
**UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE**

**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

MAESTRÍA DE EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS II

# “Auditoría de la gestión de seguridad de la Wan de la Cacpe Loja a nivel físico y lógico”

TESIS DE GRADO

**Autor**: Jaramillo, Carlos Miguel

**Tutor:** Ing. Torres, José Luis

SANGOLQUI, JULIO 2014

**Certificado director – codirector**

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

# CERTIFICADO

Ing. José Luis Torres MBA

**CERTIFICAN**

Que el trabajo titulado "Auditoría de la Gestión de Seguridad de la WAN de Cacpe Loja a nivel físico y lógico", realizado por Carlos Miguel Jaramillo Castro, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Debido a la culminación y buena forma del presente documento, si recomiendo su publicación.

El mencionado trabajo consta de un documento empastado y un disco compacto el cual contiene los archivos en formato portátil de Acrobat (pdf). Autorizan a Carlos Miguel Jaramillo Castro, que lo entregue a Ing. Rubén Arroyo, en su calidad de Director de la Carrera.

*Sangolqui, Julio del 2014*

Ing. José Luis Torres MBA

DIRECTOR

**Autoría de responsabilidad**

UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE

MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

# DECLARACIÓN DE RESPONSABILIDAD

*Carlos Miguel Jaramillo Castro*

DECLARO QUE:

El proyecto de grado denominado "Auditoría de la Gestión de Seguridad de la Wan de Cacpe Loja a nivel físico y lógico", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

*Sangolqui, Julio del 2014*

Carlos Miguel Jaramillo Castro

**Autorización (publicación biblioteca virtual**)

UNIVERSIDAD DE LAS FUERZAS ARMADAS

ESPE

MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

**AUTORIZACIÓN**

Yo, Carlos Miguel Jaramillo Castro

Autorizo a la UNIVERSIDAD DE LA FUERZAS ARMANDAS-ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo "Auditoría de la Gestión de Seguridad de la Wan de Cacpe Loja a nivel físico y lógico", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

*Sangolqui, Julio del 2014*

_____

Carlos Miguel Jaramillo Castro

# DEDICATORIA

Este proyecto de Tesis está dedicado muy especialmente a mi familia, quienes me han sabido apoyar incondicionalmente para la culminación de mi carrera profesional. A todas las personas que me han ayudado a ser una mejor persona y profesional en el proceso de mi vida.

*Jaramillo Castro Carlos Miguel*

## AGRADECIMIENTO

A Dios, que me llena de Fe para seguir adelante. De manera especial a mis padres, por su esfuerzo confianza y dedicación para ayudarme a cumplir una meta más en mi vida. A las personas que me han extendido su mano cuando yo los necesitaba. A la CACPE Loja, que me abrió sus puertas para la elaboración de la auditoría y a la Ing. Verónica Quinde España, Directora de Tecnología de la CACPE Loja, por su colaboración y brindarnos la ayuda e información necesaria para la culminación de este proyecto. Al Ing. José Luis Torres y a la Ing. Nancy Velásquez, por su guía y conocimientos que me ayudaron para la culminación total del tema propuesto.

*Jaramillo Castro, Carlos Miguel*

**ÍNDICE GENERAL**

# ÍNDICE TABLAS

# Índice Gráficos

## RESUMEN

La Cooperativa, es una entidad financiera nacida hace más de 20 años, desde su aparición en el mercado, ha impulsado nuevos servicios para la ciudadanía, para lo cual ha implementado equipos y sistemas informáticos, que han aportado considerablemente en el desarrollo de cada uno de los procesos. En la actualidad, ha implementado un Data Center, donde se encuentran los activos informáticos, sistemas informáticos, en los que se procesa toda la información. También se encuentran ubicados los sistemas de redes, telecomunicaciones y servicios, que son utilizados por el personal ubicado a nivel de las provincias de Loja, El Oro y Zamora Chinchipe. De la información que se genera, procesa y acopia en los servidores y sistemas de almacenamiento, son de carácter confidencial y sumamente critica. Para garantizar la seguridad de esta información, se ha tomado en consideración la implementación de controles que garanticen la confidencialidad, integridad y disponibilidad de la misma. El objetivo es evaluar la gestión de la seguridad tanto a nivel físico como el lógico, para lo cual se utilizó normativas y estándares aceptados a nivel internacional, para mejorar las condiciones de seguridad en el ámbito informático. Para la aplicación de las normativas y la obtención de resultados, se ha utilizado la metodología descriptiva. Para la recolección de información se utilizó normas como la ISO 27002, con la metodología White Box de Auditoría. Finalmente, para la obtención de resultados se utiliza la metodología basada en riesgos con lo cual se obtuvieron los porcentajes de riesgos altos, medios o bajos.

**ACTIVO INFORMÁTICO, AUDITORÍA INFORMÁTICA, SGSI, ISO/IEC 27001:2005, HALLAZGOS.**

## ABSTRACT

The Cooperative, is a financial institution founded over 20 years ago, since its appearance in the market has prompted new services for the public, for which it has deployed teams and computer systems, during this time has contributed significantly to the development of each of its processes. Currently, has implemented a Data Center, which are arranged each computing assets, plus computer systems where all information is processed. Within the same network systems, telecommunications and services that are used by the main office, but its agencies and branches also located in the provinces of Loja, El Oro and Zamora Chinchipe. From the information generated, processed, and collected on servers and storage systems, we can mention the following: customers, credit, accounting, investment, among others, which is confidential and highly critical. To ensure the security of this information is taken into account the implementation of controls to ensure the confidentiality, integrity and its availability, which is proper managed by authorized persons. The goal set for this work was to evaluate the safety management, both physical and logical level, for which regulations and internationally accepted standards are used and have been implemented by many different kind companies to improve security conditions in the computer field. For the implementation of policy and outcome, we used descriptive methodology. To collect information standards such as ISO 27002, the White Box Audit methodology was used. Finally, to obtain the results risk-based methodology is used, whereby the percentages of high, medium or low risk were obtained.


**COMPUTER ACTIVE, COMPUTER AUDIT, ISMS, ISO/IEC 27001:2005, FINDINGS.**

# CAPÍTULO 1

## 1.1. Introducción

Hoy en día, toda organización requiere medidas de protección, es un requisito indispensable para las empresas del siglo XXI, el aplicar metodologías de seguridad, tanto físicas como lógicas. Prácticamente la información se convirtió en el tesoro más grande, por lo tanto la seguridad y cuidado de estás, a través de las redes, permite que una organización prevalezca a lo largo del tiempo.

En la era de la información, todo ordenador es accesible desde Internet, y, en especial los servidores, están expuestos diariamente a un elevado número de ataques. Un servidor poco actualizado, con contraseñas débiles o sin una correcta planificación de la seguridad es una víctima fácil.

Así mismo, un inadecuado diseño de las redes corporativas, tanto a nivel local, como en los enlaces de comunicación, una inadecuada configuración de los equipos, fallo en el software o hardware, o una debilidad en el proceso operacional o contramedida técnica, provoca vulnerabilidades que pueden ser utilizadas por personas inescrupulosas, a quienes se les facilitaría cometer actos ilegales o robo de información.

Al aplicar diferentes análisis de comprobación, al Data Center, a las redes, sistemas de comunicación y procesos críticos, se podrá evaluar la seguridad, tanto física como lógica, ejecutando un análisis activo de los diferentes sistemas existentes, en busca de posibles vulnerabilidades.

La intención del proyecto es realizar la auditoría de gestión de seguridad de la WAN, tanto a nivel físico como lógico, y, de esta manera, determinar la posibilidad de la existencia de vulnerabilidades, originadas por inadecuadas configuraciones.

Todos los problemas de seguridad descubiertos, serán presentados al propietario de los procesos, generando un plan de acción que sea aplicable, para la mitigación de los mismos.

## 1.2. Justificación e Importancia

La información, los procesos, sistemas, redes que le brindan apoyo, constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información, son esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Uno de los mayores problemas que afronta la esfera informática, es el nivel de la Seguridad de la Información (SI). El proceso de auditoría de sistemas, a nivel de seguridad, es uno de los aspectos fundamentales, para medir el estado de la seguridad en los servidores y en las redes de los sistemas informáticos.

La auditoría de sistemas, comprende la revisión y la evaluación de los controles, sistemas, procedimientos informáticos, equipos de cómputo y comunicación de la organización, que participan en el procesamiento de la información, a fin de que, por medio del señalamiento de cursos alternativos, se logre una utilización más eficiente y segura, que servirá para una adecuada toma de decisiones.

Por lo tanto, la auditoría de la gestión de seguridad de la WAN a nivel físico y lógico, debe comprender, no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que, además habrá que evaluar, los sistemas de información en general, desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

La auditoría de sistemas, es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios, para que los sistemas sean confiables y con un buen nivel de confiabilidad. Además se debe evaluar todo: informática, organización de centros de información, hardware y software.

Los objetivos principales que constituyen la auditoría de sistemas son: el control de la función informática, el análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento de la normativa existente y la revisión de la eficaz gestión, de los recursos informáticos, materiales y humanos. Este tipo de auditoría, sobre la gestión de la seguridad de la WAN, se realizará sólo, bajo el consentimiento

escrito de los propietarios de los sistemas y demás infraestructura tecnológica, sobre los cuales vamos a realizar las pruebas; requisito indispensable tanto para el auditor, como para el auditado.

En este tipo de análisis, además de descubrir las vulnerabilidades presentes en los equipos, se procede al diseño y recomendación, para mitigar las mismas, con el objetivo de evaluar las repercusiones reales de cada una de ellas y la peligrosidad específica en su entorno.

### 1.3. Planteamiento del problema

La auditoría de gestión de seguridad de la WAN, tanto a nivel físico como lógico, incluirá un examen de la arquitectura, la revisión de la documentación, entrevistas con los administradores de los procesos críticos, para entender el funcionamiento interno de los procesos, la inspección de la configuración de implementación, tanto de la parte física como de la parte lógica.

Se intenta detectar y mitigar las vulnerabilidades en servidores internos, comunicaciones no seguras en la red corporativa (Wireless, LAN y WAN), inadecuadas configuraciones de software, vulnerabilidades físicas, así como accesos no autorizados a redes, sistemas y servidores de la institución, en definitiva potenciales vectores de ataque, que pueden provocar robo de información sensible, daños tanto a nivel operacional y de imagen institucional.

### 1.4. Formulación del problema a resolver

**La problemática se centra en tres preguntas:**

- ¿Las seguridades físicas existentes, son las adecuadas y están dentro de los parámetros óptimos de seguridad?
- ¿Las seguridades lógicas existentes, son las adecuadas y están dentro de los parámetros óptimos de seguridad?
- ¿Existe algún plan de seguridad a seguir dentro de la empresa, en cuanto a la parte informática?

## 1.5. Objetivo General

Desarrollar una Auditoría de gestión de seguridad de la WAN, a nivel físico y lógico, mediante herramientas y técnicas de auditoría informática, para determinar posibles vulnerabilidades y proponer alternativas de solución.

## 1.6. Objetivos Específicos

- Analizar y determinar las vulnerabilidades físicas, del Data Center y sitios que alojen los equipos de las comunicaciones de la red corporativa (LAN y WAN).
- Analizar y determinar las vulnerabilidades lógicas, en las configuraciones de hardware, software, redes, comunicaciones y demás elementos tecnológicos que formen parte de los procesos críticos.
- Adquirir un inventario de hardware y software, mediante el uso de herramientas y técnicas de auditoría informática.
- Generar un análisis del nivel de seguridad.

## 1.7. Reseña Histórica

La Institución, fue fundada el 14 de Enero de 1991, con la finalidad de formar una institución que brinde servicios financieros para la ciudadanía. Estas instituciones como se conceptualizó en la Constitución aprobada en el 2008, dan atención a los sectores con menor acceso a servicios financieros y promueve el desarrollo económico de sus asociados, a través del financiamiento de actividades productivas con alto impacto en las economías locales, facilitando un mayor bienestar y mejor nivel de vida de sus asociados. Hoy se está hablando de una Institución de Ahorro, que ha logrado posicionarse entre las más importantes de la región sur del país.

En el año 2005, se realizó un cambio de la imagen interna institucional, así mismo, se acopló la estructura orgánica funcional, a los nuevos requerimientos para cumplir con la normatividad y requerimientos de la ley de instituciones financieras. Además se aprobó los nuevos estatutos, reglamento interno, reglamento de

elecciones, y demás reglamentos, normas y procesos de conformidad a lo requerido por los organismos de control.

Desde Agosto del 2006, por iniciativa de los principales directivos, con la finalidad de cubrir las necesidades de salud, se creó el centro médico que lleva su mismo nombre, cuyo fin está encaminado a ofrecer a los socios y familiares, así como a sus funcionarios una atención en salud, con garantías y facilidades necesarias, equipándolo con implementos de última tecnología y así brindar un servicio de calidad.

Hoy por hoy, el centro médico, se ha convertido en un lugar de gran acogida, entre las personas que necesitan de sus servicios, así lo mencionan quienes a diario se acercan para aprovechar las asistencias médicas en especialidades como: medicina general, hebeatría (atención de adolescentes) y pediatría (atención de niños).

El 30 de Abril del 2008, por sus buenos antecedentes dentro del mercado financiero, la Institución pasó al control y supervisión de la Superintendencia de Bancos y Seguros, Entidad que, mediante resolución Nº SBS-INIF-DNIF2-2008-288: "Calificar a la Institución de Ahorro, para que se sujete al control y supervisión de la Superintendencia de Bancos y Seguros del Ecuador, y a las normas contenidas en la ley general de instituciones del sistema financiero, el reglamento emitido mediante decreto ejecutivo Nº 354 y sus reformas; y a las disposiciones que expida la Superintendencia de Bancos y Seguros"; con fecha 15 de Diciembre de 2008, la institución de control, emite el certificado de autorización Nº 2008-C-154 para su funcionamiento.

Por medio de diversas líneas de crédito, ha logrado la reactivación económica de la región sur del país, a través del apoyo a los sectores productivos, principalmente a los de menor tamaño, que han generado fuentes de empleos directos e indirectos.

Estas líneas se encuentran cubiertas por medio de un seguro de desgravamen con una cobertura del 50% del saldo del crédito, hasta un monto máximo de $10.000, constituyéndose en un seguro único en el sistema financiero por sus características.

En la actualidad, la Institución sobresale en la región sur del país, porque es una Entidad con estabilidad democrática, con disciplina financiera probada, con atractivos reales para sus inversionistas y con buenas credenciales de estabilidad.

### 1.8. Misión

"Somos una Institución de Ahorro y Crédito socialmente responsable, que satisface las necesidades de sus socios y clientes brindando productos y servicios financieros de calidad, con eficiencia y personal comprometido para aportar al desarrollo y crecimiento económico de la región sur del país".

### 1.9. Visión

"Ser una institución sustentable y competitiva en el sistema financiero popular y solidario en la región sur del país, impulsando el crecimiento y desarrollo socio-económico de nuestros socios y clientes".

### 1.10. Ubicación Geográfica

La Institución, desde su creación funciona en pleno corazón de la ciudad de Loja.

Posteriormente, debido al incremento de socios y con el afán de brindar una mejor atención a la ciudadanía, expande sus servicios, creando dos agencias más, así: Agencia Norte y la Agencia Sur. La Institución sigue creciendo, por lo que en la actualidad cuenta con 9 sucursales que se encuentran ubicadas en:

- Catamayo, Cariamanga, Saraguro, Catacocha, Alamor, Malacatos, Vilcabamba, en la provincia de Loja.
- Balsas en la provincia de El Oro.
- Yanzatza en la Provincia de Zamora Chinchiche.

### 1.11. Estructura Organizacional

La Institución, tiene delimitado sus funciones y obligaciones, mediante una estructura organizacional, en la cual, se ocupan cargos dependiendo de sus labores dentro y fuera de la organización. *Véase Anexo A.*

Esta estructura organizacional fue rediseñada y aceptada por los altos directivos de la Institución, el 19 de Abril del 2013. A continuación, se hablará de los departamentos más importantes que se verán involucrados dentro de este proyecto.

### 1.11.1. Consejo de Administración

Es el órgano directivo y administrativo de la Institución, encargado de dictar las políticas y normas internas para el funcionamiento interno de la institución. Está conformado por 5 integrantes seleccionados por los socios de la Institución y designados en las siguientes dignidades: Presidente, Vicepresidente, Secretario y dos Vocales Principales.

### 1.11.2. Consejo de Vigilancia

Es el órgano de control interno de la Institución, en temas de aplicación, alcances y ejecución de la normativa, planes y presupuestos; controla, supervisa e informa al Consejo de Administración acerca de los riesgos que puedan afectar a la Institución. Está conformado por 3 integrantes seleccionados por los socios de la Institución y designados en las siguientes dignidades: Presidente, Secretario y Vocal.

### 1.11.3. Gerente General

Es la pieza central para el funcionamiento interno de la Institución, es la persona encargada en tomar las decisiones tanto administrativas como financieras, busca mejorar el rendimiento y estabilidad.

Decide sobre las inversiones a realizar para mejorar la eficiencia de los procesos internos de la Institución. Administra el crecimiento de la institución y es el encargado de aplicar normas, reglamentos establecidos por las entidades de control, así mismo, es responsable de informar sobre el desenvolvimiento de la Institución.

### 1.11.4. Dirección de Tecnología de la Información

Es el área crítica de la Institución, debido a que es el área encargada del análisis, desarrollo, puesta en marcha, control y mantenimiento de la parte tecnológica de la institución.

Tiene a su cargo el departamento de equipos de cómputo, redes de telecomunicación e infraestructura tecnológica. Dentro de sus departamentos posee: el de administración de seguridades de la información de TI, el departamento de soporte tecnológico y Help Desk y el departamento de administración de la información.

Este departamento, se mantiene bajo la vanguardia de la información y de la tecnología, por tal motivo, maneja planes de acción, de actualización o de generación de nuevos proyectos, para mejorar las seguridades y la eficiencia de cada uno de los procesos de la Institución.

## 1.12. Arquitectura de Hardware

### 1.12.1. Topología de la Red

La red informática de la Institución, maneja una topología de tipo estrella extendida, debido a que, todo se centraliza en la oficina matriz y es repartido a todos los servidores Branch de cada agencia y sucursal. *Véase Anexo B.*

Para asegurar un correcto desenvolvimiento de los procesos y al utilizar la topología tipo estrella extendida, se diseñó la misma para poder incluir medios de respaldo y así evitar posibles interrupciones de los servicios, con lo cual se dispone de canales de comunicación redundantes y sistemas de cableado estructurado con conexiones dobles para cada usuario.

### 1.12.2. Conexiones Externas

Las conexiones externas en la Institución, tiene como proveedor de servicios de red a la empresa CONECEL S.A., también denominado CLARO, que se encarga de la parte de enlaces y conexiones hacia el exterior, dando soporte, cuando existan problemas relacionados con los enlaces de comunicación externas. *Véase Anexo C*

Mediante los router, de propiedad de “CONECEL”, se tiene conexiones al exterior hacia las diferentes sucursales, ubicadas en las Provincia de Loja, El Oro y Zamora Chinchipe, estas son:

- De matriz hacia la sucursal Catamayo

- De matriz hacia la sucursal Cariamanga
- De matriz hacia la sucursal Saraguro
- De matriz hacia la sucursal Catacocha
- De matriz hacia la sucursal Alamor
- De matriz hacia la sucursal Malacatos
- De matriz hacia la sucursal Vilcabamba
- De matriz hacia la sucursal Balsas
- De matriz hacia la sucursal Yanzatza

En cuanto a las conexiones externas con las Agencias tanto Norte como Sur, la Institución, posee sus propios enlaces, los cuales son transmitidos mediante antenas radiales. De igual manera, existe un contrato de servicio con la empresa TELCONET, la que se encarga de proveer el servicio de Internet para la oficina matriz y de ésta, ser repartida al resto de agencias y sucursales, ubicadas en las provincias de Loja, El Oro y Zamora Chinchipe.

### 1.12.3. Servidores

En la actualidad, el uso de la Tecnología en los procesos que dan valor al negocio ha ido incrementando notablemente, por tal motivo, la información se volvió el elemento más valioso para las instituciones y el procesamiento de la información se convirtió un proceso crítico de cada empresa, en tal virtud, posee algunos equipos encargados de esta actividad y brindan servicios diferentes, los mismos que se encuentran ubicados en racks para su protección y seguridad. *Véase Anexo D.*

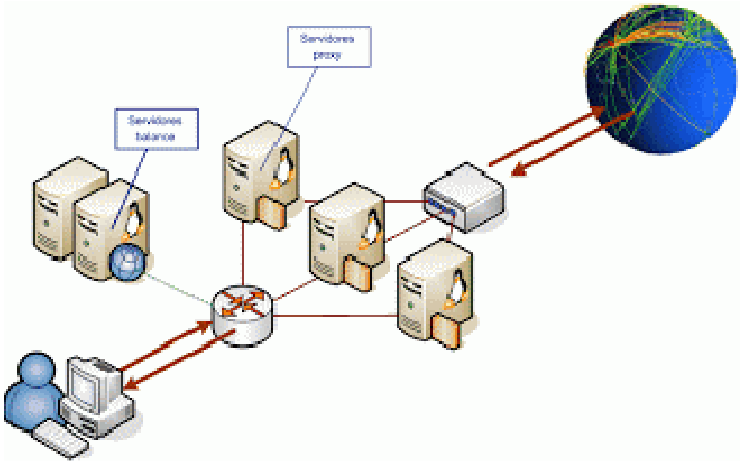


Gráfico No. 1: Diagramas de Servidores

Cabe indicar que los servidores existentes, que se dedican a los múltiples procesos de la Institución, se encuentran definidos dentro de DMZ para su organización y protección.

*Servidor Central del Sistema:* Principal Servidor de la Institución, considerado el corazón de todos los procesos, debido a que en él, se encuentra almacenado el sistema central de procesamiento financiero, que proporciona los servicios de cada uno de los módulos que conforman el Sistema.

Este servidor, es el más robusto de todos, esto, porque procesa cientos de transacciones a la vez, por lo que tiene grandes características, tanto de procesamiento, como de almacenamiento.

El sistema financiero instalado en este servidor es el de la Empresa 

Dentro de este Servidor, también se encuentra incluido el software de base de datos, el mismo que almacena la información de las transacciones. El software que se escogió para esta funcionalidad es el denominado 


*Servidor de Arreglo de Discos:* Provee servicios de almacenamiento de datos en arreglo de discos, así como el servicio de base de datos al sistema central, este servidor está definido por el modelo cliente servidor. Hace referencia a aquellas computadoras que están dedicadas a ejecutar y prestar servicios.

La base de datos, maneja grandes cantidades de información que deben estar seguras, tiene un sistema gestor de base de datos, que proporciona una herramienta de apoyo a la toma de decisiones, al mismo tiempo que proporciona transacciones de usuarios y así tiene una información actualizada y consistente.

*Servidor de Antivirus:* Posee el software de antivirus que da los servicios de actualización y protección, a las computadoras terminales de la Institución, éste se maneja, de forma de cliente servidor y cualquier anomalía o intento de intrusión es reportado de forma inmediata, evitando una propagación y contaminación de los equipos de cómputo.

El software instalado para este medio es la de la empresa [redacted] llamado [redacted] el mismo que tiene configurado las reglas y normas para cumplir con la protección en línea de cada uno de los equipos.

*Servidor de Telefonía:* Provee el servicio de telefonía IP, el mismo que es utilizado por el personal de la institución, para poder mantener contacto con sus departamentos, agencias y sucursales. Así mismo, promueve la comunicación entre los socios de la Institución y los diferentes empleados, para realizar consultas u operaciones financieras.

El software que utiliza este servidor, para brindar la respectiva prestación, es el denominado [redacted] el mismo que ofrece muchas características flexibles y que permite implementar algunos servicios como:

- Fax virtual
- Mensajes de voz
- Cola de llamadas
- Saludos personalizados
- Call Center
- Follow me
- Re direccionamiento de llamadas
- Despedidas personalizadas
- Entre otros.

*Servidor de Video Vigilancia:* Posee en software de video vigilancia, utilizando la tecnología IP, el mismo que graba las imágenes, sonidos y videos provenientes de las cámaras, ubicadas en diferentes áreas del edificio matriz, de las agencias y las sucursales, para controlar los accesos y diferentes áreas críticas de las instalaciones.

El equipamiento que se utiliza para este servicio es en la marca [redacted], y provee de características para la transmisión de la información como son: el video, imágenes y sonido, concentrándose de todas las sucursales y agencias en la oficina matriz. Así mismo se posee cámaras CCTV que se conectan al servidor para realizar las grabaciones de seguridad. Cabe recalcar que, la mayoría de las cámaras son de tecnología IP.

*Servidor de Correo:* Provee el servicio de correo electrónico a todos los empleados, administrativos, para envió de mensajes internos, envió de información, documentos, reportes o cualquier tipo de datos de importancia para el funcionamiento de la Institución.

Para el desarrollo y puesta en marcha del servicio, el correo electrónico fue implementado utilizando [redacted] y mediante clientes de correo como el [redacted] [redacted] pueden tener acceso en cada uno de los equipos de la red corporativa.

Así mismo, se ha dado de alta el servicio de correo electrónico mediante Web, utilizando la aplicación [redacted], el mismo que se encuentra activo y se puede ingresar por medio de la página web de la Institución.

*Servidor de Proveedores Externos:* Este servidor pertenece a la empresa Moneygram y es utilizado para poder acceder al sistema de envío y recepción de dinero, por medio de esta empresa, la misma que puede emitir o recibir giros de cualquier parte del mundo.

*Servidor de Aplicaciones Internas:* En este servidor se encuentran instalados dos sistemas: uno es el de riesgos y el otro el financiero. Estos sistemas son empleados para los procesos críticos, así: el rastreo de riesgos financieros, el de análisis financiero y el crecimiento del patrimonio de la Institución.

*Servidor de Monitoreo de Red:* Ayuda a controlar el consumo de ancho de banda, y, a rastrear el tráfico que se genera en la red corporativa, no sólo de la matriz, sino a nivel general, para poder canalizar de mejor manera el ancho de banda optimizando los recursos existentes.

Para esto, se ha configurado y generado consultas específicas, utilizando wireshark, el cual analiza cada uno de los puertos y protocolos para obtener el tráfico y poder solucionar problemas de redes de comunicación.

*Servidor de Esquema de Replicación:* Este servidor presta la configuración, para poder realizar la réplica de la información almacenada en la base de datos y generada por el sistema central.

Este servidor aún se encuentra en etapa de desarrollo, debido a que se están tomando las consideraciones necesarias, para asegurar que la información replicada, sea confiable y esté disponible en todo momento, por estos motivos, aún no se encuentra puesto en producción.

*Servidor de Control de Contenido:* Es el servidor utilizado para la protección y control de los accesos de la red interna hacia el internet, permite autorizar o bloquear y definir los sitios para los que se redirige el acceso de cada uno de los usuarios.

Para esto se ha instalado y configurado el 

el mismo que utiliza plug-ins y listas negras que son de dominio general, las cuales se actualizan diariamente y que puede añadirse sitios que a lo mejor afectarían el desenvolvimiento de los procesos como lo son:

- Páginas de redes sociales.
- Páginas de intercambio de información.
- Música en línea.
- Videos en línea.
- Correos externos.
- Salas de chat, etc.

*Servidor Branch de sucursales:* Ubicado uno en cada sucursal, estos servidores son utilizados por el sistema central financiero para conectarse y brindar el acceso a cada uno de los módulos, así como el reflejo de cada transacción realizada por los usuarios del Sistema.

*Servidor de Telefonía de Sucursales:* Este servidor provee los servicios de telefonía, de cada una de las agencias y sucursales. El software que utiliza este servidor para brindar el servicio es el denominado 

el mismo que ofrece muchas características flexibles y que permite implementar varios servicios como:

- Fax virtual
- Mensajes de voz
- Cola de llamadas
- Saludos personalizados

- Call Center
- Follow me
- Re direccionamiento de llamadas
- Despedidas personalizadas
- Entre otros.

Son servidores que se reflejan con el servidor central de telefonía ubicado en la matriz.

### 1.12.4. Equipos de Comunicaciones

En la actualidad, el uso de la tecnología en los procesos que dan valor al negocio ha ido incrementándose notablemente, por tal razón, se han creado equipos, que ayuden a la comunicación y transmisión de los datos, a cada una de las computadoras utilizándolos para la generación y procesamiento de la información. *Véase Anexo E.*

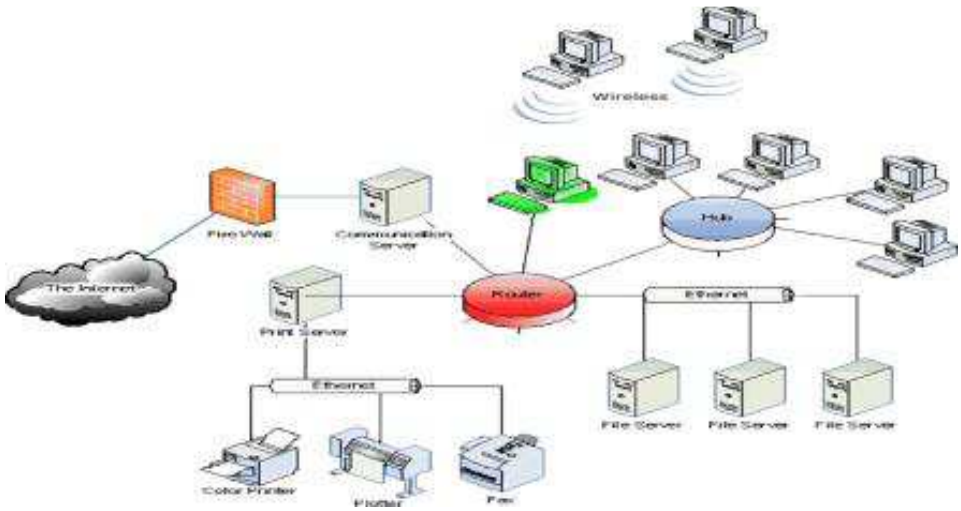


Gráfico No. 2: Diagramas de Medios de Comunicación

Cabe indicar que los equipos de comunicación existentes, que se dedican a los múltiples procesos de transmisión de datos de la Institución, se encuentran definidos dentro de DMZ para su organización y protección.

*Routers:* Un router o también conocido como enrutador o encaminador de paquetes, es un dispositivo, que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred, un

conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador (mediante bridges), y que por tanto tienen prefijos de red distintos. (González R. , 2013)

*Switch:* Un conmutador o switch, es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local. (Sánchez, 2012).

*Gateways:* Una pasarela, puerta de enlace o Gateway, es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino. El Gateway o puerta de enlace, es normalmente un equipo informático configurado, para dotar a las máquinas de una red local (LAN), conectadas a él, de un acceso hacia una red exterior, generalmente realizando para ello, operaciones de traducción de direcciones IP (NAT: Network Address Translation).

Esta capacidad de traducción de direcciones, permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo, para dar acceso a Internet, a los equipos de una red de área local, compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. (Murillo García, 2007)

*Access Points:* Un punto de acceso inalámbrico (WAP o AP por sus siglas en inglés: Wireless Access Point), en redes de computadoras, es un dispositivo, que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica.

Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos

inalámbricos. Muchos WAPs pueden conectarse entre sí, para formar una red aún mayor, permitiendo realizar roaming. (Rendon, 2012)

## 1.13. Inventario de Hardware

### 1.13.1. Hardware en General

Se compone del siguiente equipamiento:

- 1 firewall utilizado como puerta de enlace
- 11 Servidores divididos en:
  - Matriz
    - Servidor Central del Sistema
    - Servidor de Arreglo de Discos
    - Servidor de Antivirus
    - Servidor de Telefonía
    - Servidor de Video Vigilancia
    - Servidor de Correo
    - Servidor de Proveedores Externos
    - Servidor de Aplicaciones Internas
  - Agencia Norte
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Agencia Sur
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Saraguro
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Yanzatza
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Catamayo
    - Servidor Branch del Sistema

    - Servidor de Telefonía
  - Sucursal Malacatos
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Vilcabamba
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Catacocha
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Cariamanga
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Alamor
    - Servidor Branch del Sistema
    - Servidor de Telefonía
  - Sucursal Balsas
    - Servidor Branch del Sistema
    - Servidor de Telefonía
- 7 PC´s para promover servicios
  - 1 para monitoreo de red
  - 3 para aplicaciones internas
  - 1 para control de permisos de internet
  - 1 para esquema de replicación
  - 1 para almacenamiento de video vigilancia.
- 79 PC´s distribuidos en la Institución divididos en:
  - 40 PC´s en la casa Matriz.
  - 4 PC´s entre la Agencia Norte y Sur.
  - 35 PC´s distribuidas en las Sucursales ubicadas en las Provincias de Loja, El Oro y Zamora Chinchipe.
- Cableado Categoría 5e y 6

- 1 Disco de Almacenamiento en red.
- 4 Routers distribuidos en:
  - 1 Router de provisión de internet
  - 1 Router de provisión de datos.
  - 1 Router de transmisión de datos.
  - 1 Router de conexión con proveedores externos.
- 1 Gateway telefónico.
- 17 Swicthes de comunicación, distribuidos en:
  - 3 switches de distribución de datos en la red interna.
  - 1 switch para la DMZ.
  - 1 switch para el correo, monitoreo y web.
  - 1 switch entre servidor de datos y firewall
  - 9 switch distribuidos 1 por cada sucursal y uno por agencia.
- 1 access point que provee acceso a la red y a internet.
- 2 antenas de transmisión para la agencia norte y sur.
- Conexión a internet que provee la empresa TELCONET.

### 1.13.2. Características de Servidores

Las características de hardware que tiene cada servidor es:

- ***Servidor Central del Sistema***
  2 Procesadores
  Memoria Ram
  3 Discos Duros de 100 GB


- ***Servidor de Antivirus***
  Procesador Ghz
  Memoria Ram
  Disco Duro de 160 Gb


- ***Servidor de Telefonía***
  Procesador Ghz
  Memoria Ram

Disco Duro de 200 GB

- ***Servidor de Video Vigilancia***

  Procesador

  Memoria Ram

  2 Discos Duros de 1 TB

- ***Servidor de Correo***

  Procesador Ghz

  Memoria Ram

  Disco Duro de 200 GB

- ***Servidor de Proveedores Externos***

  Procesador GHz

  Memoria Ram

  Disco Duro 250 GB

- ***Servidor de Aplicaciones Internas***

  Procesador Ghz

  Memoria Ram

  Disco Duro de 150 GB

- ***Servidor Branch de Sucursales***

  Procesador GHz

  Memoria Ram

  Disco Duro de 150 GB

### 1.13.3. Características de Networking

Las características de hardware que tiene los equipos de networking es:

- ***Puerta de Enlace***

  Marca:

  Modelo:

- ***Gateway Telefonía***

  Marca:

Modelo: 


- ***Multimodem Telefonía***

  Marca:

  Modelo: 


- ***Provisión de Internet***

  Marca:

  Modelo: 


- ***Provisión de Datos***

  Marca:

  Modelo: 


- ***Proveedores Externos***

  Marca:

  Modelo: 


- ***Transmisión de Datos***

  Marca:

  Modelo: 


- ***Switch de Datos y Firewall***

  Marca:

  Modelo: 


- ***Switch de Proxy y Mail***

  Marca:

  Modelo: 


- ***DMZ para Servidores***

  Marca:

  Modelo: 


- ***Switch Distribución de Datos piso 1***

  Marca:

  Modelo: 


- ***Switch Distribución de Datos piso 2***

  Marca: 

Modelo:

- ***Switch Distribución de Datos piso 3***

  Marca:

  Modelo:

- ***Switch Distribución de Datos Agencias y Sucursales***

  Marca:

  Modelo:

### 1.13.4. Inventario de Software

La Institución, dispone del siguiente licenciamiento de software:

Tabla No. 1

Inventario de Software Licenciado

| DESCRIPCIÓN | CANTIDAD |
|---|---|
| **Activation E media CS-Estándar Edition** | 1 |
| **Ase Dev Sol 64** | 1 |
| **Ase Ent Edition** | 1 |
| **Ase-Enterprise 12.** | 1 |
| **CAL Win Server Windows** | 2 |
| **Sistema Financiero** | 8 |
| **Desarrollo de centro de Costos** | 1 |
| **Diseño sistema informático Proveeduría** | 1 |
| **Security Bussiness Edition** | 55 |
| **Hyperior Report -Licencias-** | 2 |
| **100BSS antivirus** | 53 |
| **Microsoft Office** | 1 |
| **Microsoft Visio** | 1 |
| **Microsoft Win Terminal** | 27 |
| **Windows SERVER CAL** | 29 |

CONTINUA

| | |
|---|---|
| **Office … s SNGL OLP N** | **8** |
| **Módulo de Gestión de Riego Operativo** | 1 |
| **Módulo de Gestión de Riesgo Mercado y Liquidez** | 1 |
| **Módulo de Gestión de Riesgo de Crédito** | 1 |
| **Ms-SQL Cal** | 1 |
| **Ms-SQL server** | 1 |
| **Office Standa** | 9 |
| **Remote Desktop** | 12 |
| **Replication** | 1 |
| **SCO UNIX OPENSERVER** | 4 |
| **Software vinculación clientes y socios** | 1 |
| **SOLARIS** | 2 |
| **SQL Server Std SQLvrStd** | 54 |
| **SQL User Cal Single LICSAPk OLV NL** | 1 |
| **Adaptive Server Enterprise-SBE** | 8 |
| **Open Server-Seat License- To Unix** | 3 |
| **Replication Server For Sun Solaris** | 2 |
| **Win SvrStd SNGL LICSAPk OLV NL 1Y** | 1 |
| **Windows Premium** | 1 |
| **Windows Serv WinSvrStd** | 1 |
| **Windows** | 1 |
| **Windows** | 4 |
| **Windows** | 1 |
| **Windows** | 43 |

### 1.13.5. Inventario de Usuarios

Para el correcto funcionamiento de cada uno de los procesos de la Institución, se han creado usuarios que han sido asignados con perfiles de usuario, los mismos que se encuentran con accesos al sistema dependiendo de los procesos a su cargo, así como en cada una de las agencias y sucursales distribuidas en las Provincias de Loja, El Oro y Zamora Chinchipe.

Para la matriz existen 79 usuarios creados y distribuidos en cada una de las áreas. Los inventarios presentados en el presente trabajo, han sido obtenidos mediantes varias técnicas, entre las cuales han sido, la revisión de los registros físicos de cada activo informático, así como la utilización de las herramientas enunciadas en capítulos posteriores.

Debido al carácter de confidencialidad y nivel de riesgo sobre la existencia y disponibilidad de los equipos, tanto servidores, redes y telecomunicaciones, así como del Software de la Institución, en el presente trabajo se han colocado especificaciones básicas, con lo cual se asegura la confidencialidad de la información vertida en este proyecto.

# CAPÍTULO 2

## ESTADO DEL ARTE

### 2.1. Estado del arte a nivel mundial y local

#### 2.1.1. Nivel de Acreditaciones a nivel mundial de la ISO/IEC 27001:2005

El número de certificaciones, se ha incrementado considerablemente en los últimos años, como demostración de la relevancia que tiene la protección de la información, para el desarrollo de las actividades de las organizaciones y de esta forma, mantener y desarrollar el tejido industrial de los diferentes países y el mundo entero.

Desde el año 1993, la ISO, realiza una encuesta mundial, en la que recaba información del número de certificaciones emitidas, para los distintos sistemas de gestión, sujetos a ser certificados en base a normas ISO.

Esta información, se encuentra en el documento denominado ISO Survey, donde se informa de manera detallada y al año vencido (p.ej. la publicación del presente año, refleja los totales para el año anterior completo a fecha 31 de Diciembre), del resultado, en el número de certificaciones acreditadas con referencia a las regiones, países, sectores industriales, de mayor implantación entre otros, tanto para ISO/IEC 27001, como para otros sistemas de gestión (ISO/IEC 9001, ISO 14001, ISO 22000, ISO 50001, entre otros).

La fuente para este relevamiento son los organismos de certificación existentes en los distintos países.

A los efectos de esta encuesta, se trabaja específicamente, con los organismos acreditados por miembros nacionales de la IAF (International Accreditation Forum). La IAF, es una asociación internacional, que representa a los organismos de acreditación de los países. Como una excepción, los datos incluyen los certificados emitidos en Rusia, que son acreditados localmente por un organismo que no es miembro de la IAF.

El relevamiento, realizado por la ISO, genera un conjunto de informes y datos agrupados en diferentes planillas, que se encuentran disponibles para el público. Las bases generadas, contienen la información del número de certificados desde el año 1993 al 2012. Para todos los certificados, se genera información por región geográfica, por país, así como el número de sitios por cada uno de los países.

El número de certificados retirados, también se encuentra detallado. Para las normas ISO 9001, ISO 14001, ISO/IEC 27001 e ISO 50001, la información también, está disponible por sector industrial.

### 2.1.2. Análisis de los Datos de la certificación ISO/IEC 27001:2005

Tomando exclusivamente los datos de las certificaciones ISO/IEC 27001:2005 podemos realizar diferentes análisis. De un total de **19577** certificados considerados al 2012, la distribución por continente es la que se presenta a continuación:


Gráfico No. 3: Certificaciones Emitidas de la ISO/IEC 27001:2005

América del sur y central, representa, la región con el segundo mayor crecimiento respecto del 2011, con una tasa del 35 %, siendo África, la primera con un crecimiento del 60%.

Los países con más certificados emitidos son:

Tabla No. 2

Top 10 países con Certificados ISO/IEC 27001:2005

| Top 10 países con certificados ISO/IEC 27001 – 2012 | | |
|---|---|---|
| ***1*** | Japón | 7199 |
| ***2*** | Reino Unido | 1701 |
| ***3*** | India | 1600 |
| ***4*** | China | 1490 |
| ***5*** | Romania | 866 |
| ***6*** | China, Taipei | 855 |
| ***7*** | España | 805 |
| ***8*** | Italia | 495 |
| ***9*** | Alemania | 488 |
| ***10*** | Estados Unidos | 415 |

El país de América Latina, con más certificados emitidos, es Colombia, con 58, seguido por Brasil, con 53 y por último Argentina, con 33 emisiones realizadas.

### 2.1.3. Evolución de los certificados ISO/IEC 27001:2005, emitidos en América del Sur y Central

Considerando, América del Sur y Central, al 2012 se contaban con 203 certificados emitidos, destacándose una tasa del 35% de crecimiento respecto del 2011.

| Argentina | Bolivia | Brazil | Chile | Colombia | Costa Rica | República Dominicana | Ecuador | El Salvador | Guatemala | Honduras | Panama | Perú | Puerto Rico | Trinidad | Uruguay |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 33 | 1 | 53 | 23 | 58 | 7 | 5 | 3 | 1 | 1 | 1 | 2 | 7 | 2 | 1 | 7 |

Gráfico No. 4: Certificaciones Emitidas en Latinoamérica de la ISO/IEC 27001

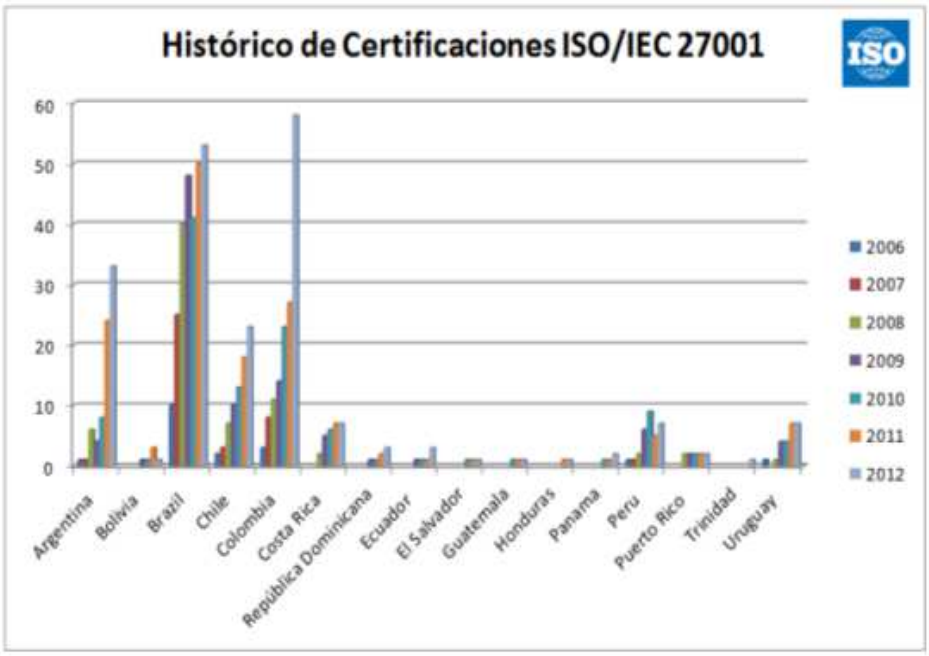


Gráfico No. 5: Histórico de Certificaciones Emitidas en Latinoamérica de la ISO/IEC 27001:2005

En los diferentes países de América Latina, los últimos años, se ha mantenido el ritmo de crecimiento y obtención de certificaciones ISO/IEC 27001:2005 en la región.

Se destaca, no obstante que grandes países de la región, tienen aún un número muy bajo de empresas y organizaciones certificadas ISO/IEC 27001:2005.

Sin duda, resta un gran trabajo de concientización y difusión, a nivel general en nuestras sociedades, respecto del valor de la seguridad de la información, la protección de datos, y el verdadero valor de la obtención de la certificación ISO/IEC 27001:2005. (ISO, 2013)

## 2.2. Marco Teórico

Con el crecimiento acelerado de las tecnologías de información, la utilización de servidores desempeña un papel importante en el negocio de las empresas, provocando a su vez un incremento de la dependencia de los mismos, en los distintos procesos, donde la calidad es fundamental, para conseguir rentabilidad en la producción. La necesidad de realizar pruebas de calidad de la seguridad, converge hacia el aseguramiento de la eficiencia y confidencialidad de la información.

La Auditoría de Sistemas, es el conjunto de técnicas, que permiten detectar deficiencias en las organizaciones que utilizan tecnologías de información y en los sistemas que se desarrollan u operan en ellas, incluyendo los servicios externos de computación, redes de comunicación, que permitan efectuar acciones preventivas y correctivas para eliminar las fallas y carencias que se detecten.

Se verifica la existencia y aplicación de todas las normas y procedimientos requeridos, para minimizar, las posibles causas de riesgos, tanto en las instalaciones y equipos, como en los programas computacionales y los datos, en todo el ámbito del Sistema: usuarios, instalaciones, equipos.

La auditoría de SI, analiza los procesos relacionados únicamente con la seguridad, ésta puede ser física, lógica y locativa, pero siempre orientada a la protección de la información. La SI, se preocupa por la integridad y disponibilidad de la información, mientras que, la auditoría de sistemas, incluye otras características referentes a los aspectos administrativos, es éste, el punto de mayor diferencia.

### 2.2.1. Normas y Estándares Internacionales

Hoy en día, existen varias normas y estándares que han sido desarrolladas, para establecer requisitos y directrices para el diseño de infraestructura de telecomunicaciones, cableados estructurados, Data Center, etc., como por ejemplo:

- *TIA/EIA 942:* Es el estándar de la infraestructura de telecomunicaciones, para centros de datos. La lista que a continuación se detalla, muestra su propósito:

- El propósito de esta norma, es establecer los requisitos y directrices para el diseño e instalación de un centro de datos o sala de ordenadores.

- Está dirigido, a los diseñadores, que necesitan una comprensión integral del diseño del centro de datos, incluyendo la planificación de instalaciones, el sistema de cableado y el diseño de la red.

- Facilita la planificación de centros de datos, en el proceso de desarrollo de la construcción (arquitectura, instalaciones y TI). (Peñaloza Figueroa)

- *TIA/EIA-568-C:* Es el estándar, que contiene las normas, que permitan el diseño e implementación de sistemas de cableado estructurado, para edificios comerciales y entre edificios en entornos de campus.

  La mayor parte de las normas, definen los tipos, distancias, conectores, arquitecturas de sistema, terminación, características de rendimiento, requisitos de instalación y métodos de prueba de sistemas de cableado estructurado instalado. (Congdon, 2005)

- *ANSI TIA/EIA-569: E*s la norma de construcción para espacios y recorridos de telecomunicaciones comerciales, normativa que se creó en 1990, como resultado de un esfuerzo conjunto de la Asociación Canadiense de Normas (CSA) y Asociación de las Industrias Electrónicas (EIA); la misma que nos indica los elementos, para la construcción de espacios y recorridos de telecomunicaciones. (Joskowicz, 2013)
- *ANSI TIA/EIA-606-A:* Es la norma que especifica, la administración de un sistema genérico de cableado de telecomunicaciones, que prestará apoyo a un ambiente multi-producto, multi-vendedor.

  Proporciona, un enfoque de administración uniforme, siendo independiente de las aplicaciones que pueden cambiar varias veces, durante la vida de la infraestructura de telecomunicaciones.

  Establece pautas para propietarios, usuarios finales, fabricantes, consultores, contratistas, diseñadores, instaladores y administradores de centros, implicados en la administración de la infraestructura de telecomunicaciones. (Chiguano, 2008)

- *TSB-67:* Es la norma que contiene tanto, las especificaciones como los procedimientos de medición y la certificación de enlaces de cableados UTP (cables y conexiones), ya instalados, regidos por la norma TIA-568A. Así mismo, establece los métodos y parámetros de medición, para determinar los límites de Pase/Falla o el criterio de cada parámetro de prueba, la exactitud y los requerimientos de los instrumentos de medición para las pruebas de campo. (Pérez, 2000)

### 2.2.2. Norma ISO/IEC 27000:2005

Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de la normativa que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI), una introducción breve, es la descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI.

A semejanza de otras normas ISO, la ISO/IEC 27000:2005 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044 con 27799 finalizando la serie formalmente en estos momentos. La Norma ISO/IEC 27000:2005, viene a ser la evolución del estándar de buenas prácticas ISO creado en 1995. (ISO, ISO/IEC 27002:2005, 2005)

### 2.2.3. Norma ISO/IEC 27002:2005

Para el presente desarrollo de auditoría, haremos uso de la ISO/IEC 27002:2005, la misma que es una guía de buenas prácticas, que describe los objetivos de control y controles recomendables en cuanto a SI.

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios.

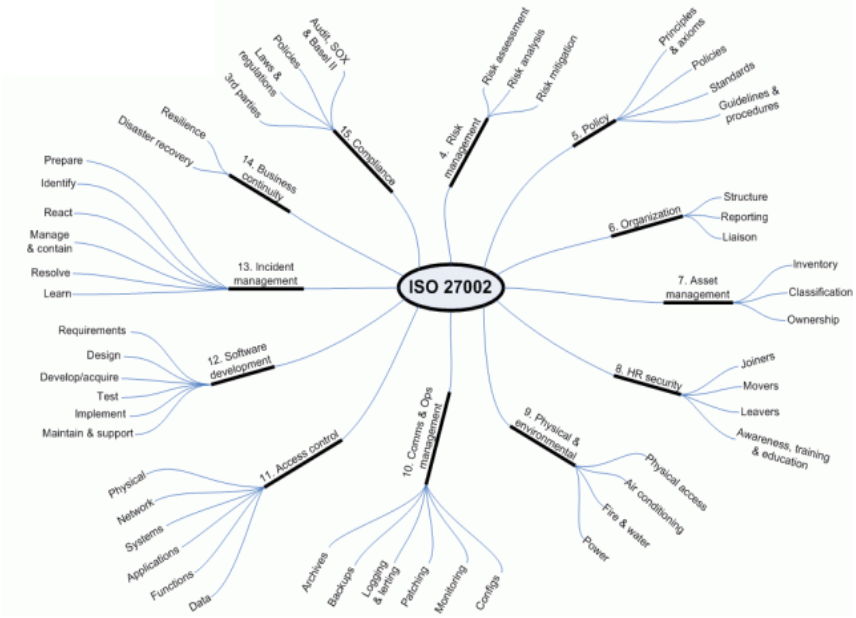


Gráfico No. 6: Estructura de la ISO/IEC 27002:2005

Dentro de los dominios utilizaremos el de áreas seguras, seguridad de los equipos, control de accesos, los mismos que poseen sus objetivos de control.

### 2.2.3.1. Alcance de la ISO/IEC 27002:2005


Gráfico No. 7: Alcance de la ISO/IEC 27002:2005

Este Estándar Internacional va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo, así como, proporciona un lineamiento práctico para desarrollar estándares de seguridad organizacional y

prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

Los objetivos delineados en este estándar internacional, proporcionan un lineamiento general, sobre los objetivos de gestión de seguridad de la información, generalmente aceptados.

Los objetivos de control y los controles de este estándar internacional son diseñados para ser implementados y para satisfacer los requerimientos identificados por una evaluación del riesgo.

#### 2.2.3.2. Estructura del Estándar

Este estándar contiene 11 cláusulas de control de seguridad conteniendo colectivamente un total de 39 categorías de seguridades principales y una cláusula introductoria que presenta la evaluación y tratamiento del riesgo.

Cada cláusula contiene un número de categorías de seguridades principales. Las once cláusulas (acompañadas por el número de categorías de seguridad principales incluidas dentro de cada cláusula) son:

- *Política de seguridad (1):* proporciona a la gerencia, la dirección y soporte para la seguridad de la información.
- *Aspectos organizativos de la seguridad de la información (2):* la organización interna, tiene como objetivo manejar la seguridad de la información y mantener la seguridad de la información y los medios de procesamiento de información de la organización.
- *Gestión de activos (2)*: asigna responsabilidades por cada uno de los activos de la organización.
- *Seguridad ligada a los recursos humanos (3):* se estipula las responsabilidades que debe seguir la organización y las seguridades referentes al personal a su cargo, durante su selección, trabajo y cese de funciones.

- *Seguridad física y ambiental (2):* se refiere a un perímetro de seguridad física, seguridad del cableado, mantenimiento y control de la temperatura de los equipos, etc.

- *Gestión de comunicaciones y operaciones (10)*: asegura la operación correcta y segura de los medios de procesamiento de la información.

- *Control de acceso (7):* consiste en tener un registro y autenticación de usuarios, gestión de privilegios y contraseñas, etc.

- *Adquisición, desarrollo y mantenimiento de los sistemas de información (6).*

- *Gestión de incidentes en la seguridad de la información (2):* recomienda trabajar con reportes de los eventos y debilidades de la seguridad de la información.

- *Gestión de la continuidad del negocio (1):* desarrollo de planes para la continuidad del negocio, para asegurar la reanudación oportuna de las operaciones esenciales, en caso de alguna falencia.

- *Cumplimiento (3):* prioriza el cumplimiento de requisitos legales, para evitar violaciones a cualquier ley, regulación estatutaria, reguladora o contractual y cualquier requerimiento de seguridad.

### 2.2.4. Norma ISO/IEC 27004

Publicada el 15 de Diciembre de 2009. No es certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida, aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001:2005.

Se creó para complementar a la norma ISO/IEC 27001:2005, ya que la norma 27001 destaca que los controles tienen que ser medibles, por esta razón la ISO/IEC 27004, nos enseña cómo debemos medir dichos controles, su objetivo consiste en hacerlos medibles.

Esta normativa, nos sirve de ayuda, para guiarnos sobre la creación y el uso de las mediciones con el fin de poder evaluar la eficiencia del sistema de gestión de la información aplicada a los controles y seguridad.

La normativa ISO/IEC 27004, está centrada sobre el modelo PLAN-DO-CHECK-ACT, también conocido como PDCA, el cual consiste en ser un ciclo continuo.

#### 2.2.4.1. Objetivo de la ISO/IEC 27004

En los procesos de mediciones se tienen que cumplir una serie de objetivos, los cuales son:

- Indicar y avisar los valores de seguridad de la entidad.
- Realizar una evaluación de la eficiencia del sistema de gestión de SI.
- Incluir niveles de seguridad, que sirvan de guía para las revisiones del Sistema de Gestión de SI, lo que provocará nuevas entradas para auditar y ayudar a mejorar la seguridad de la entidad.
- Realizar una evaluación de la efectividad de la implementación de los controles de la seguridad de la entidad.

#### 2.2.4.2. Objetivos de la medición de la seguridad

Los objetivos de la medición de SI en relación con el SGSI incluyen:

- Evaluar la eficacia de los controles aplicados o grupo de controles.
- Verificar el grado en el que se fijaron las necesidades de seguridad y saber si han sido cumplidas.
- Facilitar la mejora del rendimiento de SI en cuanto a los riesgos de negocio de la organización global.
- Proporcionar información para la revisión por parte de la dirección para facilita la toma de decisiones relacionadas con el SGSI y justificar la necesidad de mejora de la aplicación del SGSI. (Corletti, 2007)

## 2.3. Marco Conceptual

### 2.3.1. Firmas Auditoras

En el mundo, existen varias empresas, dedicadas al negocio de auditoría, dentro de las cuales las ocho más grandes, también conocidas como las Big Eight (en inglés, las "ocho grandes"), se fueron fusionando entre ellas, hasta formar las Big Five (las "cinco grandes"). A partir de la desaparición de Arthur Andersen en 2002, las cuatro sobrevivientes son conocidas como las " Big Four". Ellas son: Deloitte, PricewaterhouseCoopers, Ernst & Young y KPMG.

- *Deloitte Touche Tohmatsu Limited:* También llamada Deloitte, es la primera firma privada de servicios profesionales del mundo, por volumen de facturación (32.400 millones de dólares en 2011), por encima de PricewaterhouseCoopers, y una de las llamadas Cuatro Grandes Auditoras (Big Four auditors en inglés). Calificada en los últimos 4 años, como el lugar número uno, para lanzar una carrera por la revista BusinessWeek.

  Los servicios que ofrece a nivel global, giran en torno a cuatro áreas funcionales: consultoría, impuestos, asesoría jurídica, asesoría financiera y auditoría. Estos servicios pueden variar en cada firma miembro de Deloitte.

  De acuerdo con la web de la organización, en 2011 Deloitte, cuenta con más de 182000 profesionales, en 150 países del mundo.

  En Ecuador, se estableció desde 1966. Cuentan con oficinas en Quito y Guayaquil, un grupo gerencial formado por más de 350 profesionales al servicio de sus clientes. Como en otros países el servicio de Deloitte, se basa en la experiencia de escuchar a sus clientes, comprender sus necesidades y ofrecerles soluciones reales y oportunas; liderando las prácticas de auditoría, enterprise risk services y soluciones gerenciales. (Deloitte Touche Tohmatsu Limited Ecuador, 2014)

- *PwC:* Anteriormente llamado Price Waterhouse Coopers, es la segunda firma de servicios profesionales más importantes del mundo, por volumen de facturación

(32.200 mil millones de USD en 2013), que emplea a más de 180 000 personas en 157 países.

Aunque, sus orígenes se remontan a 1849, la configuración actual, de 1998, es fruto de la fusión entre Price Waterhouse y Coopers & Lybrand. PwC, es la segunda firma más grande de las llamadas Big Four (Cuatro Grandes). PwC, está organizada en tres grandes líneas de negocio: auditoría, consultoría y asesoramiento legal y fiscal. Desde el punto de vista jurídico, PwC es una red de firmas independientes y de propiedad local, que comparten una misma marca y una serie de metodologías y estándares de calidad.

En abril de 2014 PwC, completó la adquisición de la consultora estratégica Booz & Company, pasando ésta a formar parte de la red de firmas de PwC y cambiando su nombre a Strategy & (pronunciado en inglés “Strategy and”).

Cuentan con oficinas en Quito y Guayaquil, un grupo gerencial formado por más de 300 profesionales, al servicio de sus clientes. (Price Waterhouse Coopers Ecuador, 2011)

- *Ernst & Young*: Mundialmente conocida como EY, es una de las mayores firmas de servicios profesionales del mundo, que incluyen: auditoría, impuestos, finanzas, contabilidad, servicios de cálculos, estudios actuariales y asesoramiento en la gestión de la empresa. Según la revista Forbes, a finales del año 2012, por su tamaño es la octava mayor empresa privada de los Estados Unidos.

  EY, es una organización con operaciones en todo el mundo, que consiste en varias empresas miembros. Durante mucho tiempo, EY ha reconocido que la globalización, es un tema trascendental de nuestros tiempos. Su respuesta ha sido transformar a la organización, para lograr adaptarnos a las cambiantes necesidades de sus clientes.

  Cuentan, con oficinas en Quito, un grupo gerencial formado por más de 200 profesionales al servicio de sus clientes. (Ernst & Young , 2014)

- *Klynveld Peat Marwick Goerdeler:* También conocido mundialmente como *KPMG*, es una entidad suiza, coordinadora de una red global de firmas independientes de servicios profesionales, que ofrece servicios de auditoría, fiscales y de asesoramiento financiero y de negocio en 156 países.

  Es una de las cuatro firmas más importantes del mundo de servicios profesionales, las Big Four.

  KPMG International, opera como una red de firmas miembro, que trabaja en estrecha colaboración con sus clientes, ayudándolos a reducir los riesgos y las oportunidades de captar.

  Clientes de las firmas miembro, incluyen: corporaciones de negocios, los gobiernos y las agencias del sector público y las organizaciones sin fines de lucro. KPMG, posee un estándar consistente de servicio, basada en la alta orden de las capacidades profesionales, conocimiento de la industria y el conocimiento local.

  Contribuye al funcionamiento eficaz de los mercados internacionales de capital, usando habilidades, experiencia, pasión y recursos para potenciar el cambio y la búsqueda de soluciones sostenibles a los problemas locales y globales. Apoyan, las reformas que fortalecen la credibilidad de los mercados y su responsabilidad social. Cree, que la reforma similar debe extenderse al ámbito profesional. (Klynveld Peat Marwick Goerdeler, 2013)

  Otras firmas de auditoría importantes, que han desarrollado el negocio a través de sus sucursales en el mundo son:

  - Mazars.
  - AUREN.
  - HLB International.
  - BDO International.
  - Grant Thornton International.
  - Moore Stephens International.
  - PKF International.

- RSM International.
- GMV Asociados y UHY International.
- BZR Contadores y Auditores, etc.

### 2.3.2. Herramientas Tecnológicas

Dado el incremento de las tecnologías, se vincula así mismo el desarrollo de aplicaciones, en este caso, nos interesan aquellas que son creadas con la meta de poder automatizar el proceso de pruebas de seguridad, que se realizan sobre los diferentes equipos informáticos de una empresa. Dentro de la disponibilidad de sistemas y software, podemos encontrar algunas de estas herramientas, las mismas que están relacionadas con las pruebas de White Box:

- *BackTrack:* Es una distribución de GNU/Linux pensada y diseñada para la auditoría de seguridad y relacionada con la SI en general. Incluye una larga lista de herramientas de seguridad, entre las que se destacan numerosos escáneres de puertos y vulnerabilidades, archivos de exploit, sniffers, herramientas de análisis forense y herramientas para la auditoría Wireless. (Cárdenas, 2010)
- *Nessus Vulnerability Scanner:* Escáner de vulnerabilidades en diversos sistemas operativos. Esta tecnología desarrollada por la empresa NESSUS, que consiste en un Daemon, realiza el escaneo en el sistema operativo, buscando puertos abiertos y después ejecutar varios exploits para atacarlo. (Nessus, 2012)
- *Nmap:* Es un programa de código abierto, que sirve para efectuar rastreo de puertos. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática. (Mifsud, 2012)
- *Wireshark:* Es un analizador de protocolos, que tiene una licencia libre GPL, utilizado para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos y como una herramienta didáctica de educación.

  La funcionalidad que provee es similar a la de tcpdump, pero añade una interfaz gráfica, muchas opciones de organización y filtrado de la información. (Gómez, 2011)

- *Core Impact:* Es el software comercial más completo y revolucionario, que ha desarrollado CORE SECURITY TECHNOLOGIES, utilizado a nivel corporativo, para evaluar la seguridad de los sistemas de redes, sistemas de punto final, usuarios de correo electrónico, aplicaciones web y redes inalámbricas. Esto permite a los administradores de red o personal encargado de SI, la evaluación de riesgos y la ejecución de una metodología profesional, para el proceso de pruebas de intrusión. (Castro, 2010)

- *SysAid:* Es un dominio web, basado en herramientas de software de TI. Se encarga de automatizar los procesos de ayuda de escritorio, la configuración del hardware, la supervisión del activo, las licencias de software, generar inventarios de hardware y software; y demás tareas y proyectos. Realiza escaneos y test automáticos en la red local.

  SysAid, provee los detalles necesarios de cada equipo informático en la red y permite su control de forma remota. (SysAid, 2002)

### 2.3.3. Activos Informáticos

Son los bienes de una organización, que se encuentran relacionadas de manera directa o indirecta con la actividad informática, entre los cuales se encuentran:

- Medios de comunicación que se utilizan para la transmisión de datos, tales como: redes, correo electrónico.
- Medios magnéticos y ópticos de almacenamiento de información como: cintas, discos.
- Programas y aplicaciones de la empresa, ya sea desarrollados por la misma, o adquiridos por terceros.
- Manuales, procedimientos y reglamentaciones afines al área informática.

### 2.3.4. Seguridad Informática

La seguridad informática o seguridad de tecnologías de la información, es el área de la informática que se enfoca en la protección de la infraestructura computacional y

todo lo relacionado con la misma, especialmente la información contenida o circulante en cualquier tipo de medio.

Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software (bases de datos, metadatos, archivos, etc.), hardware y todo lo que la organización valore (activo) y signifique un riesgo, si esta información llega a manos de otras personas no autorizadas.

#### 2.3.4.1. Objetivos

La seguridad informática, debe establecer normas que minimicen los riesgos a la información o infraestructura informática.

Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática, minimizando el impacto en el desempeño de los trabajadores y de la organización en general.

La seguridad informática está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- La infraestructura computacional: Es una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización.

  La función de la seguridad informática en esta área, es velar que los equipos funcionen adecuadamente y anticiparse en caso de fallas, robos, incendios, sabotaje, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

- Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información.

Debe protegerse el sistema en general, para que el uso del mismo, no pueda poner en riesgo la seguridad de la información y tampoco que la información que manejan o almacenan sea vulnerable.

- La información: es el principal activo. Utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

### 2.3.5. Seguridad Física

Mediante la seguridad física, se evita el acceso no autorizado, daños o intromisiones en las instalaciones, así como a la información de la organización; ya que los servicios de procesamiento de información, deben ubicarse en áreas seguras y protegidas, en un perímetro de seguridad, definido por barreras y adecuados controles de entrada.

#### 2.3.5.1. Seguridad Física del Edificio

La seguridad física, es uno de los aspectos más olvidados, a la hora de la implementación de la infraestructura de tecnología. Es muy importante ser consciente, que por más que nuestra empresa esté muy bien asegurada en el aspecto físico.

Se deberá tener en cuenta que, existen personas como: ladrones, espías, o simplemente gente resentida con la institución, quienes aprovechándose de la falta de controles de acceso, video, etc., pueden provocar daños o robo de información.

Al asegurar los activos, se busca minimizar el riesgo de que cualquier persona ingrese a recursos informáticos específicos. Así mismo, se trata de que el centro de procesamiento de datos, esté ubicado en un lugar seguro, sin vulnerabilidades de acceso.

Deberían existir políticas de seguridad bien planteadas, diseñadas y desarrolladas, que cubran la gran mayoría de aspectos, para que exista un verdadero sistema de gestión de SI, así mismo, debe haber planes de seguridad, que ayuden a tomar decisiones seguras, para cuando se genere un acceso físico no autorizado, a algún recurso informático de la empresa.

#### 2.3.5.2. Control de Accesos

Todos los sitios, en donde se encuentren sistemas de procesamiento de datos informáticos o de almacenamiento, deben estar protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo, registro de entradas y salidas, guardias de seguridad, detectores metálicos, etc.

### 2.3.6. Área de Tecnología

Dentro de toda institución, ya sea de ámbito público o privado, grande, mediana o pequeña, el uso de la tecnología, se hace imperativo para el desenvolvimiento de las actividades y procesos del negocio, con lo que, la información es procesada, mejorando la disponibilidad de la información y disminuyendo el tiempo con el cual se ejecuta un determinado proceso.

Dado este punto de vista, toda empresa, en la actualidad, dispone de un departamento de sistemas, el mismo que está conformado por profesionales de la rama, quienes son los encargados de administrar, todos los activos informáticos y asegurar que la información esté segura y disponible en todo momento.

De igual manera, se han dispuesto espacios físicos, adecuados para la instalación de toda la parte informática, implementando medidas de control, que aseguren su óptimo y correcto funcionamiento.

#### 2.3.6.1. Departamento de Sistemas

El departamento de sistemas, está a cargo de toda la parte informática de la Institución, siendo esta área, una ayuda importante para la continuidad del negocio y del servicio, confidencialidad de los datos y la integridad del mismo.

Este departamento apoya a la vez, de forma computacional, a las actividades que posee toda organización, ya sea de gerencia, departamentos y otras áreas que utilizan recursos informáticos, realizando el mantenimiento y administración de las redes, sistemas y equipos computacionales de la Institución.

Recopila la información, como a su vez actualiza y mantiene los datos de los procesos que posee la Institución, con la finalidad de que esté al servicio de cada departamento.

El departamento de sistemas, se encuentra ubicado en el cuarto piso del edificio matriz. En la figura a continuación, se evidencia como está estructurada el área de sistemas.


Gráfico No. 8: Estructura del departamento de sistemas

### 2.3.6.2. Cuarto de Servidores

El cuarto de servidores es un lugar muy importante para la Institución, ya que se almacena toda la información de la organización, además de solventar otros servicios que posee la institución.

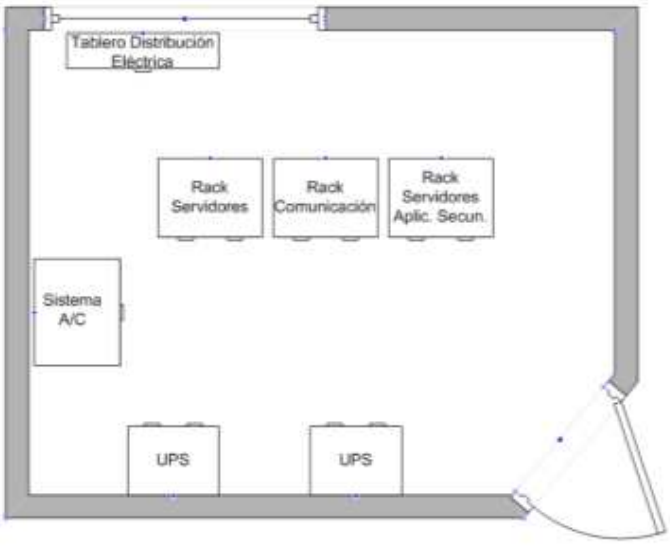


Gráfico No. 9: Estructura del cuarto de servidores

En el cuarto de servidores o centro de procesamiento de datos se actualiza la información precisa de la institución, siendo aporte fundamental para la integridad de los datos, es decir, sin este tipo de procesamiento, la divulgación de la información no sería muy a menudo y no tendrían confidencialidad en el momento de intercambiar la información de los usuarios finales.

### 2.3.7. Inventario de Cumplimiento Seguridades Físicas

Para poder realizar la auditoría de gestión de la WAN a nivel físico y determinar el nivel de la seguridad física en la actualidad en la Institución, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel físico. *Véase Anexo F.*

#### 2.3.7.1. Control de Accesos

Un sistema de control de accesos, administra el ingreso a áreas restringidas, y evita así que personas no autorizadas o indeseables tengan la libertad de acceder a la empresa. Así mismo, con un sistema de control de accesos se puede tener conocimiento de horarios de ingreso, egreso de las instalaciones y también poder tener un control histórico de entradas de personas a todas las áreas (para poder tener en cuenta quienes podrían ser los posibles responsables de algún siniestro).

Existen dos partes que se debe tener en cuenta que son: el acceso del personal autorizado y el acceso de visitantes.

- *Control de Personal Autorizado:* Para poder determinar, el nivel de seguridad física, con respecto al control del personal en la Institución, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel físico. *Véase Anexo G.*

  La composición esquemática de un sistema de control de accesos de personas sería:

  - Llaves de seguridad
  - Tarjetas Magnéticas, Ópticas infrarrojas, Wiegand

- Tarjetas Holográficas, de semiconductores, con memoria de lectura láser
- Tarjetas Electromagnéticas, Infrarrojas, Ultrasónicas
- Códigos
- Teclados electrónicos
- Cerraduras de combinación
- Biométricos de Huellas Digitales, Firmas, Voz o Iris de Ojo.

- *Control de visitas:* Existen distintas etapas en el proceso de control de visitas, en las que surge la necesidad de identificar rigurosamente a una persona. Una de ellas es obviamente el momento de ingreso a áreas críticas, pero también se pueden necesitar estos sistemas cuando la persona se registra para dar mantenimiento o instalar nuevos componentes, o cuando necesita acceder a un sitio de trabajo o a un sistema de cómputo. *Véase Anexo H.*

  A medida que la identificación de personal se usa más ampliamente y está más automatizada, sólo las personas habilitadas pueden ingresar a las áreas donde se encuentran los sistemas de información.

  Existen distintas clases de sistemas de identificación:

  - Tarjetas de identidad
  - Números de identificación personal (NIPs)
  - Sistemas de bio-identificación (de la voz, de la mano, de huellas digitales o de retina)
  - Fotografía digitalizada
  - Código de barras
  - Firma electrónica
  - Contraseñas

#### 2.3.7.2. Seguridades Secundarias

Existen muchas formas para controlar el acceso de personal o lo que estas personas realizan dentro de áreas críticas como los son el Data Center, cuarto de armarios de distribución de red o el departamento de sistemas. *Véase Anexo I.*

Por ejemplo se pueden utilizar los siguientes elementos de verificación y control:

- Circuito cerrado de televisión
- Lector biométricos
- Sistemas de apertura por teclado numérico
- Sensores de rotura de vidrios.
- Sensores de movimiento.

#### 2.3.7.3. Amenazas Externas y del Entorno

Existen muchos tipos de amenazas, que pueden afectar considerablemente el negocio, o producir un fallo total de toda la infraestructura, tanto física como tecnológica, para evitar en lo posible esto, se deben aplicar medidas de protección y respaldo. Por ejemplo las más probables que se pueden presentar son:

- *Terremotos:* Los terremotos son una serie de sacudidas del terreno debido al choque entre las placas tectónicas o la liberación de energía, en el curso de una reorganización brusca de los materiales de la corteza terrestre, debido a superar el estado de equilibrio mecánico.

  Respecto a la hora de invertir en estas medidas, depende mucho de la situación geográfica de la entidad, por ejemplo, si estuviéramos en un país como Japón, donde los terremotos están a la orden del día, sería totalmente necesaria y fundamental dicha inversión, pero si fuese como el caso de Ecuador, donde nunca se da ningún terremoto importante, ya que sus posibilidades son mínimas, dichas inversiones serán menores.

  Se recomienda el uso de plataformas de goma, las cuales absorben parte de las vibraciones generadas por los terremotos, además del uso de mesas anti vibraciones, ya que sin ellas podrían dañar los discos duros donde se guarda la información vital.

- *Incendios:* El fuego es el principal factor que debemos considerar cuando se instala un Data Center, debido a que los equipos que se encuentran en el mismo, son lo más valioso de la empresa por ser los encargados de generar valor al negocio. Por tal motivo se hace necesario determinar el porcentaje de cumplimiento de la seguridad en cuanto a incendios. *Véase Anexo J.*

Los fuegos son ocasionados por cortocircuitos, cigarros mal apagados, etc., y estos ocasionan gravísimos daños, tanto materiales como personales.

Para el centro de procesamientos de datos, debido a la gran cantidad de los componentes electrónicos y la delicadeza de los mismos, ante cualquier agente extintor, así como las ventajas que prestan; se deben salvaguardar de manera especial al personal que labora en él, así como a los equipos y procurar el mínimo impacto ambiental, para ello se pueden utilizar los siguientes elementos de detección y extinción:

- Centrales de incendio
- Luces estroboscópicas
- Sirenas de alarma
- Sistemas de alarma analógicos
- Sistemas de detección analógicos
- Sistemas de extinción automática

- *Inundaciones: C*onsisten en la ocupación del agua, en zonas que están libres de ella, esto debido por al desbordamiento de ríos, subidas de marea, o por avalanchas causadas por terremotos. *Véase Anexo K.*
  Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Estos problemas son graves, pues son los que más daño hacen a la entidad, debido a que cualquier sistema eléctrico en contacto con el agua, puede ser mortal para los empleados de la entidad y se perderá toda la última información obtenida, además de la pérdida del equipo electrónico, que dejara de funcionar y no acepta reparación alguna.

Se recomienda el uso de detectores de agua, los cuales, al dispararse corten automáticamente la corriente eléctrica para evitar males mayores. Para su detección se recomienda avisar a las autoridades necesarias (bomberos, policía, etc.), con el fin de terminar con dicho problema, se tendrá que cortar la corriente

eléctrica, en caso de que el sistema de seguridad no haya podido hacerlo. Nunca deberá hacerlo el personal de la entidad.

- *Tormentas eléctricas:* Consisten en fenómenos atmosféricos, los cuales pueden ocasionar graves daños físicos a la entidad, estos daños pueden ser desde fuegos ocasionados por las tormentas, hasta picos de tensión, los cuales pueden destrozar nuestros equipos informáticos con sus respectivos datos.

  Se recomienda el uso de pararrayos, estos consisten en una varilla de metal, puesta en el tejado o en la parte más elevada del edificio de la entidad, la cual tiene un cable de cobre, que va a parar a una plancha del mismo metal, introducida a unos metros bajo tierra.

  En caso de que un rayo toque el pararrayos, el sistema implementado, descargará toda la energía hacia la tierra, evitando de esta manera, posibles daños en todos los activos informáticos de la Institución, así como del tendido eléctrico interno.

#### 2.3.7.4. Controles de Backup

Un back up, consiste en una copia de seguridad en formato digital, de la documentación de los datos de la entidad, es un conjunto de archivos, los cuales son almacenados con el fin de protegerlos ante cualquier daño interior o exterior a la entidad. *Véase Anexo L.*

Estas copias de seguridad son útiles, ya que nos sirven para restaurar un equipo informático, después de haber ocurrido un ataque, un desastre, para recuperar archivos que hayan sido borrados sin querer, y lo más importante de todo, es que es obligatorio, pues es necesario guardar los datos.

Se recomienda la implementación de cajas fuertes y procedimientos para almacenar las copias de respaldos de los datos. Estos se deben ubicar en lugares seguros contra incendios, inundaciones y terremotos.

Existen muchos soportes para la realización de estas copias, actualmente en el mercado pueden encontrarse:

- Casetes digitales
- Cintas de audio digital.
- Cintas magnéticas de cartucho.
- Cartuchos de cinta de 8 mm.
- Cintas de nueve pistas.
- Tocadiscos de cintas.
- Discos ópticos.
- Worm.
- Discos externos

#### 2.3.7.5. Controles Eléctricos

Con la parte eléctrica se debe tener mucho cuidado, debido a que es la fuente de alimentación de todos los equipos del centro de cómputo, con esta finalidad se deben considerar algunos aspectos y así asegurar un continuó suministro del fluido eléctrico. *Véase Anexo M.*

Es importante tener contratadas dos compañías independientes suministradoras de electricidad, evitando de esta manera la falta de alimentación eléctrica.

En caso de no disponer de una segunda fuente de energía externa, se debe salvaguardar la continuidad de la corriente mediante baterías que aseguren automáticamente y sin interrupción el funcionamiento adecuado de la instalación al menos durante 60 horas o bien grupos electrógenos.

Existen muchas formas de prevención como por ejemplo:

- Sistemas de alimentación ininterrumpida
- Sistemas de generación eléctrica
- Tableros de transferencias automáticas
- PDU (unidad de distribución de energía).

Así mismo, existen eventos muy comunes en la parte de control eléctrico, como lo son:

- *Picos de Tensión:* Los picos de tensión, son otro problema que puede tener cualquier entidad y consiste en una sobrecarga en la corriente eléctrica, provocando pequeños daños en los equipos informáticos.

Se recomienda el uso de SAIS, los cuales consisten como dicen sus siglas, en un sistema de alimentación ininterrumpida, gracias a estos dispositivos, en caso de que exista un pico de tensión, mantendrá al equipo, en un estado a salvo de cualquier posible daño.

### 2.3.7.6. Controles Ambientales y del Entorno

Cuando hablamos de seguridad ambiental, nos estamos refiriendo a los procedimientos, procesos y controles con el fin de controlar los efectos de la naturaleza, los cuales pueden dañar seriamente al personal de la entidad, equipos informáticos y los datos de la empresa.

Debido a la permanente facilidad de dañarse los equipos electrónicos cuando se exponen al calor, es conveniente su instalación en salas debidamente acondicionadas que permitan un control riguroso de la temperatura y humedad del ambiente. *Véase Anexo N.*

Para su cuidado y prevención de riesgos, se utilizan los siguientes sistemas tecnológicos:

- Sistemas de aire acondicionado
- Sensores de temperatura
- Sensores de humedad

### 2.3.7.7. Seguridad Física de Datos

Deben protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo, es necesaria, para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

Así mismo, se debe considerar la ubicación y eliminación de los equipos. Se requieren controles especiales de protección, contra amenazas físicas, para

salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

Hacer que los vigilantes de seguridad, impidan a cualquiera (empleados, visitas, personas de soporte TI, mensajeros, personal de mudanzas) sacar equipos informáticos de las instalaciones sin autorización escrita. Estar especialmente atento a puertas traseras, rampas de carga, salidas para fumadores. Para hacer los chequeos más eficientemente, se toma en consideración el uso de códigos de barras. El objetivo principal, es el evitar la pérdida, daño, robo o puesta en peligro, de los activos e interrupción de las actividades de la organización.

### 2.3.7.8. Seguridad Física de Servidores

Para mejorar la protección, organización y la seguridad de los servidores de cualquier empresa, hoy en día se utilizan algunos implementos de seguridad que son diseñados para este objetivo. *Véase Anexo O.*

Se pueden enumerar algunos como son:

- *Racks:* Los racks o gabinetes de organización, han sido analizados y diseñados para el albergue de los activos informáticos, incrementando su nivel de seguridad con elementos a prueba de fuego, contra golpes, cerraduras manuales o electrónicas, mejorando el nivel de circulación de aíre, entre otras características, que serán importantes al momento de implementación de un Data Center.

### 2.3.7.9. Seguridad Física de Equipos de Redes

De igual manera, para la organización, distribución y aseguramiento de los equipos de redes de cualquier data center en una organización, se debe utilizar los mismos componentes o herramientas de seguridad enunciados en el ítem anterior, donde se especifica, por ejemplo los armarios rack que ofrecen protección contra golpes, robos de equipos y acceso a los equipos. *Véase Anexo P.*

Así mismo, se debe tener en cuenta los otros sistemas de seguridad como lo son los teclados numéricos, tarjetas magnéticas o lectores biométricos, que hacen posible incrementar la seguridad en los equipos de redes.

#### 2.3.7.10. Seguridad Física de Equipos de Telecomunicaciones

Los equipos de telecomunicaciones, que son utilizados para la transmisión de información a larga distancia, también deben contar con sistemas de seguridad, que aseguren la permanencia, continuidad de operación y el posible robo de los equipos. *Véase Anexo Q.*

Se puede enumerar algunos sistemas como por ejemplo tenemos:

- APS (Unidad de Generación Autónomo)
- Repetidoras de comunicaciones
- Sistemas de monitoreo
- Cercas eléctricas
- Sensores infrarrojos
- Paneles solares

### 2.3.8. Seguridad Lógicas

Es muy importante ser consciente, que por más que la empresa sea muy segura desde el punto de vista de ataques internos y externos, como por ejemplo hackers, virus, ingeniería social; la seguridad de la misma será nula, si no se ha previsto, como combatir alguno de estos tipos de amenazas.

La seguridad lógica es uno de los aspectos más olvidados, a la hora del diseño de un sistema informático.

El desarrollo de la auditoría de gestión de seguridad de la WAN a nivel lógico, consiste en la evaluación de las aplicaciones, barreras lógicas (software) y procedimientos de control (normativas, estándares, etc.), como medidas de prevención y contramedidas, ante amenazas a los recursos e información confidencial, con lo cual se determina el nivel de seguridad aplicado en el ámbito lógico, para precautelar la disponibilidad y confiabilidad de la información.

Refiriéndose de esta manera, a los controles y mecanismos de seguridad, implementados a los medios de acceso remoto, medios de almacenamiento de datos, sistemas críticos y principalmente a la información.

Para lograr el objetivo del proceso de auditoría de la gestión de seguridad de la WAN a nivel lógico, se procederá a enunciar algunos de los elementos críticos con los que se debe tratar, para evitar ataques o fugas de información dentro de la empresa. Así mismo, se enunciara las normas que se aplicaran para el control de las seguridades.

#### 2.3.8.1. Piratas Informáticos

Su actividad consiste en la copia ilegal de programas, rompiendo sus sistemas de protección y licencias. Luego éstos, se distribuyen de manera abierta, a través de internet o cualquier tipo de medio de almacenaje tecnológico.

Dentro de estos podemos enunciar los siguientes:

- *Hackers:* Es un vocablo utilizado por los informáticos, para referirse a un experto en varias o en alguna rama técnica relacionada con la informática tales como: programación, redes de computadora, sistemas operativos, tecnología informática.

  Es una persona apasionada, por descubrir o aprender nuevas cosas y entender el funcionamiento de estos, para bien o para mal. Pueden romper seguridades en los sistemas de una empresa, por diversión o explotar datos privados, pero la ética hacker no permite divulgar esos datos privados ya que sería un acto de vandalismo.

- *Crackers:* Es una persona con grandes conocimientos informáticos y con un propósito de luchar en contra de lo que está prohibido, empieza a investigar la forma de bloquear o traspasar protecciones hasta lograr su objetivo.

  Los crackers, usan programas propios o bajados del internet gratuitamente, con estos programas, se intenta desbloquear claves de acceso con generadores automáticos de claves.

  Se distinguen varios tipos de crackers:

- *Lammer:* Es una persona con pocos conocimientos informáticos, que consiguen herramientas ya creadas para atacar ordenadores. Ejecutan aplicaciones, sin saber que están causando grandes daños.
- *Trasher:* Son personas que buscan en la basura y en papeleras, número de tarjetas de crédito, claves de acceso, cuentas bancarias, cuentas de correo, cuentas de sistemas críticos.; para cometer estafas y actividades fraudulentas a través del Internet.
- *Insiders:* Crackers corporativos, empleados de las empresas que atacan desde dentro, movidos usualmente por motivos de venganza.

Luego de ver, como nuestro sistema puede verse afectado por varios motivos y principalmente por la falta de seguridad física, es importante recalcar, que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos, sino por medios lógicos, contra información almacenada y procesada dentro de los activos informáticos de la Institución.

El activo más importante que se posee una empresa es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que aseguren la información. Estas técnicas, las brinda la seguridad lógica.

Es decir, que la seguridad lógica, consiste en la aplicación de barreras y procedimientos, que resguarden el acceso a los datos y sólo se permita acceder a ellos, a las personas autorizadas para hacerlo.

Los objetivos que plantean este tipo de seguridades son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y sea imposible modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizado los datos, archivos y programas correctos.
- Que la información transmitida, sea recibida, sólo por el destinatario al que ha sido enviada.
- Que la información recibida, sea la misma que ha sido transmitida.

- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia, para la transmisión de información.

#### 2.3.8.2. Virus Informático

Los virus informáticos, son programas de software, desarrollados por personas con conocimientos definidos sobre programación, que se ejecutan y se propagan local o mundialmente, realizando copias de sí mismo, en archivos o documentos, infectando otros ordenadores conectados dentro de la red de área local o dentro de las redes WAN.

La principal característica, es el consumo de recursos que ocasionan problemas, tales como: la pérdida de productividad, que la PC no este 100% funcionando, pérdida de información. Otra característica es que tienen la capacidad de replicarse por todo el ordenador, ya sea localmente o por medio de redes que no tienen seguridades adecuadas.

Los virus pueden causar diferentes acciones como:

- Unirse con un programa instalado en la computadora, permitiendo la propagación.
- Mostrar en la pantalla, mensajes o imágenes humorísticas, pero molestas.
- Hacer lento el procesamiento de la computadora o bloquear la misma.
- Eliminar información importante, almacenada en el disco, a veces, impidiendo el funcionamiento de la computadora.
- Reducir el espacio de almacenamiento en el disco.
- Molestar al usuario cerrando ventanas, moviendo el ratón.

Un virus, puede propagarse por medio del usuario que acepta, o de forma involuntaria, instala el virus, o si no, el virus actúa replicándose por la red; de esta manera, el sistema operativo comienza a sufrir una serie de comportamientos no deseados y esos comportamientos, pueden dar pista que existe un virus.

Las contaminaciones más frecuentes realizadas por el usuario se encuentran en:

- Mensajes que ejecutan automáticamente programas.
- Ingeniería social, mensajes como “Ejecute este programa y gane un premio”.
- Entrada de información infectada en discos de otros usuarios.
- Instalación de software que contienen programas maliciosos.
- Por unidades extraíbles de almacenamiento infectadas.

En la actualidad los medios más comunes y frecuentes para la propagación de los virus son por medio de las unidades extraíbles denominadas memorias USB. (Viera, 2005)

### 2.3.9. Seguridad en el Acceso de la Información

La seguridad en el acceso a la información es muy importante, por lo tanto los datos de la empresa deben ser sumamente protegidos contra todo tipo de riesgos, que constantemente se interceptan en la organización, poniendo en peligro de que la información precisa sea divulgada ocasionando graves problemas, en todo tipo de trabajo, por eso se ve factible, colocar o implementar herramientas o estándares, como una forma de protección para dichos problemas.

### 2.3.10. Acceso a la Información

Se asegura, que se limite el acceso a información privada desde un ordenador, por medios de autenticación. Si verifica contraseñas y tiempos de vida de cada contraseña, así como, un registro de los cambios a la información y por quien han sido modificados. Se verifica firewalls para la restricción de puertos que no se estén usando y que se registren las vulnerabilidades de dichos puertos.

### 2.3.11. Control de Sistemas e Informática

El control de sistemas e informática, consiste en examinar los recursos, las operaciones, los beneficios y los gastos de las producciones, de los organismos sujetos a control, con la finalidad de evaluar la eficacia y eficiencia administrativa, técnica y operacional.

Así mismo de los sistemas (planes, programas y presupuestos, diseño, software, hardware, seguridad y respaldos) adoptados por la empresa. Existe otra definición sobre el "control técnico" en materia de sistemas e informática, y esta, se orienta, a la revisión del diseño de los planes, diseños de los sistemas, la demostración de su eficacia, pruebas de productividad de gestión, el análisis de resultados, niveles y medios de seguridad, respaldo y el almacenamiento.

Los controles pueden ser de dos tipos: control visual, que permite eliminar muchos riesgos de forma sencilla, y los controles de validez, que se basan en estadísticas, que indican posibles riesgos inminentes, de tal forma que se pueda prevenir. Un control es una muestra de acciones ejecutadas, su función es establecer, ejecutar, modificar y mantener actividades de control, de modo que la fiabilidad global del sistema sea aceptable.

Se detallan algunos de los controles más importantes:

- *Controles de autenticidad:* Para verificar la identidad de un usuario, que quiera tomar alguna acción en el sistema, como passwords, números de identificación personal.
- *Controles de precisión*: Para asegurar la corrección de la información y procesos en el sistema, como un programa o rutina, que controle el tipo de dato ingresado.
- *Controles de completitud*: Asegurarse, de que no hay pérdida de información y que todo proceso se concluya adecuadamente, como revisar que no haya dos campos vacíos.
- *Controles de redundancia*: Para asegurar, que la información es procesada una sola vez.
- *Controles de privacidad:* Impedir que usuarios no autorizados accedan a información protegida.
- *Controles de auditoría*: Tratar de asegurar que queden registrados cronológicamente todos los eventos que ocurren en el sistema. Este registro es muy importante para responder preguntas, determinar irregularidades, detectar las consecuencias de un error. Deben mantenerse dos tipos de auditoría: la auditoría de cuentas y la auditoría de operaciones.

- *Controles de existencia*: Asegurar la disponibilidad continua de todos los recursos y datos del sistema.
- *Controles de salvaguarda de activos*: Para asegurar que todos los recursos dentro del sistema están protegidos de la destrucción o corrupción.
- *Controles de eficacia*: Asegurar que el sistema alcanza sus objetivos.
- *Controles de eficiencia*: Asegurar que el sistema utiliza el mínimo número de recursos, para conseguir sus objetivos.

### 2.3.12. Inventario de Cumplimiento Seguridades Lógicas

Para poder determinar el nivel de seguridad de la red, actualmente en la Institución, se realiza la auditoría de gestión de seguridad de la WAN a nivel lógico, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo R.*

#### 2.3.12.1. Seguridad de Sistemas Operativos

Un sistema operativo (SO), software básico que controla una computadora. Un SO, es en sí mismo, un programa de computadora. Sin embargo, es un programa muy especial, quizá el más complejo e importante en una computadora, debido que el mismo pone a funcionar toda la parte de hardware y software, para un objetivo específico.

Además, proporciona la facilidad para que los usuarios se comuniquen con la computadora y sirve de plataforma a partir de la cual se corran programas de aplicación.

Para poder determinar el nivel de la seguridad lógica de los sistemas operativos como están en la actualidad, en la Institución, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo S.*

### 2.3.12.2. Seguridad de Software

Los utilitarios o utilidades, son programas diseñados, para realizar una función determinada, por ejemplo un editor, un depurador de código o un programa para recuperar datos perdidos o borrados accidentalmente en el disco duro.

El término utilitario se refiere normalmente al software que resuelve problemas relacionados con la administración del sistema de la computadora.

Existen en nuestros medios programas utilitarios que nos ayudan a resolver gran cantidad de problemas, entre ellos tenemos las llamadas utilidades Norton, Disk Manager.

En informática, una utilidad, es una herramienta que realiza:

- Tareas de mantenimiento
- Soporte para la construcción y ejecución de programas
- Las tareas en general

Para poder determinar el nivel de la seguridad lógica del Software como están, en la actualidad, en la Institución, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo T.*

### 2.3.12.3. Seguridad de Equipos de Comunicaciones

Los equipos de comunicación hoy en día, han evolucionado al extremo, de que en su interior, a parte de su hardware, se han introducido software, el mismo que ayuda a configurar y asegurar las comunicaciones y de esta manera siempre evolucionar para mejorar el rendimiento.

Para esto debemos considerar el administrar los siguientes ítems:

- Firmware
- Medios de acceso a la configuración

- Sistemas operativos de equipos de comunicación
- Túneles
- VPN

Para poder determinar, el nivel de la seguridad lógica del software de los equipos de networking como están, en la actualidad, en la Institución, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo U.*

### 2.3.12.4. Seguridad de Servidores

Un servidor, es una computadora diferente a las de uso común, que da servicio a otros ordenadores llamados clientes. También se suele denominar a un servidor, como una aplicación informática, que realiza determinadas tareas, en beneficio de otras aplicaciones clientes.

Ofrece servicio de acceso a aplicaciones, archivos o información, permite almacenar y acceder a archivos de una computadora y servicios de aplicaciones, que los realiza el usuario final.

Para esto, se han determinado el análisis, diseño e implementación de los siguientes tipos de servidores que ayuden al control del acceso y la seguridad:

- Servidores DHCP
- Servidores DNS
- Servidores WINS
- Servidores PROXY
- Servidores NAT
- Servidores PAT

Para poder determinar, el nivel de la seguridad lógica del software y configuraciones de los servidores, como están en la actualidad, en la Institución, se hace necesaria la utilización de medios de obtención de la información.

Por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo V.*

### 2.3.12.5. Seguridad de Firewalls

Un cortafuego (firewall en inglés), es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo, comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados, para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos, sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos, pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Todos los mensajes, que entren o salgan de la Intranet pasan a través de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados.

También es frecuente conectar a los cortafuegos a una tercera red, llamada «zona desmilitarizada» o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La SI abarca más ámbitos y más niveles de trabajo y protección. Existen distintos tipos de firewalls, que pueden ser clasificados de diversas maneras en:

- Firewall en Hardware
- Cisco Asa
- IDS
- IPS
- Firewall en Software

- Aplicaciones
- Redes
- Shorewall
- Seguridad AAA

Para poder determinar, el nivel de la seguridad lógica del software y configuraciones de los equipos firewall, como están en la actualidad, en la Institución, se hace necesaria la utilización de medios de obtención de la información.

Por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo W.*

### 2.3.12.6. Seguridad de Bases de Datos

Una base de datos o banco de datos, es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca, puede considerarse una base de datos, compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

Actualmente, y debido al desarrollo tecnológico de campos como la informática y la electrónica, la mayoría de las bases de datos están en formato digital (electrónico), y por ende, se ha desarrollado y se ofrece un amplio rango de soluciones al problema del almacenamiento de datos.

Existen programas denominados Sistemas Gestores de Bases de Datos (SGBD), que permiten almacenar y posteriormente, acceder a los datos de forma rápida y estructurada. Las propiedades de estos SGBD, así como su utilización y administración, se estudian dentro del ámbito de la informática. Las aplicaciones más usuales son para la gestión de empresas e instituciones públicas.

También son ampliamente utilizadas, en entornos científicos con el objeto de almacenar la información experimental. Existen muchas formas de clasificar a las bases de datos.

Una de ellas es según el contenido:

- Bases de datos bibliográficas
- Bases de datos de texto completo
- Bases de datos estáticas
- Bases de datos dinámicas

Para poder determinar, el nivel de la seguridad lógica del software y configuraciones de las bases de datos como están, en la actualidad, en la Institución, se hace necesaria la utilización de medios de obtención de la información, por tal motivo, se ha creado un formulario de checklist, el mismo que revisa los aspectos más básicos de la seguridad a nivel lógico. *Véase Anexo X.*

# CAPÍTULO 3

## METODOLOGIA DE INVESTIGACION

### 3.1. Ubicación Geográfica del Proyecto de Investigación

El presente proyecto, se lo desarrollara en el Data Center de la Institución, ubicada en la Provincia de Loja, donde se analizara las seguridades del mismo, tanto a nivel físico como lógico de los activos informáticos del Data Center, donde se encuentra almacenada la información de cada uno de los procesos que se genera en la Institución.

### 3.2. Metodología de Investigación

La investigación puede ser de varios tipos, y en tal sentido se puede clasificar de distintas maneras, sin embargo es común hacerlo en función de su nivel, su diseño y su propósito.

Sin embargo, dada la naturaleza compleja de los fenómenos estudiados, por lo general, para abordarlos, es necesario aplicar no uno sino una mezcla de diferentes tipos de investigación. De hecho es común, hallar investigaciones que son simultáneamente descriptivas y transversales, por sólo mencionar un caso.

El nivel de investigación: Este, se refiere al grado de profundidad con que se aborda un fenómeno u objeto de estudio.  Así, en función de su nivel, el tipo de investigación puede ser: descriptiva, exploratoria o explicativa.

#### 3.2.1. Investigación Descriptiva

En las investigaciones de tipo descriptiva, llamadas también investigaciones diagnósticas, buena parte de lo que se escribe y estudia sobre lo social, no va mucho más allá de este nivel. Consiste, fundamentalmente, en caracterizar un fenómeno o situación concreta, indicando sus rasgos más peculiares o diferenciadores.

En la ciencia fáctica según Bunge, la descripción consiste en responder a las siguientes cuestiones:

- ¿Qué es? > Correlato.
- ¿Cómo es? > Propiedades.
- ¿Dónde está? > Lugar.
- ¿De qué está hecho? > Composición.
- ¿Cómo están sus partes, si las tiene, interrelacionadas? > Configuración.
- ¿Cuánto? > Cantidad

El objetivo de la investigación descriptiva es llegar a conocer las situaciones, costumbres y actitudes predominantes, a través de la descripción exacta de las actividades, objetos, procesos y personas. Su meta no se limita a la recolección de datos, sino a la predicción e identificación de las relaciones que existen entre dos o más variables.

Los investigadores, no son meros tabuladores, sino que, recogen los datos sobre la base de una hipótesis o teoría, exponen y resumen la información, de manera cuidadosa y luego analizan minuciosamente los resultados, a fin de extraer generalizaciones significativas que contribuyan al conocimiento.

#### 3.2.1.1. Etapas de la Investigación Descriptiva

Para proceder a realizar una investigación descriptiva de la mejor manera, se deben cumplir las siguientes etapas:

- Examinan las características del problema escogido.
- Lo definen y formulan sus hipótesis.
- Enuncian los supuestos en que se basan las hipótesis y los procesos adoptados.
- Eligen los temas y las fuentes apropiadas.
- Seleccionan o elaboran técnicas para la recolección de datos.
- Establecen categorías precisas, a fin de clasificar los datos, que se adecúen al propósito del estudio y permitan poner de manifiesto, las semejanzas, diferencias y relaciones significativas.

- Verifican la validez de las técnicas empleadas para la recolección de datos.
- Realizan observaciones objetivas y exactas.
- Describen, analizan e interpretan los datos obtenidos, en términos claros y precisos.

### 3.2.1.2. Recolección de Datos de la Investigación Descriptiva

En el informe de la investigación, se señalan los datos obtenidos y la naturaleza exacta de la población de donde fueron extraídos. La población a veces llamada universo o agregado constituye siempre una totalidad. Las unidades que la integran pueden ser individuos, hechos o elementos de otra índole.

Una vez identificada la población con la que se trabajará, se decide, si se recogerán datos de la población total o de una muestra representativa de ella. El método elegido dependerá de la naturaleza del problema y de la finalidad para la que se desee utilizar los datos, para esto tenemos dos métodos:

- *Población total:* Muchas veces, no es difícil obtener información acerca de todas las unidades que componen una población reducida, pero los resultados no pueden aplicarse a ningún otro grupo, que no sea el estudiado.
- *Muestra de la población:* Cuando se trata de una población excesivamente amplia, se recoge la información a partir de unas pocas unidades cuidadosamente seleccionadas, ya que si se aborda cada grupo, los datos perderían vigencia, antes de concluir el estudio.

  Si los elementos de la muestra, representan las características de la población, las generalizaciones basadas en los datos obtenidos, pueden aplicarse a todo el grupo.

### 3.2.1.3. Expresión de Datos de la Investigación Descriptiva

Los datos descriptivos, se expresan en términos cualitativos y cuantitativos. Se puede utilizar uno de ellos o ambos a la vez.

- *Cualitativos (mediante símbolos verbales):* Se usan en estudios cuyo objetivo es examinar la naturaleza general de los fenómenos. Los estudios cualitativos proporcionan una gran cantidad de información valiosa, pero poseen un limitado grado de precisión, porque emplean términos cuyo significado varía para las diferentes personas, épocas y contextos.
  Los estudios cualitativos contribuyen a identificar los factores importantes que deben ser medidos. (Visión cientificista).

- *Cuantitativos (por medio de símbolos matemáticos):* Los símbolos numéricos que se utilizan para la exposición de los datos provienen de un cálculo o medición. Se pueden medir las diferentes unidades, elementos o categorías identificables.

### 3.2.1.4. Tipos de Investigación Descriptiva

Tomando en cuenta que las siguientes categorías no son rígidas, muchos estudios pueden encuadrarse sólo en alguna de estas áreas, y otros corresponden a más de una de ellas. Encuestas, estudio de interrelaciones y estudios de desarrollo.

- *Estudios tipo encuesta:* Se llevan a cabo, cuando se desea encontrar la solución de los problemas que surgen en organizaciones educacionales, gubernamentales, industriales o políticas. Se efectúan minuciosas descripciones de los fenómenos a estudiar, a fin de justificar las disposiciones y prácticas vigentes o elaborar planes más inteligentes que permitan mejorarlas.
  Su objetivo no es sólo determinar el estado de los fenómenos o problemas analizados, sino también comparar la situación existente, con las pautas aceptadas.

  El alcance de estos estudios varía considerablemente; pueden circunscribirse a una nación, región, estado, sistema escolar, de una ciudad o alguna otra unidad. Los datos pueden extraerse, a partir de toda la población o de una muestra cuidadosamente seleccionada. La información recogida puede referirse a un gran número de factores relacionados con el fenómeno o sólo a unos pocos aspectos recogidos. Su alcance y profundidad, dependen de la naturaleza del problema.

- *Estudios de interrelaciones:* Si el objeto es, identificar las relaciones que existen entre los hechos para lograr una verdadera comprensión del fenómeno a investigar, los estudios de esta índole son los estudios de casos, estudios causales comparativos y estudios de correlación.
- *Estudio de casos:* El investigador, realiza una indagación intensiva de una unidad social o comunidad. Para ello recoge información acerca de la situación existente en el momento en que realiza su tarea, las experiencias y condiciones pasadas y las variables ambientales que ayudan a determinar las características específicas y conducta de la unidad. Después de analizar las secuencias e interrelaciones de esos factores, elabora un cuadro amplio e integrado de la unidad social, tal como ella en realidad funciona.

El interés en los individuos, no es considerándolo como personalidad única, sino como tipos representativos. Se reúnen los datos a partir de una muestra de sujetos cuidadosamente seleccionados y se procuran extraer generalizaciones válidas sobre la población que representa la muestra.

El objetivo de los estudios de casos consiste en realizar una indagación a profundidad dentro de un marco de referencia social; las dimensiones o aspectos de dicho marco dependen de la naturaleza del caso estudiado.

El estudio de casos, debe incluir una considerable cantidad de información acerca de: personas, grupos y hechos, con los cuales el individuo entra en contacto y la naturaleza de sus relaciones con aquéllos. Los seres humanos desarrollan una constante interacción con diversos factores ambientales, por eso es imposible comprender su conducta sin examinar tales relaciones. Los datos deben provenir de muchas fuentes. Se puede interrogar a los sujetos, mediante entrevistas o cuestionarios y pedirles que evoquen experiencias pasadas o sus deseos y expectativas presentes. Se estudian documentos personales como: diarios y cartas, efectuando, distintas mediciones físicas, psicológicas o sociológicas. Se puede interrogar a padres, hermanos y amigos de los sujetos, analizar archivos de los tribunales, escuelas, hospitales, empresas o instituciones sociales.

Los estudios de casos son similares a las encuestas, pero en ellos hay un estudio intensivo de una cantidad limitada de casos representativos, en lugar de reunir datos de pocos aspectos de un gran número de unidades sociales. Tiene un alcance más limitado pero es más exhaustivo que el de encuestas, y le da mayor importancia a los factores cualitativos.

- *Estudios causales comparativos:* Si además de pretender descubrir, cómo es un fenómeno, se quiere saber de qué manera y por qué ocurre, entonces se comparan las semejanzas y diferencias entre fenómenos, para descubrir los factores o condiciones, que parecen acompañar o contribuir a la aparición de ciertos hechos y situaciones. Por la complejidad y naturaleza de los fenómenos sociales, es menester estudiar las relaciones de causalidad. Este tipo de estudio, se usa en los casos, en que los investigadores no pueden manejar una variable independiente y establecer los controles requeridos en los experimentos.

  En un estudio causal comparativo, el investigador analiza la situación vital, en la cual, los sujetos han experimentado el fenómeno que se quiere investigar. Después de estudiar las semejanzas y diferencias que hay entre dos situaciones, podrá describir los factores que parecen explicar la presencia del fenómeno en una situación y su ausencia en la otra.

  Esta indagación tiene su origen en el método utilizado por John Stuart Mill, para descubrir las situaciones causales, que establece que: “si dos o más instancias del fenómeno investigado tienen sólo una circunstancia en común, en la cual todas las instancias concuerdan, es la causa (o efecto) del fenómeno dado”. Este método proporciona al investigador la doble posibilidad de control sobre sus conclusiones acerca de las relaciones de causalidad.

- *Estudios de correlación:* Se utilizan, para determinar la medida en que dos variables se correlacionan entre sí, es decir el grado en que las variaciones que sufre un factor se corresponden con las que experimenta el otro.

  Las variables, pueden hallarse estrecha o parcialmente relacionadas entre sí, pero también es posible que no exista entre ellas relación alguna. Puede decirse, en general, que la magnitud de una correlación, depende de la medida en que los

valores de dos variables aumenten o disminuyan en la misma o en diferente dirección.

Si los valores de dos variables aumentan o disminuyen de la misma manera, existe una correlación positiva; si, en cambio, los valores de una variable aumentan en tanto que disminuyen los de la otra, se trata de una correlación negativa; y si los valores de una variable aumentan, los de la otra pueden aumentar o disminuir, entonces hay poca o ninguna correlación.

En consecuencia, la gama de correlaciones se extiende desde la perfecta correlación negativa hasta la no correlación o la perfecta correlación positiva. Las técnicas de correlación, son muy útiles en los estudios de carácter predictivo.

Si bien, el coeficiente de correlación, sólo permite expresar en términos cuantitativos el grado de relación que dos variables guardan entre sí, no significa que tal relación, sea de orden causal.

Para interpretar el significado de una relación, se debe recurrir al análisis lógico, porque la computación estadística, no dilucida el problema. Sus riesgos son los mismos que en los estudios causales comparativos.

- *Estudios de desarrollo:* Consiste en determinar, no sólo las interrelaciones y el estado en que se hallan los fenómenos, sino también los cambios que se producen en el transcurso del tiempo. En él, se describe el desarrollo que experimentan las variables durante un lapso, que puede abarcar meses o años. Abarca estudios de crecimiento y de tendencia.

- *Estudios de crecimiento:* Se refieren a la identificación de los diversos factores interrelacionados que influyen sobre el crecimiento en sus diferentes etapas, saber en qué momento se tornan observables los diversos aspectos y cuándo surgen, permanecen estacionarios, alcanzan su desarrollo óptimo, y, finalmente, decaen. Para el estudio del desarrollo humano se usan dos métodos: las técnicas lineales y las de corte transversal. En ambos tipos de investigación, se deben efectuar una serie de observaciones sistemáticas.

El objetivo de las técnicas lineales es, medir el grado de crecimiento de determinados niños en distintas edades, por ejemplo; y en los de corte transversal, no se medirían los mismos niños a intervalos regulares, sino se efectuaría un registro de medidas de diferentes niños pertenecientes a distintos grupos de edad.

Los estudios de corte transversal, incluyen generalmente, a una mayor cantidad de sujetos, y describen un número menor de factores de crecimiento, que los estudios lineales. La técnica de corte transversal, se usa con más frecuencia por su bajo costo y porque ocupa menos tiempo; la técnica lineal es la más adecuada, para estudiar el desarrollo humano.

Ambas técnicas, plantean problemas de muestreo: en los de corte transversal es posible que los diferentes sujetos de cada nivel de edad, no sean comparables; los lineales obtienen información de un número limitado de sujetos, sin la confiabilidad de muestras más amplias, asimismo la dificultad para el investigador de evaluar y perfeccionar con cierta frecuencia sus técnicas, pues una vez iniciada la investigación no es posible interrumpirla para modificar o mejorar los procedimientos empleados. Para estudios lineales, hacen falta apoyos económicos y un equipo de trabajo ininterrumpido durante años.

- *Estudios de tendencia*: Consisten en obtener datos sobre aspectos sociales, económicos y políticos y en analizarlos posteriormente, para identificar las tendencias fundamentales y predecir los hechos que pueden producirse en el futuro.

En ellos se combinan a veces técnicas históricas, documentales y las que se usan en las encuestas. Resulta aventurado formular predicciones basadas en los datos de tendencia social, porque las condiciones económicas, los avances tecnológicos, las guerras, las aspiraciones individuales y otros hechos imprevisibles, pueden modificar de manera repentina el curso esperado de los acontecimientos.

A causa de los innumerables factores impredecibles que pueden ejercer influencia sobre los fenómenos sociales, la duración de los análisis de tendencia,

afecta en una medida considerable, la validez de la predicción; la mayoría de las predicciones de largo alcance constituyen meras estimaciones, en tanto que, las que se refieren a lapsos más breves, gozan de mayores posibilidades de certeza.

#### 3.2.1.5. Evaluación de la Investigación Descriptiva

Algunos problemas con que a veces tropiezan los investigadores, se refieren a exámenes críticos de los materiales originales, el vocabulario técnico, la formulación de hipótesis, la observación y experimentación, y la generalización y predicción.

### 3.2.2. Investigación Exploratoria

Es aquella que se efectúa sobre un tema u objeto desconocido o poco estudiado, por lo que sus resultados constituyen una visión aproximada de dicho objeto, es decir, un nivel superficial de conocimiento. Este tipo de investigación, de acuerdo con Sellriz (1980), puede ser:

- Dirigidos a la formulación más precisa de un problema de investigación , puesto que se carece de información suficiente y de conocimiento previo del objeto, materia de estudio, resulta lógico que la formulación inicial del problema sea imprecisa.

  En este caso la exploración, permitirá obtener nuevo datos y elementos, que pueden conducir a formular con mayor precisión las preguntas de investigación.

- Conducentes al planteamiento de una hipótesis: cuando se desconoce al objeto de estudio, resulta difícil formular hipótesis acerca del mismo.
  La función de la investigación exploratoria es, descubrir las bases y recabar información, que permita como resultado del estudio, la formulación de una hipótesis.

  Las investigaciones exploratorias son útiles por cuanto sirve para familiarizar al investigador con un objeto, que hasta el momento le era totalmente desconocido y sirve como base para la posterior investigación descriptiva.

Puede crear, en otros investigadores el interés por el estudio de un nuevo tema o problema y ayudar a precisar o a concluir con la formulación de una hipótesis, sobre cierto caso.

### 3.2.3. Investigación Explicativa

Se encarga de buscar el porqué de los hechos, mediante el establecimiento de relaciones causa-efecto. En este sentido, los estudios explicativos pueden ocuparse tanto de la determinación de las causas (investigación postfacto), como de los efectos (investigación experimental), mediante la prueba de hipótesis. Sus resultados y conclusiones constituyen el nivel más profundo de conocimientos.

La investigación explicativa intenta dar cuenta de un aspecto de la realidad, declarando su significatividad, dentro de una teoría de referencia, a la luz de leyes o generalizaciones, que dan cuenta, de hechos o fenómenos que se producen en determinadas condiciones.

Dentro de la investigación científica, a nivel explicativo, se dan dos elementos:

- Lo que se quiere explicar: Trata del objeto, hecho o fenómeno que ha de explicarse, es el problema generado por la pregunta que necesita una explicación.
- Lo que se explica: La explicación se deduce (a modo de una secuencia hipotética deductiva) de un conjunto de premisas compuesto por: leyes, generalizaciones y otros enunciados que expresan regularidades que deben que acontecer.

  En este sentido, la explicación es siempre una deducción de una teoría que contiene afirmaciones que explican hechos particulares. (Hernández, Fernández, & Baptista, 1997)

## 3.3. Auditoría Informática

La auditoría informática es un proceso llevado a cabo, por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los

fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costos, valor y barreras, que obstaculizan flujos de información eficiente.

En si la auditoría informática es de 2 tipos que son:

- *Auditoría Interna*: es aquella que se hace adentro de la empresa; sin contratar a personas de afuera.
- *Auditoría Externa*: como su nombre lo dice, es aquella en la cual la empresa contrata a personas de afuera, para que haga la auditoría en su empresa.

Auditar consiste principalmente en estudiar los mecanismos de control usando estrategias, para determinar los cambios que se deberían realizar, para la consecución de los objetivos propuestos. Los mecanismos de control pueden ser: directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos de la auditoría informática son:

- El análisis de la eficiencia de los sistemas informáticos
- La verificación del cumplimiento de la normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.

Sus beneficios son:

- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reprocesos, rechazos, reclamos, entre otros).

- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

- Desempeño
- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad
- Privacidad

Generalmente se puede desarrollar la auditoría informática, en algún área o combinación de las siguientes áreas:

- Gobierno corporativo
- Administración del ciclo de vida de los sistemas
- Servicios de entrega y soporte
- Protección y seguridad
- Planes de continuidad y recuperación de desastres

La necesidad de contar con lineamientos y herramientas estándar, para el ejercicio de la auditoría informática, ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL.

Actualmente la certificación de ISACA, para ser CISA (Certified Information Systems Auditor), es una de las más reconocidas y avaladas por los estándares internacionales, ya que el proceso de selección consta de un examen inicial, bastante extenso y la necesidad de mantenerse actualizado, acumulando horas (puntos) para no perder la certificación.

### 3.3.1. Clasificación de las Auditorías Informáticas

La operatividad de los sistemas ha de constituir entonces la principal preocupación del auditor informático. Para conseguirla, hay que acudir a la realización de controles técnicos generales de operatividad y controles técnicos específicos de operatividad, previos a cualquier actividad de aquel.

Dentro de las áreas generales, es posible establecer los siguientes tipos de Auditoría:

- *Auditoría Informática de Explotación:* Se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos magnéticos para otros informáticos, órdenes automatizadas para lanzar o modificar procesos industriales, etc. Para realizar la explotación informática, se dispone de la materia prima (los datos), que sean necesarios transformar, sometiéndose previamente a controles de integridad y calidad.

  La transformación se realiza por medio del proceso informático, el cual está dirigido por programas. Obtenido el producto final, los resultados son sometidos a controles de calidad, y finalmente son distribuidos al cliente, al usuario. En ocasiones, el propio cliente realiza funciones de reelaboración del producto terminado.

  Con el fin de mantener el criterio finalista y utilitario, el concepto de centro productivo ayuda a la elaboración de la auditoría de la explotación, que consiste en auditar, las secciones que la componen y sus interrelaciones.

  Las básicas son: la planificación de la producción y la producción misma de resultados informáticos. El auditor debe tener en cuenta, que la organización informática, está supeditada a la obtención de resultados en plazo y calidad, siendo subsidiario a corto plazo, cualquier otro objetivo. Se quiere insistir nuevamente, en que la operatividad es prioritaria, al igual que el plan crítico diario de producción, que debe ser protegido a toda costa. Para esto se tomaron los siguientes criterios:

  - *Control de entrada de datos:* Se analiza la captura de información, plazos y agenda de tratamiento y entrega de datos, corrección en la transmisión de

datos entre plataformas, verificación de controles de integridad y calidad de los mismos, se realizan de acuerdo a norma.

- *Planificación y Recepción de Aplicaciones:* Se auditarán las normas de entrega de aplicaciones, verificando cumplimiento y calidad de interlocutor único. Deberán realizarse muestras selectas de la documentación de las aplicaciones explotadas. Se analizarán las librerías que los contienen en cuanto a su organización y en lo relacionado con la existencia de planificadores automáticos o semiautomáticos.

- *Centro de Control y Seguimiento de Trabajos:* Se analizará cómo se prepara, se lanza y se sigue la producción diaria de los procesos Batch, o en tiempo real (Teleproceso). Las aplicaciones de teleproceso están activas y la función de explotación se limita a vigilar y recuperar incidencias, el trabajo Batch absorbe buena parte de los efectivos de explotación. Este grupo determina el éxito de la explotación, ya que es el factor más importante en el mantenimiento de la producción.

- *Operadores de Centros de Cómputos:* Destaca el factor de responsabilidad ante incidencias y desperfectos. Se analiza las relaciones personales, coherencia de cargos y salarios, la equidad de turnos de trabajos.
  Se verificará, la existencia de un responsable del centro de cómputo, el grado de automatización de comandos, existencia y grado de uso de manuales de operación, existencia de planes de formación, cumplimiento de los mismos y el tiempo transcurrido, para cada operador desde el último curso recibido.

  Se analizará cantidad de montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del sistema hasta el montaje real.

- *Centro de Control de Red y Centro de Help-desk:* El centro de control de red, suele ubicarse en el área de explotación. Sus funciones se refieren al ámbito de comunicaciones, estando relacionado con la organización de comunicaciones, software del departamento de sistemas. Debe analizarse la

fluidez de esa relación y el grado de coordinación entre ambos, se verificará la existencia de un punto focal único, desde el cual, sean perceptibles todas las líneas asociadas a los Sistemas.

El centro de Help-desk, es el ente, en donde se atienden las llamadas de los usuarios-clientes, que han sufrido averías o incidencias, tanto de software como de hardware. En función del cometido descrito, y en cuanto a software, está relacionado con el centro de control de red.

- *Auditoría Informática de Sistemas:* Se ocupa de analizar las actividades que realiza el departamento de sistemas, en todas sus facetas. Hoy en día, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones, líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de sistemas.

  A continuación se detallan los grupos a revisar:

  - *Sistemas Operativos*: Proporcionados por el fabricante junto al equipo. Engloba los subsistemas de teleproceso, entrada/salida, etc. Los sistemas deben estar actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones, si éstas se han producido. El análisis de las versiones de los S.O. permite descubrir posibles incompatibilidades entre algunos productos de software, adquiridos por la instalación y determinadas versiones. Deben revisarse los parámetros de las librerías importantes de los sistemas, especialmente si difieren de los valores aconsejados por el constructor.
  - *Software Básico*: Conjunto de productos que, sin pertenecer al S.O., configuran completamente los sistemas informáticos, haciendo posible la reutilización de funciones básicas no incluidas en aquél. ¿Cómo distinguir ambos conceptos? La respuesta tiene un carácter económico.

    El software básico, o parte de él, es abonado por el cliente a la firma constructora, mientras el sistema operativo y algunos programas muy básicos, se incorporan a la máquina, sin cargo al cliente.

Es difícil decidir, si una función debe ser incluida en el SO o puede ser omitida. Con independencia del interés teórico, que pueda tener la discusión de si una función es o no integrante del SO, para el auditor, es fundamental conocer los productos de software básico que han sido facturados aparte.

Los conceptos de S.O. y software básico tienen fronteras comunes, la política comercial de cada compañía y sus relaciones con los clientes determinan el precio y los productos gratuitos y facturables.

Otra parte importante del software básico, es el desarrollado e implementado en los sistemas informáticos por el personal informático de la empresa, que permite mejorar la instalación. El auditor debe verificar que el software no agrede, no condiciona al sistema, debe considerar el esfuerzo realizado en términos de costos, por si hubiera alternativas más económicas.

- *Software de Teleproceso*: Se ha agregado del apartado anterior de software básico por su especialidad e importancia. Son válidas las consideraciones anteriores, nótese la especial dependencia que el software del tiempo real tiene respecto a la arquitectura de los sistemas.
- *Tunning*: Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto.

Las acciones de Tunning deben diferenciarse de los controles y medidas habituales que realiza el personal de sistemas. El Tunning posee una naturaleza más revisora, estableciéndose previamente, planes y programas de actuación, según los síntomas observados.

Los Tunning pueden realizarse:

- Cuando existe la sospecha de deterioro del comportamiento parcial o general del sistema.
- De modo sistemático y periódico, por ejemplo cada seis meses. En este último caso, las acciones de Tunning son repetitivas y están planificadas y organizadas de antemano.

- El auditor informático deberá conocer el número de Tunning realizados el último año, sus resultados, analizará los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

- *Optimización de los Sistemas y Subsistemas:* El departamento de sistemas, debe realizar acciones permanentes de optimización, como consecuencia de la información diaria obtenida a través de Log, Account-ing, etc. Actúa igualmente, como consecuencia de la realización de Tunnings pre programado o específico.

  El auditor, verificará que las acciones de optimización fueron efectivas y no comprometieron la operatividad de los Sistemas ni el "plan crítico de producción diaria" de explotación.

- *Administración de Base de Datos*: Es un Área, que ha adquirido una gran importancia, a causa de la proliferación de usuarios y de las descentralizaciones informáticas de las empresas, el diseño de las bases de datos, ya sean relacionales o jerárquicas, se ha convertido en una actividad muy compleja y sofisticada, por lo general, desarrollada en el departamento de sistemas, y de acuerdo con las áreas de desarrollo y los usuarios de la empresa.

  El conocimiento de diseño y arquitectura de dichas bases de datos, por parte de los sistemas, ha cristalizado en la administración de las mismas. Aunque esta descripción es la más frecuente en la actualidad, los auditores informáticos, han observado algunas disfunciones, derivadas de la relativamente escasa experiencia, que tiene el personal sistemas, sobre la problemática general de los usuarios de las bases de datos.

  Comienzan a percibirse hechos tendientes a separar el diseño y la construcción de las bases de datos, de la administración de las mismas. Sin embargo, esta tendencia es aún poco significativa.

  El auditor informático de bases de datos, deberá asegurarse que explotación conoce suficientemente las que son accedidas por los procedimientos que ella ejecuta. Analizará los sistemas de salvaguarda existentes, que competen

igualmente a explotación. Revisará finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

- *Investigación y Desarrollo*: El campo informático sigue evolucionando rápidamente. Multitud de compañías, de software mayoritariamente, aparecen en el mercado.

  Como consecuencia, algunas empresas no dedicadas en principio a la venta de productos informáticos, están potenciando la investigación de sus equipos de sistemas y desarrollo, de forma que sus productos, puedan convertirse en fuentes de ingresos adicionales.

- *Auditoría Informática de Comunicaciones y Redes:* Se ha producido un cambio conceptual muy profundo en el tratamiento de las comunicaciones informáticas y en la construcción de los modernos sistemas de información, basados en redes de comunicaciones muy sofisticadas.

  Para el auditor informático, el entramado conceptual que constituyen las redes nodales, líneas, concentradores, multiplexores, redes locales, etc., no son sino el soporte físico-lógico del tiempo real.

  El lector debe reflexionar sobre este avanzado concepto, que repetimos: Las comunicaciones son el soporte físico-lógico de la informática en tiempo real. El auditor informático tropieza con la dificultad técnica del entorno, pues ha de analizar situaciones y hechos alejados entre sí, y está condicionado a la participación del monopolio telefónico, que presta el soporte en algunos lugares.

  Ciertamente, la tarea del auditor es ardua en este contexto. Como en otros casos, la auditoría de este sector, requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales. No debe olvidarse, que en entornos geográficos reducidos, algunas empresas optan por el uso interno de redes locales, diseñadas y cableadas con recursos propios.

  El entorno del online, tiene una especial relevancia en la auditoría informática, debido al alto presupuesto anual, que los alquileres de líneas significan. El auditor de comunicaciones, deberá inquirir sobre los índices de

utilización de las líneas contratadas, con información abundante, sobre tiempos de desuso.

Deberá proveerse de la topología de la red de comunicaciones, actualizada. La desactualización de esta documentación, significaría una grave debilidad. La inexistencia de datos sobre cuántas líneas existen, cómo son y dónde están instaladas, supondría que se bordea la inoperatividad informática.

Sin embargo, y como casi siempre, las debilidades más frecuentes e importantes en la informática de comunicaciones, se encuentran en las disfunciones organizativas. La contratación e instalación de líneas, va asociada a la instalación de los puestos de trabajo correspondientes (monitores, servidores de redes locales, ordenadores personales con tarjetas de Comunicaciones, impresoras, etc.). Todas estas actividades deben estar muy coordinadas y a ser posible, dependientes de una sola organización.

- *Auditoría Informática de Desarrollo de Proyectos o Aplicaciones:* La función de desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones. A su vez, engloba muchas áreas, tantas, como sectores informatizables que tiene la empresa.

  Muy escuetamente, una aplicación recorre las siguientes fases:

  - Prerrequisitos del usuario (único o plural), y del entorno.
  - Análisis funcional.
  - Análisis orgánico. (Pre programación y Programación).
  - Pruebas.
  - Entrega a explotación y alta para el proceso.

  Finalmente, la auditoría informática deberá comprobar la seguridad de los programas, en el sentido de garantizar que, los ejecutados por la máquina, son totalmente los previstos y no otros.

  Una razonable auditoría informática de aplicaciones pasa indefectiblemente por la observación y el análisis de las siguientes consideraciones:

- *Revisión de las metodologías utilizadas:* Se analizarán éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de las mismas.

- *Control Interno de las Aplicaciones*: La auditoría informática de desarrollo de aplicaciones deberá revisar las mismas fases, que presuntamente ha debido seguir el área correspondiente de desarrollo. Las principales son:

    - Estudio de viabilidad de la aplicación.
    - Definición lógica de la aplicación.
    - Desarrollo técnico de la aplicación.
    - Diseño de programas.
    - Métodos de pruebas.
    - Documentación.
    - Equipo de programación.

- *Satisfacción de Usuarios*: Una aplicación eficiente y bien desarrollada teóricamente, deberá considerarse un fracaso, si no sirve a los intereses del usuario que la solicitó. Surgen nuevamente las premisas fundamentales de la informática eficaz: fines y utilidad. No puede desarrollarse de espaldas al usuario, sino contando con sus puntos de vista durante todas las etapas del Proyecto. La presencia del usuario proporcionará además grandes ventajas posteriores, evitará reprogramaciones y disminuirá el mantenimiento de la aplicación.

- *Control de Procesos y Ejecuciones de Programas Críticos*: El auditor no debe descartar la posibilidad de que se esté ejecutando un módulo, lo que no corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de aplicaciones.

    Se está diciendo, que el auditor habrá de comprobar fehaciente y personalmente la correspondencia biunívoca y exclusiva entre el programa

codificado y el producto obtenido como resultado de su compilación y su conversión en ejecutables mediante la linkeditación (Linkage Editor).

Obsérvense las consecuencias de todo tipo que, podrían derivarse del hecho de que, los programas fuente y los programas módulos, no coincidieran, provocando graves retrasos y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial-informático, etc.

Esta problemática ha llevado a establecer una normativa muy rígida en todo lo referente al acceso a las Librerías de programas.

Una informática medianamente desarrollada y eficiente, dispone de un solo juego de librerías de programas de la instalación. En efecto, explotación debe recepcionar programas fuente, y solamente fuente. ¿Cuáles? Aquellos que, desarrollo hayan dado como buenos.

La asumirá la responsabilidad de:

- Copiar el programa fuente que desarrollo de aplicaciones ha dado por bueno en la librería de fuentes de explotación, a la que nadie más tiene acceso.
- Compilar y linkeditar ese programa, depositándolo en la librería de módulos de explotación, a la que nadie más tiene acceso.
- Copiar los programas fuente que les sean solicitados para modificarlos, arreglarlos, etc., en el lugar que se le indique. Cualquier cambio exigirá pasar nuevamente al punto 1.

Ciertamente, hay que considerar las cotas de honestidad exigible a explotación. Además de su presunción, la informática se ha dotado de herramientas de seguridad sofisticadas que permiten identificar la personalidad del que accede a las librerías.

No obstante, además, el equipo auditor intervendrá los programas críticos, compilando y linkeditando nuevamente los mismos para verificar su biunivocidad.

- *Auditoría de la Seguridad Informática:* Abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Igualmente, a este ámbito pertenece la política de seguros.

  La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

  La decisión de abordar una auditoría informática de seguridad global en una empresa, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida.

  Tal estudio comporta con frecuencia la elaboración de "Matrices de Riesgo", en donde se consideran los factores de las "Amenazas", a las que está sometida una instalación y de los "Impactos", que aquellas pueden causar cuando se presentan.

- *Auditoría de la seguridad:* Es una de las herramientas más eficaces que existen para ayudar a mantener la seguridad. Es recomendable establecer niveles de auditoría de acuerdo a los entornos, como parte de la estrategia de seguridad global. La auditoría de la seguridad, debería identificar los ataques, ya tengan éxito o no, que supongan un riesgo para su red, o los ataques contra recursos considerados como valiosos, en la evaluación de riesgos.

  En fin, es una revisión formalizada, para validar las medidas de protección, referentes a las seguridades implementadas a la infraestructura tecnológica, de acuerdo con estándares aceptados internacionalmente, la misma que identifica los riesgos, sobre la base de la política de seguridad ejecutada.

  El objetivo de la auditoría es verificar que cada regla de la política de seguridad se aplique correctamente y que todas las medidas tomadas, conformen un todo coherente. Una auditoría de seguridad garantiza, que el conjunto de disposiciones tomadas por la empresa se consideren seguras.

Las auditorías de la seguridad, son importantes para la gestión eficaz de la seguridad, como proceso continuo de planificación, análisis y corrección de seguridad de la infraestructura tecnológica, cuando es necesario.

- *Auditoría de la seguridad física:* La auditoría de la seguridad física, garantiza la integridad de los activos humanos, tecnológicos, la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de ésta. También está referida a las protecciones externas (acondicionamiento, sistemas anti intrusión, cableado estructurado, control ambiental, arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

  La misma, verifica características de construcción y componentes de edificación e instalaciones del recinto, sistemas que impiden y/o detectan un acceso no autorizado a las instalaciones, componentes que garantizan, la grabación de la actividad, dentro de las zonas de acceso, sistema de suministro eléctrico, sistema de cableado estructurado (telefonía, servidores, comunicaciones de datos, etc.), sistemas de control ambiental

  La auditoría de la seguridad física, no se debe limitar a comprobar la existencia de los medios físicos, sino también su funcionalidad, racionalidad y la seguridad.

- *Auditoría de la seguridad lógica:* Se centra en auditar aspectos técnicos de la infraestructura tecnológica, contemplando tanto aspectos de diseño de la arquitectura desde el punto de vista de seguridad, como aspectos relacionados con los mecanismos de protección, desplegados para hacer frente a todo tipo de incidentes lógicos.

  Se refiere a la revisión de los controles, normas, políticas o procedimientos de los métodos de autenticación de los sistemas de información, encriptaciones, firewalls, antivirus, actualizaciones, configuraciones de los sistemas y políticas de respaldos, de acceso de información, etc., que resguarden el acceso a los datos y sólo permita acceder a ellos, a las personas autorizadas para hacerlo, asegurar que los usuarios, puedan trabajar sin una supervisión minuciosa y no

puedan modificar los programas, ni los archivos que no correspondan, que la información recibida sea la misma que ha sido transmitida, que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

### 3.3.2. Importancia de la Auditoría Informática

La auditoría, permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización.

El auditor, debe mantener independencia mental, profesional y laboral, para evitar cualquier tipo de influencia en los resultados de la misma.

La técnica de la auditoría, siendo por tanto aceptables, equipos multidisciplinarios formados por titulados en ingeniería informática e ingeniería técnica en informática y licenciados en derecho especializados en el mundo de la auditoría.

### 3.3.3. Pruebas y Herramientas para efectuar una Auditoría Informática

En la realización de una auditoría informática, el auditor puede realizar las siguientes pruebas:

- *Pruebas sustantivas*: Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.
- *Pruebas de cumplimiento*: Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Las principales herramientas de las que dispone un auditor informático son:

- Observación
- Realización de cuestionarios
- Entrevistas a auditados y no auditados

- Muestreo estadístico
- Flujogramas
- Listas de chequeo
- Mapas conceptuales

En la actualidad se puede hacer uso de una o varias metodologías para obtener mejores resultados. (Universidad Nacional Autonoma de México, 2008)

## 3.4. Metodologías de Auditorías Informáticas

Existen diferentes enfoques para abordar una auditoría Informática de los activos de una organización. Se hace uso de metodologías de revisión de seguridad reconocidas a nivel internacional, como es el caso de OSSTMM, OWASP, OWISAM y OISSG, ISSAF para garantizar la seguridad de los activos de nuestros clientes.

Dependiendo de sus necesidades, se propone la realización de auditorías de seguridad, apoyadas en CVSS v2, siguiendo los siguientes enfoques:

- Auditoría Black Box: Se denomina “Black Box” a aquel enfoque, en el que el auditor no posee conocimientos de la infraestructura tecnológica subyacente. Esta revisión de seguridad, es ideal para simular ataques realizados por parte de personal externo a la organización.
- Auditoría White Box: Se denomina “White Box “, debido a que se facilita información técnica sobre los activos a auditar, incluyendo, según los activos analizados, información tal como usuario, contraseñas y mecanismos de seguridad existentes. Con este enfoque, el auditor no necesita dedicar un esfuerzo extra, a la búsqueda de información y permite focalizar los esfuerzos en aquellos elementos que son críticos para su negocio.

### 3.4.1. White Box

Para esta metodología de prueba, se debe tener el conocimiento completo de la infraestructura a ser probada, incluyendo los diagramas de red, código fuente, la

información y de direccionamiento IP. Las pruebas White box proporcionan un grado de sofisticación que no está disponible con las pruebas de recuadro negro, como el auditor es capaz de consultar e interactuar con los objetos que componen una aplicación, lugar, sistemas, etc.

White box testing, simula lo que podría suceder durante un "trabajo interno", o después de una "fuga" de información sensible, donde el atacante tiene acceso al código fuente, diseños de red, falencias en las seguridades físicas y posiblemente algunas contraseñas.

Los servicios ofrecidos, por empresas de pruebas de penetración cubren una gama similar, desde un simple escaneo de una organización del espacio, de direcciones IP para abrir los puertos y banderas de identificación, a una auditoría completa de las aplicaciones, sistemas de seguridad, etc.

Un ejemplo de un sistema de White Box, sería en el circuito de pruebas en la que alguien está mirando a las interconexiones entre cada componente y la verificación de que cada conexión interna, está funcionando correctamente.

Otro ejemplo de un campo diferente podría ser un auto-mecánico, que se ve en el funcionamiento interno de un coche para asegurarse de que todas las partes individuales están funcionando correctamente para asegurar que el auto se maneja adecuadamente. La principal diferencia entre las pruebas Black Box y White Box son las zonas en las que optan por centrarse.

En términos más simples, las pruebas Black Box, se centran en los resultados y se proporciona muy poca información al auditor. Si no, se toma una acción y produce el resultado deseado, el proceso que se utiliza realmente para lograr ese resultado, es irrelevante.

Las pruebas de White Box, en cambio, se ocupan de los detalles. Se centran en el funcionamiento interno de un sistema, y sólo cuando todas las vías han sido probados y la suma de las partes de una aplicación, se puede demostrar que se contribuye al todo, es la prueba completa.

#### 3.4.1.1. Ventajas de Pruebas de White Box

Pruebas de White Box, es uno de los dos más grandes métodos de prueba utilizados en la actualidad. Tiene principalmente tres ventajas:

- La introspección: esto le da al usuario o probador la oportunidad de probar internamente lo que permite una mejor perspectiva de los objetos y los módulos dentro del software. Esto es efectivo, cuando la interfaz gráfica de usuario, está cambiando con frecuencia.

- Identificación: Al pasar por cada línea de la prueba, es capaz de revelar lo que los casos de prueba se han aplicado al objetivo y enumera la cantidad de líneas que aún no se han ejecutado.

- Eficacia: Este tipo de pruebas proporciona al usuario final o al proveedor, de la confianza de que cada camino, ha sido probado en cierta medida, lo que debería limitar la cantidad de errores dentro de una aplicación. Las pruebas de White Box es la prueba más eficaz, ya que el más completo cuando analice una aplicación individual.

De acuerdo a lo expuesto anteriormente, la metodología a utilizar para el desarrollo del proyecto de tesis será la de White Box, que facilitará la información necesaria y demás requerimientos para el desarrollo de la misma. En cuanto, a las técnicas de investigación se utilizarán las técnicas de investigación de campo, esto debido, a que la misma, está dirigida a recolectar la información primaria, utilizando métodos como la observación, la entrevista, la encuesta, el test, etc. (Chavez, 2009)

# CAPÍTULO 4

# ANÁLISIS DE RESULTADOS OBTENIDOS

## 4.1. Análisis de Mediciones Recopiladas Seguridades

La auditoría de gestión de seguridades de la WAN a nivel físico y lógico, consistió en un examen objetivo, independiente, sistemático y profesional, de las actividades operativas y/o financieras de la organización, practicando con posterioridad a su ejecución, para sobre la evaluación del control interno, verificar la forma en la que estas se ejecutaron mediante la recopilación de evidencia, que una vez analizada, permitirá formarse una opinión que será emitida a través del correspondiente informe, y debe contener comentarios, conclusiones y recomendaciones y, en el caso de efectuar examen de los niveles de cumplimiento, el respectivo dictamen profesional.

Con la identificación de eventos, la gerencia reconoce que la incertidumbre existe, lo que se traduce en no poder conocer con exactitud, cuando y donde, un evento pueda ocurrir, así como tampoco las consecuencias financieras. En este componente, se identifican los eventos con impacto negativo (vulnerabilidades) y con impacto positivo (oportunidades).

Las vulnerabilidades son errores que permiten realizar acciones desde fuera, sin permiso del administrador del sistema, incluso se puede suplantar a un usuario común. Actualmente, existen muchas amenazas que tratan de acceder remotamente a ordenadores, ya sea para hacerlos servidores ilegales o robar información privada.

Con la evaluación de riesgos, se determina los riesgos a partir de dos perspectivas: probabilidad e impacto. Entre las técnicas se utiliza: determinar riesgos y medir los objetivos relacionados.

En la evaluación de riesgos, la gerencia considera eventos previstos e inesperados y los riesgos inherentes que es el riesgo en una organización en ausencia de acciones, que podrían alterar el impacto o la frecuencia de ocurrencia de los riesgos y los riesgos residuales, que resultan después de que, la gerencia ha

implantado efectivamente acciones para mitigar el riesgo inherente, estos son evaluados.

Con la evaluación, se obtiene una matriz de riesgos, ponderando la probabilidad de ocurrencia e impacto en los objetivos de control. Para la evaluación de las seguridades físicas y lógicas se utilizarán los siguientes niveles de impacto, probabilidad y riesgo.

Tabla No. 3

Escala de Probabilidad para la Evaluación de Riesgos

| Escala probabilidad | | |
|---|---|---|
| **1** | Bajo | No es probable que suceda pero es posible |
| **2** | Medio | Bastante probable que suceda alguna vez |
| **3** | Alto | Probable que suceda inmediatamente o en un breve período de tiempo |

Tabla No. 4

Escala de Impacto para la Evaluación de Riesgos

| Escala de impacto | | |
|---|---|---|
| **1** | Insignificante | El peligro representa una amenaza mínima a la seguridad y normal funcionamiento de la organización |
| **2** | Bajo | Daños menores, daños materiales, pérdida financiera y/o publicidad negativa para la organización |
| **3** | Medio | Daños graves, daños materiales importantes, pérdida financiera considerable y/o publicidad negativa para la organización |
| **4** | Alto | Puede ocasionar la suspensión del negocio por un tiempo prudencial |
| **5** | Extremo | Puede ocasionar la suspensión del negocio por un tiempo extendido o su desaparición |

Tabla No. 5

Escala de Riesgo para la Evaluación de Riesgos

| Escala de riesgo | | |
|---|---|---|
| **11>=15** | Riesgo Extremo | Las actividades de esta categoría contienen niveles de riesgo inaceptables, incluida la posibilidad de daños catastróficos y críticos. |
| **6>=10** | Riesgo Moderado | Las actividades de esta categoría contienen algún nivel de riesgo que probablemente no suceda. Las empresas deben considerar qué se podría hacer para gestionar el riesgo y evitar resultados negativos. |
| **1>=5** | Riesgo Bajo | Las actividades de esta categoría contienen un riesgo mínimo que probablemente no suceda. Las empresas pueden continuar con estas actividades de acuerdo con lo planificado. |

Las respuestas al riesgo, deben ser evaluadas, en función de alcanzar el riesgo residual alineado con los niveles de tolerancia al riesgo y puedan estar enmarcadas en evitar el riesgo, reducir el riesgo, transferir o cambiar el riesgo o simplemente aceptar el riesgo.

Los costos de diseñar e implementar una respuesta deben ser considerados, así como los costos de mantenerlas. Estos pueden ser medidos de manera cualitativa o cuantitativamente, típicamente la unidad de medición es consistente con la utilizada en el establecimiento de los objetivos y tolerancia al riesgo. La gerencia debe considerar, los riesgos adicionales que puedan resultar de una respuesta, así como también las posibles oportunidades que se generen con la implementación de las mismas.

Para esto utilizaremos una matriz de riesgos, que es una herramienta, que permite organizar la información sobre los riesgos de las empresas y visualizar su magnitud, con el fin de establecer las estrategias adecuadas para su manejo. Los

mapas de riesgos pueden representarse con gráficos o datos. Los gráficos corresponden a la calificación de los riesgos con sus respectivas variables y a su evaluación de acuerdo con el método utilizado en cada empresa.

Los datos pueden agruparse en tablas, con información referente a los riesgos; a su calificación, evaluación, controles y los demás datos, que se requieran para contextualizar la situación de la empresa y sus procesos, con respecto a los riesgos que la pueden afectar y a las medidas de tratamiento implementadas.

De acuerdo a lo enunciado, y una vez aplicados los respectivos checklist, tanto de las seguridades físicas como lógicas, se han hecho hallazgos unos de mayor impacto y otros que han sido pensados para mejorar la seguridad, los cuales van a ser analizados y posteriormente se darán las respectivas recomendaciones para su mejora.

### 4.2. Análisis de Mediciones Recopiladas Seguridades Físicas

Independientemente del objetivo de este proyecto, se procedió a recolectar la información y posterior a esto se realizó el análisis respectivo, obteniendo las matrices de riesgos de cada uno de las categorías establecidas para las seguridades físicas, pero los resultados obtenidos no fueron colocados en este documento, debido a un acuerdo de confidencialidad establecido con la institución, ya que al tratarse de una institución financiera, sería un riesgo demasiado elevado, poner al público dicha información.

Los resultados obtenidos fueron presentados en otro documento independiente a este proyecto, el mismo, que fue entregado a los propietarios de cada uno de los procesos, para su revisión con lo cual, se podrán revisar los niveles obtenidos y de esta manera, poder implementar planes de mejora o actualización.

### 4.3. Análisis de Mediciones Recopiladas Seguridades Lógicas

Independientemente del objetivo de este proyecto, se procedió a recolectar la información y posterior a esto se realizó el análisis respectivo, obteniendo las matrices de riesgos de cada uno de las categorías establecidas para las seguridades lógicas, pero los resultados obtenidos no fueron colocados en este documento, debido

a un acuerdo de confidencialidad establecido con la institución, ya que al tratarse de una institución financiera, sería un riesgo demasiado elevado, poner al público dicha información.

Los resultados obtenidos fueron presentados en otro documento independiente a este proyecto, el mismo, que fue entregado a los propietarios de cada uno de los procesos, para su revisión con lo cual, se podrán revisar los niveles obtenidos y de esta manera, poder implementar planes de mejora o actualización.

# CAPITULO 5

# CONCLUSIONES Y RECOMENDACIONES

## 5.1. Conclusiones

Una vez finalizada la auditoría a la gestión de la seguridad de la WAN a nivel físico y Lógico, utilizando las metodologías expuestas para el presente proyecto y las normas existentes, aceptadas y utilizadas a nivel internacional, se han obtenido la información de las seguridades físicas en forma general, las de control de acceso de personal, de gestión de riesgos, de acceso a la información, así como para las seguridades lógicas en forma general, de los sistemas operativos, del software, de los equipos de comunicación, de servidores, firewalls y bases de datos, los mismos que utilizando matrices de riesgos, se ha realizado el análisis correspondiente con lo cual se han obtenido resultados que nos indican el nivel de seguridad, en cada uno de los aspectos antes mencionados.

En lo que respecta a las seguridades físicas, la Institución ha implementado controles y sistemas que ayuden a salvaguardar los activos informáticos donde se almacena y procesa la información

*Nota:* Algunas de las conclusiones que se llegó a obtener una vez finalizada la auditoría en las seguridades físicas, fueron excluidas del presente documento, de acuerdo al acuerdo de confidencialidad establecido con la institución.

Las conclusiones excluidas, fueron plasmadas en otro documento que fue entregado, para uso exclusivo del personal que la institución autorice para su uso, aceptado todas las conclusiones para poder conocer los niveles en que se encuentra la seguridad física.

En lo que respecta a las seguridades lógicas, la Institución ha implementado controles y sistemas que ayuden a salvaguardar la información, que se procesa en los activos informáticos.

*Nota:* Algunas de las conclusiones que se llegó a obtener una vez finalizada la auditoría en las seguridades físicas, fueron excluidas del presente documento, de acuerdo al acuerdo de confidencialidad establecido con la institución.

Las conclusiones excluidas, fueron plasmadas en otro documento que fue entregado, para uso exclusivo del personal que la institución autorice para su uso, aceptado todas las conclusiones para poder conocer los niveles en que se encuentra la seguridad lógica.

Como conclusión final, la Institución, ha invertido en el análisis e implementación de las seguridades, tanto a nivel físico como lógico, pero a pesar de esto, existen ciertos puntos de interés, por lo que, es preciso revisar cada categoría y mejorar o implementar nuevos controles, para tener la seguridad de que, los activos informáticos sean accedidos, sólo por las personas autorizadas y que la información sea precisa, confiable y se encuentre siempre disponible.

## 5.2. Recomendaciones

- Realizar nuevas auditorías de tipo informático, con la finalidad de determinar todas las posibles vulnerabilidades y niveles de seguridad en todos los aspectos, para garantizar que la información sea confiable.
- Realizar una revisión de los valores obtenidos dentro de las seguridades físicas, generar un plan de acción para mitigar los riesgos de nivel alto, que puedan afectar considerablemente y producir interrupciones del servicio y del negocio.
- Realizar una revisión de los valores obtenidos dentro de las seguridades lógicas, generar un plan de acción para mitigar los riesgos de nivel alto, que puedan afectar considerablemente y producir interrupciones del servicio y del negocio.
- Implementar los controles recomendados en cada una de las observaciones, con la finalidad de mitigar las vulnerabilidades y lograr nuevos niveles de seguridad.
- Documentar todos los procedimientos que se encuentren implementados o que se tengan en consideración implementar, con la finalidad de tener precedentes para poder determinar si son eficaces o no, o implementar planes de actualizaciones.

*Nota:* Algunas de las recomendaciones que se establecieron de acuerdo a los niveles obtenidos al final de la auditoría en las seguridades tanto físicas como lógicas, fueron excluidas del presente documento, de acuerdo al acuerdo de confidencialidad establecido con la institución.

Las recomendaciones excluidas, fueron plasmadas en otro documento que fue entregado, para uso exclusivo del personal, que la institución autorice para su uso, aceptado todas las recomendaciones, para poder generar planes de implementación, actualización o acción, que ayuden a mitigar las vulnerabilidades encontradas.

Se hace hincapié que estas recomendaciones se las ejecute en su totalidad y una vez desarrolladas generar nuevamente una auditoria de la gestión de la información, con la finalidad de determinar si los controles o procesos implementados o actualizados, son los adecuados y de esta manera obtener nuevos niveles de seguridad tanto en lo físico como en lo lógico.

# BIBLIOGRAFÍA


Cárdenas, J. (2010). *Conceptos sobre Backtrack.* Obtenido de http://www.slideshare.net/julescc/back-track

Castro, J. (2010). *Core Impact.* Obtenido de http://jasmin6.wordpress.com/2010/09/08/core-impact/

Chavez, J. (2009). *Black Box vs. White Box*. Obtenido de http://jchaveznet.wordpress.com/2009/03/27/black-box-vs-white-box/

Chiguano, G. (2008). *Normas ANSI/TIA/EIA para Cableado de Telecomunicaciones.* Obtenido de http://www.xuletas.es/ficha/normas-ansitiaeia-para-cableado-de-telecomunicaciones/

Congdon, H. (2005). *La Nueva Generación de Estándares de Cableado.* Obtenido de http://www.ampnetconnectnews.com/descargas/amp/TIA568-C-CIM_Sept-08.PDF

Corletti. (2007). *ISO/IEC 27001:2005 e ISO/IEC 27004.* Obtenido de http://www.criptored.upm.es/descarga/ISO-27001_e_ISO-27004.zip

*Deloitte Touche Tohmatsu Limited Ecuador*. (2014). Obtenido de http://www.deloitte.com/view/es_EC/ec/conozcanos/deloitte-en-ecuador/

*Ernst & Young* . (2014). Obtenido de http://www.ey.com/EC/es/About-us

Gómez, C. (2011). *Wireshark: Análisis de Tráfico y Detección de Claves.* Obtenido de http://es.scribd.com/doc/75866065/WIRESHARK-ANALISIS-DE-TRAFICO-Y-DETECCION-DE-CLAVES

González, R. (2013). *Conceptos Básicos de Enrutamiento.* Obtenido de http://www.ditae.uat.edu.mx/ver2013/xtras/ConceptosBasicosRoutingRicardo.pdf

Hernández, R., Fernández, C., & Baptista, L. (1997). *Metodología de la Investigación.* Obtenido de http://www.upsin.edu.mx/mec/digital/metod_invest.pdf

ISO. (2005). *ISO/IEC 27002:2005.* Obtenido de http://www.iso27000.es/iso27000.html

ISO. (2013). *ISO Survey.* Obtenido de http://www.iso.org/iso/home/standards/certification/iso-survey.htm

Joskowicz, J. (2013). *Cableado Estructurado.* Obtenido de http://iie.fing.edu.uy/ense/asign/ccu/material/docs/Cableado%20Estructurado.pdf

*Klynveld Peat Marwick Goerdeler*. (2013). Obtenido de http://www.kpmg.com/Global/en/about/citizenship/Pages/default.aspx

Mifsud, E. (2012). *Zenmap - Nmap.* Obtenido de http://recursostic.educacion.es/observatorio/web/es/software/software-general/1050-zenmap?start=1

Murillo García, M. (2007). *Curso sobre Redes.* Obtenido de http://www2.configurarequipos.com/manuales/curso-de-redes.pdf

Nessus. (2012). *Guía del Usuario de Nessus.* Obtenido de http://static.tenable.com/documentation/nessus_5.0_user_guide_ESN.pdf

Peñaloza Figueroa, M. (s.f.). *Diseño y cableado de un Centro de Datos.* Obtenido de http://in.unsaac.edu.pe/~mpenaloza/cursos/docs/Cableado%20de%20un%20Centro%20de%20Datosx6.pdf

Pérez, P. (2000). *Arquitectura de Redes - Parámetros de Cableado de Cobre.* Obtenido de http://www1.frm.utn.edu.ar/medidase2/varios/parametros_redes1.pdf

*Price Waterhouse Coopers Ecuador*. (2011). Obtenido de http://www.pwc.ec/acerca-de-nosotros/index.aspx

Rendon, E. (2012). *Conceptos Access Point.* Obtenido de http://www.slideshare.net/ejrendonp01/access-point-12084186

Sánchez, L. (2012). *Conceptos de Switch.* Obtenido de http://es.scribd.com/doc/92442149/Concepto-de-Switch

SysAid. (2002). *SysAid Keep IT simple*. Obtenido de http://www.ilient.es/web-based-help-desk-software.htm

Universidad Nacional Autonoma de México. (2008). *Auditoría en Informática. La Auditoría como Actividad Profesional.* Obtenido de http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

Viera, M. (2005). *Amenazas, Utilerías y Mantenimiento de Software.* Obtenido de http://hecman.jimdo.com/hacker-ycracker/clasificación-de-crackers/