$ 8,22** |
| ***Trasporte y Viatico*** | | | | | | | | | | | | | | |
| Transporte | Persona | 3 | $ 0,50 | **$ 1,50** | 3 | $ 0,50 | **$ 1,50** | 3 | $ 0,50 | **$ 1,50** | 3 | $ 0,50 | **$ 1,50** | **$ 6,00** |
| Alimentación | Persona | 3 | $ 3,00 | **$ 9,00** | 3 | $ 3,00 | **$ 9,00** | 3 | $ 3,00 | **$ 9,00** | 3 | $ 3,00 | **$ 9,00** | **$ 36,00** |
| ***Servicios y Alquiler de Equipos*** | | | | | | | | | | | | | | |
| Internet | Hora | 10 | $ 0,64 | **$ 6,40** | 8 | $ 0,64 | **$ 5,12** | 6 | $ 0,64 | **$ 3,84** | 1 | $ 0,64 | **$ 0,64** | **$ 16,00** |
| Comunicaciones y Telefonía | Recarga | 3 | $ 2,30 | **$ 6,90** | 0 | $ - | **$ -** | 3 | $ 2,30 | **$ 6,90** | 0 | $ - | **$ -** | **$ 13,80** |
| Grabadora | día | 1 | $ 5,00 | **$ 5,00** | 1 | $ 5,00 | **$ 5,00** | 1 | $ 5,00 | **$ 5,00** | 0 | $ - | **$ -** | **$ 15,00** |
| Equipo (PC) | Hora | 4 | $ 0,46 | **$ 1,84** | 5 | $ 0,46 | **$ 2,30** | 8 | $ 0,46 | **$ 3,68** | 0 | $ - | **$ -** | **$ 7,82** |
| ***Recursos Humanos (Cancelación 50% )*** | | | | | | | | | | | | | | |
| Honorarios Personal Técnico $400 x Mes c/u/ 240 Horas * Mes | Personas 3 Personas * 2 Meses | 3 | $ 400,00 | $ 400,00 | $ 2.400,00 | $ - | $ - | 0 | $ - | $ - | | $ - | $ - | $ 2.400,00 |
| **TOTAL Por Actividad** | | | | **$ 81,51** | | | **$ 88,47** | | | **$ 29,92** | | | **$ 149,28** | **$ 2.743,43** |

## **ANEXO No. 10**. Cronograma de Actividades ASI

*Auditoria de Seguridad Informática*

Área de Informática

lunes, 13 de septiembre de 2010

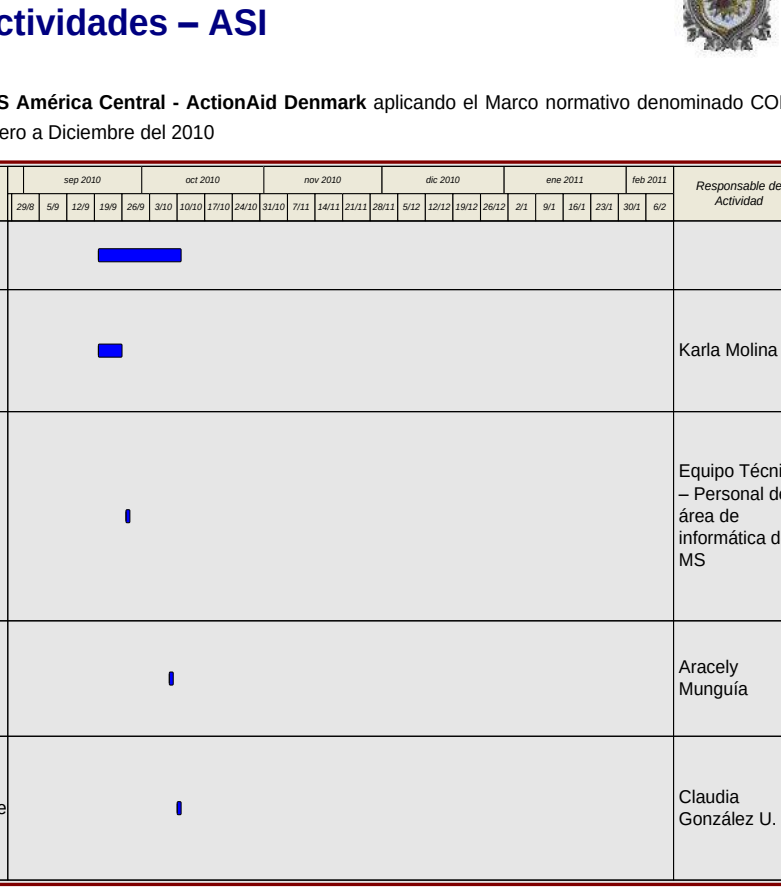
MS América Central
actionaid denmark

# Cronograma de Actividades – ASI

**Objetivo General:**

Desarrollar e Implementar un Modelo de Auditoria de Seguridad Informática al Organismo Internacional **MS América Central - ActionAid Denmark** aplicando el Marco normativo denominado COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), durante el periodo de Enero a Diciembre del 2010

| Id. | Actividad | Comienzo | Fin | Duración (# Semanas) | Frecuencia en la semana | Recursos | Instrumentos/ Requerimientos | Responsable de Actividad |
|---|---|---|---|---|---|---|---|---|
| 1 | **DESARROLLO DEL PROCESO DE AUDITORIA** | **20/09/2010** | **10/10/2010** | **3s** | | | | |
| 2 | Elaboración de Propuesta general de Auditoria de Seguridad Informática y Cronograma de Actividades de Auditoria | 20/09/2010 | 25/09/ 2010 | ,86s | 1 vez | PC, USB | • Investigaciones de contenido sobre el tema y Subtema. | Karla Molina |
| 3 | Reunión con el Sr. Jan Borsheim - Administrador Reginal de MS. y con el Sr Denis Urbina – Administrador logístico | 27/09/2010 | 27/09/ 2010 | ,14s | 1 vez | Cuaderno de Notas Transporte | • Documento de Especificaciones<br>• Cronograma de Trabajo<br>• Constancia de Solicitud para desarrollo de trabajo seminario de graduacion | Equipo Técnico – Personal del área de informática de MS |
| 4 | Visita: Estudio de Sitio | 08/10/2010 | 08/10/ 2010 | ,14s | 1 vez | Cuaderno de Notas Transporte, Cámara, USB. | • Documento de Especificaciones<br>• Cronograma de Trabajo | Aracely Munguía |
| 5 | Reunión Equipo técnico de Auditoria | 10/10/2010 | 10/10/ 2010 | ,14s | 1 vez | Cuaderno de Notas Transporte | • Información recogida a través de la visita de Sitio. | Claudia González U. |




***ASI** (Auditoria de Seguridad Informática)

*Auditoria de Seguridad Informática*

Área de Informática

lunes, 13 de septiembre de 2010

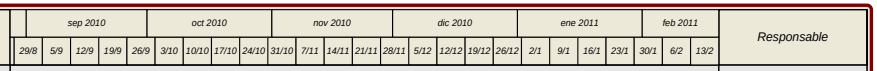
MS América Central
actionaid denmark

# Cronograma de Actividades – ASI

**Objetivo General:**

Desarrollar e Implementar un Modelo de Auditoria de Seguridad Informática al Organismo Internacional **MS América Central - ActionAid Denmark** aplicando el Marco normativo denominado COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), durante el periodo de Enero a Diciembre del 2010

| Id. | Actividad | Comienzo | Fin | Duración (# Semanas) | Frecuencia en la semana | Recursos | Instrumentos/ Requerimientos | Responsable |
|---|---|---|---|---|---|---|---|---|
| 1 | **FASE I: PLANEACION DE LA AUDITORIA** | **11/10/2010** | **31/10/2010** | **3s** | | | | |
| 2 | Revisión Preliminar | 11/10/2010 | 15/10/2010 | ,71s | 2 veces | Cuaderno de Notas Transporte, Cámara, USB | • Encuesta<br>• Entrevistas<br>• Cuestionario al personal del Área y de la organización<br>• Documentación sobre la organización<br>• Pruebas de consentimiento | Claudia González |
| 3 | Revisión Detallada | 18/10/2010 | 22/10/2010 | ,71s | 2 veces | Cuaderno de Notas Transporte, Cámara, USB | • Entrevistas- cuestionario a usuarios<br>• Pruebas de consentimiento Pruebas compensatorias o sustantivas) | Aracely Munguía |
| 4 | Elaboración del Informe 1ra Fase. | 25/10/2010 | 27/10/2010 | ,43s | 1 vez | PC, USB | • Información obtenida a través de los instrumentos | Claudia González |
| 5 | Reunión con el Equipo de Auditoria y personal de apoyo institucional | 29/10/2010 | 29/10/2010 | ,14s | 1 vez | Cuaderno de Notas Transporte | • Borrador de informe de la fase I. | Equipo Técnico – Personal del área de informática de MS |




***ASI** (Auditoria de Seguridad Informática)

*Auditoria de Seguridad Informática*

Área de Informática

lunes, 13 de septiembre de 2010

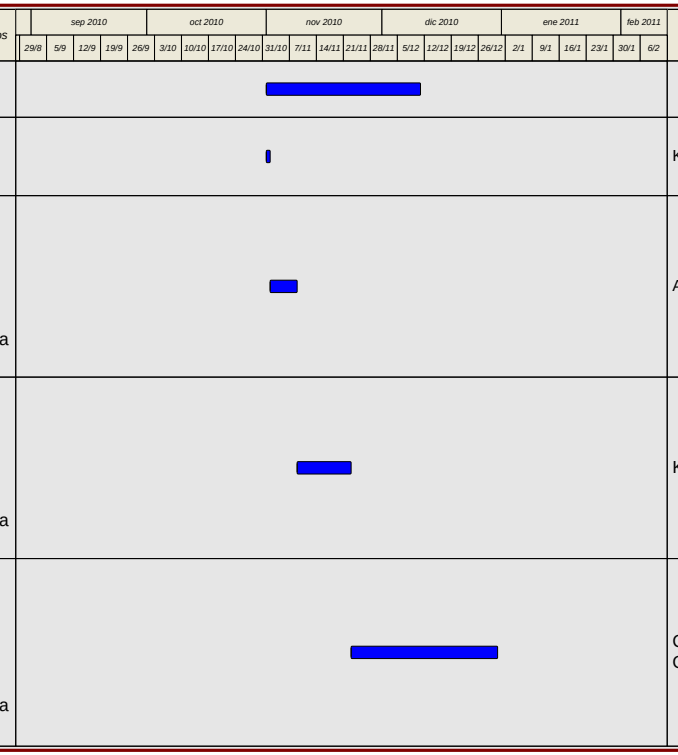
MS América Central
actionaid denmark

# Cronograma de Actividades – ASI

**Objetivo General:**

Desarrollar e Implementar un Modelo de Auditoria de Seguridad Informática al Organismo Internacional **MS América Central - ActionAid Denmark** aplicando el Marco normativo denominado COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), durante el periodo de Enero a Diciembre del 2010.

| Id. | Actividad | Comienzo | Fin | Duración (# Semanas) | Frecuencia en la semana | Recursos | Instrumentos/ Requerimientos | Responsable |
|---|---|---|---|---|---|---|---|---|
| 1 | **FASE II: EXAMEN Y EVALUACION** | **01/11/2010** | **10/12/2010** | **5,71s** | | | | |
| 2 | Reunión Equipo técnico de Auditoria | 01/11/2010 | 01/11/2010 | .14s | 1 vez | Cuaderno de Notas Transporte | • Formato de instrumentos | Karla Molina |
| 3 | Evaluación de la Dirección Informática Políticas, Control Interno | 02/11/2010 | 08/11/2010 | 1s | 3 veces | Cuaderno de Notas Transporte, Cámara, USB, Herramienta de Aplicación y medición | • Entrevistas<br>• Encuestas<br>• Cuestionarios<br>• Listas de Verificación<br>• Plan de Auditoria | Aracely Munguia |
| 4 | Evaluación Recursos de TI (Aplicaciones, Información, Infraestructura, Personas.) | 09/11/2010 | 22/11/2010 | 2s | 6 veces | Cuaderno de Notas Transporte, Cámara, USB, Herramienta de Aplicación y medición | • Entrevistas<br>• Encuestas<br>• Cuestionarios<br>• Listas de Verificación<br>• Plan de Auditoria | Karla Molina |
| 5 | Evaluación de la Contratación Externa y Riesgo Informático | 23/11/2010 | 30/12/2010 | 5,43s | 3 veces | Cuaderno de Notas Transporte, Cámara, USB, Herramienta de Aplicación y medición | • Entrevistas<br>• Encuestas<br>• Cuestionarios<br>• Listas de Verificación<br>• Plan de Auditoria | Claudia González |




***ASI** (Auditoria de Seguridad Informática)

*Auditoria de Seguridad Informática*

Área de Informática

lunes, 13 de septiembre de 2010

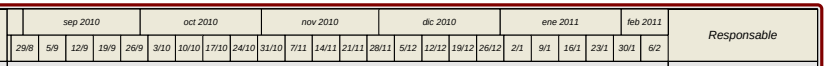
MS América Central
actionaid denmark

# Cronograma de Actividades – ASI

**Objetivo General:**

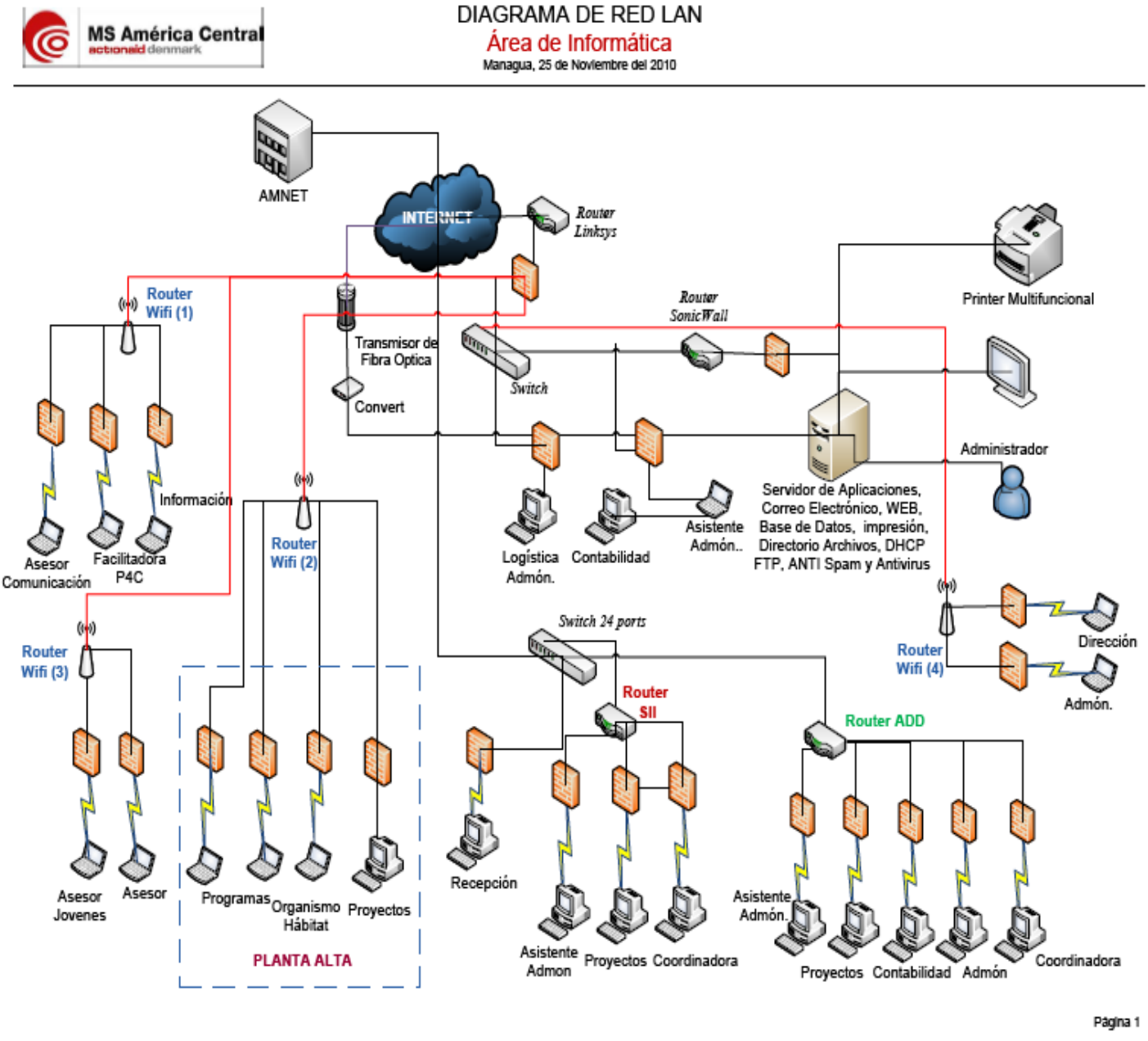
Desarrollar e Implementar un Modelo de Auditoria de Seguridad Informática al Organismo Internacional **MS América Central - ActionAid Denmark** aplicando el Marco normativo denominado COBIT (Objetivos de Control para Tecnología de Información y Tecnologías relacionadas), durante el periodo de Enero a Diciembre del 2010.

| Id. | Actividad | Comienzo | Fin | Duración (# Semanas) | Frecuencia en la semana | Recursos | Instrumentos/ Requerimientos | Responsable |
|---|---|---|---|---|---|---|---|---|
| 1 | Elaboración de Diseños gráficos de: Distribución de Plantas, Plano de Acceso y Seguridad y la simulación de la Red local | 27/11/2010 | 28/11/2010 | ,29s | 1 vez | Cuaderno de Notas, USB, PC, Programas: Visio 2007. | • Esquemas manuales obtenidos a través de la observación | Karla Molina |
| 2 | Elaboración de Informe | 29/11/2010 | 09/12/2010 | 1,57s | 1 vez | Avances Act anteriores, Pc, Herramienta de Aplicación | • Información obtenida a través de los instrumentos | Equipo Técnico |
| 3 | Reunión con el Equipo de Auditoria y personal de apoyo institucional | 10/12/2010 | 10/12/2010 | ,14s | 1 vez | Cuaderno de Notas Transporte | • Borrador de informe Fase II. | Equipo Técnico – Personal del área de informática de MS |
| 4 | **3RA FASE: COMUNICACIÓN DE RESULTADOS Y EL SEGUIMIENTO** | **13/12/2010** | **21/01/2011** | **5,71s** | | | | |
| 5 | Elaborar informe final del proceso de auditoria | 13/12/2010 | 28/01/2011 | 6,71s | | Cuaderno de Notas Transporte | 1ro y 2do borrador de fase I y fase II. | Equipo Técnico |
| 6 | Presentación y discusión del Informe final con el personal de apoyo institucional y la Alta Dirección | 31/01/2011 | 31/01/2011 | ,14s | | Cuaderno de Notas Transporte, PC | Propuesta de Informe Final | Equipo Técnico – Personal del área de informática de MS |
| 7 | Revisión y Correcciones finales para la entrega al Tutor y a la Dirección del Departamento de Informática | 01/02/2011 | 04/02/2011 | ,57s | | Cuaderno de Notas Transporte, PC | Informe Final | Equipo Técnico |




***ASI** (Auditoria de Seguridad Informática)

**ANEXO No. 11**. Diagrama de Red LAN



## **ANEXO No. 12**. Vulnerabilidad de la Red LAN – SW NESSUS 4.4

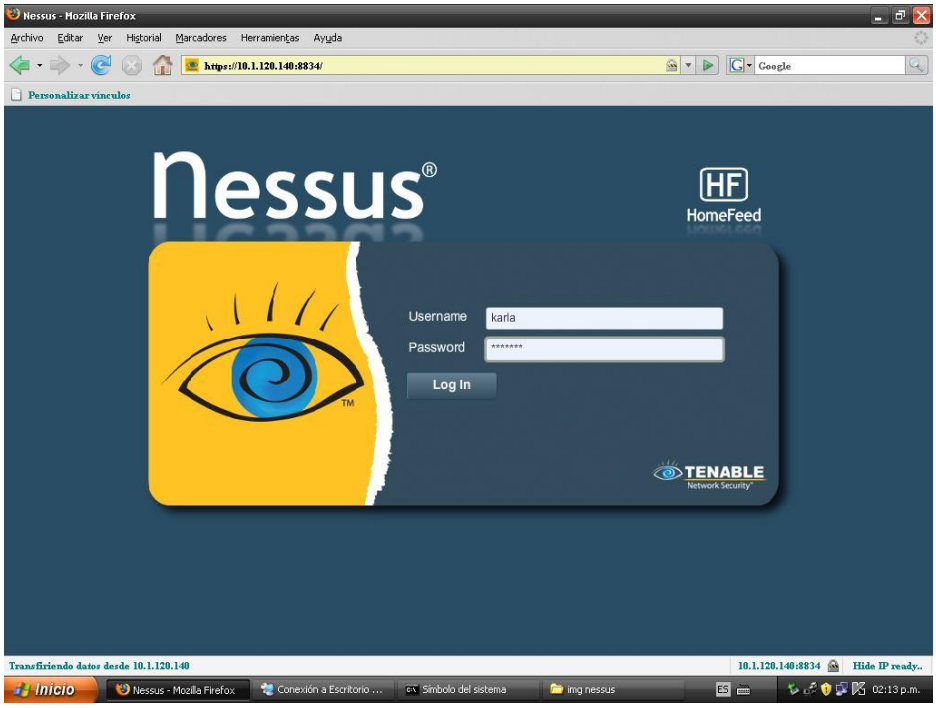
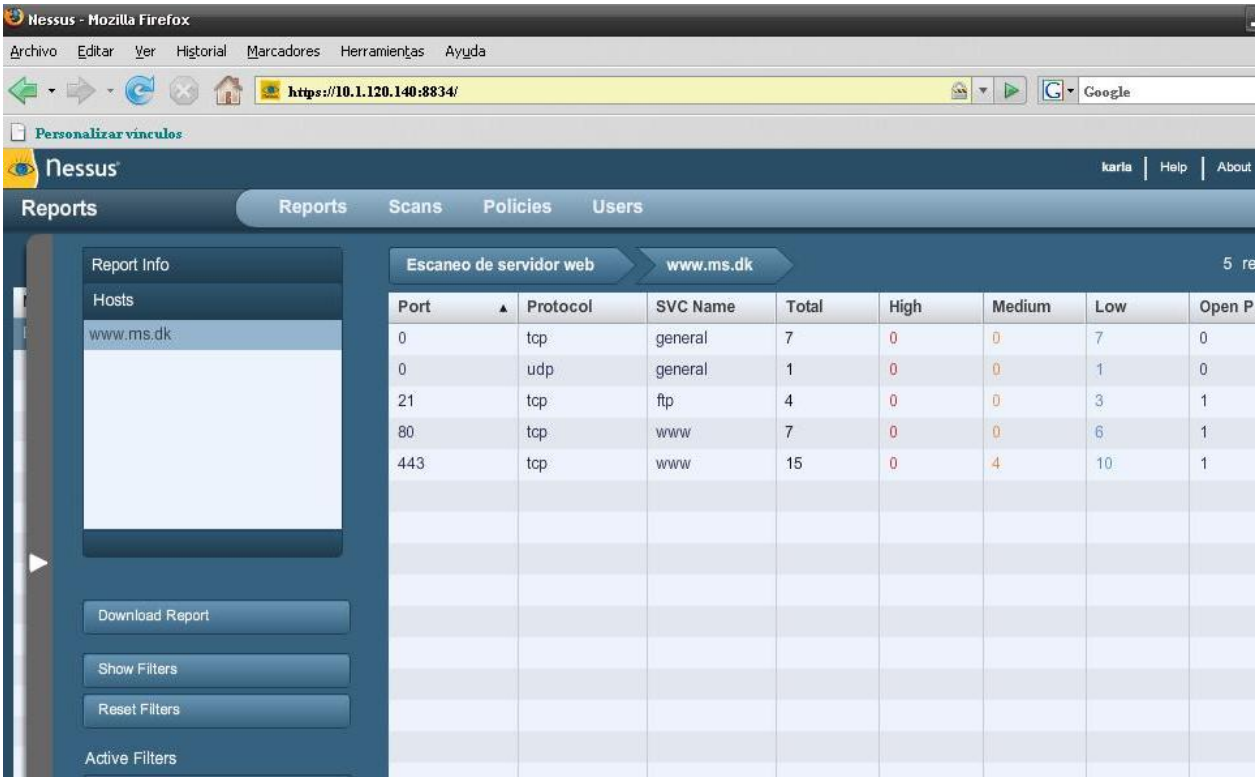



***Figura 12.1.*** Acceso Remoto a la Plataforma NESSUS




| Port | Protocol | SVC Name | Total | High | Medium | Low | Open P |
|---|---|---|---|---|---|---|---|
| 0 | tcp | general | 7 | 0 | 0 | 7 | 0 |
| 0 | udp | general | 1 | 0 | 0 | 1 | 0 |
| 21 | tcp | ftp | 4 | 0 | 0 | 3 | 1 |
| 80 | tcp | www | 7 | 0 | 0 | 6 | 1 |
| 443 | tcp | www | 15 | 0 | 4 | 10 | 1 |

***Figura 12.2.*** Report Scann www.ms.dk

## NESSUS REPORT WEB

### List of PlugIn IDs

**>PRINT**

**The following plugin IDs have problems associated with them. Select the ID to review more detail.**

| PLUGIN ID# | # OF ISSUES | PLUGIN NAME | SEVERITY |
|---|---|---|---|
| 10815 | 1 | Web Server Generic XSS | Medium Severity problem(s) found |
| 26928 | 1 | SSL Weak Cipher Suites Supported | Medium Severity problem(s) found |
| 20007 | 1 | SSL Version 2 (v2) Protocol Detection | Medium Severity problem(s) found |
| 42873 | 1 | SSL Medium Strength Cipher Suites Supported | Medium Severity problem(s) found |
| 22964 | 4 | Service Detection | Low Severity problem(s) found |
| 10302 | 2 | Web Server robots.txt Information Disclosure | Low Severity problem(s) found |
| 10386 | 2 | Web Server No 404 Error Code Check | Low Severity problem(s) found |
| 24260 | 2 | HyperText Transfer Protocol (HTTP) Information | Low Severity problem(s) found |
| 10107 | 2 | HTTP Server Type and Version | Low Severity problem(s) found |
| 43111 | 2 | HTTP Methods Allowed (per directory) | Low Severity problem(s) found |
| 43067 | 1 | Web Application Tests Disabled | Low Severity problem(s) found |
| 10287 | 1 | Traceroute Information | Low Severity problem(s) found |
| 25220 | 1 | TCP/IP Timestamps Supported | Low Severity problem(s) found |
| 51891 | 1 | SSL Session Resume Supported | Low Severity problem(s) found |
| 21643 | 1 | SSL Cipher Suites Supported | Low Severity problem(s) found |
| 10863 | 1 | SSL Certificate Information | Low Severity problem(s) found |
| 11936 | 1 | OS Identification | Low Severity problem(s) found |
| 19506 | 1 | Nessus Scan Information | Low Severity problem(s) found |
| 12053 | 1 | Host Fully Qualified Domain Name (FQDN) Resolution | Low Severity problem(s) found |
| 34324 | 1 | FTP Supports Clear Text Authentication | Low Severity problem(s) found |
| 10092 | 1 | FTP Server Detection | Low Severity problem(s) found |
| 45590 | 1 | Common Platform Enumeration (CPE) | Low Severity problem(s) found |
| 46180 | 1 | Additional DNS Hostnames | Low Severity problem(s) found |

## PORT WWW (443/TCP)

### WWW.MS.DK

**Scan Time**

| | |
|---|---|
| Start time: | **Sat Nov 06 15:04:33 2010** |
| End time: | **Sat Nov 06 15:10:23 2010** |

**Number of vulnerabilities**

| | |
|---|---|
| High | 0 |
| Medium | 4 |
| Low | 27 |

**Remote Host Information**

| | |
|---|---|
| Operating System: | **Microsoft Windows Server 2003** |
| DNS name: | **www.ms.dk** |
| IP address: | **217.145.50.22** |

**ANEXO No. 13**. Evaluación del Riesgo Informático – Implementación Matriz de Riesgo

MS América Central
actionaid denmark

## AUDITORIA EN SEGURIDAD INFORMATICA

### EVALUACION DEL RIESGO INFORMATICO

**Fecha de Aplicación:** 19/11/2010

**Doc No.** IM- EVR 01
**Aplicado Por:** Karla Molina G

**Matriz de Riesgo**

**Grado de Impacto (US$ miles)**

| Amenazas | Probabilidad | Servidores y Equipos de Conexión de Red | Terminales/ PC | Datos | Instalaciones | Personal | Servicio de Internet | Aplicaciones en Red | Correo Electrónico | Sistemas UPS | Riesgo Total | Efectividad del Control | Riesgo Residual |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Incendio | 1% | 10 | 5 | 1 | 62 | 41 | 60 | 0 | 20 | 10 | 2,09 | 100% | 0 |
| Inundación | 1% | 10 | 1 | 1 | 22 | 8 | 1 | 0 | 1 | 10 | 0,54 | 90% | 0,1 |
| Acceso no autorizados a información Confidencial | 20% | 1 | 1 | 12 | 1 | 0 | 0 | 62 | 10 | 0 | 17,40 | 50% | 8,7 |
| Mal uso de los recursos | 50% | 12 | 6 | 0,5 | 10 | 15 | 8 | 0,5 | 0,5 | 10 | 31,25 | 50% | 15,6 |
| Carga de SW malicioso | 30% | 1 | 20 | 25 | 0 | 0 | 0 | 0 | 0 | 0 | 13,80 | 90% | 1,4 |
| Ataques a la Red | 30% | 10 | 30 | 60 | 0 | 0 | 20 | 20 | 20 | 0 | 48,00 | 80% | 9,6 |
| Fallas en el servicio de energia | 5% | 0,5 | 0,5 | 2 | 0 | 0 | 0,5 | 0,5 | 0,5 | 1 | 0,28 | 90% | 0,0 |
| Virus | 30% | 2 | 3 | 1 | 0 | 0 | 20 | 20 | 10 | 0 | 16,80 | 80% | 3,4 |

| DESCRIPCION APLICACIÓN INTRUMENTO MATRIZ DE RIESGO | | |
|---|---|---|
| **Amenaza** | Amenaza identificada para cada uno de los elemento a evualuar | |
| **Probabilidad** | Indica cuan probable es que esa amenaza actué, con independencia de los controles que existan o que se establezcan. La certeza es el 100% y la imposibilidad es 0%. Cada porcentaje de cada fila es manejado en forma independiente. | |
| **Recursos** | Se indica para cada uno de los activos a proteger cual es el importe de la perdida media estimada que ocasionaría esa amenaza e ese activo | |
| | *Servidores* | Computadores centrales que soportan las bases de datos, la gestión del correo electrónico, la red internet y otros servicios |
| | *Terminales* | Puestos de trabajo computarizados |
| | *Datos* | Información de la Organización |
| | *Instalaciones* | Parte física, incluyendo edificio, mobiliario, componentes de red (cableado, "routers", "bridges", "switches"), etc |
| | *Personal* | Recursos humanos. |
| | *Servicio de Internet* | Monitoreo y Control del Servicio, Utilización de los Recursos de TI |
| | *Aplicaciones en Red* | Recursos de Trabajo para el Personal , Seguridad y Disponibilidad de las Aplicaciones en la Red . |
| | *Correo Electronico* | Servicio para usuarios de la Red, Via de comunicación intena |
| | *Sistema UPS* | Sistema ante fallas del Servicio Electrico |
| **Riesgo Total** | Sumariza los productos de la probabilidad de la amenaza por el impacto, de toda la fila<br>RT ***(Riesgo Total)*** = **Probabilidad** x **Impacto promedio** | |
| **Efectividad del Control** | Efectividad del control actuante, o sea que nivel de riesgo total se puede mitigar | |
| **Riesgo Residual** | Resulta de aplicar la efectividad del control al riesgo total. | |

MS América Central
actionaid denmark

# AUDITORIA EN SEGURIDAD INFORMATICA

## EVALUACION DEL RIESGO INFORMATICO

**Fecha de Evaluación:** 29/11/2010

**Doc No.** IM- EVR 02
**Evaluado Por:** Karla Molina G

**Descripción Análisis de los Recursos**

| Recurso | Amenaza | Vulnerabilidad | Control Existente | Recomendación |
|---|---|---|---|---|
| Sevidores y Equipos de Conexión de Red | Incendio, Inundaciones, Acceso no Autorizado, Mal uso de los Recursos, Ataques a la Red, Fallas en el servicio de Energia. | • No existe un documento específico de políticas de seguridad de TI<br>• No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible.<br>No existe un Plan de Contingencia | El documento actual de IPS Orientado al Staff no actualizado | Establecer un procedimiento de actualización periódica del documento<br>Diseñar un Plan de Seguridad de TI.<br>Diseñar un Plan de Contingencia |
| Terminales/ PC | Incendio, Inundaciones, Acceso no Autorizado, Mal uso de los Recursos, Carga de SW Malicioso, Ataques a la Red, Fallas en el servicio de Energia, | • No existe un procedimiento para verificar todos los boletines de advertencia e informativos con respecto al uso de software malicioso.<br>• No existe un documento formal para el registro de la entrega o retiro de recursos de TI al personal.<br>• No extiste un Plan de Contingencia | El documento actual es el Inventario para el control de equipos y este se actualiza anualmente. | Verificar periódicamente los boletines y dar a conocer a los usuarios.<br>Establecer un procedimiento de actualización periódica del documento<br>Diseñar un Plan de Contingencia |
| Datos | Acceso no Autorizado, Mal uso de los Recursos, Carga de SW Malicioso, Ataques a la Red, Fallas en el servicio de Energia, | • Los medios de respaldo y los procedimientos para su restauración no están guardados en un lugar seguro y lejos del sitio actual.<br>• No existe un plan de clasificación de información o en su lugar una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida. | Se define usuarios con perfil limitado | |
| Instalaciones | Incendio, Inundaciones, Acceso no Autorizado, Mal uso de los Recursos, Fallas en el servicio de Energia, | • No existe un procedimiento de actualización de planes de contingencia. | El documento actual de políticas no actualizado | Establecer un procedimiento de actualización periódica del documento |

| Descripción Análisis de los Recursos | | | | |
|---|---|---|---|---|
| **Recurso** | **Amenaza** | **Vulnerabilidad** | **Control Existente** | **Recomendación** |
| **Aplicaciones en red** | Acceso no Autorizado, Mal uso de los Recursos, Ataques a la Red, Fallas en el servicio de Energia. | • No existe un procedimiento de revisión periódica de archivos logs de los servidores. No existe un procedimiento de actualización de planes de contingencia. | Se define usuarios con perfil limitado<br>Firewall corporativo | Establecer un plan de contingencia que contemple este tipo de amenazas. |
| Correo Electrónico | Acceso no Autorizado, Mal uso de los Recursos, Ataques a la Red, Fallas en el servicio de Energia, | • No existe un procedimiento formal documentado ante la caida del sistema.<br>• No hay monitoreo continuo del flujo de informaci ón procesado por el servidor de Correo. | Sevidor Temporal para la recepcion de correos electronicos ante la caida del Sistema.<br>Filtro para correos basuras<br>Firewall corporativo, limita el envio masivo de correos electronicos de un IP determinada | Definir nuevas políticas sobre uso de correo, negar envió de cadenas, ríos de información no laboral, posible fuente de virus y perdida de datos |
| **Sistema de UPS** | Incendio, Inundaciones, Mal uso de los Recursos, Fallas en el servicio de Energia, | • Sin procedimiento de actualización de planes de contingencia | Plan de contingencia no actualizado | Crear un plan de contingencia para cubrir este tipo de amenazas |

# ANEXO No. 14.

## IMAGENES

**Captura de Imágenes (Observación, Chequeos y Pruebas)**

## **ANEXO No. 14**. Captura de Imágenes (Observación, Chequeos y Pruebas)

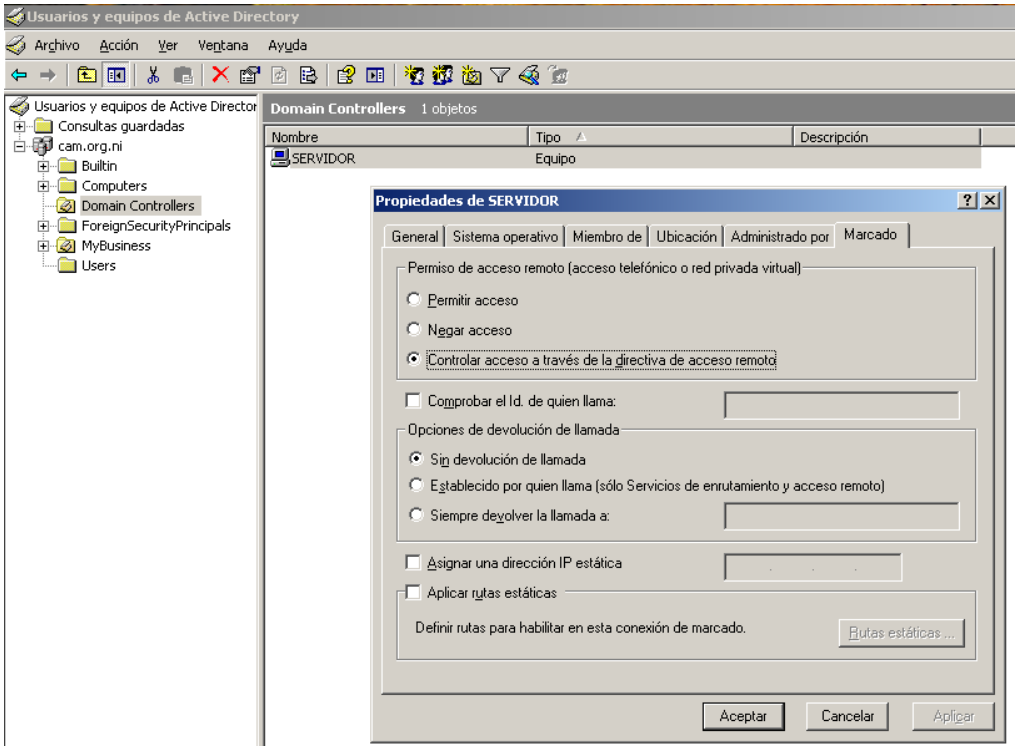



***Figura 14.1.*** Active Directory/Domain Controllers/ Pantalla Propiedades del Servidor/ Pestaña Marcado

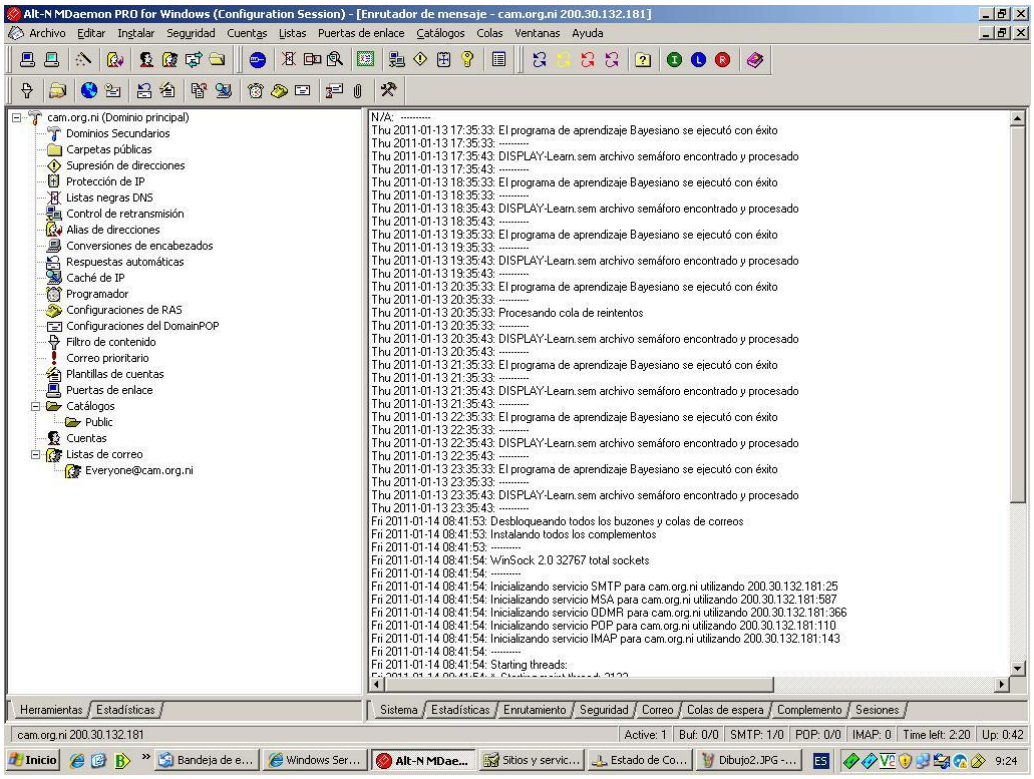



***Figura 14.2.*** Plataforma MDaemon- Pantalla Estadísticas

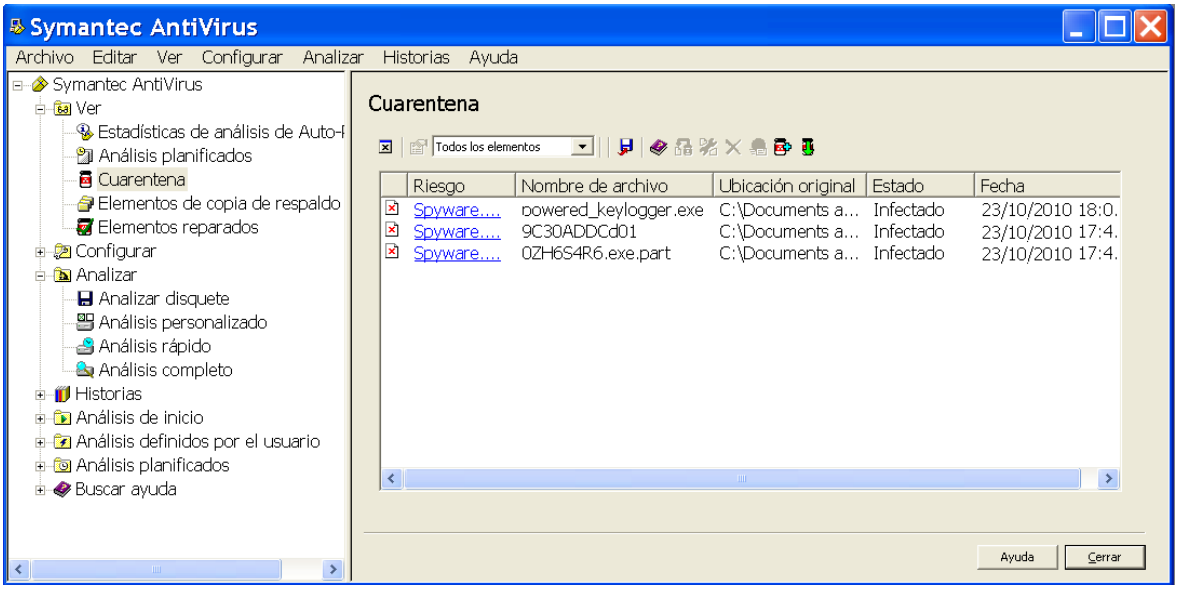



***Figura 14.3.*** Pantalla de Prueba SW AntiVirus- Descarga de Software Malicioso desde Internet e Instalación a Equipo Usuario 2 para la detección de Virus y Spyware.

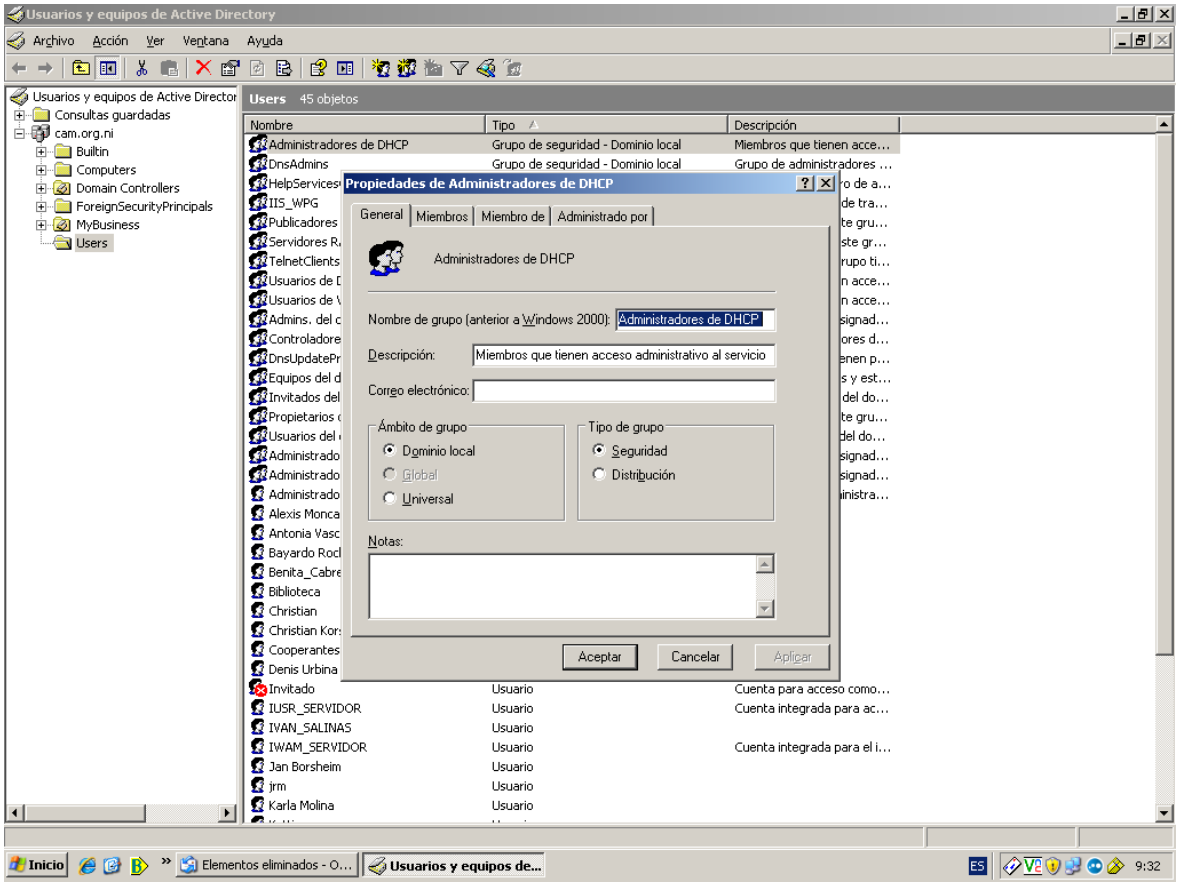



***Figura 14.4.*** Active Directory/Users/ Pantalla Propiedades de Admon de DHCP/ Pestaña General

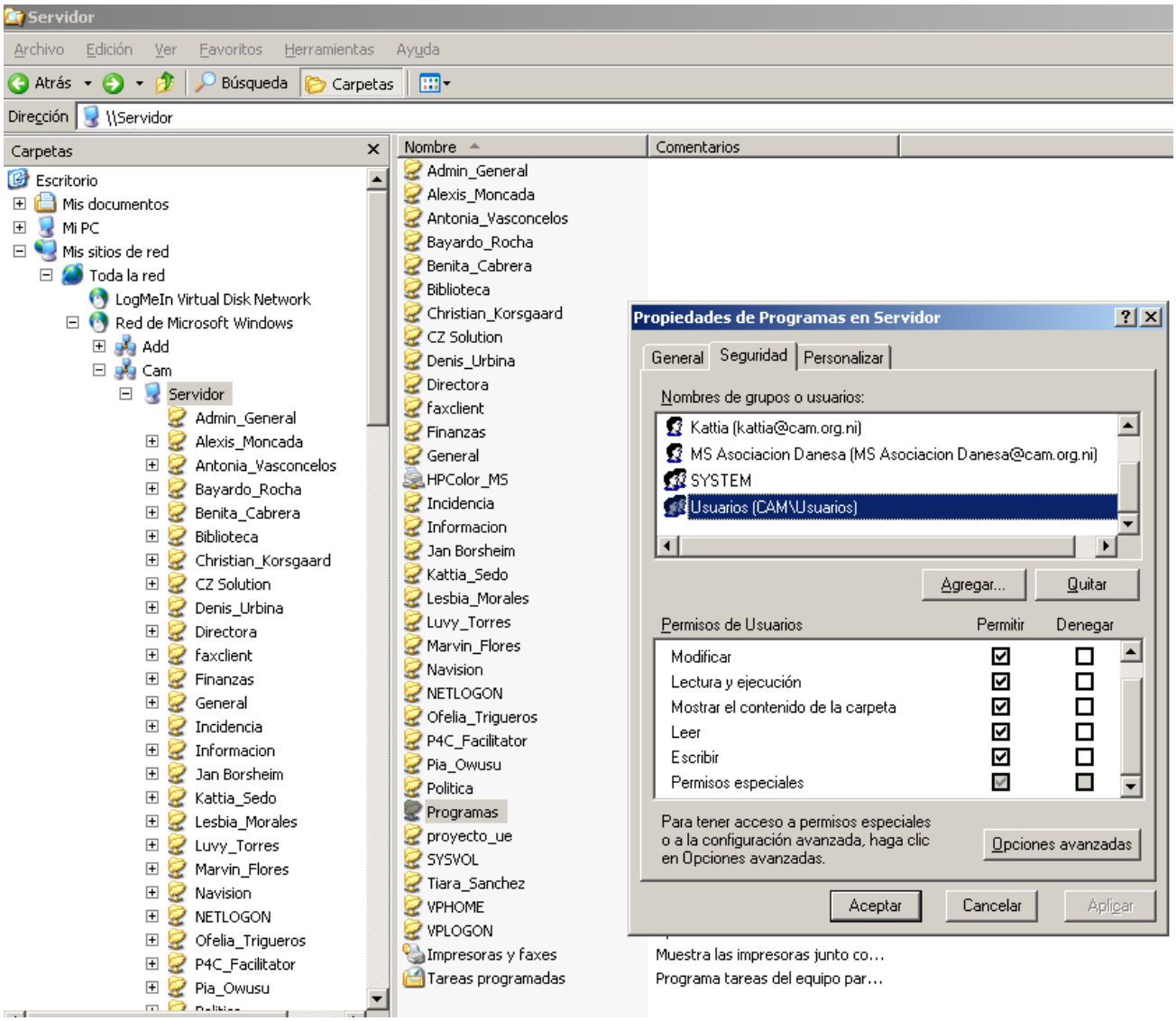



***Figura 14.5.*** Pantalla Propiedades de Programa en Servidor/ Pestaña Seguridad

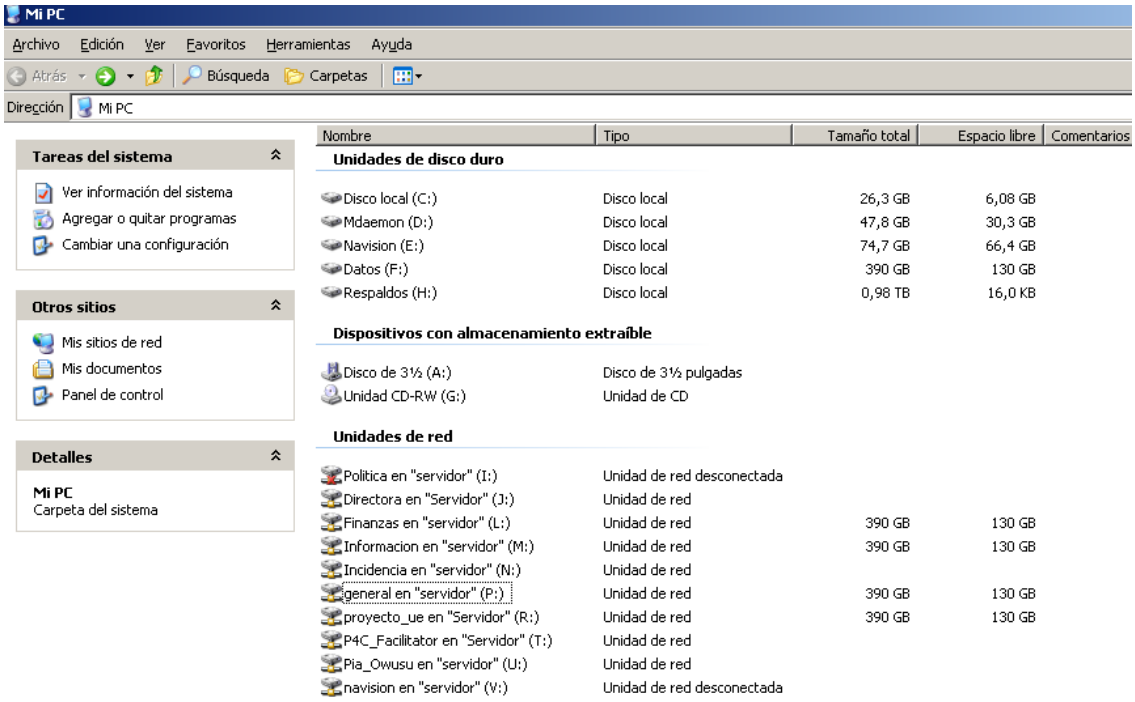



***Figura 14.6.*** Pantalla Arquitectura de la Información desde SERVIDOR

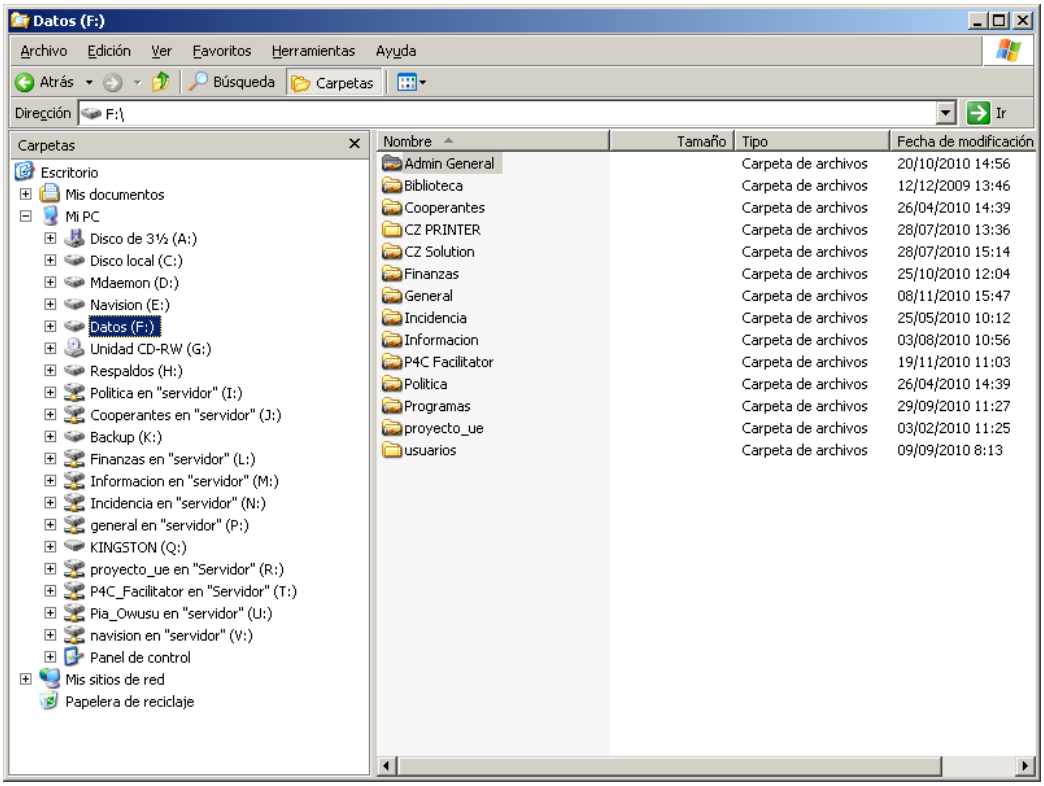



***Figura 14.7.*** Pantalla Arquitectura de la Información desde Unidad Datos (F:)

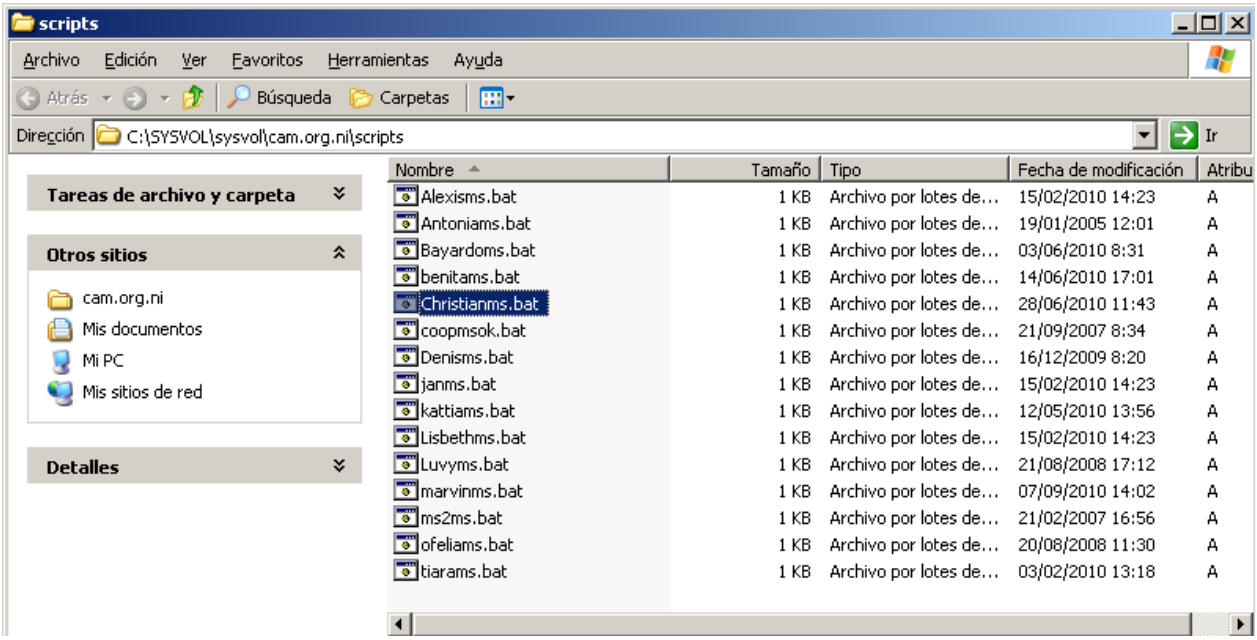



***Figura 14.8.*** Scripts

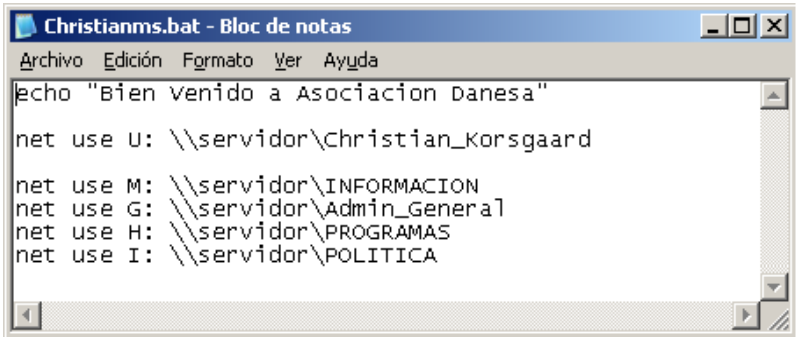



***Figura 14.9*** Scripts Chistianms.bat


***Figura 14.10.*** Pantalla Plataforma Software Navision Financials v8.Q3- Control de ACCESO desde Usuario Ofelia (Asistente Administrativo)

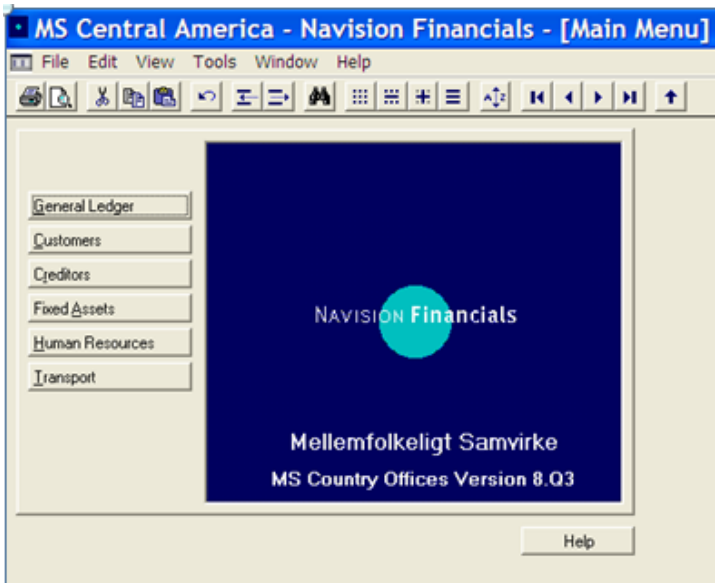



***Figura 14.11.*** Pantalla Plataforma Software Navision Financials v8.Q3 desde Usuario Ofelia (Asistente Administrativo)

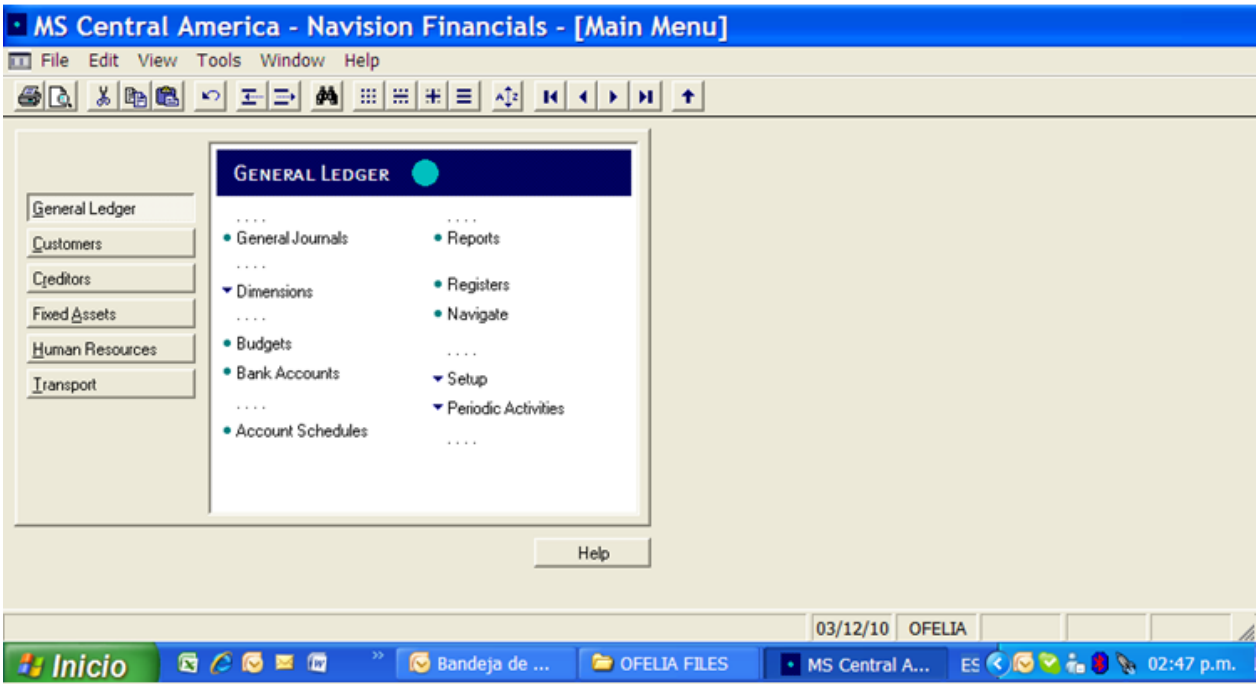



***Figura 14.12.*** Pantalla Plataforma Software Navision Financials v8.Q3 – General Legder desde Usuario Ofelia (Asistente Administrativo)

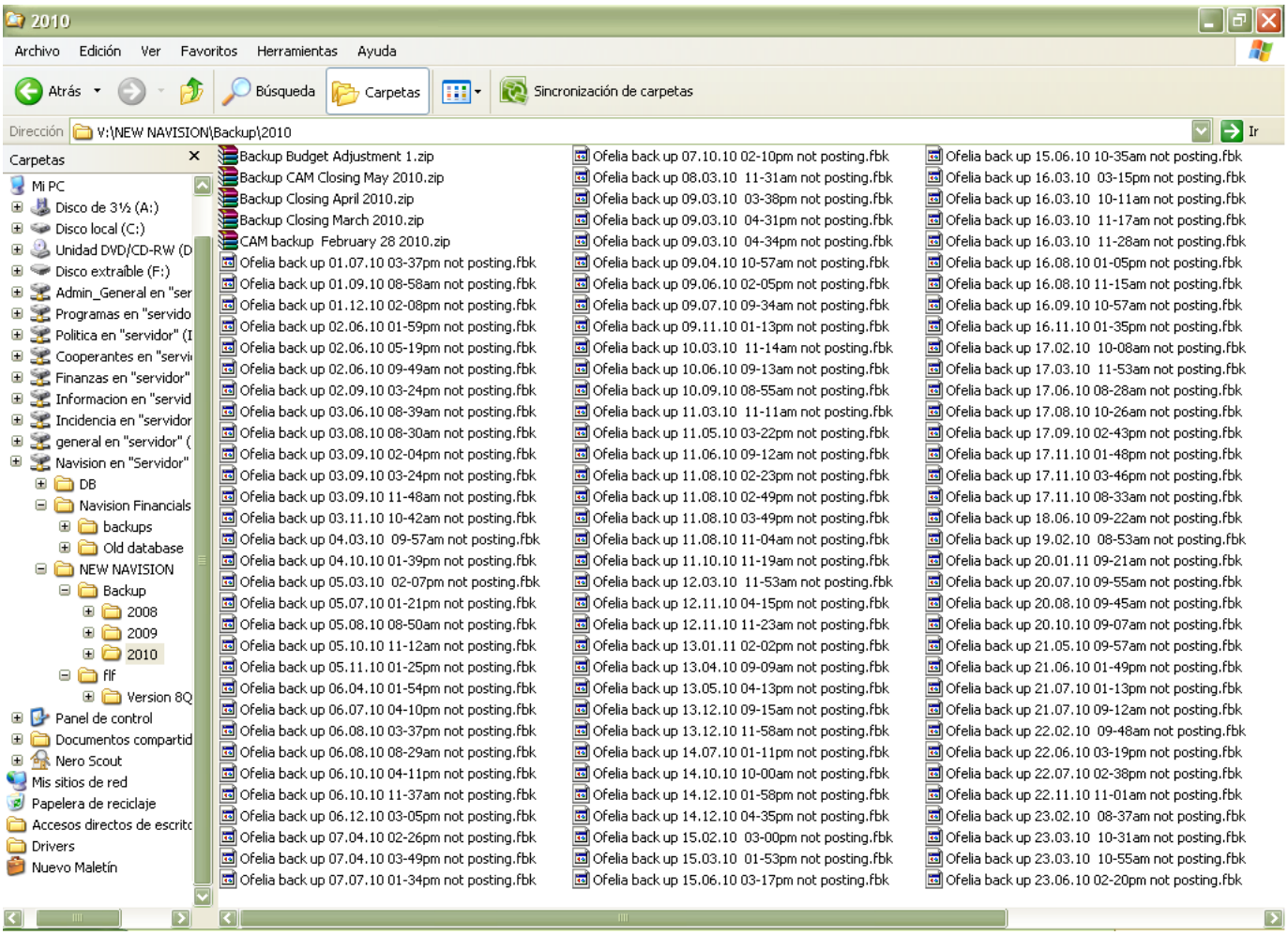



***Figura 14.13.*** Pantalla Back-up de Datos Registrados desde el Sistema Contable

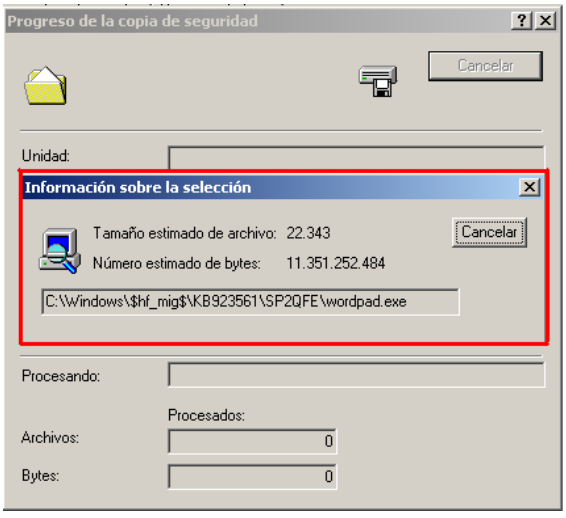



***Figura 14.14.*** Pantalla desde Servidor – Procedimiento de Back-up de Información del SERVIDOR

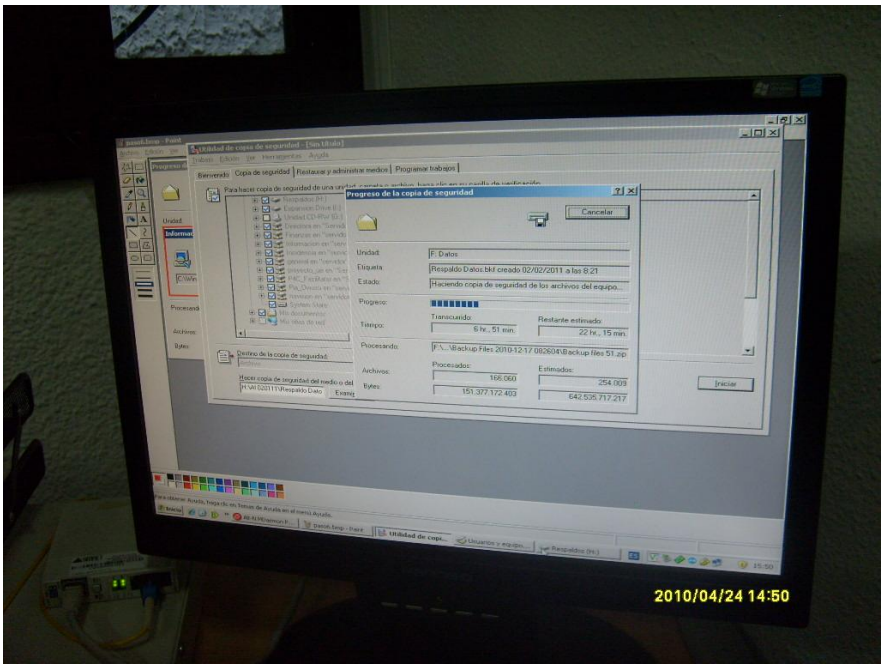



***Figura 14.15.*** Pantalla desde Servidor – Procedimiento de Back-up de Información del SERVIDOR

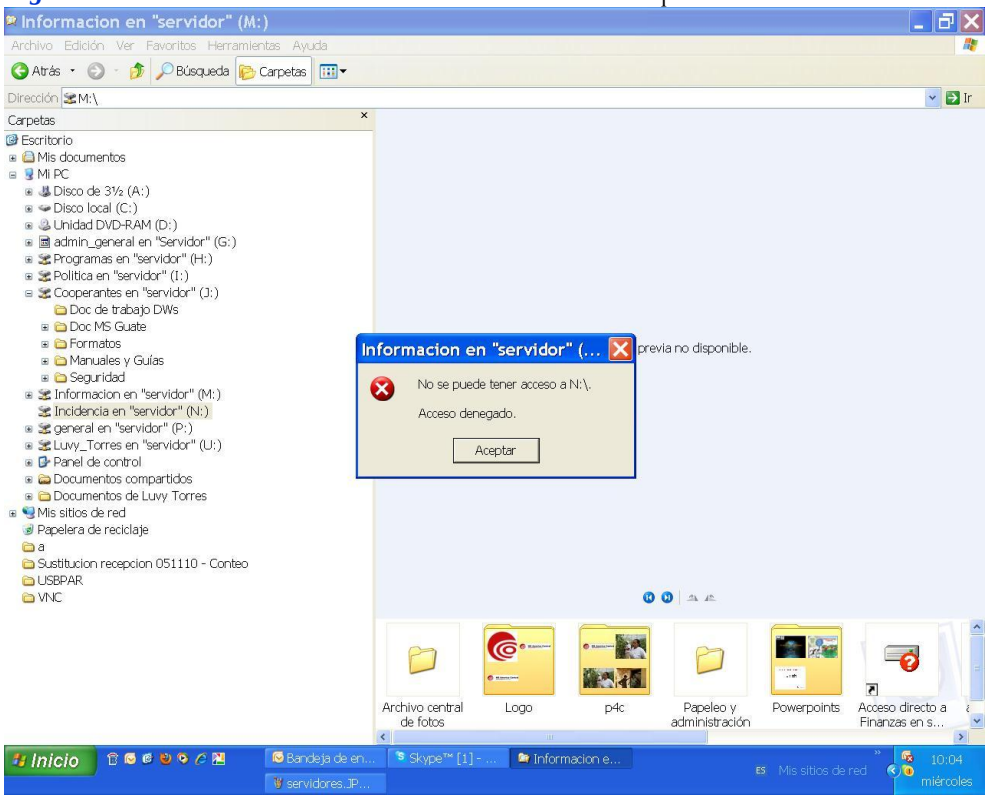



***Figura 14.16.*** Pantalla de Prueba a Usuario de Red – Control de Acceso a las Unidades de Red


***Figura 14.17.*** Hardware General SERVIDOR


***Figura 14.18.*** Hardware SERVIDOR / Switch


***Figura 14.19.*** Seguridad Física/ Extintor a 8 mts de Distancia


***Figura 14.20.*** Seguridad Física/Sistema de Alarma contra Intrusos – 1ra Planta Monitoreado por la Empresa Wackenhut


***Figura 14.21.*** Seguridad Física/ Uso de Cámara de Seguridad – Entrada Principal a las Instalaciones


***Figura 14.22.*** Seguridad Física/Control de Acceso del Personal a las Instalaciones - Recepción


***Figura 14.23.*** Seguridad Física/ Control de Acceso del Personal a las Instalaciones desde Recepción – Puerta Eléctrica


***Figura 14.24.:*** Seguridad Física/ Guarda de Seguridad en Entrada Principal a las Instalaciones


***Figura 14.25.*** Seguridad Física/ Planta Eléctrica para la Caída del Sistema Eléctrico

***Figura 14.26.*** Uso de Aire Acondicionado/ Mantenimiento de Equipos

**ANEXO No. 15.** Contrato de Auditoria

# CONTRATO DE AUDITORIA

**Por el periodo 01.01.10 a 31.12.10**

Contrato de presentación de Servicios Profesionales de Auditoría en Informática que celebran por una por una parte La Asociación Danesa para la Cooperación Internacional en sus siglas **MS- América Central**, representado por **Jan Borsheim**, en su carácter de Representante legal y Administrador Regional del Organismo Internacional y que en lo sucesivo se denominara el *"Cliente"* , por otra parte el Departamento de Computación de la Unan Managua, representado por las Br. Karla Vanessa Molina Gutiérrez, Br Claudia Regina González Urroz y la Br. Araceli del Carmen Munguía Alfaro, a quien se denomina "El Equipo Auditor", de conformidad con las declaraciones y clausulas siguientes:

**DECLARACION**

**I.El cliente declara:**

a)Que es una Auditoria en Seguridad Informática, evaluando desde los procesos de planeación de la Dirección hasta el monitoreo y seguimiento de lo relacionado con las actividades de TI.

b)Que está representado para este acto por Jan Borsheim, con domicilio Residencial Bolonia, de la Óptica Nicaragüense 1c arriba y 1 ½ al Sur. M/D Casa Otro Mundo.

Que requiere obtener servicios de Auditoria en Seguridad Informática, por lo que ha decidido responder a la solicitud formal del Representante del Equipo Auditor de recibir el servicio del Equipo Auditor, como parte del Origen de Auditoria.

**II.Declara el Equipo Auditor:**

a) Que es una sociedad con fines académicos, constituida y existente como parte al cumplimiento de La Modalidad de Graduación de acuerdo a la forma de Culminación de Estudios, Plan 1999. Aprobada por el Consejo Universitario en sesión No. 15 del 08 de Agosto del 2003. Y que dentro de sus objetivos primordiales está el de prestar Auditoría

en Informática, evaluando la Dirección, los Recursos de TI, Outsourcing y Riesgo Informático.

**III. Declaran Ambas Partes:**

Que habiendo llegado a un acuerdo sobre lo antes mencionado, lo formalizan otorgando el presente contrato para Auditoria 2010, que contiene en las siguientes:

## CLAUSULAS

**Primera. Objeto**

El Equipo Auditor se obliga a prestar al cliente los servicios de auditoría en informática para llevar a cabo la evaluación de la Dirección informática, de los Recursos de TI, el procedimiento de Outsourcing y el Riesgo Informático enfocados desde una perspectiva de seguridad informática, que se detalla en la propuesta de servicio anexa y que forma parte de este CONTRATO.

**Segunda. Alcance del Trabajo**

El alcance de los trabajos que llevara a cabo el Equipo Auditor dentro de este contrato son:

- **Evaluar los procesos de Organización, planificación, y administración de la dirección y del área de informática de la Organismo Internacional MS América Central – Action Aid Denmark** en lo que responde a: Su organización y Dirección, Funciones y Relaciones, Estructura interna y Dirección Tecnológica, Cumplimiento de los Objetivos, Recursos Humanos, Normas, Procedimientos y políticas de Seguridad, Capacitación, Planes de Trabajo, Planes estratégicos, Controles (De dirección, detección, corrección y recuperación), Estándares, Condiciones de Trabajo, Situación presupuestal y Financiera.

- **Evaluar los recursos de TI Tomando en cuenta:** Procesos de adquisición, instalación, explotación y mantenimiento de los Recursos de TI, Mantenimiento de la Infraestructura Tecnológica, Seguridad de los sistemas, Educación y Capacitación de los Usuarios, Administración de la Configuración, datos, ambiente físico y de Operaciones, Planes de Contingencias

- **Evaluación del Outsourcing Informático o Contratación Externa;** enfocándose en las cláusulas que contemple: La seguridad y confidencialidad, Desempeño y la Capacidad del Proveedor (Mantenimiento de los Equipos, Servicio de Internet.), Los niveles de servicio contenido en el contrato por Servicio.

- Evaluación de problemas y clasificación del Riesgo Informático y su impacto en la seguridad informática.

- Y finalmente se elabora informe que contengan conclusiones y recomendaciones por cada uno de los trabajos señalados en los incisos a), b), c) y d) de esta Clausura.

**Tercera. Programa de Trabajo**

El cliente y el auditor convienen en desarrollar en forma conjunta un programa de trabajo en el que se determinen con precisión las actividades a realizar por cada una de las partes, los responsables de llevarlas a cabo y las fechas de realización.

**Cuarta. Supervisión**

El cliente o quien designe tendrá el derecho de supervisar los trabajos que se le han encomendado al Equipo Auditor dentro de este contrato y a dar por escrito las instrucciones que estime convenientes.

**Quinta. Coordinación de los Trabajos**

En mutuo Acuerdo el Cliente designara un personal de Apoyo Institucional que trabaja y apoyar las actividades que el Equipo Auditor programe tanto para las técnicas de recolección de información como los procedimientos de pruebas, reuniones y entrevistas establecidas en el programa de trabajo, por otro lado el Equipo Auditor de igual manera designara a una persona que se encargara de establecer coordinación, organización y dirección del proyecto según fechas establecidas.

**Sexta. Horario de Trabajo**

El Equipo auditoria dedicara el tiempo necesario para cumplir satisfactoriamente con los trabajos materia de celebración de este contrato, de acuerdo al programa de trabajo convenido por ambas partes y gozara de libertad fuera del tiempo destinado al cumplimiento de las actividades, por lo que no estará sujeto a horarios y jornadas determinadas.

**Séptima. Personal Asignado**

El Equipo Auditor designara para el desarrollo de los trabajos de este contrato únicamente al personal que compone al mismo.

**Octava. Relación Laboral**

El personal del Equipo Auditor no tendrá ninguna relación laboral con el Cliente y queda expresamente estipulado que este contrato se suscribe en atención a que el equipo auditor en ningún momento se considera intermediario del cliente respecto al personal que ocupe para dar seguimiento de las obligaciones que se deriven de las relaciones entre él y su personal.

**Novena. Plazo de Trabajo.**

El Equipo Auditor se obliga a terminar los trabajos señalados en la clausula segunda de este contrato en 100 días hábiles después de la fecha en que se firme el contrato y sea cobrado el anticipo correspondiente. E tiempo estimado para la terminación de los trabajos esta con relación a la oportunidades con que el cliente entregue los documentos requeridos por el Equipo Auditor y al cumplimiento de las fechas estipuladas en el programa de trabajo aprobado por las partes, por lo que cualquier retraso ocasionado por parte del personal del cliente o de los usuarios de los sistemas repercutirá en el plazo estipulado, el cual deberá incrementarse de acuerdo a las nuevas fechas establecida en el programa de trabajo.

**Decima. Honorarios**

Según estimaciones presupuestarias, el Cliente pagara al Equipo Auditor por los trabajos objeto del presente contrato, honorarios por la cantidad de U$$ 800.00 mas el impuesto al valor agregado correspondiente. La forma de pago será la siguiente.

a)US$800.00 a la firma del Contrato.
b)US$800.00 a los 5 días después a la terminación de los trabajos y presentación del informe final de Auditoria.

Por tratarse de un trabajo investigativo a interés del equipo auditor se exoneran del cobro de honorarios en este caso al Cliente.

**Undécima. Gastos Generales**

Los gastos de fotocopiados, escaneo e impresión así como de papelería, que se produzcan con motivo de este contrato correrán por cuenta del Cliente.

**Duodécima. Jurisdicción**

Todo lo no previsto en este contrato se regirá por las disposiciones relativas, contenidas en el Marco de Trabajo de Cobit 4.1.

**Decimotercero. Confidencialidad e integridad de la Información**

El cliente facilitara y dispondrá al equipo auditor toda aquella información que requiere siempre y cuando el cliente lo haya autorizado. El equipo auditor se compromete a guardar confidencialidad, integridad y la no exposición a terceros de información y datos sensitivos relacionados al ejercicio de actividades del Organismo Internacional MS - América Central.

Enteradas ambas partes del contenido y alcance legal de este contrato, lo rubrican y firman de conformidad, en original y tres copias, en la Ciudad de Managua a los 01 días del Mes de Octubre del 2010.


EL CLIENTE

EL EQUIPO AUDITOR

## **ANEXO No. 16.** GLOSARIO DE ABREVIATURAS

**AI:** Adquirir e Implementar.

**ASC:** Auditoria de sistemas computacionales

**BPR:** Business Process Re-engineering (Reestructuración de procesos Empresariales)

**BPO:** Business Process Outsourcing (Proceso de negocio de contratación externa)

**COBIT:** Control Objectives for Information and related Technology

**COSO:** Comité de Organizaciones Patrocinadoras de comisión Treadway. Estándar Aceptado a nivel internacional para el gobierno corporativo. Ver www.coso.org

**CPD´S:** Centro de Procesamiento de Datos

**DS:** Entregar y dar soporte.

**ISACA:** Systems Audit and Control Association (Asociación de auditoría y control de Sistemas de información)

**KGI:** Indicador clave meta.

**KpI:** Indicador clave desempeño.

**LOPD:** Ley de organización de protección de datos

**ME:** Monitorear y evaluar.

**OLA:** Acuerdo a nivel operativo, un acuerdo interno que cubre la prestación de servicio que da soporte a la organización de TI en su prestación de servicio.

**PO :** Planear y organizar.

**PSI:** Política de seguridad informática.

**QMS:** Sistema de administración de calidad.

**SLA :** Acuerdo de nivel de servicio.

**TI:** Tecnología de información.

**TQM:** Total Quality Management (Gestión de calidad Total).

## **ANEXO No. 17.** GLOSARIO DE TERMINOS

### *A*

**Administración de la configuración-** el control de cambios realizados a un conjunto de componentes.

**Administración de desempeño-** de Capacidad administrar cualquier tipo de medición, incluyendo mediciones de empleados, equipos, proceso, operativas o financieras.

**Arquitectura de TI-** Un marco integrado para evolucionar o dar mantenimiento a Ti existentes y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

**Arquitectura empresarial para TI-** Respuesta en la entrega de TI, provista por procesos claramente definidos usando sus recursos (aplicaciones, información, infraestructura y personas).

**Autenticación-** El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. La autenticación está diseñada para proteger contra conexiones de acceso fraudulentas.

### *B*

**Backup-** Respaldos que se deben hacer para recuperar la información ante cualquier eventualidad.

**Benchmarking-** es el proceso continuo de medir productos, servicios y prácticas contra los competidores o aquellas compañías reconocidas como líder en la industria.

**Bitácora-** Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser Fecha y hora, dirección IP origen y destino, usuarios, errores.

### *C*

**Componentes de la configuración (CI)-** Componente de una infraestructura o un artículo como una solicitud de cambio asociado con una infraestructura.

**Continuidad-** Prevenir, mitigar y recuperarse de interrupciones.

## *D*

**Desempeño-** La implantación real o el logro de un proceso.

**Directriz-**La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento.

**Dominio-** Agrupación de objetivos de control en etapas lógicas en el ciclo de vida de inversión en TI**.**

## *F*

**Fiabilidad-** es la probabilidad de que un sistema funcione o desarrolle una cierta función, bajo condiciones fijadas y durante un período determinado.

## *I*

**Infraestructura-** la tecnología, los recursos humanos y las instalaciones que permiten el procesamiento de las aplicaciones.

**Incidente-** Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o una reducción de calidad de ese servicio.

## *M*

**Madurez-** indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, alcanzar las metas y objetivos deseados.

**Matriz RACI-** ilustra quién es responsable, quién debe rendir cuentas, a quién se debe consultar e informar dentro de un marco de trabajo organizacional estándar.

**Modelo de madurez de capacidad (CMM)-** Es un modelo utilizado por muchas organizaciones para identificar las mejores prácticas, las cuales son convenientes para ayudarles a evaluar y mejorar la madurez de un proceso del desarrollo del SW.

## *O*

**Objetivo de control-** Una declaración del resultado o propósito que se desea alcanzar al implementar procedimientos de control en un proceso en particular.

**Outsourcing-** Contratación Externa

## P

**Plan de contingencia-** pasos que se deben seguir, luego de un desastre para recuperar aunque sea en parte la capacidad funcional del sistema.

**Plan de infraestructura tecnológica-** Un plan para el mantenimiento y desarrollo de la infraestructura tecnológica.

**Plan estratégico de TI-** Un plan a largo plazo, con un horizonte de 3 a 5 años, donde la gerencia del negocio de TI describe de forma cooperativa como los recursos de TI contribuirán a los objetivos estratégicos empresariales.

**Política-** Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presentes y futuras haciendo que estén de acuerdo a la filosofía, objetivos y planes estratégico establecidos por los equipos gerenciales de la empresa.

**Proceso-** Un conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos.

**Programa aplicativo-** Un programa que procesa los datos del negocio a lo largo de las actividades, tales como la captura, actualización, o consulta de datos.

**Protocolo SLIP-** es el responsable del control de error, agrupa en paquetes los datos y otras actividades que permiten a los programas TCP/IP funcionar conjuntamente,

**Protocolo PPP-** tiene las mismas funciones que SLIP, pero es más reciente y más robusto.

**Proveedor de servicios-** Organización externa que presta servicios a la organización.

## R

**Riesgo-** El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos para ocasionar pérdidas y/o daño a los activos.

**Reuters-** Los routers se utilizan en redes complejas y de gran tamaño donde hay caminos para que las señales de la red viajen al mismo destino

## S

**Segregación/Separación de tareas-** Un control interno básico que previene y detecta errores o irregularidades por medio de la asignación a individuos diferentes, de la responsabilidad de iniciar y registrar las transacciones y custodia de los activos.

## U

**Usuario-** Una persona que utiliza los sistemas empresariales.

## REFERENCIAS BIBLIOGRAFICAS

### Libros

— Echenique G. José A. Auditoría en Informática. Segunda Edición, McRae- Hill/ Interamericana Editores, S.A de C.V, México. 2001.

— Hernández, Enrique. Auditoría en Informática; Un enfoque Metodológico y práctico. Primera Edición, Compañía Editorial Continental, S.A de C.V, México. 1996.

— Muñoz Raso, Carlos. Auditoría de Sistemas Computacionales. Primera Edición, Pearson Educación, México. 2002.

— Piatinni, Mario. Et. al. Auditoria de Tecnologías y Sistemas de Información. Primera Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2008.

— Piatinni, Mario. Et. al. Auditoria de Tecnologías y Sistemas de Información. Segunda Edición, Alfaomega Grupo Editor, S.A de C.V, México. Abril 2001.

### Referencia WEB GRAFIA

— Adacsi (2010a). "COBIT". Internet Document unloaded, 07 Agosto 2010. http:// www.adacsi.org.ar/files/es/content/141/COBIT.doc

— Cobit and IT Governance Institute (2007),"COBIT 4.1", 4ta Edición, Internet Document unloaded, 07 de Agosto 2010. http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf.

— Carrasco, Manuel. Seguridad en Redes de Computadoras. Ponencia en el Ciclo de Conferencias de la UAH, Abril 2003, 27 p. Disponible en Línea en: http://www.slideshare.net/dodotis/seguridad-en-redes-de-computadoras, última visita 07 de Agosto 2010.

— Rincondelvago(año)."Valoración de Outsourcing", Disponible en: http://html.rincondelvago.com/valoracion-de-outsourcing.html, última visita 20 de Nov. 2010.

— Tecolsof (Año). "Outsourcing y Help Desk", Disponible en línea en: http://www.tecolsof.com/index.php?name=Servicios&id_cat=3, última visita 20 de Nov. 2010.

— Monografías (año). "La Auditoria informática dentro de las etapas de Análisis de Sistemas Administrativos" Disponible en Línea en:
"http://www.monografias.com/trabajos5/audi/audi.shtml. Ultima Visita 03 de Noviembre del 2010

— Monografías (año). "Auditoría de Sistema y políticas de Seguridad Informática" Disponible en Línea en: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml. Ultima Visita 03 de Noviembre del 2010

— Itgi. (año). “Criterios de Seguridad Informática”, Disponible en Línea en: http://www.itgi.org, última visita Agosto 29 de 2010

— Textos científicos (año). “Políticas de Seguridad”, Disponible en Línea en: [http://www.textoscientificos.com/redes/firewalls-distribuidos/soluciones-seguridad/politicas-seguridad/planes-seguridad], Ultima visita 07 de Agosto del 2010.

## Otros Documentos

— Introducción al Riesgo. Sena Leonardo, 2004

— DELGADO, Ajax. Et al. Auditoria en la Administración de la Red del Centro de Operación de Redes (CORE). Managua, 2007, 107 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación.

— ROJAS, Xiomara A. Et al. Auditoria de seguridad del personal, Física y Ambiental del Auto lote “Club Automotriz Nicaragüense” (CANSA). Managua, 2007, 131 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación.

— GALEANO, J. Uriel. Et al. Aplicación de Auditoría en el Departamento de Informática de DIDEMA S.A, Evaluando la Organización, Planificación, Políticas de seguridad, Contratación Externa y Administración de Proyectos. Managua, 2007, 147 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación.

— GARCIA, Alina Et al. Auditoria del Desarrollo y Mantenimiento del Sistema para el Control de Datos de Becados Internos y Externos del Departamento de Becas de la UNAN Managua en el Periodo de Sept. – Oct. 2006. Managua, 2007, 88 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación.

— CASTILLO, Fanny. Et al. Auditoria de Seguridad Lógica y Control de Acceso en el Servidor de Mi Familia. Managua, 2007, 71 p. Seminario Monográfico (Licenciado en Ciencias de la Computación). Universidad Nacional Autónoma de Nicaragua. Facultad de Ciencias e Ingenierías. Departamento de Computación.

— OCHOA Teresa, Normativa para elaborar citas bibliográficas y notas de pie de página, Nov. 2006.