CORPORACIÓN UNIVERSITARIA UNITEC

# METODOLOGÍAS DE ANÁLISIS PARA UN PROYECTO DE CONSULTORÍA EN SEGURIDAD DE LA INFORMACIÓN

PROYECTO

**CPG**

ESCUELA DE INGENIERÍA –PROGRAMA DE SISTEMAS

BOGOTÁ JUNIO 15 DE 2007

**CORPORACIÓN UNIVERSITARIA UNITEC**

# METODOLOGÍAS DE ANÁLISIS PARA UN PROYECTO DE CONSULTORÍA EN SEGURIDAD DE LA INFORMACIÓN

PROYECTO

**CPG**

**RICARDO ANDRÉS ÁLVAREZ PINZÓN**

CÓD. 36041074

**LUIS EDUARDO NOVO DÍAZ**

CÓD. 36041068

**JOAHNNA LORENA PORRAS MORENO**

CÓD. 36031016

DOCENTE

**ING. DUILIO A. BUELVAS P.**

**ESCUELA DE INGENIERÍA –PROGRAMA DE SISTEMAS**

**BOGOTÁ JUNIO 15 DE 2007**

RICARDO ANDRÉS ÁLVAREZ PINZÓN

LUIS EDUARDO NOVO DÍAZ

JOAHNNA LORENA PORRAS MORENO

FIRMA

NOMBRE: _____

PRESIDENTE DEL JURADO

FIRMA

NOMBRE: _____

JURADO 1

FIRMA

NOMBRE: _____

JURADO 2

FIRMA

NOMBRE: _____

JURADO 3

## AL LECTOR

"Seguid! Seguid! Y sin la ruta umbrosa
El paso os cierra levantado monte,
Subid hasta su cumbre tenebrosa
Y ved el horizonte!"

**J. A. SILVA**

## AGRADECIMIENTOS

Nuestros más sinceros agradecimientos a la Corporación Universitaria Unitec y a los docentes que con su experiencia y profesionalismo nos han aportado grandes conocimientos y han logrado crear en nosotros una mentalidad de liderazgo y profesionalismo que será de gran ayuda en nuestro nuevo camino.

Especial agradecimiento al Ingeniero Duilio A. Buelvas P. por su gran ayuda en el desarrollo de este proyecto.

# CONTENIDO

# I. LISTA DE TABLAS

## II. INTRODUCCIÓN

Actualmente las empresas carecen de controles para el manejo de la información siendo este el activo más importante de toda empresa. Por lo tanto se hace necesario la implementación de consultorías que establezcan parámetros de seguridad de acuerdo a estándares internacionales que permitan a las organizaciones mantener la integridad, confiabilidad y confidencialidad de la información.

Para el desarrollo de una consultoría exitosa es necesario tener conocimiento de los estándares internacionales sobre manejo y seguridad de la información.

Durante el desarrollo de la presente consultoría se entrevistaron a las dos personas que tienen el mayor conocimiento y experiencia en el manejo y tratamiento de la información.

## III. OBJETIVO GENERAL

- Aplicar los conocimientos adquiridos durante el módulo del Curso de Preparación de Grado, en un proyecto de implementación de consultoría de seguridad a un sistema de información, teniendo en cuenta parámetros específicos de análisis basados en estándares de seguridad establecidos, y siguiendo ciertas métricas de apoyo que ayudarán a alcanzar los objetivos específicos que serán definidos más adelante.

## IV. OBJETIVOS ESPECÍFICOS

Reconocer las políticas y procedimientos de la empresa en cuanto a la manipulación y custodia de la información.

Basados en la norma ISO 17799 confrontar si la empresa cumple con los estándares de las políticas de seguridad en el sistema de Información.

Implementar el uso de herramientas de verificación para llevar un control y registro de la consultaría que se lleva a cabo.

Realizar un reporte con todos los hallazgos encontrados por medio de las listas de verificación.

Presentar un informe detallado a la gerencia donde se indiquen las anomalías que se presentan en la seguridad de la información.

## V. CONSIDERACIONES

Para comenzar a plantear la definición y los conceptos de la consultoría de Sistemas e Informática, debemos posicionarnos en ¿Qué es CONSULTORÍA?, El término de Consultoría muchas veces se ha empleado incorrectamente y con frecuencia solo se le considera como una evaluación cuyo único fin es detectar errores y señalar fallas. Pero la consultoría y el control van más allá de detectar fallas.

A. **Concepto de Consultoría.-** Es un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, etc.

B. **Función del Control.-** Una definición que es correcta y a la cual representa el valor de la Función del Control es la de ayudar a los funcionarios que tienen responsabilidad administrativa, técnica y/u operacional a que no incurran en falta. Y es por ello que aquí el control es creativo - inteligente, y constructivo de asesoramiento oportuno a todas las direcciones o gerencias a fin de que la toma de decisiones sea acertada, segura y se logren los objetivos, con la máxima eficiencia.

   De que, en dicha entidad, antes de realizarse la consultoría, ya se habían detectado fallas. El concepto de consultoría es mucho más que esto.

C. **El Control de Sistemas e Informática.-** consiste en examinar los recursos, las operaciones, los beneficios y los gastos de las

producciones (servicios y/o productos de los sistemas de información), de los organismos sujetos a control, con al finalidad de evaluar la eficacia y eficiencia administrativa técnica y/u operacional de los organismos, de acuerdo con los principios, normas, técnicas y procedimientos normalmente aceptados. Así mismo de los sistemas (planes, programas y presupuestos, diseño, software, hardware, seguridad, respaldos y otros) adoptados por la organización.

Existe otra definición sobre el "control técnico" en materia de sistemas de información, y esta se orienta a la revisión del diseño de los planes, diseños de los sistemas, la demostración de su eficacia, pruebas de productividad de la gestión, el análisis de resultados, niveles y medios de seguridad, respaldo, y el almacenamiento. Así mismo medición de la vida útil del sistema de información adoptado por la organización bajo control.

D. **Objetivos de la Consultoría y Control de Sistemas de Información.**-Los principales objetivos que constituyen a la consultoría informática son:

1. El control de la función informática Sistema de Información y la Tecnología de la Información.
2. El análisis de la eficiencia de los sistemas de información y la tecnología de información.
3. La verificación del cumplimiento de las normas generales de la organización.
4. La verificación de los planes, programas y presupuestos de los sistemas de información.

5. La revisión de la eficaz gestión de los recursos materiales y humanos.
6. La revisión y verificación de controles técnicos generales y específicos de operatividad.
7. La revisión y verificación de las seguridades.
8. Del cumplimiento de normas y estándares.
9. De la seguridad del software.
10. De la seguridad de las comunicaciones.
11. De seguridad de la base de datos.
12. De seguridad del proceso.
13. De la seguridad de las aplicaciones.
14. De seguridad física.
15. De suministros y reposiciones.
16. De contingencias.
17. El análisis del control de resultados.
18. El análisis de verificación y de exposición de debilidades.

E. **El consultor en seguridad de información.-** Es el profesional que ha de cuidar y velar por la correcta utilización de los diversos recursos de la organización y debe comprobar que se este llevando acabo una eficiente y eficaz gestión de los sistemas de información y de la Tecnología de la Información.

Cuando se aplica la consultoría y control de los sistemas de información. Nos encontramos que en ella nos da "indicios, anomalías y síntomas" que nos permiten percibir que la organización bajo control presenta problemas de resultados como de eficacia y eficiencia en los sistemas de información.

## VI. PROCEDIMIENTOS

Para hacer una adecuada planeación de la consultoría en seguridad de información, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro de la organización, sus sistemas, organización y equipo.

En el caso de la consultoría en seguridad de información, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de los dos objetivos:

1. Evaluación de los sistemas y procedimientos.
2. Evaluación de los equipos de cómputo.

Para hacer una planeación eficaz, lo primero que se requiere es obtener información general sobre la organización y sobre la función de seguridad de información a evaluar. Para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajo, el cual deberá incluir tiempo, costo, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la misma.

### A. Investigación preliminar.

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

**B. Administración.**

- Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.
- Para analizar y dimensionar la estructura por auditar se debe solicitar a nivel del área de seguridad de información
- Objetivos a corto y largo plazo.
- Recursos materiales y técnicos
- Solicitar documentos sobre los equipos, número de ellos, localización y características.
- Estudios de viabilidad.
- Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)
- Fechas de instalación de los equipos y planes de instalación.
- Contratos vigentes de compra, renta y servicio de mantenimiento.
- Contratos de seguros.
- Convenios que se tienen con otras instalaciones.
- Configuración de los equipos y capacidades actuales y máximas.
- Planes de expansión.
- Ubicación general de los equipos.
- Políticas de operación.
- Políticas de uso de los equipos.

**C. Sistemas.**

- Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.
- Manual de formas.
- Manual de procedimientos de los sistemas.
- Descripción genérica.
- Diagramas de entrada, archivos, salida.
- Salidas.
- Fecha de instalación de los sistemas.
- Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la consultoría o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

- Se solicita la información y se ve que:
- No tiene y se necesita.
- No se tiene y no se necesita.
- Se tiene la información pero:
- No se usa.
- Es incompleta.
- No esta actualizada.
- No es la adecuada.
- Se usa, está actualizada, es la adecuada y está completa.

En el caso de no se tiene y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de no se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En

caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

- Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)
- Investigar las causas, no los efectos.
- Atender razones, no excusas.
- No confiar en la memoria, preguntar constantemente.
- Criticar objetivamente y a fondo todos los informes y los datos recabados.

**D. Personal participante.**

Una de las partes más importantes dentro de la planeación de la consultoría en seguridad de información es el personal que deberá participar y sus características.

Uno de los esquemas generalmente aceptados para tener un adecuado control es que el personal que intervenga esté debidamente capacitado, con alto sentido de moralidad, al cual se le exija la optimización de recursos (eficiencia) y se le retribuya o compense justamente por su trabajo.

Con estas bases se debe considerar las características de conocimientos, práctica profesional y capacitación que debe tener el personal que intervendrá en la consultoría. En primer lugar se debe pensar que hay personal asignado por la organización, con el suficiente nivel para poder coordinar el desarrollo de la consultoría,

proporcionar toda la información que se solicite y programar las reuniones y entrevistas requeridas.

Éste es un punto muy importante ya que, de no tener el apoyo de la alta dirección, ni contar con un grupo multidisciplinario en el cual estén presentes una o varias personas del área a auditar, sería casi imposible obtener información en el momento y con las características deseadas.

También se debe contar con personas asignadas por los usuarios para que en el momento que se solicite información o bien se efectúe alguna entrevista de comprobación de hipótesis, nos proporcionen aquello que se esta solicitando, y complementen el grupo multidisciplinario, ya que se debe analizar no sólo el punto de vista de la dirección de seguridad de información, sino también el del usuario del sistema.

Para completar el grupo, como colaboradores directos en la realización de la consultoría se deben tener personas con las siguientes características: .

Técnico en seguridad de información.

Experiencia en el área de seguridad de información.

Experiencia en operación y análisis de sistemas.

Conocimientos de los sistemas más importantes.

En caso de sistemas complejos se deberá contar con personal con conocimientos y experiencia en áreas específicas como bases de datos, redes, etc. Lo anterior no significa que una sola persona tenga los conocimientos y experiencias señaladas, pero si deben intervenir una o varias personas con las características apuntadas.

## E. Pasos a seguir.

Se requieren varios pasos para realizar una consultoría. El consultor de sistemas debe evaluar los riesgos globales y luego desarrollar un programa de consultoría que consta de objetivos de control y procedimientos de consultoría que deben satisfacer esos objetivos. El proceso de consultoría exige que el consultor de sistemas reúna evidencia, evalúe fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y que prepare un informe de consultoría que presente esos temas en forma objetiva a la gerencia. Asimismo, la gerencia de consultoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de consultoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.

## F. Informe.

En si todos los encuestados respondieron la totalidad de las preguntas. Todos tienen las mismas respuestas, todos dicen prácticamente lo mismo acerca de lo que es la consultoría de sistemas en que es un sistema de revisión, evaluación, verificación y evalúa la eficiencia y eficacia con que se está operando los sistemas y corregir los errores de dicho sistema. Todos los encuestados mostraron una características muy similares de las personas que van a realizan la consultoría; debe haber un contador, un ingeniero de sistemas, un técnico y que debe tener conocimientos, práctica profesional y capacitación para poder realizar la consultoría.

Todos los encuestados conocen los mismos tipos de consultoría, económica, sistemas, fiscal, administrativa.

Para los encuestados el principal objetivo de la consultoría de sistemas es asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.

Mirando en general a todos los encuestados se puede ver que para ellos la consultoría de sistemas es muy importante porque en los sistemas esta toda la información de la empresa y del buen funcionamiento de esta depende gran parte del funcionamiento de una empresa y que no solo se debe comprender los equipos de computo sino también todos los sistemas de información desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La consultoría de los sistemas de seguridad de información es de mucha importancia ya que para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad.

# VII. ISO 17799

La implementación puede tomar de 6 meses a 2 años, dependiendo del tamaño, alcance y complejidad de su organización.

## A. Implementación del ISO 17799

La implementación de un sistema de gestión de cualquier tipo es un compromiso significativo para una organización que busca mejoras en su negocio.

Sin embargo, una buena planeación y el apoyo de la alta dirección pueden ayudar significativamente en el proceso. La buena planeación comienza con leer la norma para tener un buen entendimiento de como funciona. Una vez que tiene una copia en mano y entiende como funciona, se puede empezar el proceso de implementación.

Los pasos para implementar un Programa de Seguridad de la Información basado en el ISO 17799 vienen a continuación:

1. Obtener el apoyo de la alta dirección
2. Determinar el alcance del programa de seguridad de la información
3. Crear una organización de seguridad de la información

4. Identificar los dominios de seguridad
5. Evaluar el riesgo
6. Mitigar el riesgo
7. Consultar

Sistema de Gestión de Seguridad de la Información Una explicación de los pasos que se tienen que tomar para implementar el ISO 17799:

**Paso 1:** Obtener el apoyo de la alta dirección

obtener el apoyo de la alta dirección es el componente más crucial para el éxito de un Programa de Seguridad de la Información ISO 17799.

Puede ser difícil y tener inconvenientes con las políticas de la empresa, aunque una exitosa implementación de ISO 17799 hará que la seguridad se incorpore a la organización siendo orientada desde la alta dirección.

**Paso 2:** Determinar el alcance del programa de seguridad de la información

Una de las tareas iníciales más difíciles es definir el alcance del programa de seguridad de la Información. Esto lo define cada organización, dependiendo si el programa es centralizado por la casa matriz de cada empresa o se hará independientemente en cada sucursal de la empresa.

• ¿El Programa de seguridad de la información gobierna toda la organización, siendo éste propiedad de un oficial principal de seguridad de información (CISO[1])?

• ¿Tiene cada subsidiaria de su empresa un programa de seguridad de la información, propiedad de un oficial de la seguridad de la información autónomo (ISO information security officer)? existen razones válidas para ambos casos. Una planeación cuidadosa preparará una implementación exitosa a medida que va avanzando en el trabajo.

**Paso 3:** Crear una organización de seguridad de la información.

La creación de una organización de seguridad de la información está basada en el alcance identificado en el paso 2. Roles, responsabilidades y autorizaciones, se encuentran ahora identificados y los comités establecidos. Esto determina el establecimiento de la creación de un sistema de gestión de la seguridad de la información (information security management system isms). La organización ahora sabe "quién hace qué", y "quién tiene la autorización" en cada nivel.

**Paso 4:** Identificar los dominios de seguridad

Un dominio de seguridad es una entidad conceptual definida por parámetros de seguridad físicos y lógicos. Los parámetros definen el espacio de control. Los dominios de seguridad sirven como la base para la evaluación de riesgo. Estos pueden incluir centros de llamadas, áreas públicas, oficinas sucursales, centros de datos,

[1] Chief Information Security Officer

bodegas, centros de producción y cubículos como espacios de trabajo.

**Pasó 5:** Evaluación de Riesgos

El ISO 17799 está basado en la gestión de riesgo, y es la razón por la que se integra bien dentro de la estrategia de toda la gestión de riesgo de una organización. El ISO 17799 sólo sugiere una evaluación metódica del riesgo de seguridad, dejando el tipo y el nivel de evaluación abierto a la interpretación que una organización escoge llevar a cabo. El resultado deseado es una manera de cuantificar el riesgo para poder seleccionar controles apropiados y pertinentes del ISO 17799 requeridos para mitigar el riesgo. El BS[2] 7799-2:2002 requiere de un acercamiento sistemático para la evaluación de riesgo, incluyendo el desarrollo de un plan de tratamiento de riesgo para:

- Relacionar el riesgo a la confidencialidad, integridad y disponibilidad.
- Establecer objetivos para reducir el riesgo a un nivel aceptable.
- Determinar el criterio para aceptar el riesgo.
- Evaluar las opciones de tratamiento de riesgos.

**Pasó 6:** Mitigar el Riesgo.

Los controles de seguridad mitigan el riesgo identificado en el Paso 5. Estos son una combinación de personas, procesos y herramientas. Los controles de seguridad son identificados basados en los riesgos identificados en la evaluación. Una vez que son identificados, 10 áreas

[2] Brtisch Standard

de control de seguridad que encierran 36 objetivos de control actúan como guías para escoger sistemáticamente de una lista de 127 controles existentes de acuerdo a las necesidades de una organización. Las elecciones deben tomar en cuenta la consolidación para el ISMS y la relación de conocimientos apropiados del programa. La organización también debe tener una combinación de procesos establecida para la implementación del plan de tratamiento de riesgo y el sistema de controles seleccionados. Los controles existentes escogidos son implementados para cubrir los requisitos de control.

Los controles seleccionados pueden incluir:

- Organizacionales: Foros, comités, papeles de la dirección y del personal.
- Físicos: Portones, paredes y cercas para administrar la continuidad del negocio.
- Técnicos: "firewalls" o software antivirus para el control del acceso, desarrollo y el mantenimiento de los sistemas.
- Procedimientos: Procedimientos normales de operación, formas, políticas de seguridad y comunicaciones.
- Gobierno: Los registros, reportes y clasificaciones de activos.
- Acatamiento: Legales y contractuales.

La justificación de los controles está basada en los objetivos de control derivados del riesgo. La prioridad del despliegue es basada en la clasificación o valor de cada riesgo.

**Pasó 7:** Consultoría

La evaluación del ISO 17799 puede tomar dos formas:

1. Un programa de seguridad de la información puede ser "Gap Analized[3]".

• La intención sería determinar si las áreas de control de seguridad han sido evaluadas y/o tratadas para su conformidad.

2. Un programa de seguridad de la información puede ser "analizado para su conformidad".

• La intención sería determinar si la organización está en conformidad con sus propias "políticas".

Las consultorías pueden ser:

- Ellos mismos – una organización lleva a cabo su propia consultoría.
- Segundos – un cliente o socio lleva a cabo la consultoría.
- Terceros – un auditor independiente (ó casa certificadora) lleva a cabo la auditaría.

Se requiere de una auditaría por un tercero para la certificación y tiene el peso de haber sido dirigida independientemente. Sus clientes/reguladores pueden, por lo tanto, confiar en esta certificación independiente que es una indicación verdadera del cumplimiento del sistema de gestión. Desde los sucesos del once de septiembre, la expansión del comercio electrónico y la progresiva competencia corporativa, la protección de los activos de una organización preocupa cada vez más a las empresas. La seguridad de la información es una medida para incrementar el éxito de

[3] Analizador de brechas

sus negocios. El implementar un sistema de gestión de la seguridad de la información, tal como el ISO 17799, puede ayudar a que una organización cumpla favorablemente los incentivos de mercadotecnia, los financieros y las preocupaciones de empeño para ayudar a lograr oportunidades de crecimiento.

Asimismo, la creciente demanda de seguridad de la información está siendo estimulada por reglamentos, tales como el HIPAA[4] Sarbanes-Oxley, y el GLBA[5] 1999. El ISO 17799 proporciona un esqueleto para el sistema de gestión de la seguridad de la información de forma tal que se puede aplicar a cualquier requisito de seguridad de la Información, y debe ser ajustable a futuros reglamentos y requisitos.

Los pasos arriba delineados detallan el mayor esfuerzo requerido para proteger totalmente los activos clave de una organización a corto y largo plazo.

[4] Health Insurance Portability and Accountability Act de 1996
[5] Gramm-Leach-Bliley Act

## VIII. ANÁLISIS DE AMENAZAS

Amenaza es una condición que puede atentar contra el entorno del sistema de información (persona, máquina, suceso o idea) que, dada una oportunidad, podría dar lugar a que se produjese una violación de la seguridad (confidencialidad, integridad, disponibilidad o uso legítimo).

Una vez realizado y establecida la política de seguridad y el análisis de riesgos se habrán identificado las amenazas que han de ser contrarrestadas, dependen del diseñador del sistema de seguridad especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad en una red pueden caracterizarse modelando el sistema como un flujo de información desde una fuente.

Las cuatro categorías generales de amenazas o ataques son las siguientes:

A. **Interrupción:** un recurso del sistema es destruido o se vuelve no disponible. Este es un ataque contra la disponibilidad.

   Ejemplo de este ataque son la destrucción de un elemento hardware, como un disco duro, cortar una línea de comunicación o deshabilitar el sistema de gestión de ficheros.

B. **Intercepción:** una entidad no autorizada consigue acceso a un recurso. Este es un ataque contra la confidencialidad.

Ejemplo de este ataque interceptar una línea para capturar datos que circulen por la red y la copia ilícita de ficheros o programas (intercepción de datos).

C. **Modificación:** una entidad no autorizada no sólo consigue acceder a un recurso, sino que es capaz de manipularlo. Este es un ataque contra la integridad.

   Ejemplos de este ataque es el cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente y modificar el contenido de mensajes que están siendo transferidos por la red.

D. **Fabricación:** una entidad no autorizada inserta objetos falsificados en el sistema. Este es un ataque contra la autenticidad.

   Ejemplos de este ataque son la inserción de mensajes en una red o añadir registros a un archivo.

# IX. ATAQUES PASIVOS

En los ataques pasivos el atacante no altera la comunicación, sino que únicamente la escucha o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico, una técnica más sutil para obtener información de la comunicación, que puede consistir en:

A. **Obtención del origen y destinatario** de la comunicación, leyendo las cabeceras de los paquetes monitorizados.

B. **Control del volumen de tráfico** intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

C. **Control de las horas habituales** de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Los ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos. Sin embargo, es posible evitar su éxito mediante el cifrado de la información y otros mecanismos que se verán más adelante.

# X. ATAQUES ACTIVOS

Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos, pudiendo subdividirse en cuatro categorías:

A. **Suplantación de identidad**: el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo. Por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios, como al robar la contraseña de acceso a una cuenta.

B. **Reactuación:** uno o varios mensajes legítimos son capturados y repetidos para producir un efecto no deseado, como por ejemplo ingresar dinero repetidas veces en una cuenta dada.

C. **Modificación de mensajes:** una porción del mensaje legítimo es alterada, o los mensajes son retardados o reordenados, para producir un efecto no autorizado. Por ejemplo, el mensaje "Ingresa un millón de pesos en la cuenta A" podría ser modificado para decir "Ingresa un millón de pesos en la cuenta B".

## XI. ANÁLISIS COSTO-BENEFICIO

Este estudio se realiza considerando el costo que se presenta cuando se pierde la información vs el costo de un sistema de seguridad.
Para realizar este estudio se debe considerar lo siguiente:

Clasificar la instalación en términos de riesgo (alto, mediano, pequeño)
Identificar las aplicaciones que tengan alto riesgo.
Cuantificar el impacto en el caso de suspensión del servicio aquellas aplicaciones con un alto riesgo.
Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
La justificación del costo de implantar las medidas de seguridad.

### A. Costo x pérdida

Se deben clasificar las áreas de riesgo, que pueden ser:

1. Riesgo Computacional

   Se debe evaluar las aplicaciones y la dependencia del sistema de información, para lo cual es importante considerar responder las siguientes cuatro preguntas:

   ¿Qué sucedería si no se puede utilizar el sistema? Si el sistema depende de la aplicación por completo se debe definir el nivel de riesgo.
   ¿Qué consecuencias traería si es que no se pudiera acceder al sistema? Al considerar esta pregunta se debe cuidar la

presencia de manuales de respaldo para emergencias o algún modo de cómo se solucionó este problema en el pasado

¿Existe un procedimiento alternativo y que problemas ocasionaría? Se debe verificar si el sistema es único o es que existe otro sistema también computarizado de apoyo menor.

¿Qué se ha hecho en casos de emergencia hasta ahora? Se debe verificar si el sistema es único o es que existe otro sistema también computarizado de apoyo menor.

Que exista un sistema paralelo al menos manual

Si hay sistemas duplicados en las áreas críticas (tarjetas de red, teclados, monitores, servidores, unidades de disco, aire acondicionado).

Si hay sistemas de energía ininterrumpida UPS.

Si las instalaciones eléctricas, telefónicas y de red son adecuadas (se debe contar con el criterio de un experto).

Si se cuenta con un método de respaldo y su manual administrativo.

Cuando se ha definido el grado de riesgo se debe elaborar una lista de los sistemas con las medidas preventivas que se deben tomar y las correctivas en casi de desastre, señalando la prioridad de cada uno. Con el objetivo que en caso de desastres se trabajen los sistemas de acuerdo a sus prioridades.

**B. Consideración y Cuantificación del Riesgo a Nivel Institucional.**

Ahora que se han establecido los riesgos dentro la organización, se debe evaluar su impacto a nivel institucional, para lo cual se debe:

Clasificar la información y los programas de soporte en cuanto a su disponibilidad y recuperación.

Identificar la información que tenga un alto costo financiero en caso de perdida o pueda tener impacto a nivel ejecutivo o gerencial.

Determinar la información que tenga un papel de prioridad en la organización a tal punto que no pueda sobrevivir sin ella.

Una vez determinada esta información se debe cuantificar, para lo cual se debe efectuar entrevistas con los altos niveles administrativos que sean afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que podrían causar estas situaciones.

Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:

- Interceptación de las comunicaciones.
- Acceso no autorizado a ordenadores o Redes de ordenadores
- Perturbación de las redes.
- Ejecución de programas que modifiquen o dañen los datos.
- Declaración falsa.
- Accidentes no provocados.
- Robo de datos.
- Infiltración de datos críticos.

## C. REPORTES

Para la realización y entrega del reporte final se debe tener en cuenta la norma 060.020 (evidencia) establece que durante el curso de una consultoría, el auditor de sistemas de información debe obtener evidencia suficiente, confiable, relevante y útil para lograr los objetivos. Los resultados y conclusiones de la consultoría deben

estar apoyados por un apropiado análisis e interpretación de esta evidencia".

## D. Tipos de evidencia

Cuando se planifica el trabajo de consultoría de sistemas de información, el consultor del sistema de información debe tomar en cuenta el tipo de evidencia a obtener y sus niveles variables de confiabilidad. Por ejemplo, evidencia de consultoría obtenida de una parte independiente, es por lo general más confiable que la evidencia proporcionada por la organización que está siendo consultada. La evidencia física de consultoría es por lo general más confiable que las representaciones de un individuo. Los distintos tipos de evidencia de consultoría que el consultor de sistema de información debe considerar son:

- Evidencia física de consultoría
- Evidencia documentada de consultoría
- Representaciones y análisis.

La evidencia física de consultoría puede incluir observación de actividades, propiedad y funciones de los sistemas de información, tales como: Un inventario de medios magnéticos en una bodega externa; o un sistema de seguridad residente en un computador que esté en operación.

La evidencia documentada de consultoría puede incluir: resultado de datos extraídos; registro de transacciones programas registrados

facturas; y control de registro representación de aquellas consultorías que han sido o pueden ser evidencia documentada como: Políticas y procedimientos escritos y declaración oral y escrita Los resultados del análisis de la información a través de comparaciones, cálculos e índices pueden también ser usados como evidencia de consultoría. Disponibilidad y evidencia de consultoría El consultor de sistemas de información debe considerar el tiempo durante el cual la información existe o está disponible para determinar la naturaleza, período y extensión de las pruebas sustantivas, y si es aplicable, la prueba de cumplimiento. Por ejemplo la eficiencia de la consultoría procesada por EDI[6] y DIP[7] pueden no ser recuperables después de un período específico de tiempo si los archivos se cambian o no se respaldan. Selección de evidencia de consultoría El consultor de sistemas de información debe planificar el uso de la mejor evidencia de consultoría que sea consistente con la importancia del objetivo de la consultoría y el tiempo y esfuerzo involucrado en obtener tal evidencia.

Donde la evidencia de consultoría obtenida en la forma de representaciones orales es crítica para la opinión o conclusión de consultoría, el consultor de sistemas de información debe obtener confirmación escrita de las afirmaciones. Por ejemplo, donde la única evidencia de consultoría de que los reportes de excepción se siguen es lo que dice la administración, este es el caso en que estas afirmaciones deben obtenerse por escrito.

[6] Intercambio Electrónico de Datos
[7] Procesamiento de imágenes en documentos

La evidencia de consultoría debe ser suficiente para formarse una opinión o apoyar los resultados y conclusiones del consultor. Si, en el juicio del consultor, la evidencia de consultoría no es suficiente para apoyar resultados y conclusiones, el consultor de sistemas de información debe obtener evidencia de consultoría adicional. Por ejemplo un listado de programa puede no ser suficiente evidencia de consultoría hasta que se obtenga evidencia adicional para verificar que ésta representa el programa que actualmente se utiliza en el proceso de producción. Obtención de la evidencia de consultoría Los procedimientos utilizados para obtener evidencia de consultoría varían de acuerdo al sistema de información que está siendo consultada. El consultor de sistema de información debe seleccionar el procedimiento más apropiado para el objetivo de la consultoría. Deben considerarse los siguientes procedimientos: Consultas Observaciones Inspección Confirmación; y Reejecución Los procedimientos anteriores pueden aplicarse por medio del uso de procedimientos de consultoría manual, técnicas de consultoría asistida por computador, o una combinación de ambos, por ejemplo: Un sistema que utiliza totales de controles manuales para balancear las operaciones de ingreso de datos puede proveer evidencia de consultoría de que el procedimiento de control asegura una apropiada conciliación y registro en un reporte. El consultor del sistema de información debe obtener esta evidencia de consultoría revisando y probando este reporte; Registros de transacciones detallados pueden estar disponibles solamente en un formato legible para la máquina. Lo que requiere el consultor de

sistema de información es obtener evidencia de la consultoría utilizando técnicas de consultoría asistidas por computador.

El consultor de sistemas de información debe efectuar esta revisión general del sistema de información o del sistema como un todo en la medida que sea suficiente, en conjunto con las conclusiones derivadas de las otras evidencias de consultoría obtenidas, para proveer una base razonable de las conclusiones resultantes. Documentación de consultoría La evidencia de auditaría obtenida por el auditor SI debe estar apropiadamente documentada y organizada para apoyar los resultados y conclusiones del consultor de sistemas de información.

En aquellas situaciones donde el consultor de sistemas de información crea que no es posible obtener suficiente evidencia de la consultoría, debe registrar este hecho en una manera consistente con la comunicación de los resultados de consultoría en un reporte en calidad de restricción al alcance (limitación).

# XII. ENTORNO DE CONSULTORÍA

La organización sobre la cual se va a implementar la consultoría es La cadena de Hoteles Royal, sobre la cual de ahora en adelante y durante el desarrollo de todo el proyecto nos vamos a referir como la cadena de Hoteles, ya que debido razones de seguridad y aspectos legales no fue permitido el uso de la razón social ni de ningún logo. La cadena esta constituida por 8 hoteles de los cuales 6 se encuentran en la ciudad de Bogotá y los otros dos en Cali y Medellín.

La red se encuentra segmentada en 1 subred por cada hotel por medio de unos Enrutadores cisco 2800 las redes se encuentran interconectadas con la central de la cadena, en donde se encuentran todos los servidores de aplicación, bases de datos, servicios de correo, Proxy, firewall, salida de Internet. Por lo anterior los equipos que se encuentran en cada uno de los diferentes hoteles son los servidores de archivos de interfaces que se en cargan de recibir la información de la planta telefónica y tarificar las llamadas que se hacen en las habitaciones y los cargos realizados en el restaurante, bar. Y diferentes ambientes que hay en los hoteles, y enviarlos por medio de la interface al sistema de información llamado Opera, software que se implemento a principios de este año y fue desarrollado por la empresa Micros Fidelio Argentina. El sistema se encuentra implementado en 2 servidores con 2 procesadores Xeon de 3.66 GHz y 5 GB de memoria cada uno, las bases de datos están montadas sobre una plataforma Oracle, y 3 servidores de aplicación con la misma configuración que los anteriores, la plataforma cuenta con sistema de distribución de cargas que

se encarga de repartir entre los 3 servidores de aplicación, a todos los usuarios que se vayan autenticando, con el fin de no sobrecargar ninguno de los servidores y mejorar los tiempos de respuesta.

Los dos servidores de base de datos cuentan con un sistema de espejos que se encarga de copiar las modificaciones que se hacen de una de las bases de datos a la otra, y axial permitir el acceso a las dos al tiempo y a la misma información sin tener inconvenientes.

El sistema de información Opera se encarga de manejar toda la gestión hoteleramente hablando, es decir registro de huéspedes, manejo de cuentas, ocupación, estadísticas, eventos, etc. Pero igualmente el resto de las áreas operacionales cuentan con otros sistemas, por ejemplo el Área de compras e inventarios maneja un software llamado TCR, que igualmente esta contenido tanto las bases de datos como las aplicaciones en un servidor de la central independiente a los servidores de Opera. La Gestión financiera se maneja por medio de un software llamado Uno Enterprise igualmente centralizado como los anteriores.

La muestra cuantitativamente hablando que va a ser tenida en cuenta es muy pequeña debido al tiempo de las personas que se debían entrevistar y a la disponibilidad de las mismas, pero cualitativamente es inmensa ya que las personas que van a ser entrevistadas son el Gerente de información y tecnología y el jefe de operación de Informática y Tecnología, quienes son personas de alta importancia para la organización.

# XIII. PLAN DE CONTINGENCIA

## A. OBJETIVO

Formular un adecuado Plan de Contingencias, que permita la continuidad en los procedimientos informáticos, así como enfrentarnos a fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores pérdidas posibles en forma rápida, eficiente y oportuna; buscando la mejora de la calidad en los servicios que brinda el grupo de IT

## B. PLAN DE SEGURIDAD

### Formulación del Procedimiento de Recuperación de Fallas y/o Desastres

Es importante definir los procedimientos y acciones a seguir antes, durante y después de la ocurrencia de la falla, siniestro o desastre dentro de la organización a fin de recuperar la total o mayor parte de información, archivos y equipos informáticos, evitando así la pérdida de tiempo y dinero. Las actividades a realizar en el Procedimiento de Recuperación de fallas y/o desastres se pueden clasificar en tres etapas:

- Actividades previas a la contingencia.
- Actividades durante la contingencia.
- Actividades después de la contingencia

## C. ACTIVIDADES PREVIAS A LA CONTINGENCIA

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de protección de la

información y equipos informáticos, que nos aseguren el proceso de recuperación de los mismos

**Establecimiento de un Procedimiento.**

En esta fase de Planeamiento se debe de establecer los procedimientos relacionados con:

**Sistemas de Información:** La organización deberá tener un inventario de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional. La relación de Sistemas de Información deberá detallar los siguientes datos:

- Nombre del Sistema.
- Lenguaje o Paquete con el que fue creado el Sistema, programas que lo conforman tanto programas fuentes como programas objetos, rutinas, macros, etc.
- Las unidades que usan la información del Sistema.
- El volumen de los archivos que trabaja el Sistema.
- El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
- El equipamiento necesario para un manejo óptimo del Sistema.
- La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.

**Equipos de Cómputo:** Se tendrá en cuenta:

- Inventario actualizado de los equipos

- Pólizas de Seguros Comerciales.

## D. Obtención y Almacenamiento de los Respaldos de Información (BACKUPS)

- Backups del Sistema Operativo
- Backups del Software Base
- Backups del Software Aplicativo
- Backups de los Datos

Los funcionarios del la organización, deben realizar su propia copia de la información en la carpeta de seguridad que le fue asignada, este procedimiento se debe hacer usualmente el último día hábil de cada mes.

**Políticas (Normas y Procedimientos de Backups):** Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente.

- Respaldo de Información de movimiento entre los períodos que no se cuenta con Backups (backups increméntales).
- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiable.

## XIV. ACTIVIDADES DURANTE EL DESASTRE

Una vez presentada la Contingencia, se deberá ejecutar las siguientes actividades:

### Plan de Emergencias

Este procedimiento deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre la contingencia.

Si bien es cierto la integridad de las personas es lo primordial, se deben adoptar medidas con el fin de asegurar la información:

### Si hay riesgo de daño en el equipo de computo

- Apagar los equipos inmediatamente después de haber detectado el siniestro.
- Desconexión del equipo para su retiro del lugar del siniestro.
- Alejarse rápidamente del mismo.
- Informar si es posible al área de IT.
- De ser necesario y sin esperar la intervención de un ingeniero de sistemas usar extintores.

### Entrenamiento

El personal del la organización debe tomar conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y ello, demanda actuar con seriedad y responsabilidad para esto y dadas las capacitaciones que se dan en la organización relacionadas con

seguridad industrial prevención y manejo de siniestros, es conveniente que todos los funcionarios participen de estas actividades.

## XV. ACTIVIDAD DESPUÉS DE LA CONTINGENCIA

**Evaluación de Daños.**
Inmediatamente después que la contingencia ha terminado, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

**Priorización de actividades del Procedimiento.**
La evaluación de daños reales y su comparación contra el procedimiento, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en pro de las actividades urgentes.

**Ejecución de Actividades.**
La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el procedimiento de acción.

## XVI. EVALUACIÓN DE RESULTADOS

Una vez concluidas las labores de Recuperación del los Sistemas que fueron afectados por la contingencia, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, como se comportaron los equipos de trabajo, etc.

**Retroalimentación del Procedimiento**
Con la evaluación de resultados, debemos de optimizar el procedimiento original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro punto a evaluar es de cual hubiera sido el caso de no haber tenido en la organización el Plan de Contingencia.

## XVII. SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información (conjunto de datos y/o documentos) registrada, procesada, almacenada, compartida, transmitida o recuperada se rige por los siguientes aspectos:

- El usuario de la información debe negar el acceso a la información a aquellas personas que no tengan derecho.
- Garantizar el acceso a la información de las personas que si deben tener acceso Jefes superiores y responsables de la seguridad de la información

**Acceso no Autorizado**
Sin adecuadas medidas de seguridad se puede producir accesos no autorizados a:

- Control de acceso a servidor de bases de datos y servidor de dominios

- Computadores personales y/o terminales de la red.
- Información confidencial.

**Control de Acceso a Servidor de bases de datos y servidor de Dominios**

- El acceso al área de Informática estará restringido
- Sólo ingresa al área el personal que trabaja en la misma.
- El ingreso de personas extrañas solo podrá ser bajo una autorización del responsable del área.
- Siempre esta área deberá permanecer cerrada, limpia y organizada.
- Las visitas al centro de computo por personas ajenas a la entidad, podrán hacerlo solo con autorización e identificación personal y solo para realizar labores del área.
- Esta área deberá recibir aseo y mantenimiento por lo menos una vez cada mes.

**Acceso Limitado a las terminales**

Cualquier terminal que puede ser utilizado debe ser encerrado en un área segura, de tal manera que no sean usados, excepto por aquellos que tengan la autorización

**Restricciones que pueden ser aplicadas:**

- Determinación de los períodos de tiempo para los usuarios o las terminales.
- Asignación del usuario por terminal o del terminal por usuario.
- Limitación del uso de programas para usuario o terminales.
- Límite de reconocimientos para la verificación del usuario.
- Tiempo de validez de las contraseñas.

- Uso de contraseñas, cuando un terminal no sea usado pasado un tiempo predeterminado (Bloqueos de 5 - 10 minutos).

## XVIII. NIVELES DE ACCESO

**Nivel de consulta de la información:** Solo lectura.
**Nivel de mantenimiento de la información:** Administración de Bases de Datos.
**Ingreso:** Insertar datos nuevos sin modificar los existentes.
**Actualización:** Modificar la información sin eliminar datos.
**Borrado:** Se divide en dos clases de acuerdo a la clase se información manejada Lógico y Físico.

## XIX. MEDIDAS PREVENTIVAS ANTE AMENAZAS

### Extinguidores Manuales

Todo el personal designado para usar extinguidores de fuego debe ser entrenado en su uso,

Colocando adecuadas cubiertas plásticas para todo el equipo, escritorios, puede ayudar a reducir el daño ocasionado por el humo y/o agua.

Cuando no se cuenta con sistemas automáticos contra incendio y se vea o perciba señales de fuego, entonces se debe actuar con rapidez para poder apagar el incendio

**Instalaciones Eléctricas**
Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones y la información podría quedar temporalmente fuera de servicio

En nuestro medio se han podido identificar tres problemas de energía más frecuente:

- Fallas de energía.
- Bajo y alto voltaje.
- Variación de frecuencia.
-

Existen dispositivos que protegen de estas consecuencias negativas:

- Estabilizadores
- Sistemas de alimentación ininterrumpida (SAI o UPS: UNINTERRRUPTIBLE POWER SISTEM)

## XX. COMO PREVER LAS FALLAS QUE GENERAN ALTAS TEMPERATURAS

**Polos a tierra**
En la actualidad la organización, cuenta con este sistema por lo que sólo se ha considerado un mantenimiento preventivo de una vez al año, con el fin de comprobar la resistencia y las conexiones.

**Fusibles**
Si una parte de un computador funde un fusible se debe desconectar el equipo.

A continuación debe desconectarse el cable de poder que lleva al equipo y buscar la falla que ha hecho saltar el fusible.

**Extensiones Eléctricas y capacidades**

- Las extensiones eléctricas deben estar fuera de las zonas de paso.
- Se debe utilizar canaletas adecuadas para cubrir los cables.
- Tanto los tomas de corriente como las extensiones eléctricas deben tener polo a tierra.

**Garantizar el Suministro Eléctrico**

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, los computadores, monitores, las impresoras y los demás periféricos.

Un corte de la alimentación de la unidad principal puede:

Hacer que desaparezca la información que hay en la memoria.

Se interrumpe el proceso de escritura en el disco.

Se puede perder información de importancia que necesita el sistema operativo

Interrumpir impresión.

Se interrumpen las comunicaciones.

El sistema queda expuesto a picos y subidas de tensión.

Normalmente se desconectan los equipos cuando se va la corriente, pero esto no siempre es posible.

**UPS o SAI. (SISTEMA DE ENERGIA ININTERRUMPIBLE)**

La UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico, es energía de seguridad para un sistema de computación,

## XXI. ANTE ACCIONES HOSTILES

**El Robo**

Mantener el servidor y los equipos en el data center hay que asegurarse de que se refrigere adecuadamente.

Asegurarse que el personal es de confianza, competente y conoce los procedimientos de seguridad.

Registrar cada salida y entrada de equipos de cómputo de la organización.

**El Sabotaje**

El peligro más temido por los centros de computo es el sabotaje.

La protección contra el sabotaje requiere:

- Una selección rigurosa del personal.
- Buena administración de los recursos humanos.
- Buenos controles administrativos.
- Buena seguridad física en los lugares donde están los principales componentes del equipo.
- Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

No existe un plan o una recomendación simple para resolver el problema de la seguridad. Algunas medidas que se deben tener muy en cuenta para tratar de evitar las acciones hostiles son:

- Mantener adecuados archivos de reserva (backups).

- No confiarse en los vigilantes externos a la entidad.
- Identificar y establecer operaciones criticas cuando se planea el respaldo de los servicios y la recuperación de otras actividades.
- Montar procedimientos para remitir registros de almacenamiento de archivos y recuperarlos.

## XXII. MEDIDAS DE PRECUACION Y RECOMENDACIÓN

**En Relación al Centro de Cómputo**

Se deben evitar, las grandes ventanas, las cuales además de que permiten la entrada del sol y calor, que son inconvenientes para los equipos pueden ser un riesgo para la seguridad de los mismos.

Se debe tener cuidado que en la oficinas no existan materiales que sean inflamables.

El acceso al centro de computo debe estar restringido al personal no autorizado.

El acceso a los archivos de información contenidos en los equipos, debe estar controlado mediante la verificación de la identidad de los usuarios autorizados.

Asignar a una sola persona la responsabilidad de la protección de los equipos en cada área.

## XXIII. SEGURIDAD EN REDES

### A. Problemas Básicos

**El observador.**

El observador es uno de los principales problemas de seguridad y uno de los problemas más urgentes de cualquier red.

Si un intruso es paciente, él puede simplemente mirar los paquetes que fluyen de aquí para allá a través de la red.

No toma mucha programación el análisis de la información que fluye sobre la red.

Un ejemplo simple es un procedimiento de login remoto. En el procedimiento login, el sistema pedirá y recibirá el nombre y contraseña del usuario a través de la red.

**Autenticación**

El procedimiento de login remoto muestra el problema de autenticación.

¿Cómo presenta usted credenciales al anfitrión remoto para probar que usted es usted?.

¿Cómo hace usted esto, de forma que no se repita por el mecanismo simple de una jornada registrada?.

**Autorización**

Aún cuando usted puede probar que usted es quien dice que es, simplemente, ¿Qué información debería permitir el sistema local accesar a través de una red?.

Este problema de autorización parecería ser simple en concepto, pero considerar los problemas de control de acceso, cuando todo el sistema tiene su autorización remota de usuario, el problema de autorización sería un problema de seguridad bastante serio, en donde intervienen los conceptos de funciones autorizadas, niveles de autorización, etc.

### Componentes de Seguridad

Para un intruso que busque acceder a los datos de la red, la línea de ataque más prometedora será una estación de trabajo de la red. Debe habilitarse un sistema que impida que usuarios no autorizados puedan conectarse a la red y copiar información fuera de ella.

El administrador de la red debe clasificar a los usuarios de la red con el objeto de darles el nivel de seguridad adecuado.

### Protegiendo la Red

Las Estaciones de trabajo sin flopy disk y puertos USB; una posible solución para poder impedir la copia de programas y datos fuera de la red en disquetes y memorias, y que a través de ellos ingresen virus y otros programas dañinos a la red, es el uso por los usuarios vulnerables con estaciones de trabajo sin flopy disk ni puertos USB.

## XXIV. CASOS DE EMERGENCIA PARA LOS EQUIPOS DE COMPUTO

### A. De las Emergencia Físicas

### CASO A: Error físico de disco de un Servidor.

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

Ubicar el disco dañado.

Avisar a los usuarios que deben salir del sistema.

Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.

Bajar el sistema y apagar el equipo.

Retirar el disco dañado y reponerlo con otro del mismo tipo, formatearlo

Restaurar el último backup en el disco

Recorrer la información que se encuentran en dicho disco y verificar su buen estado.

**CASO B: ERROR DE MEMORIA RAM**

En este caso se dan los siguientes síntomas:

- El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
- Ante procesos mayores se congela el proceso.
- Arroja errores con mapas de direcciones hexadecimales.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las siguientes acciones:

- Avisar a los usuarios que deben salir del sistema.
- El servidor debe estar apagado, dando un correcto apagado del sistema.
- Ubicar las memorias dañadas.
- Retirar las memorias dañadas y reemplazarlas por otras iguales o similares.
- Retirar la conexión del servidor con la red, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
- Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia la red, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

- Probar los sistemas que están en red en diferentes estaciones.
- Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

**CASO C: CASO DE INCENDIO TOTAL**

En el momento que se de aviso de alguna situación de emergencia general, se deberá seguir al pie de la letra los siguientes pasos.

En ese momento cualquiera que sea el proceso que se esté ejecutando en el Computador Principal, se deberá enviar un mensaje (si el tiempo lo permite) de "Salir de Red y Apagar Computador",

Tomando en cuenta que se trata de un incendio se debe tratar en lo posible de trasladar el servidor fuera del local.

## B. De las Emergencias Lógicas de Datos

**CASO A: ERROR LOGICO DE DATOS**

- Caída del servidor de archivos por falla de software de red.
- Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
- Bajar incorrectamente el servidor de archivos.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

**PASO 1:** Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos y cargar el sistema operativo de red.

**PASO 2:** Deshabilitar el ingreso de usuarios al sistema.

**PASO 3:** Cargar una utilidad que nos permita verificar el contenido de los discos duros del servidor.

**PASO 4:** Al término de la operación de reparación se procederá a habilitar Las entradas a las estaciones para manejo de soporte técnico, se procederá a revisar las bases de datos.

Verificar que los índices estén correctos, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

**CASO B: CASO DE VIRUS**

Dado el caso de que se presente virus en el computador se procederá a lo siguiente:

**Para servidor:**

Se contará con un antivirus que aísle los virus que ingresan al sistema llevándolo a cuarentena

El antivirus muestra el nombre del archivo infectado y quién lo usó.

Estos archivos (exe, com, drv, dll.) serán reemplazados del disquete original de instalación o del backup.

Si los archivos infectados son aislados y aún continua el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, y debe ser retirada de la red y proceder a su revisión.

## XXV. INFORME FINAL DE LA CONSULTORÍA

El día 14 de junio se realizaron las labores de visita entrevista y recolección de registros en las instalaciones de la cadena de hoteles. La duración de la visita fue de aproximadamente 4 horas. Las personas entrevistadas fueron el gerente de Información y Tecnología, Ing. Jorge Castro y el jefe de operaciones Información y Tecnología, Ing. Mauricio Martínez.

Según los puntos de la norma ISO 17799 se encontraron las siguientes incidencias:

### A. Responsabilidades de la Gestión Gerencial

- No existe documentación alguna sobre las políticas de seguridad del sistemas de información, esto debido a que se encuentran en proceso de desarrollo, ya que se están reestructurando todos los procesos de la gestión de Información y Tecnología y por tanto la seguridad de los mismos. Además no existen controles regulares para verificar la efectividad de las políticas por la misma inexistencia de las mismas no ha sido tomado en cuenta.
- No existen roles y responsabilidades definidos para las personas implicadas en la seguridad, ya que no están formalizadas y no se han aclarado las funciones especificas en el Área de I&T[8].
- No hay una revisión periódica de la seguridad por una empresa externa, tanto del entorno lógico como físico.

[8] Informática y Tecnología

- No existe un programa de capacitación para la formación en seguridad ya que se presupone que esto es directamente manejado por la empresa que maneja el Outsourcing de Seguridad.
- No existe un procedimiento para realizar una clasificación de la información, por la misma razón mencionada en los puntos anteriores, de la inexistencia de procedimientos y parámetros determinados. Y por la ausencia de clasificación también fueron descartados los procedimientos de etiquetado de la información.
- No se le es informado a los usuarios que no deben probar las vulnerabilidades del SI por que no esta definido en el reglamento
- No existe registrado un plan de continuidad del negocio y análisis de impacto aunque si se han tomado medidas no formales al respecto. Y por lo anterior tampoco existe un desarrollo, reacción e implantación de planes de continuidad.
- No existe una revisión de la política y de la conformidad técnica, debido a la ausencia de las políticas y los procedimientos documentados.

**B. Responsabilidades de la Gestión la gestión Operativa**

- No existen controles adicionales al personal propio y ajeno ya que no se han implementado dispositivos o algún otro control por que ya se han implantado opciones de seguridad dentro de las instalaciones
- No existen políticas formalizados con respecto a la limpieza en el puesto de trabajo
- No existe seguridad sobre la documentación de SI ya que no hay documentos sobre los cuales aplicarla.

- No existen acuerdos para el intercambio de información y software ya que no están contemplados por la alta gerencia debido a la seguridad, por ser información confidencial.
- No se protege el acceso a los equipos desatendidos (equipos en bodegas o en proceso de baja), ya que se encuentran en depósitos seguros.
- No existen controles criptográficos a causa de que no hay parámetros definidos y no han sido contemplados por la alta gerencia debido a los altos costos de los certificados.

## XXVI. ACCIONES CORRECTIVAS, MEJORAS Y RECOMENDACIONES

Según los hallazgos realizados:

- Se recomienda de manera urgente establecer políticas de seguridad e implementarlas a toda la organización debido a que son el eje fundamental para cualquier gestión de la seguridad de la información. Esto puede ser llevado a cabo basándose en las normas ISO 17799 e ISO 9001 para efectos de futuras certificaciones

- Por la misma ausencia de las políticas no existe ningún método de control para verificar su funcionamiento lo cual también es necesario implementar para verificar el funcionamiento de las políticas

- Al momento de implementar una gestión para la seguridad de la información se deben dejar establecidos los roles y papeles de las persona que van a intervenir en los procesos, para aclara las responsabilidades y funciones

- Se recomienda que las revisiones periódicas que se hagan una ves implementado el sistema de gestión de las seguridad de la información, sean realizadas por una empresa externa con el fin de asegurar la transparencia y fidelidad de la información recogida.

- Es imprescindible la capacitación de todo el personal que tenga acceso y manipule la información haciéndoles conocer que esta es el activo mas importante de la organización y por tal razón deben cuidarla y manejarla de la mejor forma posible, guardando la confidencialidad de toda la información a la que tienen accesos, e igualmente y muy importante que tengan conocimiento de las políticas y de la gestión de las mismas.

- El correcto manejo de la información y de la seguridad de la misma dependen también de la organización que se tenga de ella, y para eso es necesario tener un correcto etiquetamiento y clasificación de la información para lo cual se pueden usar métodos de inventario.

- Aunque existen controles de acceso físico, se recomienda la implementaciones de controles magnéticos digitales o biométricos para el acceso a las áreas seguras ya que de estas metodologías se puede llevar un mejor control de accesos y permisos al personal

- Sin dejar de ser algo importante el aseo de las estaciones y puesto de trabajo puede llegar a ser algo que sin pensarlo puede llegar a afectar la seguridad (integridad) de los equipos de computo y aunque se detecto que las áreas eran relativamente organizadas y limpias, también se encontró que no están formalizadas y se recomienda documentar esta políticas

- Al momento de tener las políticas establecidas y documentadas se recomienda aplicar seguridades a toda la documentación generada, e implementar controles de modificación sobre los mismos.

- Es aconsejable la adquisición de certificados digitales y controles criptográficos para el manejo remoto de la información

- Aunque existen planes de contingencia no se encuentran documentados por tal razón no todo el personal que pertenece a la gestión de seguridad sabe como reaccionar en momento de algún imprevisto

En general a la organización carece de muchos puntos, hablando basados en la norma ISO 17799 para lograr tener implementada una gestión de la seguridad de la información de manera completa y que arroje resultados eficientes, es decir que aseguren la calidad, fidelidad, fiabilidad, confidencialidad e integridad de la información.

## XXVII. CONCLUSIONES

Una vez finalizada la consultoría se evidenció que la organización no cuenta con políticas de seguridad documentadas.

Al tomar como referencia la norma técnica ISO 17799 se logró establecer las personas encargadas del manejo de la infamación no tienen conocimiento de su existencia

Se constató que la utilización de las listas de verificación son de suma importancia para el informe final ya que nos arroja las deficiencias específicas sobre las cuales hay que implementar los correctivos.

# XXVIII. FUENTES

## INTERNET

BSI México - Normas y publicaciones [PDF] BSI México 2007. Disponible en internet en la dirección: [http://www.bsiamericas.com/normas.

Belkis Valero A. Nancy del Valle Aguilar Andara – Tesbelk- Articulo de Internet- Monografias.com – Disponible en la dirección: http://www.monografias.com/trabajos13/tesbelk/tesbelk2.shtml nancyaguilar@hotmail.com

Barroeta C., Yleana C. (1998) titulado "La auditoría como apoyo Técnico y Financiero requerido por las Microempresas Valeranas". Trabajo de grado para optar al título de Licenciado en Administración de empresas. Universidad Valle del Momboy.

**melissa rivera hurtado -** melissa_mili[arroba]hotmail.com- 2006- Titulado."Auditoria" Disponible en la dirección

http://www.monografias.com/trabajos32/auditoria/auditoria.shtml

Guissella Zoraida Moscoso Salazar -Franklin Olivera Safora – 2006- "Metodología para la evaluación de riesgos de activos de TI en entidades financieras Disponible en la dirección" - isbib.unmsm.edu.pe/bibvirtualdata/monografias/ingenie/olivera_sf/cap3.pdf -

Hispasecurity-Seguridad Informática-Articulo de Internet 2001. Disponible en Internet en la dirección: http://www.virusprot.com/art4.html