Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS

Sergio Enrique Lemus Mendoza
Asesorado por el Ing. Roberto Sánchez de León

Guatemala, agosto de 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

SERGIO ENRIQUE LEMUS MENDOZA
ASESORADO POR EL ING. ROBERTO SÁNCHEZ DE LEÓN

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, AGOSTO DE 2011

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Juan Álvaro Díaz Ardavin
EXAMINADOR	Ing. Edgar Josué González Constanza
EXAMINADOR	Ing. José Ricardo Morales Prado
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha diciembre de 2009.

Sergio Enrique Lemus Mendoza

Guatemala 08 de junio de 2011

Oficina de lingüística
Facultad de ingeniería
Universidad de San Carlos de Guatemala

A quien interese:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **SERGIO ENRIQUE LEMUS MENDOZA**, con número de carnet **200312544**, titulado: "**GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS**" y el mismo cumple con las normas dadas en el PROPEDÉUTICO DE TESIS o en los TALLERES DE REDACCIÓN Y ORTOGRAFÍA impartidos por la FACULTAD DE INGENIERÍA.

Sin otro particular, me suscribo de usted, atentamente,

Licda. Sandra Elizabeth Villatoro Gamarro de Alvarado
Colegiado Activo No. 15,878
Revisor ortográfico y de redacción del trabajo de graduación

Guatemala, 05 de mayo de 2011

Ingeniero

Carlos Azurdia

Tutor de trabajos de graduación

Facultad de ingeniería

Universidad de San Carlos de Guatemala

Ingeniero Azurdia:

Deseándole éxitos en sus actividades diarias me dirijo a su persona para informarle que he revisado el trabajo de graduación del estudiante Sergio Enrique Lemus Mendoza quien se identifica con carné 200312544 y le notifico que el mismo cumple con los objetivos planteados al inicio, por lo que doy por finalizado su trabajo de graduación satisfactoriamente.

Sin nada más que agregar, me despido de usted agradeciéndole su atención a la presente.

Atentamente,

Ing. ROBERTO SANCHEZ DE LEON
Ciencias y Sistemas
Colegiado # 6631

Ing. Roberto Sánchez de León

Asesor de trabajo de graduación

Colegiado No. 6631

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 1 de Junio de 2011

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **SERGIO ENRIQUE LEMUS MENDOZA**, carné **2003-12544**, titulado: **"GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, de trabajo de graduación titulado ***"GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS."****, presentado por el estudiante SERGIO ENRIQUE LEMUS MENDOZA, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pèrez Turk
Director, Escuela de Ingenierìa Ciencias y Sistemas

Guatemala, 10 de agosto 2011

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.280.2011

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **GUÍA PARA LA AUDITORÍA DE REDES DE COMPUTADORAS,** presentado por el estudiante universitario **Sergio Enrique Lemus Mendoza,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, agosto de 2011

/cc

ACTO QUE DEDICO A:

Mis padres Enrique Lemus y Marbel Roxana Mendoza de Lemus, quienes con su esfuerzo y dedicación me permitieron concluir mis estudios; me guiaron por el camino correcto con ejemplo de vida. Este logro es tanto suyo como mío.

Mis hermanos Marta, Diego y José con quienes convivo y comparto diariamente; quienes siempre me motivaron a salir adelante.

Mis amigos Omar Meza y Sergio Rodríguez porque recorrimos el camino universitario juntos.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Administrador Persona encargada de todas las tareas de mantenimiento de un sistema informático.

Adware Programa que automáticamente se instala y ejecuta en la computadora del usuario. En algunas ocasiones estos programas incluyen subrutinas que representan un problema para la privacidad del usuario.

Auditoría Analiza y estudia a fondo sistemas informáticos para prevenir un mal funcionamiento o corregir malos procedimientos.

Backup Copia de la información que se posee en los servidores de un sistema informático, con el fin de tener un respaldo de la misma, para recuperarla si los servidores sufrieran algún daño.

DES Estándar de cifrado de datos.

Dúplex Forma de comunicación entre dos dispositivos y ocurre cuando la información viaja en dos sentidos, es decir, se pueden enviar y recibir datos por el mismo enlace, pero no al mismo tiempo.

Firewall	Dispositivo que filtra los paquetes que entran y salen de una red; con el objetivo de que cumplan con las políticas implementadas por el administrador de red.
FTP	Protocolo de transferencia de archivos.
Full-dúplex	Forma de comunicación entre dos dispositivos. Ocurre cuando los dispositivos envían y reciben información simultáneamente.
Hardware	Dispositivos físicos que componen una computadora o una red de computadoras.
Host	Computadoras conectadas a una red. Los usuarios las utilizan para tener acceso a la red y para proveer o utilizar servicios.
HTTP	Protocolo de transferencia de hipertexto.
Hub	Dispositivo que transmite toda la información que recibe en varias direcciones. En el modelo de referencia OSI se encuentra ubicado en la capa 1.
Herramienta	Módulo de un programa, encargado de realizar una tarea en especial.
IDEA	Algoritmo internacional de cifrado de datos.

Internet Conjunto de redes de computadoras conectadas a nivel global por medio de dispositivos de enlace de red. Está compuesta por millones de redes públicas y privadas ubicadas por todo el mundo.

ISO Organización internacional para la estandarización.

Linux Sistema operativo basado en los sistemas *Unix*. Es de código abierto y posee varias distribuciones, entre ellas están *Ubuntu* y *Fedora*.

Malware Programa que busca dañar una computadora de forma transparente al usuario. Existen muchas formas de *malware*, algunas de ellas son los virus de computadoras.

OSI Interconexión de sistemas abiertos.

PKI Infraestructura de clave pública.

POP Protocolo de oficina de correos.

Router Dispositivo de *hardware* que permite conectar redes de computadoras. Su principal objetivo es dirigir el tráfico de red hacia su destino, utilizando distintos algoritmos de enrutamiento.

Simplex Comunicación entre dos dispositivos que ocurre en una sola vía. Por lo que un dispositivo sólo puede enviar información a un destinatario.

SMTP	Protocolo simple de transferencia de correo.
Sniffer	Programa que busca capturar las tramas de red. Su principal objetivo es monitorear la red de computadoras para detectar fallos o verificar filtraciones de información.
Sistema operativo	Conjunto de programas que busca proveer de una interfaz al usuario para que éste se pueda comunicar con el *hardware* de la computadora.
Software	Componentes intangibles de una computadora. Su función es controlar el *hardware* o brindar herramientas al usuario para que pueda realizar sus tareas.
Spyware	Programa que se instala de forma anónima en una computadora para recopilar información sobre las actividades realizadas por el usuario. Después de obtener la información sobre el usuario, el programa la envía a empresas publicitarias o a las personas interesadas.
Switch	Dispositivo de *hardware* que conecta varias computadoras en una red de computadoras. Su principal característica es que envía el tráfico únicamente por la interfaz que va hacia la computadora de destino.

RESUMEN

En un inicio las redes de computadoras estaban conformadas por una cantidad muy pequeña de computadoras y eran muy pocas las que existían alrededor del mundo. Solo empresas de gran envergadura podían contar con una red de computadoras. En ese tiempo cada red tenía sus propias reglas de comunicación y sus propios protocolos. Por lo que resultaba prácticamente imposible conectar una red con otra.

Para evitar esta incompatibilidad entre redes de computadoras se comenzaron a crear estándares. Es así como nace el modelo OSI el cual busca establecer una serie de estándares en cuanto a la arquitectura de red de computadoras se refiere.

Cuando las redes de computadoras comenzaron a implantar los estándares, fue posible interconectarlas y éstas fueron creciendo de manera acelerada, sin embargo, fue entonces cuando comenzó a surgir un problema a nivel de seguridad, debido a que la información podía estar al alcance de cualquier persona con acceso a la red. Desde el auge de las redes de computadoras hasta estos días, se han implementado métodos para hacer más seguras las transmisiones en una red, los cuales buscan identificar las posibles áreas débiles de un sistema informático, para corregir el error e implementar políticas y reglas que permitan hacer más seguro un sistema.

OBJETIVOS

General

Crear reglas y lineamientos que guíen a los administradores de las pequeñas y medianas empresas a implementar un sistema informático, el cual sea seguro y además investigue, analice sistemas que permitan administrar y monitorear los sistemas informáticos.

Específicos

1. Investigar los distintos tipos de auditoría de redes y las herramientas que le brindan soporte al auditor.

2. Investigar los estándares aplicados a la seguridad informática.

3. Mostrar al lector la forma adecuada de llevar a cabo una auditoría de redes interna.

4. Investigar técnicas y métodos de seguridad informática preventiva.

5. Capacidad del lector para instaurar políticas de seguridad básicas en su red.

6. Realizar un caso de estudio, en el cual se pueda evidenciar de forma práctica el funcionamiento de las herramientas para la auditoría informática.

7. Presentar un análisis de los resultados obtenidos en el caso de estudio.

INTRODUCCIÓN

Una red de computadoras está comprendida por un conjunto de *hosts* los cuales se encuentran conectados unos con otros y que buscan compartir información, recursos y servicios. La seguridad informática debe garantizar a la empresa la disponibilidad de los sistemas de información; la recuperación rápida y completa de los sistemas, la integridad y la confidencialidad de la información.

Un sistema seguro debe ser capaz de registrar y notificar al administrador de la red acerca de cualquier anomalía o evento importante que ocurra en el sistema, esto es conocido como auditoría. En la mayoría de redes por lo general, la primera medida de seguridad que se toma es instalar *firewalls*, mucho antes de que se haya identificado un problema particular de seguridad de red. Sin embargo, el uso de *firewalls* no es suficiente para hacer frente a los ataques informáticos, es por eso que es necesario implementar planes para la seguridad informática, los cuales deben incluir; políticas, reglas y normas que deben ser seguidas por los usuarios de la red. Otro método que permite hacer más seguras las comunicaciones es la criptografía, la cual permite que la información sensible esté oculta a usuarios sin autorización, lográndolo mediante un conjunto de técnicas.

Para crear una política de seguridad de red efectiva primero se deben de formular algunas preguntas difíciles relacionadas con los tipos de servicios de red y recursos cuyo acceso se permitirá a los usuarios. Cuando los usuarios tienen acceso ilimitado a la red, la implementación de una política que limite ese acceso puede resultar un tanto complicada.

1. MARCO TEÓRICO

1.1. Modelo OSI

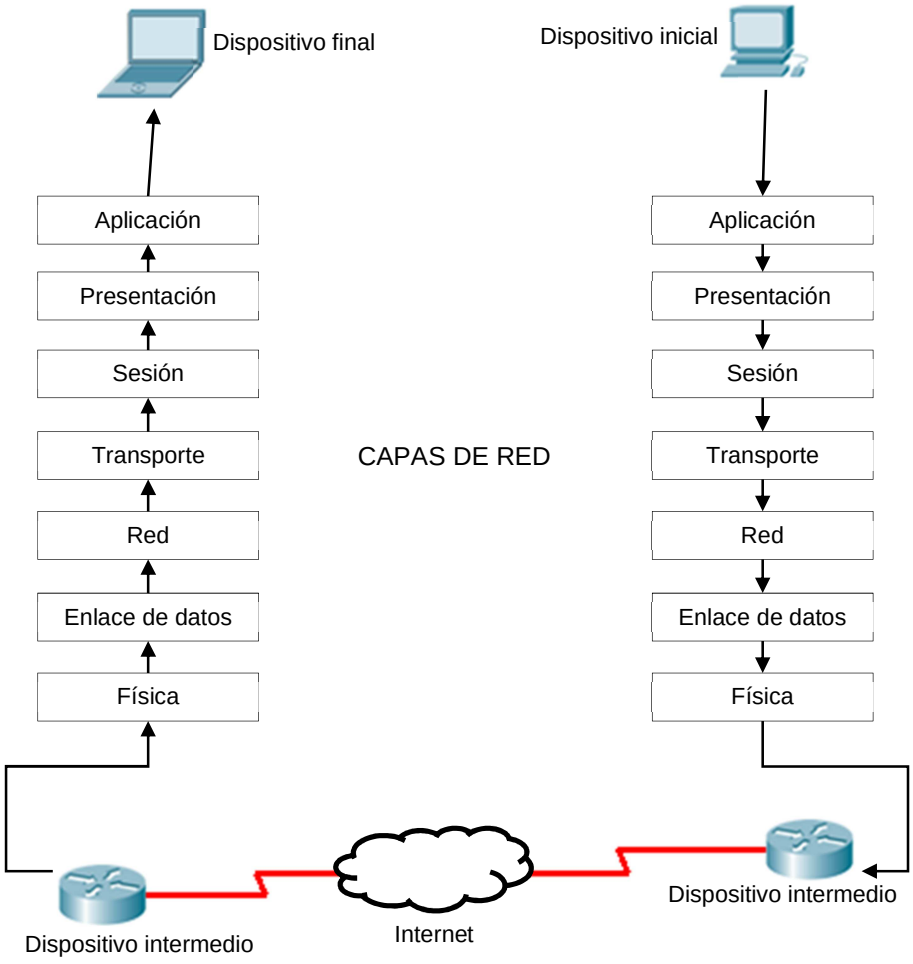
A partir de 1980 se inició el auge de las computadoras, fue entonces cuando las redes de computadoras comenzaron a ser más grandes. Durante esos años no existía un estándar por el cual los fabricantes de computadoras se debían regir, lo que generó un enorme problema entre estas redes en crecimiento. Cada empresa desarrolló su propia tecnología, por lo que la comunicación entre redes de distintas organizaciones era un enorme problema. Para evitar que este problema siguiera aumentando se decidió crear un conjunto de normas, las cuales debían ser seguidas por todos los fabricantes.

De esta forma fue creado el modelo OSI, el cual fue propuesto por la ISO y es el modelo de referencia más ampliamente conocido. Este modelo divide el trabajo de la red en siete capas y es utilizado para el diseño de redes, además permite que exista una mayor compatibilidad entre el hardware de distintos fabricantes alrededor del mundo.

Las siete capas definidas por este modelo son: física, enlace de datos, red, transporte, sesión, presentación y aplicación. En cada una de estas capas se definen estándares y protocolos, los cuales hacen posible implementar redes que se puedan comunicar con otras redes bajo el mismo modelo de estandarización.

Los paquetes que viajan a través de una red que implementa este modelo deben pasar por cada una de estas capas (ver figura 1), realizado procesos de encapsulación y desencapsulación.

Figura 1. **Modelo de referencia OSI**



Fuente: elaboración propia.

1.1.1. Capa 1: física

La capa física tiene dos objetivos principales; el primero es crear una señal que represente los bits de información de las tramas de la capa de enlace de datos, para posteriormente enviarlos a través de los medios físicos. El segundo objetivo es el de recuperar las señales que recibe de los medios físicos y transformarlas en bits, para luego enviarlos a la capa de enlace de datos como una trama.

Los tres medios más importantes mediante los cuales pueden viajar las señales son:

- Fibra óptica
- Cable de cobre
- Inalámbrico

Las señales que viajan por medio de fibra óptica se convierten en pulsos de luz. Si viajan por medio de cable de cobre, las señales son convertidas a pulsos eléctricos y para los medios inalámbricos las señales viajan como microondas. La forma de enviar o recibir estas señales puede ser simplex, dúplex o *full-dúplex*.

1.1.1.1. Codificación

La codificación sirve para transformar una cadena de bits en un código estándar y entendible tanto para el emisor como para el receptor.

Los métodos de codificación también proporcionan códigos para control, los cuales permiten identificar el inicio y el fin de una trama, por lo que ofrecen una mejor detección de errores en los medios.

1.1.1.2. Señalización

Las señales generadas deben representar un "1" o un "0" en los medios, a esta representación de los bits se le denomina método de señalización. Un bit puede ser representado, al cambiar alguna de las siguientes características en una señal:

- Amplitud
- Frecuencia
- Fase

El método de señalización más simple es el de Sin Retorno a Cero (NRZ, por sus siglas en inglés), el cual representa los bits como cambios en el voltaje, sin embargo este método no usa de forma eficiente el ancho de banda y solo es recomendado para enlaces de baja velocidad.

Otro método es el de la codificación *Manchester*. Este método usa transiciones para indicar un bit lógico. En este método un "0" es representando mediante la transición de un voltaje alto a uno bajo y el "1" es representado mediante la transición de un volate bajo a uno alto.

1.1.2. Capa 2: enlace de datos

La capa de enlace de datos le permite a dos nodos el intercambio o transferencia de tramas mediante el uso de medios físicos comunes entre los dos.

Las tramas son las unidades de datos del protocolo (PDU, por sus siglas en inglés) de la capa de enlace de datos. Esta capa soporta la comunicación y le permite a las capas superiores desligarse del proceso de colocar y recibir datos de la red. Los protocolos de esta capa son los encargados de encapsular las tramas y desencapsular los paquetes de la capa superior, también utilizan métodos de control de acceso al medio para permitir que los dispositivos puedan acceder a los medios físicos.

Una trama está compuesta por tres secciones principales:

- Encabezado: posee información para el control del direccionamiento.
- Cuerpo: contiene los datos del paquete de la capa superior.
- Cola: almacena la información de control para la detección de errores y para indicar el final de una trama.

1.1.2.1. Subcapas

Las subcapas de la capa de enlace de datos son las siguientes:

- Control de enlace lógico: agrega información a la trama, la cual es utilizada para identificar el protocolo de la capa superior que está utilizado la trama.

- Control de acceso al medio: brinda los métodos necesarios para el direccionamiento y control de datos, dependiendo del tipo de protocolo que se esté utilizando.

Los dos métodos utilizados por la subcapa de control de acceso al medio, establecen reglas las cuales les indican a los dispositivos la forma en la que compartirán datos a través de medios comunes, estos métodos son: el basado en contención y el controlado. En el método basado en contención todos los dispositivos compiten por el uso del medio, mientras que en el método controlado todos los dispositivos cuentan con cierta cantidad de tiempo para utilizar el medio.

1.1.3. Capa 3: red

La capa de red brinda servicios para intercambiar porciones de datos a través de la red entre dispositivos finales, para lograr esto la capa de red posee cuatro procesos centrales, los cuales son:

- Direccionamiento: consiste en proveer una forma para direccionar los dispositivos. Cada dispositivo debe poseer una dirección única, para que de esta forma las porciones de datos puedan llegar al destino deseado. Cuando a un dispositivo final se le otorga una dirección, se le denomina *host*.

- Encapsulamiento: consiste en agregar una dirección de origen y de destino a los paquetes de esta capa. Una vez encapsulado el paquete, este está listo para ser enviado a través de los medios. Los paquetes son las PDU de la capa de red.

- Enrutamiento: consiste en dirigir los paquetes hacia su destino. Son los enrutadores (*routers)* los dispositivos encargados de seleccionar la ruta y de dirigir los paquetes por esta ruta. Los enrutadores utilizan algoritmos para determinar estos caminos.

- Desencapsulamiento: una vez que el paquete llega a su destino, el paquete debe ser desencapsulado, este proceso es completamente inverso a la encapsulación. Después de desencapsular el paquete se obtiene la dirección de destino y se compara con el dispositivo final para comprobar que el paquete llegó efectivamente a su destino.

1.1.3.1. Protocolo de Internet

El protocolo de Internet (IP) es un servicio implementado por los protocolos de TCP/IP. Actualmente la versión más utilizada es la versión 4. El protocolo de Internet es un protocolo no orientado a la conexión, esto quiere decir que no se establece una conexión antes de enviar los paquetes, por lo tanto, estos no viajan necesariamente por la misma ruta. Además, este protocolo utiliza el método del máximo esfuerzo, esto quiere decir que no se garantiza que todos los paquetes lleguen hacia su destino.

1.1.4. Capa 4: transporte

La capa de transporte es la encargada de dividir o segmentar la información. También es responsable del reensamblaje de la información. A las PDU de esta capa se les llama segmentos.

Las tareas de esta capa son:

- Seguimiento de conversaciones individuales
- Segmentación de datos
- Reensamblaje de segmentos
- Identificación de aplicaciones

Un dispositivo final puede mantener muchas comunicaciones con varias aplicaciones de otro dispositivo final, la capa de transporte debe ser capaz de mantener estas distintas comunicaciones individuales con el *host* remoto.

Cuando dos dispositivos finales están en comunicación generan una cadena de datos, esta cadena no puede ser enviada como una sola debido a que saturaría los medios físicos, la capa de transporte es responsable de segmentar esta cadena de datos para que puedan ser enviados individualmente. A cada segmento se le debe agregar información adicional (encapsulación).

Cuando los segmentos llegan al destino, la capa de transporte debe de dirigir el segmento hacia la aplicación correspondiente. Posteriormente debe ser capaz de reensamblar todos los segmentos para formar nuevamente la cadena de datos original.

Para que la capa de transporte pueda determinar la aplicación exacta hacia la cual se debe dirigir el segmento, utiliza un número de puerto, el puerto sirve para identificar de manera única a las aplicaciones en los dispositivos finales. Este número de puerto es agregado al segmento en el proceso de encapsulación.

1.1.5. Capa 5: sesión

La capa de sesión crea, mantiene y finaliza diálogos entre las aplicaciones de origen y destino. Además, administra el intercambio de información entre las sesión activas y es capaz de reiniciar una sesión cuando esta se finaliza abruptamente.

Los principales servicios que ofrece esta capa son:

- Control de sesiones
- Manejo de sesiones paralelas
- Verificación de sesiones activas o inactivas

1.1.6. Capa 6: presentación

Los objetivos principales de la capa de presentación son:

- Codificación de datos de la capa superior
- Cifrado y descifrado

La codificación consiste en darle formato a los datos de tal forma que exista la certeza que la información enviada por la interfaz de origen pueda ser interpretada correctamente por la aplicación en la interfaz de destino.

Existen estándares definidos para los distintos tipos de información que viajan en la red. Estos estándares generalmente se identifican por medio de la extensión de un archivo y aseguran que los dispositivos conozcan la forma correcta de manipular la información recibida o enviada. Como ejemplo se tienen las imágenes, algunos de sus estándares son el formato BMP o GIF.

1.1.7. Capa 7: aplicación

La capa de aplicación brinda al usuario la interfaz necesaria entre las aplicaciones de uso cotidiano y la red de computadoras asociada con el usuario. Esta capa se encuentra en el nivel más alto del modelo de referencia OSI. Por medio de ella se accede a las capas inferiores y los servicios que éstas prestan. Además, define los protocolos que utilizan las aplicaciones para intercambiar información entre el *host* destino y origen.

Constantemente se desarrollan protocolos nuevos y más seguros para esta capa, utilizados por ejemplo por aplicaciones de correo electrónico. Esta capa posee dos formas para proporcionar acceso a una red:

- Aplicaciones: son los programas utilizados por los usuarios cotidianamente y que usan lo protocolo de esta capa para comunicarse con las capas inferiores.
- Servicios: los servicios son totalmente transparentes al usuario y son utilizados por las aplicaciones para usar algunos recursos de red. Un buen ejemplo de un servicio es la cola de impresión para utilizar una impresora compartida.

1.1.7.1. HTTP

Este protocolo se utiliza para la transferencia de datos; no está orientado a la conexión, es decir, que no almacena información sobre sus conexiones. Establece una forma de comunicación por medio de mensajes de solicitud-respuesta.

- *GET*: es un mensaje de solicitud utilizado generalmente por los navegadores de Internet para solicitar las páginas o sitios al servidor *Web*.
- *POST*: envía mensajes a los servidores *Web*. Generalmente este mensaje es utilizado cuando se envía información del usuario hacia el servidor.

1.1.7.2. FTP

Permite la transferencia de archivos de un servidor hacia un cliente y viceversa. Para lograr esta transferencia utiliza dos conexiones, una para mantener una comunicación entre el servidor y el cliente y otra para realzar la transferencia del archivo.

1.1.7.3. SMTP

Al igual que el FTP, también posee una arquitectura cliente-servidor. Este protocolo define el proceso en que se envían mensajes de correo electrónico por un servidor o un cliente.

1.1.7.4. POP

Este protocolo está ligado al SMTP y define la forma en la que se reciben correos electrónicos desde un servidor de correos. Una de sus ventajas es que le da la opción al usuario de descargar el correo a su computadora para revisarlo posteriormente sin necesidad que exista conexión a Internet o de red.

1.2. Criptografía

La criptografía puede ser definida como "las técnicas de escrituras tales que la información esté oculta de intrusos no autorizados"[1].

1.2.1. Métodos de criptografía

1.2.1.1. Esteganografía

La esteganografía busca transmitir la información oculta dentro de otro objeto, de tal forma que no se perciba que en ese objeto se transmite un mensaje oculto. Una organización mediana o pequeña no debe preocuparse demasiado por implementar métodos de encriptación, debido a que en el mercado existen muchas herramientas que brindan esta funcionalidad.

1.2.1.2. Transposición

La transposición es uno de los métodos más sencillos de criptografía. Básicamente invierte el orden de los caracteres que conforman el mensaje. Es por eso que descifrar los mensajes ocultos es relativamente sencillo, por medio de algoritmos implementados, incluso en software de distribución gratuita.

1.2.1.3. DES

El estándar de cifrado de datos (DES, por sus siglas en inglés) codifica bloques de 64 bits de longitud utilizando una clave de 56 bits.

[1] Gutiérrez Melo, Julián. "Auditoría aplicada a la seguridad en redes de computadoras". Enlace *Web*: http://www.monografias.com/trabajos10/auap/auap.shtml

1.2.1.4. IDEA

El algoritmo internacional de cifrado de datos (IDEA, por sus siglas en inglés) es una evolución del DES. Su principal cambio con respecto al DES es que utiliza una clave de 128 bits. Esta clave es de tipo privada, sin embargo, en una red institucional demasiado extensa se corre el riesgo de ser conocida por usuarios sin la autorización necesaria.

Este algoritmo también utiliza bloques de 64 bits para cifrar la información, aunque implementa nuevas técnicas. Una de esas técnicas busca evitar el problema de clave privada que se mencionó anteriormente. Por lo que además de contar con una clave privada, también posee una clave pública.

El algoritmo utiliza las claves de esta forma:

- Tiene una clave pública y que puede ser conocida por cualquier usuario de la red interna a la organización. Esta clave será usada por el emisor para cifrar el mensaje.
- Una clave privada, únicamente conocida por el usuario receptor y que será utilizada para descifrar el mensaje.

Algunos de los algoritmos que implementan esta arquitectura son:

- Algoritmo de firma digital
- RSA
- Diffie-Hellman

1.2.2. Consideraciones para elaborar un plan de seguridad

Un sistema de seguridad implica "planear, organizar, coordinar, dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad física de los recursos implicados en la función informática, así como el resguardo de los activos de la empresa"[2].

Existen aspectos que un sistema de seguridad debería tomar en cuenta, a continuación se presentan algunos de ellos:

- Definir y delegar responsabilidades
- Niveles de jerarquía administrativas
- Creación de políticas de seguridad enfocadas en:
  - Áreas específicas (dependiendo de su importancia a nivel de seguridad)
  - Toda la organización

También se deben estudiar e implementar mejores prácticas para el personal, orientadas hacia la seguridad:

- Procedimientos en casos de emergencia
- Compra de seguros para el equipo de comunicaciones
- Creación de manuales técnicos para los casos más probables

[2] Jimenez, Jose Alfredo. "Seguridad de un sistema de información".
Enlace *Web*: http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml

Un sistema de seguridad informático no se puede limitar solamente a la prevención de ataques externos o a fallos de seguridad en la red institucional. Se deben tomar en cuenta aspectos de la infraestructura física y del *hardware*, por lo que se debe planear en relación a:

- Las actividades programadas por los auditores
- Simulación de escenarios
- Sistemas de respaldo de información
- Procedimientos contra una posible pérdida de información
- Cableado físico de comunicaciones y de corriente
- Equipo de *hardware* en general (computadoras de escritorio, servidores, *routers*, *switches*, etcétera)
- Interrupción del enlace de red entre el proveedor de servicios de Internet y la red local

1.2.2.1. Etapas de elaboración

Un sistema de seguridad puede ser elaborado durante las siguientes dos etapas:

- Realización de un análisis de la situación actual, en cuanto a seguridad del *hardware*, *software* y usuarios se refiere
- Elaboración de un plan piloto de seguridad, en el cual se tomen en cuenta los aspectos investigados en la etapa uno

1.2.2.2. Plan piloto de seguridad

El plan piloto debe incluir los siguientes puntos:

- Definición de áreas restringidas
- Reglas de seguridad aplicadas a los usuarios
- Clasificación de la información, mediante niveles de relevancia para la institución
- Definición de los usuarios que tendrán acceso a la información mediante el uso de roles y grupos de usuarios
- Programación de *backups* periódicos
- Métodos que aseguren la confidencialidad y la integridad de la información
- De ser posible, crear procedimientos para replicación de bases de datos
- Mantenimiento preventivo de *hardware* y *software*

1.2.2.3. Los usuarios en un sistema de seguridad

Un plan de seguridad será exitoso en la medida que los usuarios colaboren con su implementación. Cuando se diseña un plan de este tipo, el usuario debe estar siempre como pieza fundamental del mismo, ya que son ellos quienes lo pondrán en práctica. Los usuarios deben como mínimo:

- Estar dispuestos a implementarlo
- Cumplir con las reglas establecidas
- Brindar retroalimentación sobre los procesos del mismo

1.2.2.4. Etapas de implementación

La implementación del sistema de seguridad involucra los siguientes pasos:

- Mostrar a los usuarios el beneficio que el sistema de seguridad les va a brindar
- Capacitar a todos los usuarios involucrados en el sistema
- Definir a usuarios encargados por cada área de la organización
- Implementar los procesos diseñados
- Identificar el flujo de la información en cada una de las áreas
- Identificar las áreas en donde se pueden realizar mejoras y las de mayor riesgo
- Mantener buena comunicación con los encargados de las áreas y los jefes
- Darle mantenimiento a los procesos diseñados

1.2.2.5. Beneficios

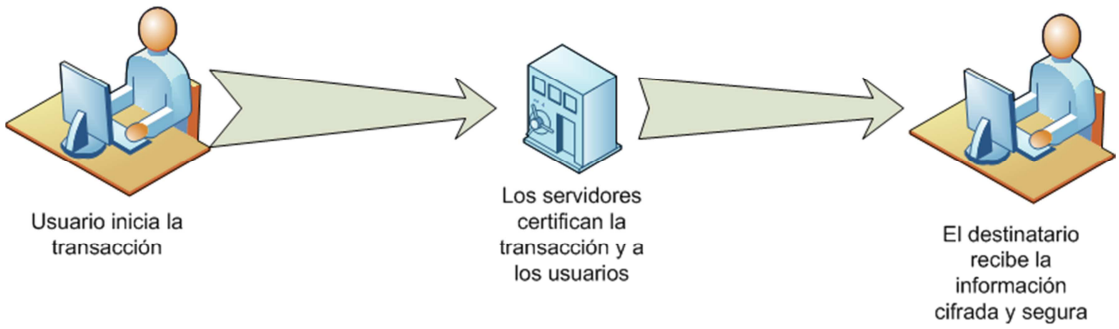
- Permite tener sistemas con un mayor nivel de control
- Los usuarios adquieren un mayor compromiso con la organización
- Se podría ver un incremento en la productividad
- Se consolidan las áreas dentro de la organización

1.2.3. Infraestructura de clave pública

"Una infraestructura de clave pública es una combinación de *hardware* y *software*, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas"[3].

La infraestructura de clave pública es en ocasiones confundida con los algoritmos de clave pública vistos anteriormente. Cabe notar que para implementar estos algoritmos, no es necesario contar con una infraestructura de clave pública. Este tema tiene que ser únicamente asociado con las entidades que certifican transacciones electrónicas y toda la infraestructura que estas deben tener. El flujo básico que se realiza mediante esta infraestructura se puede ver a continuación:

Figura 2. **Flujo básico de la infraestructura de clave pública**



Fuente: elaboración propia.

[3] "Infraestructura de clave pública".
Enlace *Web*: http://es.wikipedia.org/wiki/Infraestructura_de_clave_p%C3%BAblica

Estas transacciones pueden ser certificadas por ciertas instituciones que cumplen con una serie de estándares de seguridad. Gracias a estos métodos, los usuarios pueden autenticarse en la red y cifrar o descifrar mensajes. Esto permite que las transacciones se realicen de forma segura.

1.2.3.1. Usos de tecnología

La infraestructura de clave pública es utilizada para los siguientes procesos:

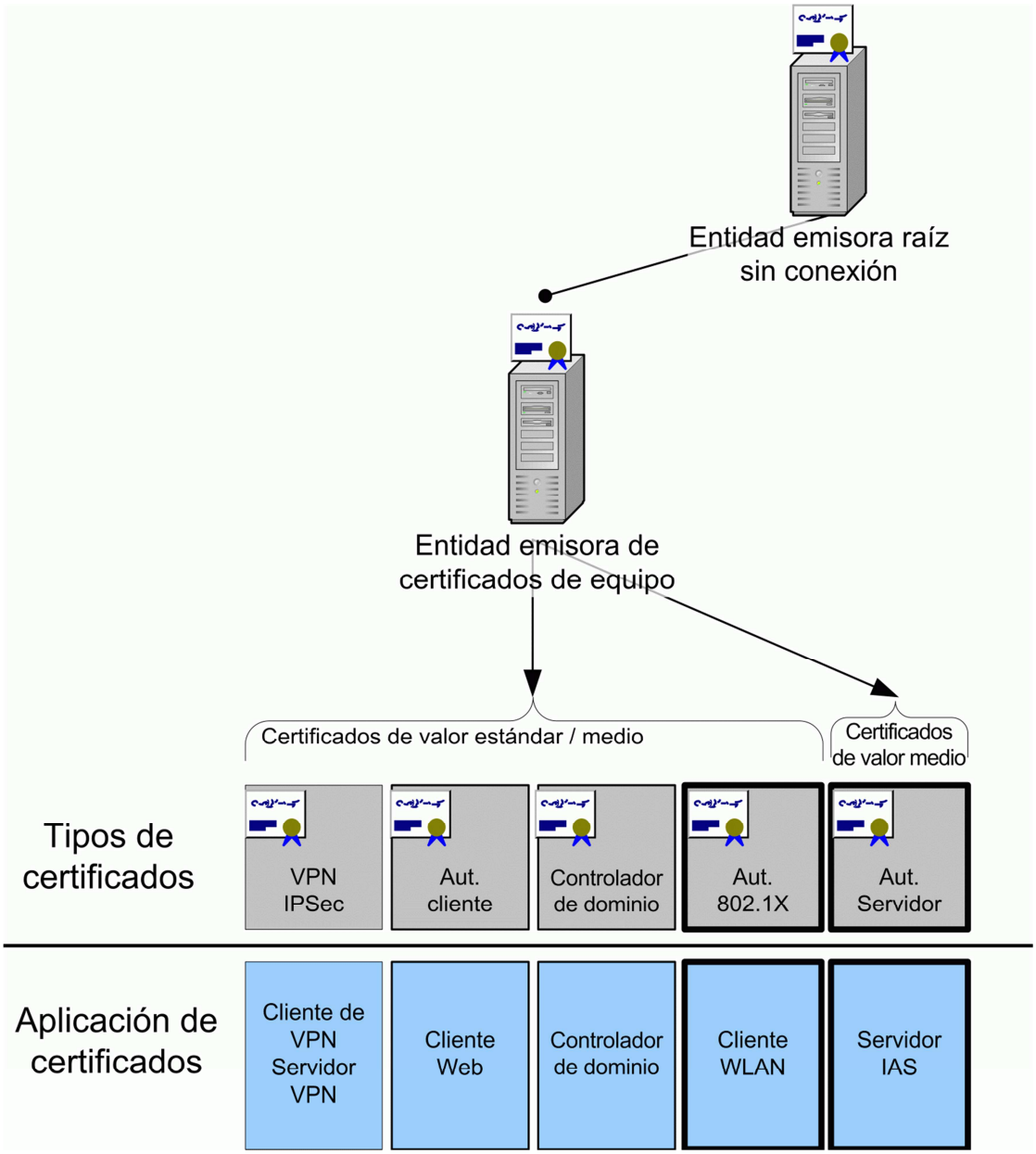
- Firmas y certificados digitales
- Identificación de usuarios
- Autenticación de sistemas
- Transacciones seguras
- Cifrado de información

1.2.3.2. Tipos de certificados

- Personal: identifica a una persona en una transacción.
- Representante: acredita a un usuario como representante de una organización.
- Servidor seguro: certifica que un servidor *Web* es seguro.
- Firma digital: garantiza la no modificación de la información y certifica que el autor del mensaje es quien dice ser.

A continuación se muestra una figura en donde se describe una posible jerarquía que una empresa certificadora debería tener:

Figura 3. **Jerarquía de autoridad de certificados**



Fuente: *Microsoft*. http://www.microsoft.com/latam/technet/articulos/wireless/pgch4.mspx.

1.2.4. Criptoanálisis

La contraparte de la criptografía es conocida como criptoanálisis, en la cual se busca como objetivo principal, descifrar el mensaje oculto.

Los dos tipos de criptoanálisis que existen son:

- Diferencial: trata de descifrar el mensaje mediante variaciones de un bit en cada intento.
- Lineal: utiliza variaciones de tipo *XOR* con cada par de bits del mensaje hasta que obtiene un bit que forma parte de la clave.

1.3. Firma digital

La firma digital permite asociar la identidad de una persona con un mensaje e identificar al autor del mismo. Además, permite:

- Asegurar la integridad del mensaje
- Garantizar que su contenido no puede ser modificado o alterado una vez que ha sido certificado

Esta firma digital se obtiene mediante un algoritmo llamado *hash*. Este algoritmo es aplicado al contenido del mensaje y posteriormente se le aplica un algoritmo de firma electrónica utilizando el método de clave pública y privada.

El algoritmo *hash* funciona en una sola vía, es decir que parte de un punto inicial hacia un punto final. Una vez que se está en el punto final es imposible regresar hacia el punto inicial. Si el destinatario no posee el número que identifica el mensaje, le será imposible obtener la información origen.

Este algoritmo debe satisfacer dos condiciones:

- Debe ser extremadamente difícil obtener dos mensajes con el mismo código de identificación
- Para lograr descifrar el mensaje de forma correcta se deben poseer tanto el código obtenido de la función *hash* como el mensaje

Algunas de las validaciones que deben aplicársele a una firma digital son:

- Vigencia del certificado
- Revocación del certificado
- Estampado digital del sello de tiempo

El sello de tiempo "es un mecanismo que permite demostrar que una serie de datos han existido y no han sido alterados desde un instante específico en el tiempo"[4].

[4] "Sellado de tiempo".
Enlace *Web*: http://es.wikipedia.org/wiki/Sellado_de_tiempo

2. SEGURIDAD INFORMÁTICA

Para un sistema informático la información es parte vital del mismo. Garantizar que la información este segura y que sea confiable deben ser algunos de los principios básicos de cualquier sistema. La seguridad informática posee métodos para alcanzar estos principios mediante la auditoría informática.

2.1. Tipos de auditoría en redes de computadoras

2.1.1. Auditoría de comunicaciones

Internet es una interconexión de redes de área amplia, ubicadas en todas partes del mundo. Mediante Internet todas estas redes se pueden comunicar unas con otras y compartir todo tipo de recursos y de información. Las redes de computadoras buscan compartir recursos, tales como: impresoras o escáneres, servicios e información, mediante bases de datos o servidores. Estas redes se pueden conectar mediante un enlace físico o inalámbrico. Una organización puede tener dos clases de redes, las cuales se definen de la siguiente forma:

- Intranet: red interna a la organización, generalmente es una red de área local.
- Extranet: red externa a la organización, pero que es propiedad y es administrada directamente por la organización, generalmente es una red de área amplia.

Estas redes utilizan los protocolos TCP/IP para conectarse, estos protocolos utilizan puertos de comunicación estandarizados, es decir que cualquier persona conoce sus puertos de transmisión, por lo que con los conocimientos adecuados puede entrar a la red y manipular el flujo de las transmisiones y obtener información importante para las organizaciones o personas individuales, tales como números de tarjetas de crédito.

Esto generalmente ocurre cuando se accede a la red interna de la organización desde Internet. Como primera medida de seguridad se puede usar el *firewall*, estos dispositivos analizan constantemente todo la información que entra desde Internet y también toda la información que sale hacia ella. Más adelante se analizaran los *firewall* en detalle.

En las organizaciones existen dos tipos de políticas, las cuales se listan a continuación:

- Políticas cerradas: está prohibido cualquier tipo de proceso o acción en la red.
- Políticas abiertas: el control sobre las acciones que se llevan a cabo en la red es mínimo o inexistente.

Este tipo de extremos, ya sea permitir control total sobre la red o denegar cualquier tipo de acción, no es recomendable, debe existir un balance el cual le permita a los usuarios realizar su trabajo con libertad pero sin afectar la integridad de la red.

A pesar de que se establezcan medidas y políticas de seguridad en una red, generalmente siempre va a existir un punto de fallo, por lo que se han creado herramientas para comprobar la eficacia de las políticas de seguridad creadas en las organizaciones, algunas de estas herramientas son: *SAFEsuite* y *COPS*. Estas herramientas poseen funcionalidades como por ejemplo: probar el nivel de seguridad de las contraseñas de los usuarios escuchando el tráfico en la red y mediante técnicas especiales buscan descifrar las contraseñas y los nombres de usuarios.

Algunos de los aspectos más importantes a estudiar en la auditoria de comunicaciones son los siguientes:

- Gestión de la red
- Monitorización de la información
- Creación e implementación de estándares

Para crear políticas de control eficaces en una red se deben de tener en cuenta los siguientes objetivos:

- Crear un departamento de comunicaciones con autoridad total sobre la red
- Poseer un inventario actualizado sobre los distintos dispositivos físicos existentes
- Vigilar las acciones sobre la red
- Control sobre los costos de operación de la red
- Crear procesos para mejorar y optimizar el rendimiento y la solución de problemas

Además de los puntos descritos anteriormente, es importante tener control sobre los niveles de accesos que tendrán los usuarios dentro de la red, por lo que se pueden crear roles que administren el nivel de permisos de los usuarios.

2.1.1.1. *Firewall*

Los *firewalls* están diseñados para bloquear el acceso no autorizado a una computadora o a una red de computadoras. Estos dispositivos son configurados para permitir o denegar las comunicaciones de red, basándose en un conjunto de reglas establecidas.

Estos dispositivos pueden ser implementados en una computadora como una herramienta de software o también pueden ser un dispositivo de hardware. Generalmente son utilizados para prevenir que usuarios ajenos a la organización accedan a la intranet desde Internet.

Todo el flujo de información que se transporta por la red debe pasar por el *firewall*, el cual analiza las tramas de red que no cumplen con las reglas configuradas. Existen cuatro mecanismos de seguridad utilizados en los *firewalls*:

- Filtrado de paquetes: este tipo de *firewall* analiza todos los paquetes que circulan en la red y permite o deniega el mismo, dependiendo de las reglas definidas por el usuario. Estos *firewalls* son difíciles de configurar, sin embargo son muy eficaces y transparentes a los usuarios.

- Nivel de aplicación: los *firewall* de aplicación son de los más efectivos, establecen mecanismos de seguridad a aplicaciones específicas, como por ejemplo a los servidores Telnet y FTP, aunque generalmente bajan el rendimiento de la red.

- Nivel de circuito: estos *firewall* aplican mecanismos de seguridad cuando las conexiones TCP o UDP están siendo establecidas. Después de aplicar estos mecanismos y que se comprueba que la conexión es segura y que está activa, los paquetes pueden fluir libremente en la red.

- Servidores proxy: interceptan todos los mensajes que entran y salen de la red. Otra funcionalidad importante de este tipo de *firewall* es la de ocultar las direcciones de red verdaderas.

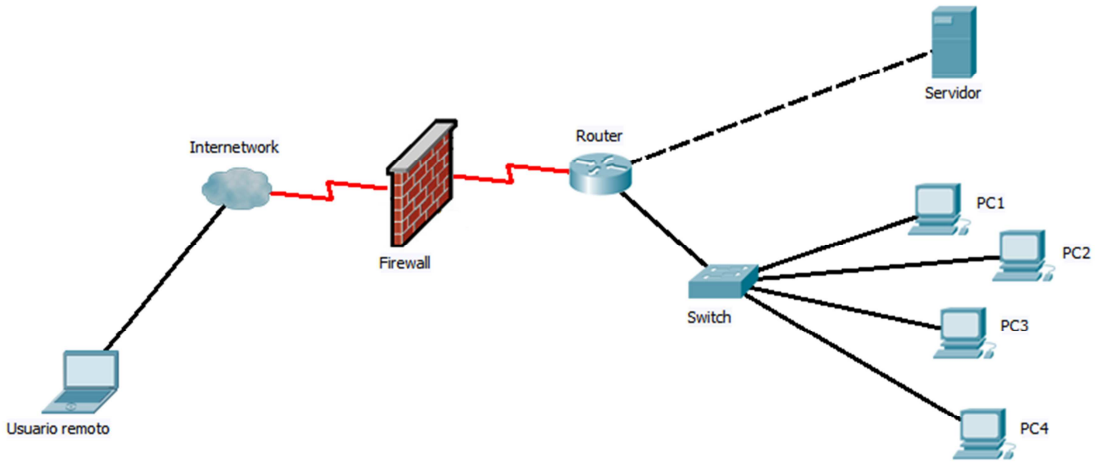
A continuación se presentan las ventajas y desventajas de un *firewall*:

Tabla I. **Ventajas y desventajas del *firewall***

Ventajas	Desventajas
Mantiene a los usuarios no autorizados fuera de la red.	No protege contra ataques de virus, por lo que la red puede ser infectada.
Permite analizar todo el tráfico de la red en un solo punto, lo que brinda más control sobre la misma.	Si algún usuario logra entrar a la red sin pasar por el *firewall*, su actividad no podrá ser monitoreada.
Permite crear grupos de usuarios y cada grupo tiene acceso a la red por medio de niveles de seguridad.	No brinda protección contra ataques de usuarios con acceso a la intranet y que buscan dañar la misma.

Fuente: elaboración propia.

Figura 4. **Ubicación del *firewall* en una red**



Fuente: elaboración propia.

2.1.2. Auditoría de la red física

La red física aglomera a todos los dispositivos de *hardware* que se encuentran interconectados. Entre éstos se encuentran los cables ya sean de cobre o de fibra óptica, los *routers*, *switchs*, computadoras, impresoras y escáneres.

Cuando se audita la parte física de una red, se debe hacer un análisis sobre los siguientes aspectos con los que la red debería cumplir:

- Debe existir control de acceso a las instalaciones con equipo de comunicación, de ser posible ubicarlo en lugar cerrado y con acceso limitado

- Los cables de comunicación deben estar protegidos para evitar la manipulación física de los mismos. Los cables de red no deben estar a la vista y de ser posible se deben separar de los cables de tendido eléctrico
- Deben existir mecanismos que controlen el tráfico en la red y que aseguren un flujo correcto sobre ella
- Procedimientos para la recuperación contra fallos en enlaces de la red
- Los cables deben estar correctamente identificados y deben existir procedimientos para su revisión periódica

2.1.3. Auditoría de la red lógica

La auditoría de la red lógica busca evitar un daño interno y debe ser capaz de detectar ataques que buscan saturar la red y minimizar su rendimiento.

Las medidas que se pueden tomar al respecto se presentan a continuación:

- Todos los usuarios deben poseer un nombre de usuario y una contraseña para acceder al sistema
- Verificar constantemente que las transmisiones se lleven a cabo únicamente entre el emisor y el receptor indicado en los paquetes de red
- Registrar en una bitácora todas las acciones llevadas a cabo por los usuarios en la red
- Utilizar protocolo seguros que permitan transmitir la información de forma cifrada
- Mantener control sobre el uso de dispositivos externos a la red, como por ejemplo memorias USB

Este tipo de medidas solo puede ser posible cuando los usuarios están debidamente identificados en la red, es decir si alguien accede anónimamente, será imposible llevar una bitácora con sus acciones o verificar sus transmisiones.

Cada usuario debe pertenecer a un grupo y este grupo debe contar con ciertos privilegios y restricciones, establecidos por los administradores de la red. Se deben tomar en cuenta los siguientes puntos en torno a los inicios de sesión de los usuarios:

- Todo usuario debe ingresar al sistema por medio de su usuario y contraseña
- Después de ingresar erróneamente cierta cantidad de veces su contraseña, su nombre de usuario deberá ser bloqueado
- Obligar a los usuarios a cambiar su contraseña periódicamente

A continuación se presentan diez puntos importantes que los administradores de red deberían tomar en cuenta:

- Poseer información sobre la tasa de errores en las transmisiones
- Contar con mecanismos para la detección de errores y su origen
- Todos los mensajes transmitidos deben estar en una bitácora que registre la computadora emisora y destino, así como la fecha y la hora
- La información importante para la organización solo puede ser accedida por personal autorizado
- Realizar análisis de riesgos para cada una de las aplicaciones utilizadas, de esta forma detectar vulnerabilidades en las mismas
- Cifrar todas las transmisiones en la red, para proteger la información transportada

- Proteger los *routers* o módems con contraseñas para que solo los usuarios autorizados puedan manipular su s*oftware*
- Crear reglas que impidan la instalación de programas no necesarios o no analizados por los administradores de red
- Impedir el acceso a los servidores
- Realizar periódicamente pruebas sobre la red para verificar su seguridad y encontrar vulnerabilidades

2.2. Evaluación de seguridad de un sistema de información

2.2.1. Importancia de la información

Generalmente cuando hablamos de informática, se tiende a asociar con las nuevas tecnologías, nuevo *hardware*, nuevo *software* o nuevos métodos de comunicación. Sin embargo muy a menudo olvidamos la información, que es la que hace posible la existencia de todos los dispositivos mencionados anteriormente.

Conocer el significado de la información dentro de un sistema informático es algo muy importante y es esencial cuando esta información es administrada mediante la tecnología moderna.

La información dentro de los sistemas de informáticos:

- Es almacenada en medios físicos tales como discos duros y es manipulada por los procesadores de las computadoras
- Dependiendo del tipo de información manejada por el sistema, está puede ser confidencial para la organización o para personas individuales

- Su correcta o incorrecta utilización queda en manos del usuario final
- Su integridad dependerá del nivel de seguridad del sistema en la que sea manejada

Generalmente la información se encuentra centralizada, y es de gran valor para la organización, sin embargo siempre está expuesta a sufrir de destrucción total o parcial, lo que involucra que no siempre esté disponible, por lo que puede causar pérdidas grandes para la organización que dependa de ella.

Cuando ocurre una catástrofe y el área física en donde se encontraban los servidores que almacenaban la información quedan inhabilitados o destruidos, la información también quedará inhabilitada o destruida si no se contaban con mecanismos o procedimientos para replicar la misma. Cuando la información está centralizada es más vulnerable. Un mecanismo para evitar que la información se encuentre centralizada en un solo lugar es la replicación.

2.2.1.1. Replicación de datos

Es el proceso de compartir información con la finalidad de asegurar la consistencia entre recursos redundantes, tanto de *software* como de *hardware*, para mejorar la fiabilidad, la tolerancia a fallos y la accesibilidad a la información. Se llama replicación de datos si los mismos datos están almacenados en múltiples dispositivos de almacenamiento. La replicación debe ser transparente al usuario. En los sistemas que replican datos existe la replicación activa y la replicación pasiva.

La replicación activa ocurre cuando en cada dispositivo de almacenamiento, se realiza la misma petición o la misma operación. La replicación pasiva ocurre cuando la operación se lleva a cabo en un solo dispositivo y posteriormente es transferido el resultado a todos los demás dispositivos de almacenamiento.

No debemos confundir los *backups* con la replicación. Un *backup* almacena una copia persistente de los datos por largos periodos de tiempo. Mientras que las réplicas son actualizadas frecuentemente y pierden rápidamente su estado histórico.

2.2.2. Características importantes de la información

2.2.2.1. Confidencialidad

La confidencialidad de la información se refiere a prevenir que esta sea divulgada a personas o sistemas no autorizados. Los sistemas intentan asegurar la confidencialidad por medio del cifrado de la información o limitando el número de ubicaciones en donde esta se pueda localizar, como por ejemplo: en bases de datos, archivos de bitácora o *backups*. También se restringe el acceso a estos lugares en donde se encuentra la información. Si alguien sin autorización obtiene la información, entonces se dice que ha ocurrido una falla de confidencialidad.

Los fallos de confidencialidad se pueden dar de muchas formas. Puede ser tan simple como que una persona que está sentada a nuestro lado mire nuestro número de tarjeta de crédito y contraseña, hasta algo más complicado, como por ejemplo: que alguien entre anónimamente a nuestra computadora desde un lugar remoto y que obtenga toda nuestra información personal. La confidencialidad es necesaria para mantener la privacidad de las personas cuya información esta almacenada en el sistema.

2.2.2.2. Integridad

Integridad de la información significa que esta no puede ser modificada sin que se tenga autorización para hacerlo y sin que quede registro en una bitácora, que avale que ese cambio fue realizado por cierta persona. La integridad de la información puede ser violada cuando se capturan los paquetes que viajan por la red y se modifica su contenido.

2.2.2.3. Disponibilidad

El objetivo de tener información almacenada en un sistema, es la de tener que esté disponible cuando sea necesario. Esto implica que los sistemas que la procesan, la infraestructura en la cual se guarda y se transporta y los mecanismos de seguridad utilizados para protegerla, deben estar siempre disponibles y funcionando correctamente.

Los sistemas alta disponibilidad buscan estar funcionando todo el tiempo, previniendo siempre aspectos como los apagones o fallas en el *software* o *hardware* de los servidores.

2.2.3. Virus informático

Un virus informático es un programa de computadora que tiene la capacidad de copiarse a sí mismo y de infectar la computadora. El objetivo de cualquier virus informático es el de dañar la computadora en donde se encuentra alojado. También posee la capacidad de difundirse de una computadora a otra. Un virus efectivo incrementa sus posibilidades de difundirse en otras computadoras por medio de la infección de archivos en una red o la infección de archivos del sistema que son accedidos por otras computadoras de la red.

Generalmente se confunde el término virus informático con otros tipos de *malware* que no poseen la capacidad de reproducirse. El *malware* incluye a los virus de computadora, los gusanos de computadora, los caballos de Troya, el *spyware* y el *adware*. Los gusanos de computadora explotan las vulnerabilidades de seguridad, para difundirse automáticamente hacia otras computadoras por medio de la red. Los caballos de Troya y los gusanos de computadora al igual que los virus pueden dañar la información o disminuir el rendimiento del sistema.

Para que un virus pueda ser capaz de replicarse el mismo, debe poder ejecutar código y escribirlo a memoria. Es por esta razón que muchos virus se adjuntan a archivos ejecutables que sean parte de programas legítimos. Cuando un usuario intenta ejecutar el programa infectado, el código del virus se ejecuta simultáneamente.

2.2.3.1. Estrategias de infección

Los virus se pueden dividir en dos tipos, basándose en su estrategia de infección cuando son ejecutados:

- Virus no residentes: estos virus son los más complicados y consisten en dos módulos. El módulo de búsqueda es responsable de buscar nuevos archivos para infectar. Por cada nuevo archivo ejecutable que el módulo de búsqueda encuentra, se llama al módulo de replicación, el cual se encarga de infectar el nuevo archivo.

- Virus residentes: poseen un módulo de replicación parecido al de los virus no residentes. Sin embargo, este módulo, no es llamado por el módulo de búsqueda. El virus carga el módulo de replicación en memoria cuando es ejecutado y se asegura que el módulo sea ejecutado cada vez que el sistema operativo es llamado para realizar cierta operación. Este módulo puede ser llamado por ejemplo cada vez que el sistema operativo ejecuta un archivo. En este caso el virus infecta todos los programas que son ejecutados en la computadora.

2.2.3.2. Métodos para evitar la detección

Para evitar la detección por parte de los usuarios, algunos virus emplean distintas formas de engaños. Por ejemplo algunos de los virus más antiguos se aseguraban que la fecha de modificación de su archivo infectado no cambiara, para hacer creer al usuario que ese archivo no había sido modificado. Algunos virus pueden infectar archivos sin incrementar su tamaño o dañar el archivo. Esto lo logran escribiendo en áreas sin utilizar de los archivos ejecutables. Estos virus son llamados de cavidad.

Algunos virus intentan evitar ser eliminados terminando los procesos asociados a los antivirus antes de que sean detectados. Mientras las computadoras y los sistemas operativos son cada vez más complejos, los virus tendrán que buscar nuevas técnicas para ocultarse.

2.2.4. Paradigmas organizacionales en cuanto a seguridad

Existen muchas formas de resolver problemas, sin embargo, generalmente se toma el proceso más conocido o el que esté de moda para resolver ese problema. Ese proceso obedece a un conjunto de ideas, de técnicas, de teorías y de metodologías. Estos procesos cambian o evolucionan conforme avanza la tecnología. A este proceso utilizado y aceptado por la mayor parte de las personas relacionadas con ese problema, se le llama paradigma.

Los paradigmas forman un papel fundamental para la ciencia, ya que a partir de ellos se desprenden las reglas que rigen el rumbo de las investigaciones y la forma en la que se resolverán los problemas por los que se originaron.

Los paradigmas cambian cuando estos no satisfacen la forma en la que se resuelven los problemas en los que son utilizados, esto sucede generalmente porque el paradigma no contempla cierta situación en especial. Es entonces cuando se produce una revolución científica, la cual busca modificar o cambiar el paradigma vigente.

Un auditor de redes de computadoras debe estar actualizado con respecto a los paradigmas que existen en las organizaciones, en cuanto a seguridad se refiere, esto es muy importante para que el auditor no se encuentre con procesos desconocidos.

A continuación se presentan algunos de los principales paradigmas de la seguridad informática:

- En la mayoría de las organizaciones se piensa que el proceso de auditoría tiene que ser planificado, implementado y que es responsabilidad únicamente del departamento de cómputo. Este paradigma debe ser cambiado y se tiene que saber que este proceso es responsabilidad tanto del usuario, como del departamento de auditoría interna

- Otro paradigma erróneo es el que involucra las instalaciones físicas. Muchas organizaciones piensan que al tener el equipo de cómputo y de comunicaciones en áreas con sistemas de seguridad, estos no podrán ser violados o accedidos de forma anómala. Sin embargo no se toma en cuenta el uso de dispositivos móviles o el acceso remoto a la intranet

- También, en algunas organizaciones, se piensa que los programas que ahí se utilizan son tan complejos que alguien ajeno a la organización no los va entender y que por lo tanto no se podrá robar información o que la información les será inútil

- En la mayoría de los casos, cuando se diseña un sistema de seguridad, no se toma en cuenta la posibilidad de un sabotaje interno, esto debido a que es el mismo personal que lo diseña el que realiza este tipo de acciones fuera de la ley. Es por eso que es importante auditar el proceso mismo del diseño de este tipo de sistemas

2.2.5. Consideraciones para la auditoría de la seguridad

A continuación se citarán las consideraciones inmediatas que se deben tener en cuenta para elaborar la evaluación de la seguridad de un sistema informático.

2.2.5.1. Uso de la computadora

El uso adecuado de la computadora ayuda a tener un mayor control sobre las operaciones que se realizan en ella y sobre las transmisiones que se originan y se dirigen hacia ella.

Algunos de los aspectos importantes que se deben tomar en cuenta en la auditoria de una computadora son las siguientes:

- Tiempo que un usuario ocupa en el uso de *software* que no está relacionado con sus labores
- Extracción del *software* que cuenta con derechos de autor, para su venta o uso ilegal fuera de la organización
- Tipos de accesos a redes externas o sistemas ajenos a la intranet, con los que cuenta la computadora

2.2.5.2. Sistema de acceso

La forma en la que se accederá al sistema es muy importante para la seguridad de la red, para evitar fraudes o robo de información se debe cumplir con las siguientes medidas:

- Control biométrico para ingresar a las instalaciones con equipo de comunicaciones
- Utilización de contraseñas de acceso
- Realización de análisis costo-beneficio en relación a la seguridad con la que se cuenta, esto debido a que a mayor seguridad mayor es el costo

2.2.5.3. Cantidad y tipo de información

Un punto de vulnerabilidad en un sistema de información ocurre cuando la información es ingresada al sistema, debido a que el tipo de información que se ingresa puede ser sensible y de alta importancia para la organización. La cantidad de información que se ingresa también es un factor de alto riesgo para el sistema.

Algunos de los aspectos a tomar en cuenta son los siguientes:

- Que la información se encuentre al alcance de personas que la utilicen con la finalidad de afectar a la organización
- La dependencia que se genera en la organización y los problemas que conllevaría si se diera el caso de una pérdida de información

2.2.5.4. Control de programación

Otro punto clave en la auditoría, es el control sobre el desarrollo del *software*. Cuando una organización posee un departamento de desarrollo, es importante que también se tengan políticas que controlen la forma en la que se desarrolla y que se verifique que la nueva herramienta realmente cumpla con las tareas para las que fue diseñada.

Es en el momento de la programación de las herramientas, cuando se puede cometer fraude ya sea de forma voluntaria o involuntaria, esto afectará directamente el desempeño de la organización, por lo que se debe controlar que:

- Todas las herramientas deben estar controladas por *software* para el control de versiones, para que de esta forma se puedan rastrear los cambios realizados, y la persona o personas que los realizaron
- Toda herramienta debe estar debidamente documentada, tanto a nivel técnico, como de usuario final
- Se debe verificar en la medida de lo posible que las herramientas desarrolladas no posean bombas lógicas
- Deben existir manuales sobre los procedimientos a tomar en caso de que una de las herramientas falle

2.2.5.5. Personal

El personal que forma parte del sistema a nivel administrativo es muy importante en la toma de decisiones sobre las políticas y las medidas de seguridad. Sin embargo, se debe tener el cuidado de no otorgar demasiados privilegios a este personal. Por lo que se presentan algunas recomendaciones a tomar en cuenta sobre el manejo del personal:

- El sistema a nivel operativo o técnico no debe depender de una sola persona. Se deben distribuir las responsabilidades entre varias personas
- Las personas a cargo del sistema deben estar debidamente capacitados en las tareas que van a realizar
- Llevar un buen control sobre la cantidad de personas a cargo y los niveles de acceso con los que cuentan
- El personal debe estar debidamente capacitado para poder actuar en situaciones de fallos en el sistema

2.2.5.6. Medios de control

Para que pueda existir una buena auditoría, la organización debe contar con medios de control, los cuales le permitan conocer el momento en el que se cometió un cambio en el sistema, el cual busca afectar la información que en él se maneja. Contar con estadísticas sobre el funcionamiento y el desempeño del sistema, también ayudará a la organización a detectar este tipo de intrusiones. Estas estadísticas actuarían como indicadores, los cuales informarían sobre las anomalías en el funcionamiento.

2.2.5.7. Rasgos del personal

Los hábitos del personal es un aspecto a tener en cuenta, generalmente las personas realizan acciones en el sistema sin darse cuenta. Estas acciones en la mayoría de los casos son involuntarias, debido a que los usuarios poseen malas prácticas en el uso de una computadora. Estas acciones pueden ocasionar:

- Negligencia al momento de realizar las tareas administrativas
- Toma de decisiones incorrectas
- Una mala administración del sistema

2.2.5.8. Instalaciones

Las instalaciones físicas en donde se almacena y resguarda el equipo de comunicaciones, son un punto de alto riesgo para la seguridad del sistema. Por lo que la auditoría deberá tomar en cuenta los siguientes puntos:

- Realizar evaluaciones constantes sobre todas las conexiones en el sistema
- Debe existir un diseño y manuales técnicos que especifiquen todo lo relacionado a las instalaciones
- Verificar un correcto flujo eléctrico entre los nodos de los equipos
- Analizar los efectos que podría ocasionar la variabilidad del flujo eléctrico sobre el *software* y *hardware*

3. CASO DE ESTUDIO

Una auditoría informática busca analizar y estudiar un entorno en particular, es por eso que los métodos y técnicas que se aplicaron en una auditoría puede que no funcionen en otra, debido a que en la práctica real es muy difícil encontrar dos escenarios semejantes. Si bien seria impráctico estandarizar una auditoria, si existen herramientas y métodos que un auditor puede utilizar para guiarse durante el desarrollo de ésta a partir de ellos deberá diseñar la forma en que la realizará.

3.1. Descripción de las herramientas de monitoreo

3.1.1. *WinAudit*

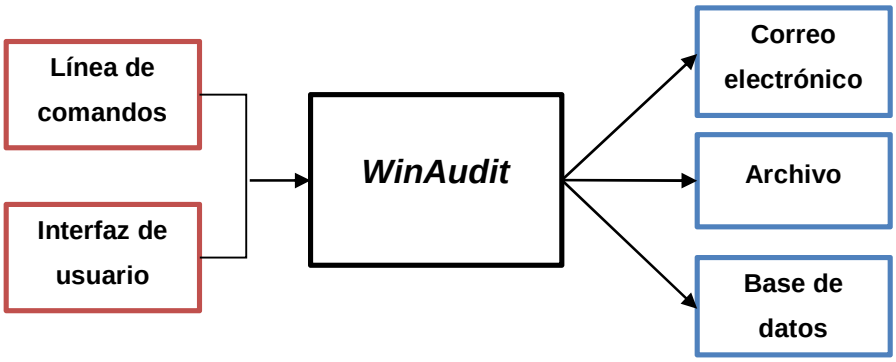
Es una herramienta de *software* que permite auditar computadoras que posean el sistema operativo *Windows*. Este programa examina todos los aspectos relacionados con la computadora. El reporte generado es desplegado como una página web, sin embargo puede ser guardado en varios formatos diferentes. Posee la funcionalidad de línea de comandos, esta es muy importante debido a que permite administrar el inventario de una red de computadoras de forma automática.

Es totalmente gratuito, soporta el escritorio remoto de *Windows* y no es necesario que sea instalado en la máquina en la que va a ser ejecutado. La forma en la que el programa genera el reporte es muy intuitiva y no se requiere de un gran nivel técnico para que este pueda ser entendido.

La versión utilizada será la 2.28.2 y los requerimientos mínimos del sistema son:

- Sistema operativo *Windows* 98 en adelante
- 128 MB de memoria RAM
- Procesador *Pentium*

Figura 5. **Forma de operación de *WinAudit***



Fuente: elaboración propia.

3.1.2. *Wireshark*

Es una herramienta para analizar paquetes. Generalmente es usada para el análisis y resolución de problemas en una red y para desarrollo de *software* y de protocolos de comunicación. Puede ser ejecutado tanto en sistemas *Linux*, como en sistemas *Windows* y *Mac OS X*. Generalmente la captura de paquetes de una interfaz requiere de permisos especiales en lagunas plataformas. Es por eso que algunas versiones de *Wireshark* deben ser ejecutadas con privilegios de súper usuario.

3.1.3. *Nmap*

Es una herramienta de código abierto para la exploración y la auditoria de seguridad de las redes informáticas. Está diseñada para escanear redes de gran tamaño, sin embargo también puede ser usado en una sola computadora. Este programa usa paquetes IP para determinar que terminales están disponibles en la red, así como para registrar los servicios que tienen activos. También identifica la versión del sistema operativo, el tipo de *firewall* que poseen, si es que tienen uno.

El programa muestra como salida una lista con los terminales escaneados, los puertos de estas terminales y su estado, es decir si están abiertos y funcionando o si están cerrados.

3.1.4. *RecueTime*

Es una herramienta en línea que permite monitorear el tiempo y la atención que los empleados le prestan a los distintos programas que utilizan en su computadora. Con los datos recopilados por esta herramienta un gerente puede determinar exactamente el tiempo que los empleados trabajan realmente, así como verificar que el *software* con el que deben trabajar esté siendo utilizado. Además este *software* nos brinda la funcionalidad de trabajo en equipo, en la cual, un usuario puede comparar su rendimiento con el rendimiento de otros usuarios.

Es importante mencionar que *RescueTime* no es una herramienta gratuita, sin embargo puede ser utilizado en su versión de prueba durante 15 días. Para poder utilizarlo primero se debe crear una cuenta en Internet para cada uno de los usuarios en el equipo de trabajo. Después se tiene que instalar el *Software* en cada una de estas computadoras.

Cuando cada usuario inicie el proceso de instalación, se le solicitará la identificación de la cuenta creada en Internet, en este momento la cuenta de Internet y la computadora en donde se está instalando el *software* quedan vinculadas, y todas las actividades realizadas en ella serán monitoreadas y enviadas al servidor en línea de *RescueTime*.

3.2. Caso de estudio de una auditoría informática

Para obtener un panorama más detallado de la auditoría informática, se presenta el desarrollo de un caso de estudio. El tema principal de este caso de estudio será la seguridad, y cada una de las áreas será estudiada en dos niveles distintos. El primer nivel consistirá en dividir en segmentos el área en cuestión. El segundo nivel dividirá a los segmentos en secciones.

Las áreas en las cuales se enfocará el caso de estudio son las siguientes:

- Seguridad del área lógica
- Procesos informáticos
- Seguridad del área física

Los objetivos de la auditoría llevada a cabo son:

- Realizar un análisis de la situación actual, en lo que a seguridad informática se refiere
- Verificar el nivel de eficiencia de los procesos de seguridad actuales

Este caso de estudio realizará la auditoría estudiando siete segmentos, a continuación se muestran los segmentos y sus secciones, los cuales conforman los dos niveles que estudiarán las áreas mencionadas:

- Estándares
  - Metodología de trabajo
  - Uso del *software*
- Sistema operativo
  - Control de acceso
  - Roles y usuarios
  - Bitácora de eventos
- *Software*
  - Control de acceso
  - Antivirus
  - *Firewall*
- Comunicaciones
  - Infraestructura
  - Protocolos
- Base de datos
  - Control de acceso
  - Bitácora de eventos
  - Replicación
  - *Backups*

- Procesos
  - Preventivos
  - Mantenimiento
  - Correctivos
- Aspectos físicos
  - Control de acceso
  - Física de datos
  - Equipos
  - Documentos

Generalmente, al realizar una auditoría informática, esta se divide en seis fases distintas. Estas fases conjuntas conforman en si la auditoría informática.

Las fases son las siguientes:

- Causas para realizar la auditoría informática
- Estrategias de la auditoría informática
- Asignación de pesos a los sectores de la auditoría informática
- Forma de operación de la auditoría informática
- Resultados obtenidos de la auditoría informática
- Creación del informe final

3.2.1. Causas para realizar la auditoría informática

La fase uno inicia el proceso de auditoría y estudia las causas que pueden llevar a un gerente a realizarla. Las personas que realizarán la auditoría deben conocer cada uno de estas causas, esto ayudará a los auditores a tener un mejor panorama del estado inicial de la organización.

Existen muchas causas por las cuales se puede iniciar una auditoría, algunas de ellas son:

- Por un mal rendimiento de la red informática
- Aumento desconocido de costos
- Sospecha de malas prácticas de parte de los empleados
- Por política de la organización
- Por aspectos legales

En este caso se busca realizar la auditoría informática a manera de dar a conocer al lector su procedimiento y todo lo que éste involucra.

3.2.2. Estrategias de la auditoría informática

Una vez que han sido definidas las causas por las que se llevará a cabo la auditoría se debe elegir la estrategia mediante la cual se desarrollará el proceso. Esta fase está conformada por dos actividades:

- Selección del personal que hará la auditoría
- Selección de los usuarios del lado de la organización a los cuales se les practicará la auditoria directamente

Los auditores deben tomar en cuenta el tamaño de la organización para diseñar el proceso acorde a las necesidades del cliente. Otro factor importante es el de la complejidad del trabajo, el cual va de la mano con el tamaño de la organización. Mientras más grande sea la infraestructura informática, más complejo será el trabajo de auditoría.

Esta estrategia deberá incluir aspectos como el equipo de *hardware* que se utilizará a lo largo del proceso, así como el recurso humano en total que será necesario ocupar. El equipo de auditores es el encargado de toda la logística del proyecto, deben coordinar y delegar las tareas sobre cada uno de los integrantes. De la estrategia dependerá el éxito o el fracaso de la auditoría, así como su costo.

Además el equipo debe elegir a la persona responsable de todo el proceso de auditoría y solicitar los nombres de los usuarios de la organización a auditar, que acompañaran al equipo auditor a lo largo del proceso.

3.2.3. Asignación de pesos a los sectores de la auditoría informática

En esta fase se realiza la asignación de pesos en relación a la importancia en cuanto a seguridad se refiere de cada uno de los sectores informáticos de la organización. Esta fase consta de las siguientes actividades:

- Asignación de pesos técnicos por parte del equipo auditor
- Asignación de pesos políticos por parte del personal de la organización a auditar
- Asignación de pesos finales

A cada segmento y a cada sección de los segmentos, se les debe asignar un peso. Existen tres tipos de pesos:

- Técnicos: son los pesos asignados por los auditores.
- Políticos: son los pesos asignados por el personal seleccionado de la organización a auditar.

- Finales: es el peso promedio para un segmento o sección, obtenido a partir del peso técnico y el peso político.

Cada una de las sumas de los pesos técnicos, políticos y finales debe ser 100. El área auditada entonces solo puede obtener un máximo de 100 puntos al finalizar la auditoría. La tabla de abajo muestra los pesos asignados a cada uno de los segmentos estudiados.

Tabla II. **Asignación de pesos a los segmentos**

Segmento	Peso técnico	Peso político	Peso final
Estándares	20	11	15,5
Sistema operativo	13	17	15,0
Software	13	17	15,0
Comunicaciones	13	11	12,0
Base de datos	15	14	14,5
Procesos	15	13	14,0
Aspectos físicos	11	17	14,0
Total	100	100	100

Fuente: elaboración propia.

Para los pesos de las secciones, el total de cada una de las sumas de los pesos técnicos, políticos y finales se ha establecido en 10.

Tabla III. **Asignación de pesos a las secciones del segmento cinco**

Sección	Peso técnico	Peso político	Peso final
Control de acceso	2	3	2,5
Bitácora de eventos	2	2	2,0
Replicación	3	1	2,0
Backups	3	4	3,5
Total	10	10	10

Fuente: elaboración propia.

Para poder ver la asignación de pesos a las secciones de los otros segmentos del caso de estudio en cuestión puede consultar el apéndice.

3.2.4. Forma de operación de la auditoría informática

Después de asignar pesos a los segmentos y a las secciones, debe iniciar la fase de entrevistas. Esta fase consta de las actividades:

- Creación de las entrevistas
- Realización de las entrevistas

Las entrevistas son una parte critica en el proceso de auditoría, si estas no están bien formuladas y si el entrevistado no colabora en responderlas lo más correctamente posible, todo el proceso de auditoría generará resultados inválidos, que no serán de mayor utilidad para la organización auditada.

El coordinador de la auditoría establecerá quien será el encargado de conducir las entrevistas, idealmente debe ser alguien con conocimientos en el área de informática. Es conveniente realizar entrevistas a la mayor cantidad de personas que sea posible y se les deben realizar muchas preguntas sobre el tema en cuestión. Se debe preparar el conjunto de preguntas que se realizan, sin embargo, se pueden agregar preguntas sobre la marcha, quedando a criterio del auditor las preguntas que realizará.

Una herramienta muy importante en esta fase son las listas de revisión y en ellas se plasman las preguntas que el auditor realizará. Una lista de revisión consta de una serie de preguntas, cada pregunta cuenta con un espacio para que el entrevistado las conteste. Al finalizar la entrevista el auditor debe asignar puntos a las respuestas obtenidas. Estos puntos pueden variar dependiendo de la persona que realiza la auditoría.

En este caso de estudio cada respuesta se calificará de 1 a 10, en donde 10 es la mejor puntuación para una respuesta. A continuación se muestran las listas de revisión utilizadas para el segmento cinco de bases de datos:

Tabla IV. **Lista de revisión para la bitácora de eventos de la base de datos**

Pregunta	Respuesta	Puntuación
¿Sabe usted si existe una bitácora de eventos en la base de datos?	Sí, tengo conocimiento de que existe una bitácora de eventos.	8
¿La bitácora de eventos almacena todos los eventos de la base de datos?	Almacena las inserciones, las modificaciones y las eliminaciones de los registros.	9

Continuación tabla IV.

¿Todas las tablas registran sus transacciones en la bitácora de eventos?	No, solo las más importantes.	6
¿Conoce usted la información que almacena la bitácora de eventos?	Si, guarda la llave primaria del registro que se afectó.	6
¿Existe una sola bitácora de eventos para todos los esquemas de la base de datos?	No, hay una bitácora por cada esquema.	7
¿Cuántos esquemas poseen en su base de datos?	Solo conozco tres, que son en los que trabajo, pero sé que hay más.	8
De las personas que tienen acceso a la base de datos, ¿Cuántas pueden modificar los registros de la bitácora de eventos?	Solo el administrador de la base de datos.	9
De las personas que tienen acceso a la base de datos, ¿Cuántas pueden consultar la información de la bitácora de eventos?	Solo el administrador de la base de datos.	9
Total		62 = 77,50%

Fuente: elaboración propia.

Tabla V. **Lista de revisión para el control de acceso a la base de datos**

Pregunta	Respuesta	Puntuación
¿Cuántas personas tienen acceso a la base de datos?	No tengo conocimiento exacto del número de personas que ingresan a la base de datos.	7
¿Quiénes tienen acceso a la base de datos?	Los programadores, el administrador de la base de datos y otras personas que realizan algunas consultas.	2
¿Qué permisos sobre la base de datos se les otorga a los programadores?	Depende de las acciones que necesiten realizar sobre las tablas en cuestión.	8
¿Existen roles y usuarios en sus base de datos?	Sí, pero no sé cuáles son.	3
¿Quién administra estos roles y estos usuarios?	El administrador de la base de datos.	7
Total		27 = 54,00%

Fuente: elaboración propia.

Tabla VI. **Lista de revisión para la replicación de la base de datos**

Pregunta	Respuesta	Puntuación
¿Existe replicación de su base de datos?	No, no existe replicación.	0
¿Estas bases de datos replicadas, se encuentra en distintas ubicaciones físicas?		0

Continuación tabla VI.

Pregunta	Respuesta	Puntuación
¿De qué forma realizan la replicación de su base de datos?		0
¿Cuántas replicaciones de su base de datos existen?		0
Total		0 = 0%

Fuente: elaboración propia.

Tabla VII. **Lista de revisión para los *backups* de la base de datos**

Pregunta	Respuesta	Puntuación
¿Se realizan *backups* a su base de datos?	Sí, si se hacen *backups* de la base de datos	9
¿Estos *backups* están programados?	No, se realizan de forma manual.	7
¿Realiza alguien de forma manual estos *backups*?	Sí, el administrador de la base de datos.	8
¿Cada cuánto se realizan los *backups*?	No lo sé.	2
¿En qué medio físico almacenan los *backups*?	No lo sé.	2
Total		28 = 56,00%

Fuente: elaboración propia.

Para poder ver los resultados de las listas de revisión de las secciones de los otros segmentos puede consultar el apéndice.

3.2.5. Resultados obtenidos de la auditoría informática

Ahora que ya se poseen las respuestas de los entrevistados, se procede a realizar los cálculos de los resultados obtenidos por los auditores. Esta fase está conformada por tres actividades, que son:

- Cálculo de los pesos finales de los segmentos y secciones
- Establecimiento de áreas a mejorar
- Establecimiento de áreas críticas

Una vez que se han calculados los pesos finales de los segmentos, ya se tienen los datos necesarios para generar un informe final de la auditoría.

A continuación se muestran los cálculos obtenidos para las secciones del segmento cinco:

Tabla VIII. **Porcentajes obtenidos para las secciones del segmento cinco**

Sección	Peso final	Porcentaje obtenido
Control de acceso	2,5	77,50%
Bitácora de eventos	2,0	54,00%
Replicación	2,0	0%
Backups	3,5	56,00%

Fuente: elaboración propia.

Ahora debemos calcular el peso final para el segmento cinco, esto lo obtenemos de la siguiente manera:

Figura 6. **Fórmula para calcular el peso final de un segmento**

$$Segmento\ N = \sum \left(\frac{p*O}{T} \right)$$

p → Peso final de la sección
O → Porcentaje obtenido en la sección
T → Peso máximo que se puede obtener en la sección

Fuente: elaboración propia.

Aplicando la fórmula anterior para la información obtenida del segmento cinco, obtenemos el siguiente peso final:

Figura 7. **Peso final del segmento cinco**

$$Segmento\ 5 = \frac{(2{,}5 * 77{,}5) + (2 * 54) + (2 * 0) + (3{,}5 * 56)}{10}$$

$$Segmento\ 5 = \boxed{\textbf{49,76\%}}$$

Fuente: elaboración propia.

Esa fórmula debe ser aplicada a todos los demás segmentos estudiados. Después de realizar estos cálculos se obtiene la tabla que se muestra a continuación:

Tabla IX. **Resultados obtenidos para los siete segmentos**

Segmento	Peso final	Porcentaje obtenido
Estándares	15,5	58,86%
Sistema operativo	15,0	82,30%
Software	15,0	85,10%
Comunicaciones	12,0	63,20%
Base de datos	14,5	49,76%
Procesos	14,0	58,88%
Aspectos físicos	14,0	78,46%
Total	100	68,26%

Fuente: elaboración propia.

Por último se muestran las gráficas obtenidas a partir de las tablas de los segmentos y las secciones. Estas gráficas estarán regidas por las siguientes reglas:

- La gráfica estará identificada por tres zonas de distinto color, los cuales son el color rojo, anaranjado y verde

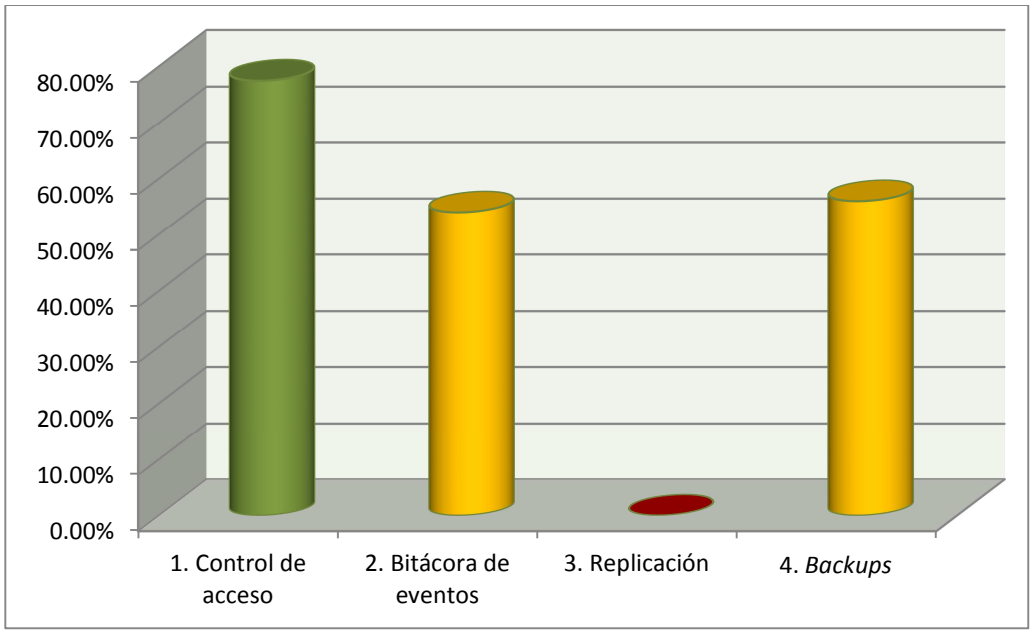
- El color verde identifica las áreas que están funcionando de la forma esperada y las acciones son a muy largo plazo

- En color anaranjado se marcan las áreas de la organización que pueden ser mejoradas, ya sea por medio de la optimización de sus procesos y estándares existentes o por medio de la implementación de algunos nuevos. Sin embargo las acciones sobre estas áreas no son urgentes

- Finalmente el color rojo identifica a las áreas críticas de la organización auditada, por lo que requiere de acciones inmediatas para corregir su rumbo

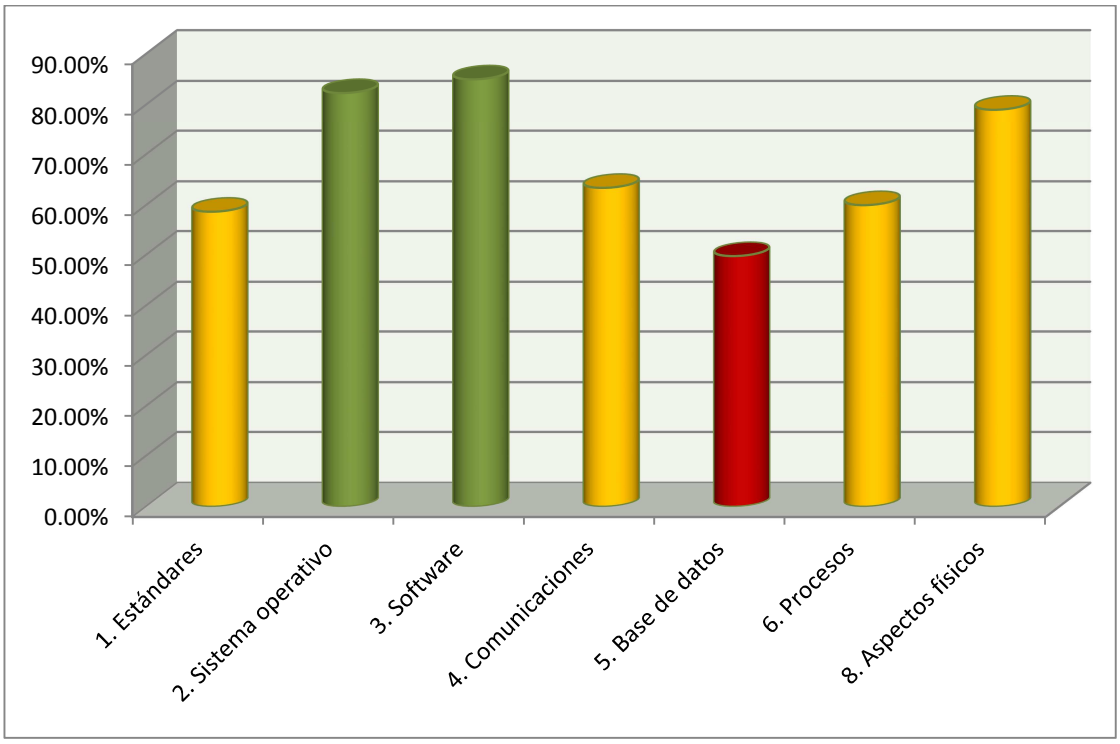
A continuación se muestran las gráficas del segmento cinco divido en secciones, y la gráfica general de todos los segmentos:

Figura 8. **Resultados de las secciones del segmento cinco**



Fuente: elaboración propia.

Figura 9. **Resultado de los segmentos analizados**



Fuente: elaboración propia.

3.2.6. Creación del informe final

Las actividades a desarrollar en esta fase son:

- Elaboración de recomendaciones
- Presentación preliminar del informe
- Entrega formal del informe al cliente

Ahora que ya se posee una base respaldada por documentos, se puede realizar un informe basado en la información que en ellos se contiene. La actividad en la cual el equipo auditor se reúne con la organización auditada para mostrarle un informe preliminar es muy importante y sirve para que el cliente pueda ver si el informe cumplirá con sus expectativas o si se debe cambiar o agregar algo.

El reporte debe incluir recomendaciones para cada una de las áreas afectadas. Las recomendaciones para las áreas rojas deben ser lo más detalladas posibles, brindado posibles soluciones al o los problemas detectados. El cliente debe ser capaz de entender a cabalidad estas recomendaciones. Las recomendaciones de las áreas amarillas, no poseen un nivel tan urgente como las primeras, pero de igual forma se deben incluir posibles soluciones a mediano plazo. Por último las recomendaciones de las áreas verdes no son obligatorias y deben ser lo más breve posibles, ya que a éstas no se les prestará atención inmediata.

3.3. Presentación de los resultados obtenidos

En la figura 9 (ver página 63) se puede apreciar que hay un segmento crítico en la organización auditada, esta es la de bases de datos. En este segmento el mayor problema se encuentra en sección de replicación. Esto se da porque esta organización no posee un proceso en el cual sea requerida la replicación de la base de datos.

Este proceso de replicación es muy importante tanto para seguridad de la información que se almacena en la base de datos, como para asegurar una mayor probabilidad de disponibilidad de la información cuando sea requerida. Se recomienda estudiar la posibilidad de adquirir equipos físicos y de capacitar al personal necesario, para que se ponga en marcha este proceso.

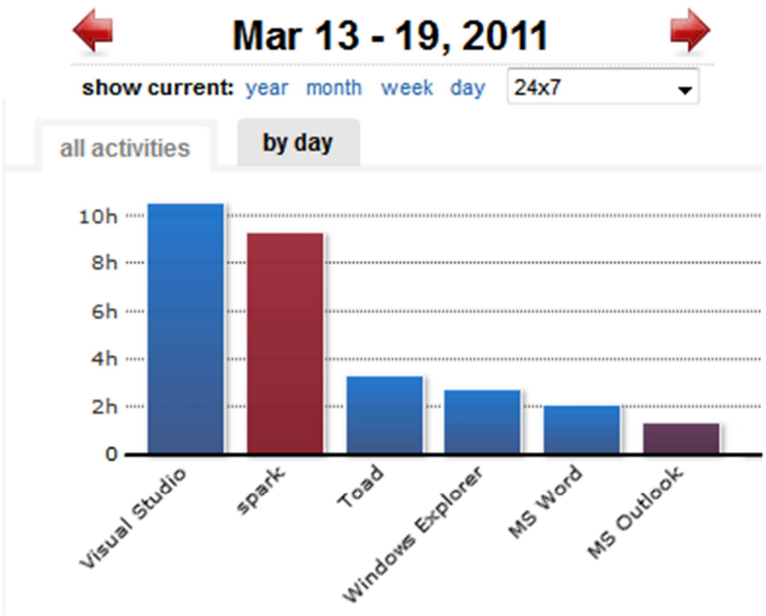
Otra sección débil en este segmento es la de bitácora de eventos. Una bitácora de eventos, es muy importante para poder tener un historial sobre todas las transacciones que se realizan en la base de datos y las tablas que son afectadas por estas transacciones.

En cuanto a los segmentos de color amarillo se refiere, en el segmento de estándares se deben reforzar los estándares ya existentes y se deben buscar métodos de motivación para que el usuario los adopte. En el segmento de las comunicaciones, se debe analizar la posibilidad de adquirir equipo de *hardware* más moderno y de volver a cablear algunas de las áreas en las cuales se ha detectado deterioro de los cables de red.

En el segmento de aspectos físicos se ha detectado la falta seguridad en el acceso a los servidores y a el equipo de *hardware* en general, se deben implementar medidas de seguridad que controlen de mejor forma el tipo de personas que ingresan a esas instalaciones, como por ejemplo el control biométrico.

También se realizó un análisis sobre la cantidad de tiempo que los usuarios ocupan en el *software* que poseen en sus computadoras, la herramienta utilizada fue *RescueTime* y a continuación se muestra una imagen con el análisis realizado a un programador:

Figura 10. **Gráfico por actividades de un programador**



Fuente: generado por el *software RescueTime.*

En la gráfica se puede apreciar que el programador pasa la mayor parte del tiempo utilizando el software de desarrollo, y que las actividades de ocio no consumen una gran parte de su tiempo.

Otro de los análisis se realizó utilizando el *software Nmap*, este programa nos permitió verificar los puertos que los usuarios tenían abiertos, los resultados se muestran a continuación:

Figura 11. **Resultados del análisis de puertos**

```
Initiating NSE at 12:38
Completed NSE at 12:38, 22.06s elapsed
NSE: Script Scanning completed.
Nmap scan report for    hectoralvarado
Host is up (0.00s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE       VERSION
25/tcp   open  smtp          Microsoft ESMTP 6.0.2600.5512
80/tcp   open  http          Microsoft IIS webserver 5.1
|_html-title: En construcci\xF3n
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  https?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
912/tcp  open  vmware-auth   VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
1036/tcp open  oracle        Oracle Database
3128/tcp open  http-proxy    Squid webproxy 2.7.STABLE6
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:  GET HEAD
3389/tcp open  microsoft-rdp Microsoft Terminal Service
MAC Address: 00:21:70:31:8A:26 (Dell)
Device type: general purpose
Running: Microsoft Windows XP
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows
```

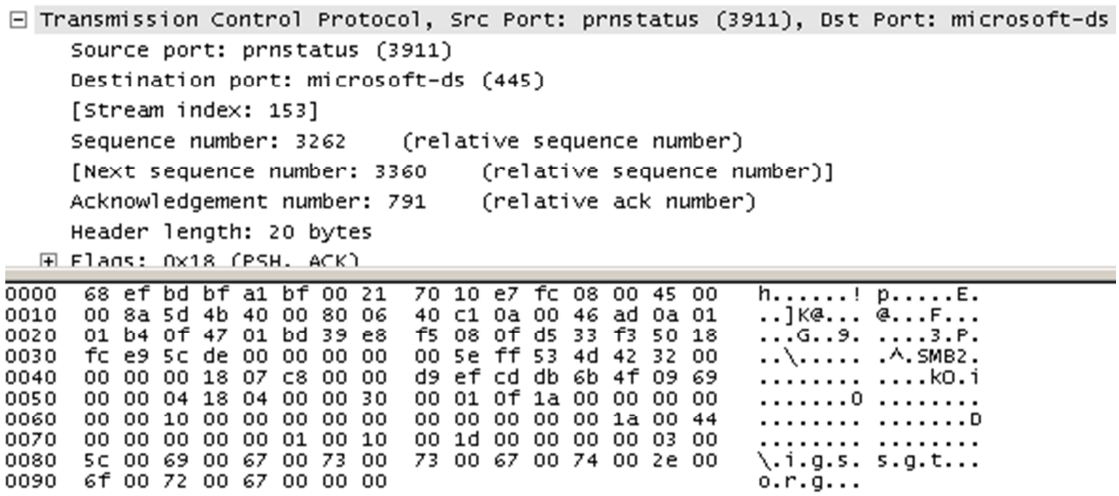
Fuente: generado por el *software Nmap.*

En esta gráfica se puede observar que el usuario posee algunos de sus puertos abiertos, por lo que el sistema no es del todo seguro y alguien podría escuchar a través de ellos.

En la figura 12 (ver página 68) se muestra el resultado de un análisis de *Wireshark*, en ella se puede apreciar un paquete que fue capturado, el cual contiene información sobre la conversación entre dos empleados. Este tipo de programas pueden parecer que invaden la privacidad, sin embargo en una red privada, cuando la información es muy sensible, es necesario verificar el tipo de información que viaja en la red.

Este tipo de herramientas permiten controlar esa información y prevenir el robo o el mal uso de la información de la organización.

Figura 12. **Resultados de paquetes capturados**



Fuente: generado por el *software Wireshark*.

Otra de las herramientas que se usó en este caso de estudio fue *WinAudit* y como se mencionó anteriormente, sirve para tener un inventario sobre las maquinas que se poseen, ya que genera un informe con el *software* que se tiene instalado, los componentes de *hardware* que conforman la terminal analizada, los servicios del sistema operativo, sus variables de entorno.

Además muestra un registro con los usuarios que han ingresado a la computadora, por lo que permite tener un buen control sobre las actividades de los usuarios en la computadora. La figura 13 (ver página 69) muestra una imagen con una pequeña parte del reporte generado.

Figura 13. **Cuadro general de una computadora analizada**

Vista General

Item	Value
Computer Name	SERGIO-LAPTOP
Domain Name	GRUPO_TRABAJO
Site Name	
Roles	Workstation, Server, SQL Server, Potential Browser, Master Browser
Description	
Operating System	Microsoft Windows 7 Home Premium 64-bit 64-Bit
Manufacturer	Hewlett-Packard
Model	HP Pavilion dv6 Notebook PC
Serial Number	CNF0190V3W
Asset Tag	
Number Of Processors	1
Processor Description	Intel(R) Core(TM) i3 CPU M 350 @ 2.27GHz
Total Memory	3904MB
Total Hard Drive	466GB
Display	AUO22EC, 15.3" (34cm x 19cm)
BIOS Version	HPQOEM - 1
User Account	Sergio
System Uptime	0 Days, 6 Hours, 20 Minutes
Local Time	2011-03-29 01:25:16

Fuente: generado por el *software WinAudit.*

4. PROPUESTA: LINEAMIENTOS PARA LA AUDITORÍA DE REDES DE COMPUTADORAS

Una auditoría, analiza y verifica los procesos o tareas diarias de una organización, con el objetivo de encontrar malas prácticas, mal funcionamiento de los procesos o áreas débiles. Debe ser practicada por un grupo de auditores de forma totalmente independiente a la gerencia.

Como ya se mostró en el caso de estudio, un auditor puede apoyarse en herramientas de s*oftware* que le ayudarán a monitorear los sistemas y la red de computadoras, pero también debe fundamentar su auditoría entrevistando directamente a algunos de los usuarios de la organización. Estas entrevistas le brindan información muy valiosa al auditor, debido a que son estos usuarios los que utilizan el sistema y el equipo de *hardware* constantemente.

Las conclusiones que se presentan en el informe final, deben ser tomadas únicamente como recomendaciones y quedará en manos de la gerencia decidir si las ejecutan o no y el momento más oportuno, dado que el auditor no cuenta con el poder necesario para llevar a cabo los cambios que propuso.

4.1. Señales de necesidad de una auditoría informática

Las empresas deben acudir a las auditorías cuando perciben señales de debilidad o mal funcionamiento, es importante saber identificar a tiempo estas señales, a continuación se presentan algunas de ellas:

4.1.1. Descoordinación y desorganización

Normalmente la desorganización ocurre cuando en una organización se cambian a una gran cantidad de empleados y la descoordinación sucede cuando se da una mala reestructuración de alguna área en particular, por lo que la podría suceder lo siguiente:

- Los objetivos del área de informática no están alineados con las metas de la organización
- La organización pasa por una etapa irregular y sus productos o servicios son entregados muy por debajo de su calidad habitual

4.1.2. Mala imagen e insatisfacción de los usuarios

Los empleados de la organización proporcionan una forma efectiva para detectar algunas de las debilidades del sistema, como por ejemplo:

- No se le brinda mantenimiento al equipo de cómputo y cuando estos fallan no son reparados prontamente
- Los requerimientos de los usuarios, en cuanto a cambios en el sistema no son atendidos oportunamente
- No se cumple con la entrega de los productos en las fechas planificadas en los cronogramas

4.1.3. Debilidades económico-financieras

Estas están relacionadas con el aspecto financiero del área de informática, generalmente sucede por el mal manejo del presupuesto del departamento. Esta debilidad se puede identificar mediante los siguientes síntomas:

- Los gastos exceden el presupuesto planificado
- El dinero del presupuesto que ha sido gastado, no ha beneficiado el área de informática
- Los gastos que si están relacionados con el área de informática no están siendo justificados adecuadamente

4.2. ¿Auditoría interna o auditoría externa?

Una vez que un gerente ha tomado la decisión de llevar a cabo una auditoría ayudado por las señales mencionadas, es necesario que determine si esta será realizada por un equipo interno, es decir, por personal de la misma organización o por personal externo. Para tomar esta decisión, primero debe conocer cuál es la diferencia entre la auditoría interna y la auditoría externa.

Básicamente una auditoría interna es llevada a cabo por personal que trabaja en la empresa auditada, así mismo los materiales utilizados son pagados por la empresa. El equipo que realiza esta auditoría es elegido por personal de la gerencia y puede ser disuelto al finalizar la auditoría si así lo desean.

Una de las mayores ventajas de contar con un equipo de auditoría interna es que puede este puede realizar auditorías periódicas, sin embargo, también tiene una desventaja bastante grande y es que en esta auditoría el equipo puede no tener una independencia total y la gerencia puede afectar su resultado final.

Por el contrario la auditoría externa es realizada por una empresa ajena, contratada por la empresa auditada. En este caso el resultado final es mucho más objetivo, debido a que el equipo que realiza la auditoría es totalmente ajeno a la gerencia de la empresa auditada.

Un aspecto que va definir si se realiza una auditoría interna o externa, es el económico. Una auditoría interna generalmente resulta mucho más costosa, debido a que debe obtener el *software* necesario y sus licencias respectivas, para llevarla a cabo, así como el recurso humano necesario. Por lo que para las pequeñas y medianas empresas puede ser más costoso. Generalmente son las empresas grandes, las únicas que pueden mantener un departamento de auditoría permanente.

4.2.1. Áreas de la auditoría informática a tomar en cuenta

La auditoría informática se puede dividir en dos ramas principales, cada una de estas agrupa distintas actividades a realizar por el equipo auditor. Estas ramas de la auditoría informática son:

- De organización: registra los cambios efectuados en la estructura organizacional del departamento de informática.
- De seguridad: se encarga de todos los aspectos relacionados con la seguridad informática.

Cada una de estas ramas puede ser auditada utilizando los siguientes criterios:

- Por su funcionamiento
- Desde el punto de vista de los usuarios
- Por la relevancia que recibe de parte de gerencia
- Desde el punto de vista de seguridad

4.3. Definición del objetivo principal de la auditoría informática

Una auditoría informática debe llevarse a cabo cuando los sistemas están funcionando completamente, ya que no tendría sentido realizar la auditoría cuando los sistemas no están en funcionamiento, debido a que no se detectarían los fallos que este pudiera tener. Dos de los objetivos fundamentales de toda auditoría informática deben ser:

- El buen funcionamiento del sistema
- La total operatividad del sistema

Estos dos objetivos pueden ser alcanzados aplicando una serie de controles técnicos globales y controles técnicos específicos.

4.3.1. Controles técnicos globales

Estos controles técnicos globales, buscan analizar y verificar que el sistema en funcionamiento tenga total compatibilidad con el sistema operativo instalado, además de verificar que el *hardware* con el que se cuenta también sea compatible con el sistema informático.

4.3.2. Controles técnicos específicos

Los controles técnicos específicos buscan analizar cada una de las aplicaciones de forma individual, su objetivo principal es verificar que estas realicen la tarea para la que fueron diseñadas de forma correcta. Estos controles varían dependiendo de la aplicación que está siendo objeto del análisis, debido obviamente a que cada aplicación funciona de forma diferente y sus tareas son distintas a las de otras aplicaciones.

El equipo de auditores debe solicitar toda la documentación técnica disponible para cada una de las aplicaciones a auditar, ya que es esta documentación la que les permitirá diseñar y realizar pruebas acorde a cada aplicación.

4.4. Técnicas para la auditoría informática

Un auditor debe intentar conseguir toda la información que le sea posible, para que de esta forma pueda generar un informe que aporte información valiosa a la gerencia a la hora de tomar decisiones. A continuación se presentan una serie de herramientas y técnicas que pueden ser utilizadas por los auditores para obtener información:

4.4.1. Cuestionarios

Generalmente los auditores inician su ejercicio auditor con una ronda de cuestionarios creados por él mismo. Estos cuestionarios son entregados al personal de la empresa auditada que fue seleccionado previamente. Los cuestionarios deben ser específicos y el auditor debe ser muy hábil en el área auditada, para obtener información relevante.

Al finalizar la ronda de cuestionarios el auditor deberá estudiar y analizar la información recabada, de tal modo que forme la base para los reportes que el auditor deberá generar.

4.4.2. Entrevistas

Las entrevistas son el primer acercamiento entre el auditor y el personal a auditar. Estas entrevistas se pueden llevar acabo de tres formas, las cuales se enumeran a continuación:

- Se le solicita al auditado la documentación específica sobre el equipo de *hardware* o el sistema que tiene a su cargo
- Se entrevista al personal sin seguir una línea de trabajo estricta, es decir, se les hacen preguntas improvisadas pero relacionadas con el tema en cuestión
- La entrevista toma un rumbo predefinido por el auditor, en donde se buscan respuestas concretas sobre el tema que al auditor le interesa

4.4.3. Listas de revisión

Un auditor con experiencia y que se desempeña de forma profesional en la materia, realiza sus cuestionarios de acuerdo a la situación en cuestión. Es importante que el auditor tenga claro que es lo que necesita saber. Las listas de revisión son un tipo de cuestionario en donde el entrevistado deberá responder a las preguntas formuladas, sin embargo, además de poseer preguntas, las listas de revisión tienen un espacio para que el auditor le asigne una puntuación a las respuestas del auditado. Esto ayudará al auditor a medir y a contrastar las áreas auditadas.

Los dos tipos de listas de revisión que un auditor puede utilizar son:

- De rango: las preguntas son respondidas por el auditado de forma libre.
- Binarias: las preguntas solo pueden ser respondidas con un sí o no.

Algunos de los aspectos más importantes que el auditor debe tomar en cuenta son:

- El auditado debe dar una respuesta clara y concluyente
- Se debe evitar que el auditado sea afectado por otras personas a la hora de responder las preguntas
- Deben ser respondidos única y exclusivamente por el auditado

Una técnica utilizada por los auditores para formular listas de revisión es la de repetir varias veces una pregunta, pero obviamente bajo una apariencia distinta. El objetivo de realizar esto es para identificar contradicciones que el mismo auditado pueda generar o contradicciones con otras personas auditadas. Cuando se detecten contradicciones el auditor deberá reformular las preguntas que llevaron a la contradicción y deberá pasar una nueva lista de revisión a los entrevistados.

Las listas de revisión son muy importantes a la hora de generar el informe final, ya que por medio de las puntaciones obtenidas para cada una de las secciones y de los segmentos de las áreas auditadas, se podrá generar un reporte en donde se le dé prioridad a ciertos segmentos por sobre otros. De esta forma la gerencia podrá tomar decisiones apoyándose en resultados concretos.

4.4.4. Trazas

En ciertas actividades de la auditoría, el auditor se verá en la necesidad de verificar que el *software* utilizado por los usuarios realice las funcionalidades para las que fue diseñado. Para llevar a cabo esto se deben emplear herramientas de *software* que permitan trazar los posibles caminos que los datos siguen a través de los programas y a la vez rastrear el camino seleccionado.

Las trazas permiten verificar que se cumplan a cabalidad las validaciones previstas en el diseño del programa, en ningún caso deben afectar o modificar el programa. Se deben prever horarios en los que se realizará esta actividad, ya que en algunas ocasiones estas herramientas suponen un incremento en la carga de los programas y de la red informática de la empresa.

4.4.5. *Logs*

Los *logs* son un registro que se puede encontrar en varios programas, en el sistema operativo y en las bases de datos. Básicamente es un historial que guarda registros sobre los cambios que fueron realizados, quién los realizó y la fecha y la hora en la que fueron realizados.

Son muy importantes ya que permiten conocer la actividad de los usuarios en el sistema. Para el auditor son una herramienta mediante la cual puede descubrir irregularidades llevadas a cabo por ejemplo en una base de datos.

4.5. Metodología de trabajo de la auditoría informática

Un auditor puede seguir la siguiente metodología para desarrollar su trabajo de auditoría:

- Definición de los objetivos y del alcance;
- Análisis de la situación actual de la empresa a auditar;
- Selección del recurso humano y de las herramientas a utilizar;
- Creación del plan de trabajo a desarrollar;
- Desarrollo del ejercicio de auditoría;
- Generación del informe con las conclusiones obtenidas.

4.5.1. Definición de los objetivos y del alcance

El trabajo de auditoría debe estar debidamente delimitado, las áreas de informática son muy extensas y si no se establecen los límites dentro de los cuales se va a desarrollar la auditoría, es muy probable que el resultado final no sea el esperado. Es por eso que el alcance juega una parte fundamental en la etapa inicial del proyecto y es necesario que al redactar el informe final se remarque este alcance.

El alcance va de la mano con los objetivos de la auditoría. Los objetivos ayudarán al auditor a fijar el camino por el cual se debe conducir la auditoría. Si los objetivos no están claros, entonces el trabajo no podrá tomar la dirección adecuada.

4.5.2. Análisis de la situación actual de la empresa a auditar

Para poder tener un buen panorama de la situación actual de la empresa a auditar es necesario llevar a cabo un estudio inicial. Este estudio debe abarcar las actividades relacionadas con el área de informática. A continuación se presenta una serie de aspectos que deben ser tomados en cuenta en el análisis.

4.5.2.1. Organización

El auditor necesita tener conocimiento de la estructura organizacional de la empresa que va a auditar, por lo que debe informarse acerca de los siguientes aspectos:

- Departamentos: identificar todos los departamentos dentro de la empresa e incluir la función principal de estos.
- Organigrama: el auditor debe obtener el organigrama general de toda la empresa.
- Relaciones de jerarquía: una vez que se posee el organigrama general, se debe verificar que este se cumpla, es decir, que se mantenga la jerarquía plasmada en él.
- Puestos de trabajo: se deben identificar todos los puestos existentes dentro de la empresa.
- Personas por puesto: el auditor debe identificar el número de personal existente por cada puesto de trabajo.
- Flujo de información: se debe realizar un flujo de información para cada uno de los departamentos identificados, en el cual se muestre el recorrido que realiza la información dentro de la empresa. Este recorrido debe estar en armonía con la jerarquía identificada en el organigrama.

4.5.2.2. Medio operacional

Un buen auditor debe conocer el medio en el que va a realizar la auditoría. Para tener un buen conocimiento de este medio es importante que el auditor conozca los siguientes puntos:

- Arquitectura del sistema: este punto se refiere tanto a la arquitectura de *software* utilizada como a la de *hardware*. De la arquitectura utilizada dependen muchos factores relacionados con la seguridad del sistema en cuestión.

- Inventario: el auditor deberá realizar un inventario de *software* y de *hardware*. La información recabada estará reflejada en un informe que detalle cada uno de los ítems inventariados.

- Comunicaciones: este punto abarca la red física de la empresa, así como todo el equipo de *hardware* relacionado. El auditor debe recabar información sobre todas las redes locales con que se cuente, así como las redes externas y los tipos de enlaces utilizados en la comunicación entre éstas.

- Ubicación geográfica: se debe identificar la ubicación geográfica de los equipos de transmisión de señal de la empresa, incluyendo también la ubicación las bases de datos y de los servidores.

4.5.2.3. Bases de datos y *software* institucional

Un buen estudio de la situación actual debe incluir información sobre el *software* utilizado por la organización y sobre las bases de datos que se poseen. Si bien en esta etapa no se profundizará en estos aspectos, es importante que se tenga conocimiento global sobre estos, para enfocar de mejor forma la auditoría.

Para lograr esto se deben analizar los siguientes aspectos:

- Obtener información sobre la existencia de sistemas de legado
- Realizar un análisis breve sobre el número de aplicaciones existentes, así como de su volumen y complejidad
- Hay que realizar un análisis sobre las bases de datos del sistema. La información más importante es la del tamaño de las bases de datos, su complejidad y el tipo de base de datos
- Si se cuenta con un departamento de desarrollo de *software*, se debe obtener información sobre la metodología que se utiliza para desarrollar las herramientas, la plataforma de desarrollo y la arquitectura utilizada
- Se debe recabar información sobre la documentación existente. Sobre la documentación que se cuenta, hay que verificar que tan importante es y si puede ser de ayuda en el momento de la auditoría

4.5.3. Selección del recurso humano y de las herramientas a utilizar

Una vez que se conoce de una forma bastante global la situación en la que se encuentra la organización, se puede proceder a seleccionar el recurso humano que se va a utilizar. Es en este momento cuando también se tiene que escoger las herramientas de *software* que ayudarán al auditor a realizar la auditoría.

Es importante que la selección del recurso humano se haga lo más cuidadosamente posible. El personal debe conocer el área que va a auditar y es recomendable realizar perfiles de auditores para cada una de las áreas en las que se va a realizar la auditoría.

4.5.3.1. Recurso humano

El número de personas que estarán involucradas en la auditoría es proporcional al tamaño de las áreas auditadas y los perfiles varían para cada una de las áreas, sin embargo, generalmente las auditorias son conducidas por profesionales graduados a nivel de licenciatura o maestría en el área que va a auditar.

A continuación se presentan algunos posibles perfiles que se pueden utilizar para los auditores:

- Administrador de bases de datos: tiene amplia experiencia en el manejo de bases de datos y conoce a fondo la forma en que operan.

- Profesional en informática: tiene experiencia y conocimientos en diversas áreas de la informática, pero no está especializado en una en específico. Generalmente se ha desempeñado más como analista de sistemas informáticos.

- Desarrollador de sistemas: posee mayormente experiencia en el desarrollo de sistemas, es el encargado de coordinar los proyectos. Conoce a profundidad las metodologías de desarrollo y tiene una alta capacidad de análisis.

- Técnico en informática: es experto en el manejo de los sistemas operativos y en el *software* de oficina, se desempeña básicamente como técnico en *help desk* y sabe resolver los incidentes de los usuarios.

- Técnico en redes: experto en el área de redes de computadoras, conoce sobre topologías, protocolos y sabe resolver problemas relacionados con mala conectividad entre redes locales y externas.

- Ingeniero en diseño de procesos: es un profesional con experiencia en el diseño o rediseño de procesos, es capaz de mejorar los procesos existentes para maximizar su eficiencia o de identificar nuevos.

4.5.3.2. Recurso material

El recurso material también juega un papel muy importante en la auditoría, el material de *hardware* se refiere al equipo físico que será auditado y el material de *software* se encarga de auditar ese *hardware*. Es importante establecer una agenda en donde se indique el horario en el que puede ser utilizado el equipo físico para que la auditoría no afecte el rendimiento del sistema en general.

El recurso material utilizado se detalla a continuación:

- *Software*: este recurso es muy importante para el auditor, generalmente se ejecutara cierto *software* sobre las computadoras auditadas, con el fin de determinar la forma de operación del sistema auditado. Otra finalidad puede ser la de monitorear la actividad del usuario dentro del sistema, para buscar actividades irregulares o procedimientos no permitidos por las políticas de la empresa.

- *Hardware*: este recurso siempre es brindado por la empresa auditada, debido a que es en el equipo de *hardware* de la empresa en donde se deben ejecutar los controles planificados, no tendría ningún sentido ejecutar la auditoria en un equipo externo a la organización auditada.

4.5.4. Creación del plan de trabajo a desarrollar

Cuando los recursos han sido asignados se puede proceder a diseñar el plan de trabajo, este plan debe ser realizado involucrando a todo el personal seleccionado, es decir, todo el equipo auditor. El plan de trabajo debe tomar en cuenta los posibles contratiempos que pudieran surgir durante la auditoría.

El equipo deberá tomar en cuenta ciertos aspectos, los cuales se listan a continuación:

- Las áreas que va a abarcar la auditoría, ya que puede ser realizada en todo el departamento de informática o sólo por áreas del mismo. El tamaño del departamento juega un papel importante en esta decisión

- Se crean las actividades que darán lugar a la auditoría

- Se establecen prioridades para las actividades creadas

- Estas actividades creadas son planificadas dentro de una agenda de trabajo con fechas y plazos, tomando en cuenta las prioridades asignadas

- Se le asignan actividades a cada uno de los recursos humanos seleccionados

- Se debe llegar a un acuerdo con la organización auditada para seleccionar el personal que será auditado

- Una vez seleccionado el personal que se auditará, se crea una agenda con la ronda de entrevistas

Después de haber concluido con las actividades de auditoría se procede a reunir toda la información obtenida para consolidarla en el informe final.

4.5.5. Desarrollo del ejercicio de auditoría

En esta etapa se realiza el ejercicio de auditoría utilizando las técnicas o métodos seleccionados. Estos métodos son totalmente independientes del área que se haya escogido para auditar. Es recomendable dividir la auditoría en áreas específicas, para que de esta forma el auditor se pueda enfocar en una sola área en particular y los resultados sean mucho más acertados.

- Métodos de trabajo:
  - Entrevistas
  - Listas de revisión
  - Muestreos
  - Recopilación de los datos obtenidos del auditado
  - Análisis y comparación de la información recopilada

- Herramientas:
  - *Software* de rastreo
  - *Software* de emulación de situaciones
  - *Software* de control

4.5.6. Generación del informe con las conclusiones obtenidas

Después de finalizar la auditoría, el equipo debe plasmar todos sus resultados y conclusiones en un informe final. Este informe reflejará el éxito o el fracaso de la auditoría, por lo que una mala presentación de los resultados puede representar que todo el trabajo realizado fue erróneo. Es necesario que se realicen varios borradores del informe y que éstos sean revisados conjuntamente con la gerencia de la organización auditada.

4.5.6.1. Estructura del informe final

La información básica con la que debe contar el informe final es:

- Fecha de inicio y de finalización de la auditoría
- Nombres del equipo auditor y su especialidad
- Nombres del personal auditado, así como sus puestos y sus responsabilidades dentro del sistema
- Herramientas utilizadas durante la auditoría
- Resumen de los sistemas informáticos auditados

Los apartados con los que puede contar el informe final se muestran a continuación.

- Objetivos y alcance
- Breve resumen de los temas principales de la auditoría
    - o Situaciones que condujeron a realizar la auditoría

- Cuerpo del reporte
  - Descripción de la situación actual
  - Actividades desarrolladas durante la auditoría
  - Áreas débiles identificadas y sus posibles amenazas al desempeño de la organización
  - Recomendaciones
  - Planes a corto, mediano y largo plazo

CONCLUSIONES

1. La firma digital es un mecanismo que permite certificar distintos tipos de entidades. Por medio de la firma digital un usuario puede confirmar que el sitio con el cual está intercambiando información es seguro y que efectivamente es quien dice ser.

2. La auditoría de computadoras, por medio de métodos de análisis y de estudio, busca identificar los posibles fallos en un sistema o las áreas más vulnerables, para corregir estas deficiencias.

3. Existen distintas técnicas que ayudan al profesional a realizar una auditoría informática. También existen herramientas de *software* especializado en la materia, que le ayudará a realizar análisis sobre el sistema auditado.

4. La criptografía es un método que permite realizar una comunicación segura. Mediante este método se pueden ocultar los mensajes de personas o usuarios no autorizados.

5. El modelo de interconexión de sistemas abiertos brinda una arquitectura en siete capas, la cual define estándares o protocolos para llevar a cabo la comunicación entre distintas redes.

6. Una auditoría puede ser realizada en distintos niveles de una red de computadoras. Se puede auditar tanto el *hardware* como el *software*, sin embargo, sobre qué áreas sea llevada a cabo dependerá de la importancia de cada una de ellas.

7. Un método de seguridad a nivel de bases de datos muy importante es el *backup*, ya que permite poseer una copia de seguridad de la información almacenada, de tal forma que si esta se llegara a perder, la información podría ser recuperada al punto en el que el *backup* fue creado.

8. Un sistema seguro debe ser capaz de garantizar los siguientes tres aspectos: confidencialidad, integridad y disponibilidad.

9. Replicar las bases de datos es un método muy efectivo para asegurar la disponibilidad y la integridad de la información en un sistema informático.

10. Un sistema seguro debe tener la capacidad de identificar las posibles amenazas, de notificar al administrador y de recuperarse de un ataque o de una perdida de información.

RECOMENDACIONES

1. Una auditoría de redes debe ser dirigida y realizada por profesionales expertos en el área, para que de esta forma se puedan crear los procedimientos adecuados.

2. Para que una auditoria tenga éxito, el equipo de auditores debe buscar obtener la total aprobación por parte de la gerencia y la colaboración de los usuarios que participaran en el proceso.

3. Cada auditoría es diferente, por lo que no se pueden utilizar los mismos procedimientos para distintos escenarios. El auditor debe ser capaz de ajustar sus métodos y técnicas para la situación en cuestión.

4. Antes de iniciar una auditoria se debe conocer el entorno y la situación del sistema, una vez que se conoce como está funcionando, se pueden definir los pasos a seguir.

5. La mejor protección contra los fallos y las amenazas siempre es la prevención, por lo que se deben crear reglas y políticas que regulen la actividad de los usuarios dentro del sistema.

6. Se deben programar *backups* a las bases de datos y estos deben ser periódicos, de tal forma que siempre exista uno reciente de la información que se encuentra almacenada.

7. El mantenimiento al sistema es otra forma de prevenir fallos. Un sistema al cual se le brinda el mantenimiento adecuado, tanto a nivel de equipo de *hardware* como de *software*, es menos probable que presente problemas de desempeño.

8. En algunas ocasiones las políticas implementadas afectan el rendimiento de los usuarios, por lo que se deben estudiar adecuadamente estas antes de llevarlas a cabo. Siempre debe existir un estudio previo.

9. No se debe pretender abarcar todo lo relacionado a la informática en una auditoría. Es mucho más factible dividir esta práctica en áreas o segmentos, mediante los cuales se les pueda dar una atención especializada a cada uno de ellos.

10. La auditoría siempre buscara identificar los problemas en un sistema y realizar recomendaciones para corregir estos defectos, sin embargo es tarea del departamento o de las personas a cargo de la informática crear los métodos y procedimientos adecuados para implementar estas recomendaciones.

BIBLIOGRAFÍA

1. *Auditoría a la seguridad de las redes*. [En línea]. [ref. de 15 diciembre de 2009]. Disponible en Web: <http://www.34t.com/box-docs.asp?doc=497>

2. BRAGG, Roberta; RHODES-OUSLEY, Mark; STRASSBERG, Keith. *Network security: the complete reference*. California: McGraw-Hill, 2003. 858 p.

3. *Certificado digital*. [En línea]. [ref. de 27 de julio de 2009]. Disponible en Web: <http://es.wikipedia.org/wiki/Certificado_digital>

4. GUTIÉRREZ MELO, Julián. *Auditoria aplicada a la seguridad en redes de computadores*. [En línea]. [ref. de 27 de diciembre de 2001]. Disponible en Web: <http://www.monografias.com/trabajos10/auap/auap.shtml>

5. JIMÉNEZ, José Alfredo. *Evaluación seguridad de un sistema de información*. [En línea]. [ref. de 03 de noviembre de 1999]. Disponible en Web: <http://www.monografias.com/trabajos/seguinfo/seguinfo.shtml>

6. MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. *Hackers secretos y soluciones para la seguridad de redes*. Madrid: McGraw-Hill, 2000. 800 p.

7. PELTIER, Thomas. *Information security policies, procedures, and standards*. Washington: Auerbach Publications, 2001. 312 p.

8. SAHAGÚN PEDRAZA, Marco Polo. *Seguridad informática*. [En línea]. [ref. de 20 de diciembre de 2004]. Disponible en Web: <http://www.monografias.com/trabajos16/seguridad-informatica/seguridad-informatica.shtml>

9. *Seguridad en redes: ¿Qué es? ¿Cómo lograrla?*. [En línea]. [ref. de 28 de febrero de 2008]. Disponible en Web: <http://www.abcdatos.com/tutoriales/tutorial/l10406.html>

10. SIYAN, Karanjit; HARE, C.; DÍAZ MENA, J. I. *Internet y seguridad en redes*. Madrid: Prentice Hall, 1996. 560 p.

11. TIPTON, Harold; KRAUSE, Micki. *Information security management handbook*. Washington: Auerbach Publications, 2008. 845 p.

APÉNDICE

Asignación de pesos a las secciones del segmento uno

Sección	Peso técnico	Peso político	Peso final
Metodología de trabajo	5	6	5,5
Uso del *software*	5	4	4,5
Total	10	10	10,0

Fuente: elaboración propia.

Asignación de pesos a las secciones del segmento dos

Sección	Peso técnico	Peso político	Peso final
Control de acceso	3	5	4,0
Roles y usuarios	4	2	3,0
Bitácora de eventos	3	3	3,0
Total	10	10	10,0

Fuente: elaboración propia.

Asignación de pesos a las secciones del segmento tres

Sección	Peso técnico	Peso político	Peso final
Control de acceso	3	5	4,0
Antivirus	3	3	3,0
Firewall	4	2	3,0
Total	10	10	10,0

Fuente: elaboración propia.

Asignación de pesos a las secciones del segmento cuatro

Sección	Peso técnico	Peso político	Peso final
Infraestructura	6	5	5,5
Protocolos	4	5	4,5
Total	10	10	10,0

Fuente: elaboración propia.

Asignación de pesos a las secciones del segmento seis

Sección	Peso técnico	Peso político	Peso final
Preventivos	3	4	3,5
Mantenimiento	4	2	3,0
Correctivos	3	4	3,5
Total	10	10	10,0

Fuente: elaboración propia.

Asignación de pesos a las secciones del segmento siete

Sección	Peso técnico	Peso político	Peso final
Control de acceso	3	4	3,5
Física de datos	3	2	2,5
Equipos	2	3	2,5
Documentos	2	1	1,5
Total	10	10	10,0

Fuente: elaboración propia.

Listas de revisión del segmento uno

Lista de revisión para la metodología de trabajo

Pregunta	Respuesta	Puntuación
¿Conoce las metodologías de trabajo utilizadas por su equipo de trabajo?	No, solo algunas.	7
¿Estás metodologías hacia qué tipo de trabajo están orientadas?	Hacia el desarrollo de sistemas y los procesos del área de informática.	9
¿Las metodologías tienen procesos y normas bien establecidos para situaciones particulares?	Sí.	9
¿Los desarrolladores siguen una metodología específica?	A veces.	6
¿De qué depende la metodología escogida para desarrollar sistemas?	Del tipo de producto que se tenga que desarrollar.	8
¿El mantenimiento a las herramientas también tiene una metodología asociada?	No.	2
¿Todos los miembros del equipo conocen las metodologías usadas?	No.	2
Total		43 = 61,43%

Fuente: elaboración propia.

Lista de revisión para el uso del *software*

Pregunta	Respuesta	Puntuación
¿El personal sigue reglas definidas para el uso correcto de las herramientas?	Solo para ciertas herramientas.	7
¿Estas reglas fueron creadas por el área de informática?	Sí.	9
¿Los usuarios fueron capacitados?	Algunos.	7
¿Quién definió que usuarios debían ser capacitados?	El gerente de cada área.	8
¿Existen manuales para cada una de las herramientas?	No.	1
¿Los manuales muestran todos los posibles escenarios con los que un usuario se podría encontrar?	No.	1
¿Cada cuánto capacitan a los usuarios?	Solo la primera vez.	6
Total		39 = 55,71%

Fuente: elaboración propia.

Porcentajes obtenidos para las secciones del segmento uno

Sección	Peso final	Porcentaje obtenido
Metodología de trabajo	5,5	61,43%
Uso del *software*	4,5	55,71%

Fuente: elaboración propia.

Peso final del segmento uno

$$Segmento\ 1 = \frac{(5,5 * 61,43) + (4,5 * 55,71)}{10}$$

$$Segmento\ 1 = \boxed{\textbf{58,86\%}}$$

Fuente: elaboración propia.

Listas de revisión del segmento dos

Lista de revisión para el control de acceso

Pregunta	Respuesta	Puntuación
¿Los usuarios poseen acceso a todas las funcionalidades del sistema operativo?	No.	9
¿Quién define a que tienen acceso los usuarios?	El área de informática.	9
¿Los usuarios pueden instalar programas en su computadora?	Solo algunos usuarios.	9
¿Todos los usuarios poseen los mismos permisos?	No.	9
¿La actividad de los usuarios es monitoreada?	No.	6
¿Utilizan herramientas especiales para monitorear a los usuarios?	No.	4
Total		46 = 76,00%

Fuente: elaboración propia.

Lista de revisión para los roles y usuarios

Pregunta	Respuesta	Puntuación
¿Cada usuario cuenta con su propio nombre de usuario y contraseña?	Sí.	9
¿Existen roles asociados a los usuarios?	Sí.	9
¿Quién define y crea los roles?	El jefe de informática.	9
¿Los privilegios de los usuarios están definidos por su rol?	Sí.	10
Total		37 = 93,00%

Fuente: elaboración propia.

Lista de revisión para la bitácora de eventos

Pregunta	Respuesta	Puntuación
¿Cuenta con una bitácora de eventos para las acciones en el sistema operativos?	Solo la que brinda por defecto el sistema operativo.	8
¿Cada una de las herramientas cuenta con su propia bitácora?	Algunas herramientas.	8
¿Quién tiene acceso a las bitácoras?	Los desarrolladores.	8
¿Cuándo ocurre un error, las bitácoras les ayudan a descubrir la fuente del problema?	En ocasiones.	8
Total		32 = 80,00%

Fuente: elaboración propia.

Porcentajes obtenidos para las secciones del segmento dos

Sección	Peso final	Porcentaje obtenido
Control de acceso	4,0	76,00%
Roles y usuarios	3,0	93,00%
Bitácora de eventos	3,0	80,00%

Fuente: elaboración propia.

Peso final del segmento dos

$$Segmento\ 2 = \frac{(4{,}0 * 76) + (3{,}0 * 93) + (3{,}0 * 80)}{10}$$

$$Segmento\ 2 = \boxed{\textbf{82,30\%}}$$

Fuente: elaboración propia.

Listas de revisión del segmento tres

Lista de revisión para el control de acceso

Pregunta	Respuesta	Puntuación
¿El uso del *software* está restringido por políticas internas?	Sí.	9
¿Quién definió estas políticas?	El área de informática.	7
¿Todos los usuarios están sujetos a ellas?	Sí.	9
¿El uso de Internet está restringido?	Sí.	9
Total		34 = 86,00%

Fuente: elaboración propia.

Lista de revisión para los antivirus

Pregunta	Respuesta	Puntuación
¿Todas las computadoras cuentan con antivirus?	Sí.	9
¿Los antivirus se actualizan periódicamente?	Sí.	9
¿Los usuarios pueden administrar las acciones del antivirus?	Algunos usuarios si pueden.	8
Total		26 = 87,00%

Fuente: elaboración propia.

Lista de revisión para el *firewall*

Pregunta	Respuesta	Puntuación
¿Su red cuenta con un *firewall*?	Sí.	9
¿Este *firewall* es un *software* instalado en un servidor o es un dispositivo físico?	Es un *software*.	9
¿Quién administra las reglas usadas por el *firewall*?	El administrador de la red.	9
¿Utiliza otro tipo de herramientas para filtrar o analizar el tráfico en su red?	No.	6
Total		33 = 82,00%

Fuente: elaboración propia.

Porcentajes obtenidos para las secciones del segmento tres

Sección	Peso final	Porcentaje obtenido
Control de acceso	4,0	86,00%
Antivirus	3,0	87,00%
Firewall	3,0	82,00%

Fuente: elaboración propia.

Peso final del segmento tres

$$Segmento\ 3 = \frac{(4{,}0 * 86) + (3{,}0 * 87) + (3{,}0 * 82)}{10}$$

$$Segmento\ 3 = \boxed{\textbf{85,10\%}}$$

Fuente: elaboración propia.

Listas de revisión del segmento cuatro

Lista de revisión para la infraestructura

Pregunta	Respuesta	Puntuación
¿Posee un inventario de todo su equipo físico?	Sí.	8
¿Brinda mantenimiento a su equipo?	Sí.	9
¿Los cables se encuentran debidamente identificados?	La gran mayoría.	7
¿Posee un diagrama general de su infraestructura?	Sí.	7
Total		31 = 74,00%

Fuente: elaboración propia.

Lista de revisión para los protocolos

Pregunta	Respuesta	Puntuación
¿Posee procedimientos y protocolos para el mantenimiento de su equipo?	Solo para cierto tipo de equipo.	7
¿Cuándo un equipo falla, existe alguna guía que indique el procedimiento a seguir?	No.	3
Total		10 = 50,00%

Fuente: elaboración propia.

Porcentajes obtenidos para las secciones del segmento cuatro

Sección	Peso final	Porcentaje obtenido
Infraestructura	5,5	74,00%
Protocolos	4,5	50,00%

Fuente: elaboración propia.

Peso final del segmento cuatro

$$Segmento\ 4 = \frac{(5{,}5 * 74) + (4{,}5 * 50)}{10}$$

$$Segmento\ 4 = \boxed{\textbf{63,20\%}}$$

Fuente: elaboración propia.

Listas de revisión del segmento seis

Lista de revisión para procesos preventivos

Pregunta	Respuesta	Puntuación
¿Implementan en su equipo de trabajo procedimientos para evitar fallas en los sistemas?	En algunas ocasiones.	5
¿Qué tipo de procedimientos implementan?	No estoy seguro.	4
¿Hacia qué se orientan estos procedimientos?	Al funcionamiento de las herramientas.	7
¿Quién define los procedimientos?	El jefe de informática.	6
Total		22 = 55,00%

Fuente: elaboración propia.

Lista de revisión para el mantenimiento

Pregunta	Respuesta	Puntuación
¿Cada cuánto tiempo le dan mantenimiento al sistema?	Depende del programa o del dispositivo.	6
¿Recibe mantenimiento de parte de un equipo especializado?	Sí.	8

Continuación lista de revisión para el mantenimiento.

¿Los dispositivos físicos son atendidos por técnicos capacitados?	En ocasiones.	6
¿Quién define estos controles?	El jefe de informática.	7
Total		27 = 66,00%

Fuente: elaboración propia.

Lista de revisión para procesos correctivos

Pregunta	Respuesta	Puntuación
¿Cuando ocurre un error, existen procedimientos definidos sobre los pasos a seguir?	Sí, en la mayoría de los casos.	6
¿Estos procedimientos ayudan a identificar la causa del problema?	Sí.	7
¿Los procedimientos actuales ayudan a reparar el fallo?	Muy pocas veces.	4
Total		17 = 56,67%

Fuente: elaboración propia.

Porcentajes obtenidos para las secciones del segmento seis

Sección	Peso final	Porcentaje obtenido
Preventivos	3,5	55,00%
Mantenimiento	3,0	66,00%
Correctivos	3,5	56,67%

Fuente: elaboración propia.

Peso final del segmento seis

$$Segmento\ 6 = \frac{(3{,}5 * 55) + (3{,}0 * 66) + (3{,}5\ * 56{,}67)}{10}$$

$$Segmento\ 6 = \boxed{\textbf{58,88\%}}$$

Fuente: elaboración propia.

Listas de revisión del segmento siete

Lista de revisión para el control de acceso

Pregunta	Respuesta	Puntuación
¿Existe algún tipo de control para ingresar a las instalaciones?	Sí.	8
¿Quién define los controles a implementar?	Un equipo encargado de las normas de seguridad.	7
¿Las personas autorizadas cuentan con algún tipo de identificación?	Sí.	8
¿Quedan registradas las entradas y salidas de todas las personas?	Sí.	9
¿Hay algún tipo de control biométrico?	Solo para algunas áreas.	7
¿Existen cámaras de seguridad en la ubicación de los servidores?	Sí.	8
Total		47 = 78,33%

Fuente: elaboración propia.

Lista de revisión para el área física de datos

Pregunta	Respuesta	Puntuación
¿Los equipos se encuentran en un lugar con vigilancia?	Sí.	9
¿Poseen alarmas o cámaras de vigilancia?	En algunos lugares.	7
¿Se conoce que equipo puede abandonar las instalaciones?	Sí.	7
Total		23 = 76,67%

Fuente: elaboración propia.

Lista de revisión para los equipos

Pregunta	Respuesta	Puntuación
¿Los servidores se encuentran fuera del alcance de los usuarios y personas ajenas a informática?	Sí.	8
¿El lugar en donde se encuentran los servidores posee refrigeración?	Sí.	8
¿Los dispositivos físicos están en un lugar seguro?	Sí.	9
¿Hay guardias que vigilen durante la noche los servidores?	Sí.	8
Total		33 = 82,50%

Fuente: elaboración propia.

Lista de revisión para los documentos

Pregunta	Respuesta	Puntuación
¿Existen políticas para el control de la documentación de los sistemas?	Sí, pero no en todos los sistemas.	7
¿Quién controla el acceso a esos documentos?	El encargado de cada sistema.	8
¿Pueden salir los documentos de las instalaciones?	Algunos.	7
¿Cómo se aseguran que los usuarios no extraigan los documentos?	Mediante controles constantes y políticas de seguridad implementadas.	8
Total		30 = 75,00%

Fuente: elaboración propia.

Porcentajes obtenidos para las secciones del segmento siete

Sección	Peso final	Porcentaje obtenido
Control de acceso	3,5	78,33%
Física de datos	2,5	76,67%
Equipos	2,5	82,50%
Documentos	1,5	75,00%

Fuente: elaboración propia.

Peso final del segmento siete

$$Segmento\ 7 = \frac{(3{,}5 * 78{,}33) + (2{,}5 * 76{,}67) + (2{,}5 * 82{,}5) + (1{,}5 * 75)}{10}$$

$$Segmento\ 7 = \boxed{\textbf{78,46\%}}$$

Fuente: elaboración propia.