CAPITULO 2

ANTECEDENTES Y MARCO CONCEPTUAL

1 ANTECEDENTES

1.1 UNIVERSIDAD FRANCISCO GAVIDIA

1.1.1 Historia

La Universidad Francisco Gavidia comienza sus actividades administrativas y de promoción el 7 de marzo de 1981, en medio de una etapa difícil y conflictiva para nuestro país.

Sin embargo, la Universidad Francisco Gavidia inicia sus actividades académicas en junio de ese mismo año con dos facultades: La de Ciencias Sociales, la cual estaba constituida por cuatro carreras de Licenciatura, tres carreras de Profesorado para desempeñarse en el nivel medio y un Técnico en Educación Parvularia; y La de Ciencias Económicas que estaba constituida por tres carreras de Licenciatura y un Técnico en el área de la comercialización.

Actualmente la Universidad Francisco Gavidia está conformada por cuatro facultades que son: Ingeniería y Arquitectura, Ciencias Jurídicas, Ciencias Sociales y Ciencias Económicas, donde se ofertan más de treinta carreras universitarias a la sociedad salvadoreña.

Los cambios que se han venido dando en la Universidad Francisco Gavidia son revisados, modificados o renovados de acuerdo a las exigencias de los avances Educativos, Tecnológicos, Sociales, Económicos, Políticos y Culturales que afectan a la sociedad tanto regional, nacional e internacional, y principalmente a la vida institucional de la Universidad.

La historia de la Universidad Francisco Gavidia se podría dividir en dos períodos, el primero desde 1981 hasta marzo de 1990, donde logra hacer notar su presencia como Centro de Estudios Superiores.

El segundo período comienza el 27 de marzo de 1990 hasta la fecha, con la elección de nuevas autoridades. La universidad dio un giro importante en su historia, así mismo al ejecutar nuevas políticas de desarrollo, ha consolidado su prestigio como institución de avanzada a nivel superior, en 1992 se funda el Centro Regional de Santa Ana que brinda una cobertura a la demanda de estudios superiores de la zona occidental de nuestro país.

En 1994 la Universidad Francisco Gavidia inicia la construcción del nuevo campus universitario, inaugurándolo el 13 de enero de 1996, el nuevo campus brinda cabida a más de 6000 estudiantes para las cuatro diferentes facultades.

1.1.2 Misión de la Universidad Francisco Gavidia

“La formación de profesionales competentes, con sentido ético, crítico y propositivo, utilizando recursos humanos, científicos y tecnológicos apropiados, para contribuir a impulsar los cambios que propicien el desarrollo sostenible del país y de la región".

1.1.3 Visión de la Universidad Francisco Gavidia

“Ser una institución de educación superior plenamente acreditada por organismos nacionales e internacionales".

1.1.4 Estructura Organizacional

A continuación se presentan tres organigramas de la Universidad Francisco Gavidia, en primer lugar la representación organizacional actual, luego la estructura de las dos unidades donde se desarrolla el proyecto: Administración Académica y Dirección de tecnología y comunicaciones.

a) **Organigrama General de la UFG**

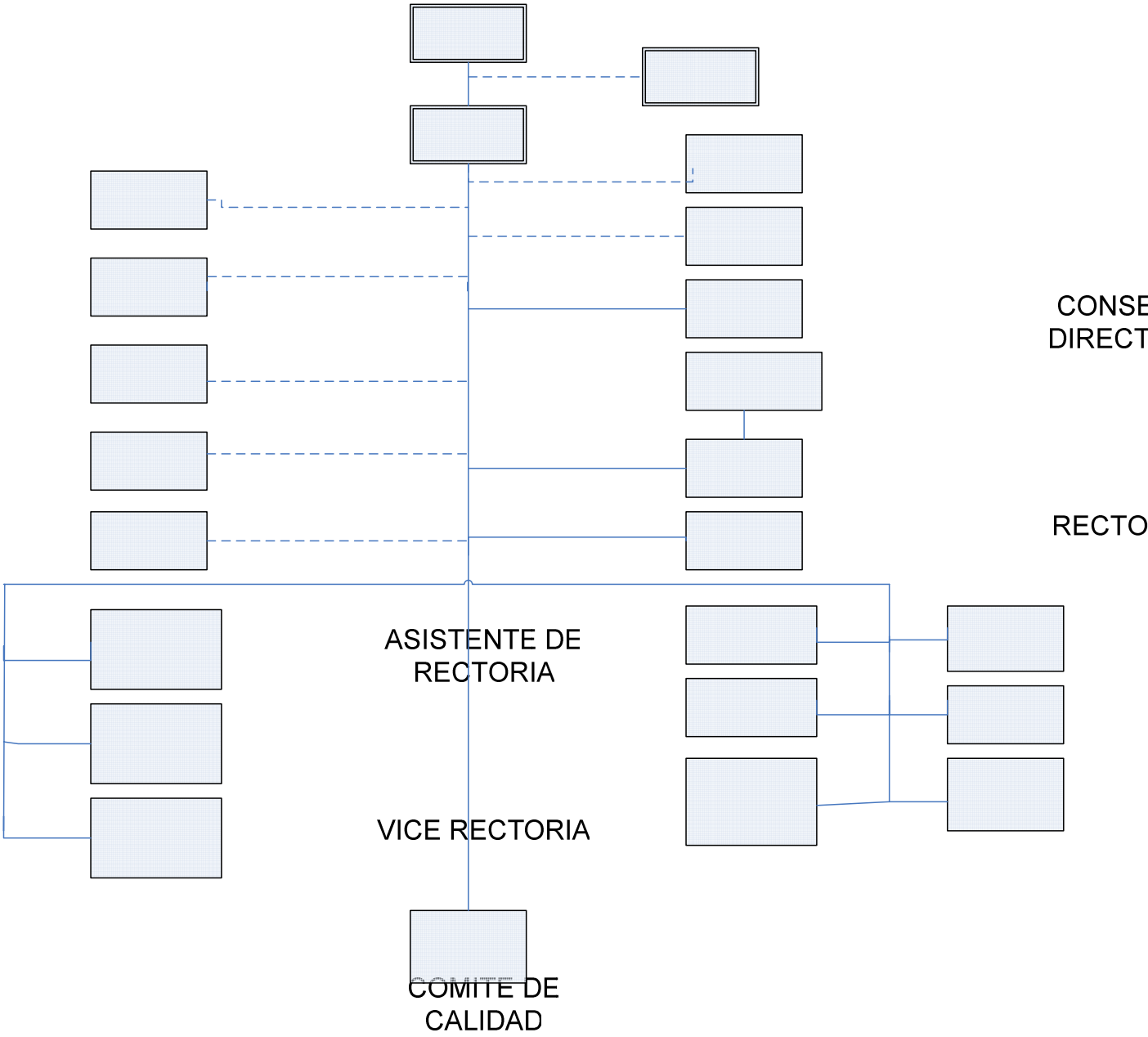


Figura 2.1 Organigrama de la UFG, tomado de la página web de la UFG (www.ufg.edu.sv)

RECTOR: ING. MARIO RUIZ

CONSEJO
ACADEMICO

CONSEJO DE
DECANOS

Unidad de Administración Académica

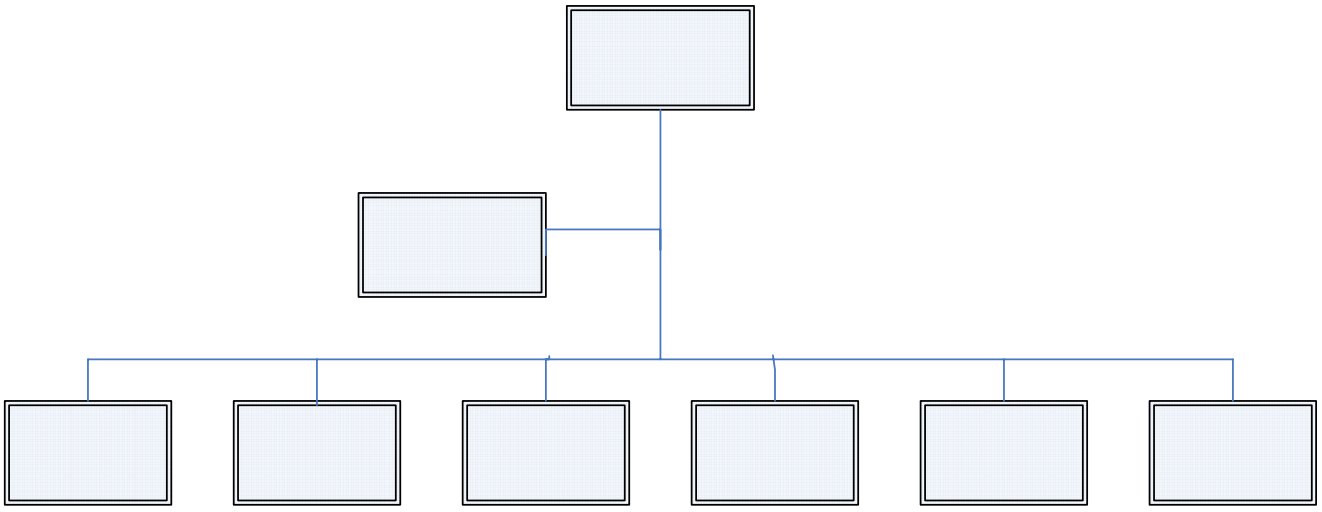


Figura 2.2 Organigrama de la Unidad de Administración Académica de la UFG

Responsable de Unidad:

JEFE DE UNIDAD: LIC. ELNER CRESPIN

ASISTENTE ADMINISTRACON

UNIDAD DE SISTEMAS

UNIDAD DE INGRESO

UNIDAD DE ATENCION AL ESTUDIANTE

Dirección De Tecnología y Comunicaciones

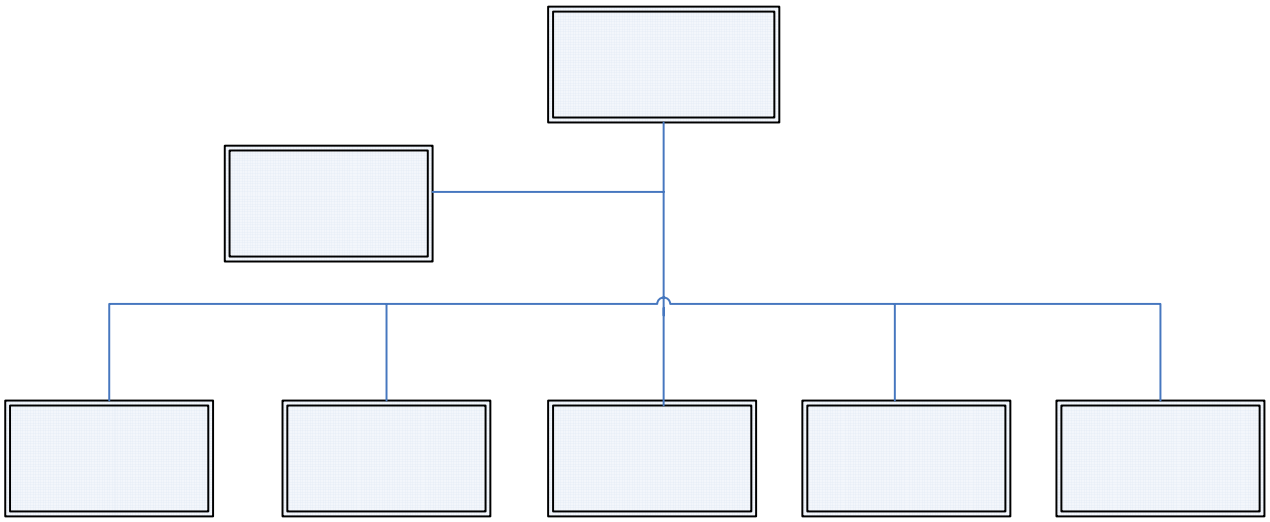


Figura 2.3 Organigrama de la Unidad de Dirección de tecnología y comunicaciones de la UFG

Responsable de Unidad:

JEFE DE UNIDAD: ING. CARLOS NEWTON

1.1.5 Tecnología y Sistemas de Información

a) **Internet**

Desde 1997 la universidad creó una página WEB que fue premiada con dos arrobas de oro. A través de esta pagina se ofrecen diversos servicios para todos aquellos usuarios que tengan Internet, tales como: correo electrónico a los estudiantes, la radio virtual con distintas programaciones y entrevistas vinculadas al quehacer universitario, el canal de televisión, la plataforma virtual "U", Internet 2. Pensando en el uso de esta tecnología todos los alumnos cuentan con su correo electrónico para poder hacer consultas a los catedráticos con relación a las notas, laboratorios o interrogantes que surgieron de las clases. También la universidad

cuenta con Internet comercial y consultas académicas, como: notas en línea, expediente académico, horarios de asignaturas, inscripción.

b) **Internet 2**

Otro recurso con el que cuenta la UFG es Internet 2, una de las principales ventajas es que la imagen que se recibe es de la misma calidad de cómo se transmite. Estas conferencias pueden ser interactivas desde donde se pueden obtener videos y tele-inmersión (la tele-inmersión es un proceso de comunicación remota entre seres humanos y/o dispositivos, mediante el cual se superan las limitaciones al estar ubicados en lugares remotos o en distintos momentos.

c) **Servicios Tecnológicos Especializados**

- **Base de Datos EBSCOhost:** Con la cual los estudiantes pueden complementar información que han adquirido en Internet.
- **Virtual U**: Donde se imparten clases virtuales no presénciales pudiendo los alumnos acceder a foros de discusión.
- **UFGTV:** Con el objetivo de reforzar los contenidos que se imparten en clases, se crea **UFGTV** canal 99, en el cual se transmiten clases presénciales que se imparten en las aulas. Este canal puede ser visto a través del cable o Internet. Una variable importante es que este canal puede ser visto por todas las personas y no solo por alumnos o profesores de la UFG.
- **La radio UFG online**: Se ha creado para mantener, sobre todo a los hijos de los salvadoreños que viven en el exterior, su identidad como salvadoreño con clases en español, historia y geografía de nuestro país.
- **APTECH:** La UFG ha obtenido una franquicia de la India, reconocida a nivel mundial como **APTECH Training Limited**, que forma especialistas en Tecnología de la Información. APTECH El Salvador brinda cursos integrales que permiten a sus estudiantes obtener la calificación de especialistas certificados.
- **FACET:** La UFG posee a la disposición de los estudiantes laboratorios especializados, tales como: **Laboratorio de telecomunicaciones FACET**, laboratorio de ingeniería eléctrica y electrónica, informática, idiomas, diseño gráfico digital.

Todos los laboratorios están interconectados entre si para la realización de prácticas asistidas y prácticas individuales como complemento a la enseñanza en clases.

- **BiblioWeb:** Otro departamento que ha tenido un cambio tecnológico es la biblioteca que pasa de ser una biblioteca convencional a una **biblioteca totalmente tecnológica**, las cuales están equipadas con un sistema computarizado y acceso a Internet, salas para acceder al catálogo en línea de la universidad, salas de referencia virtual, sala de multimedia para consultar material multimedia como CDS, DVD, y videos en formato convencional electrónico. Todas las bibliotecas cuentan con un sistema automatizado **BIBLIOWEB**, el cual permite que los estudiantes de la universidad y demás usuarios puedan acceder a la base de datos local para conocer todas las referencias de todas las colecciones bibliográficas con las que se cuenta, prestar o reservar el documento; también se ha implementado un sistema de código de barra para facilitar la gestión de préstamos y devoluciones de documentos bibliográficos entre otros.

d) **Estudios de Postgrado**

Para satisfacer la demanda de profesionales, la universidad ha diseñado dos maestrías: una en la rama de la informática y otra en la rama de la administración, siendo estos:

- Maestría en Informática aplicada en redes
- Maestría en Ingeniería de Software.
- Postgrado en Administración:
- Maestría en Administración de Negocios con especialidad en comercio electrónico.

1.1.6 Certificación con la Norma ISO 9001

Desde el año 2003, la Universidad Francisco Gavidia se certifico a través del sistema de calidad ISO 9001:2000 con el fin de lograr un mejor proceso de enseñanza-aprendizaje y óptimos procesos de apoyo o soporte al proceso educativo, tanto en la sede central como en el Centro regional de Occidente, en Santa Ana.

Esta certificación cada año es sometida a una auditoría de seguimiento en la que el ente certificador, en este caso, Latu Sistemas, verifica si la Universidad está cumpliendo y manteniendo los estándares establecidos por el sistema de gestión de calidad.

A escala institucional, hubo un proceso de sensibilización donde se dio a conocer todo lo referente al sistema de calidad. Se ha implementado un sistema de gestión de calidad que viene a constituir la herramienta para brindar un mejor servicio educativo, mejorar la calidad de los mismos y también tecnificar a través de la capacitación permanente al personal académico y administrativo. Institucionalmente, este sistema esta centrado en el proceso enseñanza-aprendizaje, es en las aulas donde se define si una institución educativa es o no de calidad.

Esta nueva base administrativa permite volver sostenible la acreditación institucional ante el Ministerio de Educación, ya que responde a las exigencias que implementa la nueva ley de educación superior.

En el futuro, la UFG tiene proyectado incluir en el sistema de gestión de calidad las funciones de proyección social y de investigación.

1.1.7 Proyectos Importantes

Actualmente la Universidad Francisco Gavidia ha ejecutado tres grandes proyectos:

a) La construcción del edificio EBLE (llamado en un inicio edificio inteligente).

b) Creación de carreras de postgrado en el área de maestrías no tradicionales en nuestro país, tales como: Redes informáticas, Ingeniería de software y comercio electrónico.
c) La certificación del Sistema de Gestión de Calidad con la Norma ISO 9001 versión 2000, siendo así la primera institución educativa a nivel superior en El Salvador y Centroamérica que efectúa este proceso. Con ello pretende brindar a la sociedad salvadoreña profesionales con excelencia tanto académica, técnica, cultural científica y humana, manteniendo así el prestigio que posee.

1.2 SISTEMA DE INFORMACION Y SEGURIDAD INFORMATICA

1.2.1 Información [1]

Se entiende por información al conjunto de datos que sirven para tomar una decisión. En consecuencia, su necesidad es evidente tanto en la planificación estratégica a largo plazo como en la fijación de estándares para la planificación a corto plazo. La información también es necesaria para el estudio de las desviaciones y de los efectos de las acciones correctoras; es un componente vital para el control. La información esta orientada a reducir la incertidumbre del receptor y tiene la característica de poder duplicarse prácticamente sin costo, no se gasta. Además no existe por si misma, sino que debe expresarse en algún objeto (papel, cinta, etc.).

1.2.2 Sistema de Información (SI) [2]

Un Sistema de Información es un subconjunto del subsistema formalizado, con distinto grado de cobertura, es mucho más que hardware de computadora, es un conjunto de recursos de: software, hardware, datos, personas y procedimientos necesarios para usar información como un recurso en la organización (Figura 2.4). Cada uno de estos cinco componentes de la SI tienen sus fortalezas y debilidades. Es importante recordar que cada componente de los sistemas de información tiene sus propios requerimientos de seguridad.

a) Software

   El principal componente de un Sistema de Información. El Software comprende lo que son aplicaciones, sistemas operativos y un gran número de comandos utilitarios. Es el componente más difícil de asegurar. La explotación de errores de programación resulta ser un factor sustancial de los ataques sobre la información.

b) Hardware

   Es el segundo principal componente de los Sistemas de Información, es la tecnología física que hospeda y ejecuta al Software, almacena y lleva los datos, y provee las interfases de entrada y eliminación de la información de los sistemas.

[1] www.heinekenteam.com.ar/Seguridad_Informatica_202003.pdf Pág. 2,3

[3] Principles of Information Security. Michael Whitman Pág 15

c) Datos

Es la información almacenada, procesada y transmitida. Los datos usualmente son el principal objeto de ataques.

d) Personas

Las personas son algunas veces amenazas a la seguridad informática y es el recurso humano de la organización.

e) Procedimientos

Son instrucciones escritas de tareas específicas. Es importante contar con procedimientos de salvaguardo de la información, educar a los empleados, después de todo, los procedimientos en realidad son información.

Figura 2.4. Componentes críticos de un Sistema de Información

1.2.3 Seguridad[3]

En general la seguridad es "la calidad o estado de ser seguro - para estar libre de peligros". Significa estar protegido contra adversarios – de los que harían daño con o sin intención. La seguridad nacional por ejemplo es un sistema de varias capas que protege la soberanía del Estado, sus bienes, recursos y su gente. De manera semejante es necesaria la aplicación de niveles apropiados de seguridad en una organización dependiendo de un sistema de varias capas. Una organización acertada debe tener las siguientes capas de seguridad:

[3] Principles of Information Security. Michael Whitman Pág 9

a) Seguridad física: Orientada a la necesidad de proteger los bienes físicos, objetos áreas de una organización de accesos no autorizados o mal empleo de estos.

b) Seguridad personal: Dirigida a proteger a los individuos o grupo de individuos quienes están autorizados para acceder a la organización y sus operaciones.

c) Seguridad operacional: Enfocada sobre la protección detalla o particular de operaciones o series de actividades.

d) Seguridad de comunicaciones: Abarca la protección de los medios de comunicación, tecnología y contenido de una organización.

e) Seguridad de redes: Es la protección de los componentes de red, conexiones y contenido.

f) Seguridad informática: Es la protección de la información y de los sistemas, y de otros elementos relacionados, tales como: políticas, conocimiento, entrenamiento y educación, todo esto es tecnología necesaria.

1.2.4 Seguridad Informática[4]

La historia de la seguridad informática inicia con la historia de la seguridad aplicada a las computadoras. La necesidad de asegurar la ubicación física del hardware de amenazas externas, se inicia inmediatamente con la llegada de los primeros mainframes (macro computadoras)[2] es aquí donde se desarrolla y se pone en uso.

El interés en la criptografía comenzó en Alemania durante la Primera Guerra Mundial, los alemanes construyeron una máquina, llamada Enigma (Figura 2.5), para ocultar sus mensajes Grupos de desarrolladores de computadoras encargados de descifrar mensajes enemigos (mensajes codificados) durante la segunda guerra mundial crearon las primeras computadoras

[4] Principles of Information Security. Michael Whitman Pág 4-7

modernas. Durante este tiempo el acceso a locaciones militares importantes era controlado con el uso de certificados, claves de acceso, reconocimiento facial. El esfuerzo necesario para el mantenimiento a la seguridad nacional, incluía investigaciones secretas y programas de contrainteligencia, eventualmente se expandían hasta los procedimientos de seguridad de computadoras incorporando tecnología sofisticada y complejos procedimientos con el fin de salvaguardar a estas computadoras.

Figura 2.5. "Enigma", maquina decodificadora de mensajes alemanes

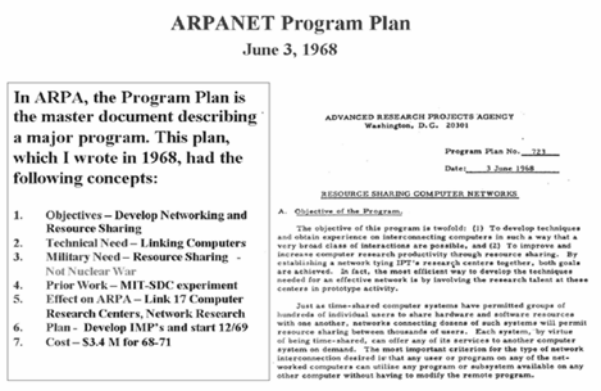
En contraste a la seguridad de las computadoras, la seguridad informática durante los primeros anos fue rudimentaria y compuesta por simples documentos clasificados. Esto no era aplicado algunas veces en proyectos de software o en sistemas operativos, porque las primeras amenazas de seguridad eran ataques físicos sobre los equipos, espionaje de productos y sabotaje.

Los 60's

Uno de los primeros problemas de seguridad documentados que no fue de naturaleza físico ocurrió a finales de los años 60's, cuando un administrador de sistemas estaba trabajando en un archivo MOTD[5] (message of the day, mensaje del día), y otro administrador estaba editando el archivo de password (claves) una falla del software mezclo los dos archivos y el archivo con las claves fue impreso en todos los dispositivos de salida (monitores) junto al mensaje del día. Durante la guerra fría de los anos 60's muy pocos mainframes estaban conectados en línea para realizar tareas sofisticadas y complejas conjuntamente, es por eso que era necesario encontrar la forma de activar la comunicación entre mainframes usando bajos niveles de procesamiento para llevar acabo la mensajeria magnética entre centros de cómputo. En respuesta a esta necesidad, la Agencia de proyectos de investigación avanzada (ARPA) del departamento de defensa de los

[5] Actividad realizada por el Administrador del S. O. UNIX, para mensajes de bienvenida al iniciar una nueva conexión

Estados Unidos inicia examinando la posibilidad de redundancia[6], diseñado un sistema de comunicación de redes para la transferencia de información de soporte militar. Larry Roberts, Conocido como el fundador de la Internet, desarrolló el proyecto desde su concepción. El proyecto fue nombrado ARPANET (Figura 2.6), y es el origen de la Internet de hoy.


ARPANET Program Plan
June 3, 1968

In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:

1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71

ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301

Program Plan No. 723
Date: 3 June 1968

RESOURCE SHARING COMPUTER NETWORKS

A. Objective of the Program.

The objective of this program is twofold: (1) To develop techniques and obtain experience on interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network tying IPT's research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at these centers in prototype activity.

Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Figura 2.6. Plan Programa ARPANET

Los 70's y 80's

Durante la próxima década, la ARPANET incrementa en popularidad y uso. En Diciembre de 1973 Robert M. "Bob", a quien se le acredita el desarrollo de la Ethernet[7], uno de los más populares protocolos de redes, indicaba que el problema fundamental de la ARPANET era la seguridad. Los sitios de usuarios remotos individuales no tenían suficientes controles y medidas de seguridad para proteger los datos de usuarios remotos no autorizados. Otro problema, era la vulnerabilidad en la estructura y formato de las claves.

Algunas de las fechas claves del surgimiento de la seguridad informática son mostradas en la Tabla 2.1

Fecha	Documento
1968	Maurice Wilkes discutía la seguridad de passwords (claves) en la revista Time-Sharing Computer Systems.

[6] La redundancia es la parte de un mensaje que podría omitirse sin que se produzca pérdida de información

[8] Estándar IEEE 802.3. Determina la forma en que los nodos de la red envían y reciben datos en un medio físico compartido.

1973	Schell, Downey y Popek examinan la necesidad de adicionar seguridad en sistemas militares.
1975	La Información Federal de estándares de procesamiento (FIPS) examina el estándar de encriptación digital (DES) en el registro federal.
1978	Bisbey y Hollingworth publican su estudio " Análisis de protección: Reporte Final" discuten un proyecto de análisis de protección creado por ARPA para mejorar el conocimiento de vulnerabilidades de seguridad de los sistemas operativos y examinan la posibilidad de una técnica automática de detección de vulnerabilidades en un sistema
1979	Dennis Ritchie pública "Seguridad sobre Unix" y "Protección de contenido para archivos de datos", discute sobre IDs de usuarios y grupos (User IDs, Group IDs) y los problemas inherentes en el sistema.
1984	Grampp y Morris escriben "Seguridad del sistema operativo UNIX". En este reporte los autores examinan 4 "practicas importantes en la seguridad informática" 1. Controles físicos de instalaciones informáticas, 2. Comisión gerencial de objetivos de seguridad, 3. Educación de empleados 4. Apuntes de procedimientos administrativos para incrementar la seguridad.
1984	Reeds y Weinnerger publican "Archivos de seguridad y el comando de encriptado para el sistema Unix". La premisa dice: "Ninguna técnica puede ser segura contra la interceptación de teléfonos y esto es equivalente en las computadoras, por lo tanto ninguna técnica puede ser segura contra el administrador de sistema o contra los usuarios privilegiados, el usuario ingenuo no tienen ninguna oportunidad".

Tabla 2.1. Fechas claves del surgimiento de la seguridad informática. [8]

Los 90's

Al cierre del siglo XX, las redes de computadoras se volvieron más comunes y también crearon la necesidad de interconectarse con otras. Esto dio crecimiento a la Internet, la primera

[8] Principles of Information Security. Michael Whitman Pág.6

manifestación de redes globales. La Internet se hizo más accesible al público en general hasta en los 90´s, desarrollándose previamente los dominios de gobierno (.gov), academia (.edu), y la industria profesional (.com). La Internet trajo conectividad virtual a todas las computadoras que podían alcanzar una línea telefónica o una red de área local (LAN). Después la Internet fue comercializada, la tecnología fue penetrando a todos los rincones del planeta.

El Presente

Hoy en día, la Internet ha traído millones de inseguridades dentro de las redes de computadoras y en las comunicaciones con otras redes. La necesidad para asegurar la información almacenada en nuestras computadoras esta ahora influenciada por la seguridad implementada por otras computadoras, con las cuales esta conectada.

El modelo de seguridad informática de la NSTISSC[9] envuelve un concepto desarrollado por la industria de seguridad informática conocida como el triangulo de C.I.A[10] este ha sido considerado el estándar de la industria de seguridad informática desde el desarrollo de los mainframes. Este se basa sobre tres características principales de la seguridad que describe la utilidad de la información: Confidencialidad, Integridad y Disponibilidad. La seguridad de estas tres características de la información sigue siendo tan importante hoy en día, pero están limitados de alcance, por que estos no acompañan de forma constante los cambios de ambiente de la industria de las computadoras.

Las amenazas a estas características envuelven una vasta colección de eventos, incluyendo daños accidentales o intencionales, destrucción, robo, modificaciones no autorizados, u otro mal empleo de personas o amenazas no humanas.

Características Críticas de la Información[11]

El valor de la información viene de acuerdo a las características que posee. Algunas de las características de la información cambian, ocasionalmente incrementando, pero usualmente

[9] National Security Telecommunications and Information System Security Committee www.nstissc.gov
[11] CIA. Computer Security Industry(Industria de Seguridad Informatica)
[12] Principles of Information Security. Michael Whitman Pág 10-14

decrementan. Algunas veces las características incrementan su valor de acuerdo a la necesidad del usuario. Por ejemplo durante un instante la información es un factor crítico para el usuario, pero a menudo esta pierde todo su valor si esta es enviada demasiado tarde. A continuación se analizan las características críticas de la información más importantes:

a) Disponibilidad

   Se entiende por disponibilidad, el grado que un dato está en el lugar, momento y forma que es requerido por el usuario autorizado.

b) Exactitud

   La información es exacta cuando esta libre de equivocaciones o errores y tiene el valor que el usuario final espera. Si la información contiene un valor diferente de las expectativas del usuario debido a modificación intencional o no intencional de su contenido, esta no logra exactitud.

c) Autenticidad

   Esta propiedad permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. De este modo se evita que un usuario envíe una información haciéndose pasar por otro.

d) Confidencialidad

   Se entiende por confidencialidad el servicio de seguridad, o condición, que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados.

e) Integridad

   Se entiende por integridad el servicio de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por el personal autorizado.

   El concepto de integridad significa que el sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga.

f) Utilidad

La utilidad de la información es la calidad o estado de tener valor para cierto propósito o fin. La información tiene valor cuando esta sirve para un propósito en particular. Esto significa que si la información esta disponible, pero no esta en un formato adecuado para el usuario final, esta no es útil.

g) Posesión

La posesión de la información es la calidad o estado de tener posesión o control de algunos objetos o elementos. La información expresa que esta en posesión si esta ha sido obtenida, independientemente de la forma u otra característica.

1.3 AUDITORÍA Y AUDITORÍA INFORMÁTICA

1.3.1 Evolución y Desarrollo de la Auditoría[12]

Existe la evidencia que alguna especie de auditoría se practicó en tiempos remotos. El hecho que los soberanos exigieran el mantenimiento de las cuentas de su residencia por dos escribanos independientes, pone de manifiesto que fueron tomadas algunas medidas para evitar desfalcos en dichas cuentas. A medida que se desarrollo el comercio, surgió la necesidad de las revisiones independientes para asegurarse de la adecuación y finalidad de los registros mantenidos en varias empresas comerciales. La auditoría como profesión fue reconocida por primera vez bajo la Ley Británica de Sociedades Anónimas de 1862 y el reconocimiento general tuvo lugar durante el período de mandato de la Ley "Un sistema metódico y normalizado de contabilidad era deseable para una adecuada información y para la prevención del fraude". También reconocía..."Una aceptación general de la necesidad de efectuar una versión independiente de las cuentas de las pequeñas y grandes empresas". Desde 1862 hasta 1905, la profesión de la auditoría creció y floreció en Inglaterra, y se introdujo en los Estados Unidos hacia 1900. En Inglaterra siguió haciéndose hincapié en cuanto a la detección del fraude como objetivo primordial de la auditoría.

[12] http://www.monografias.com/trabajos12/condeau/condeau.shtml

En 1912 Montgomery dijo: En los que podría llamarse los días en los que se formó la auditoría, a los estudiantes se les enseñaba que los objetivos primordiales de ésta eran:

- La detección y prevención de fraude.
- La detección y prevención de errores

El crecimiento de la auditoría independiente en lo Estados Unidos, se desarrollaba la auditoría interna y del Gobierno, lo que entró a formar parte del campo de la auditoría. A medida que los auditores independientes se percibieron de la importancia de un buen sistema de control interno y su relación con el alcance de las pruebas a efectuar en una auditoría independiente, se mostraron partidarios del crecimiento de los departamentos de auditoría dentro de las organizaciones de los clientes, que se encargarían del desarrollo y mantenimiento de unos buenos procedimientos del control interno, independientemente del departamento de contabilidad general. Progresivamente, las compañías adoptaron la expansión de las actividades del departamento de auditoría interna hacia áreas que están más allá del alcance de los sistemas contables. En estos días, los departamentos de auditoría interna son revisiones de todas las fases de las corporaciones, en las que las operaciones financieras forman parte.

1.3.2 Concepto de Auditoría[13]

En la actualidad el término "auditoría" se ha mal utilizado o se le da una interpretación incorrecta, para ello se han tomado algunos conceptos muy validos en el presente.

a) La palabra auditoría proviene del latín "auditorius", y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

b) Por otra parte, La Real Academia Española lo define como: Revisor de Cuentas colegiado. En un principio esta definición carece de la explicación del objetivo fundamental que persigue todo auditor: evaluar la eficiencia y eficacia.

[13] Auditoría en Informática, Lic. José Antonio Echenequi García, Pág.2, 3.

c) Si se consulta el Boletín de Normas de auditoría del Instituto mexicano de contadores nos dice: " La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo son de carácter indudable."

d) El término Auditoría significa inspeccionar, revisar, verificar, investigar.

e) Examen crítico que se realiza con el objetivo de evaluar la eficiencia y eficacia de operación de una sección o de la totalidad de un organismo para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación.

f) Es una evaluación cuyo fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase "Tiene Auditoría" como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas, la función de auditoría es una parte fundamental del concepto de seguridad. [14]

g) Es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que la han sido prescritas. [15]

Características de la Auditoría Tradicional[16]

Existen ciertas características que se observan en la auditoría tradicional o financiera, las cuales se mencionan a continuación:

- Su función inicial, es estrictamente económico-financiero
- Debe ser absolutamente independiente
- No tiene carácter ejecutivo, ni son vinculantes sus conclusiones
- Contiene elementos de análisis, verificación y de exposición de debilidades y disfunciones

[14] http://www.lafacu.com/apuntes/informatica/audit_infor/default.htm,Auditoría.
[15] Auditoría Informática Un enfoque práctico. Mario G. Piattini, Pág. 4
[16] http://www.monografias.com/trabajos5/audi/audi.shtml

- Todas las sugerencias se plasman en un documento que al final recibe el nombre de recomendaciones.

1.3.3 Generalidades[17]

La auditoría nace como un órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico-financiera, y los casos inmediatos se encuentran en las peritaciones judiciales y las contrataciones de contables expertos por parte de Bancos Oficiales.

La función auditoría debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes.

La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.

1.3.4 Tipos de Auditoría

Existen diferentes tipos de auditoría, que según el objeto de estudio, y la finalidad con que se realiza, definen el tipo de auditoría, siendo estas.

- **Auditoría Externa**
- **Auditoría Financiera**
- **Auditoría Fiscal**
- **Auditoría Integral**
- **Auditoría Interna o de Campo**
- **Auditoría Interna y Auditoría Contable Financiera**
- **Auditoría Informática**

[17] Grupo Editorial Océano, Enciclopedia de la Auditoría Tomo I, Pág.40, 167,1187

1.3.5 Auditoría Informática[18]

A finales del siglo XX, los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, *Los Sistemas de Información de la Empresa*.

La Informática hoy, está intrínseca en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información. Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una Universidad, un Ministerio o un Hospital son tan empresas como una Sociedad Anónima o empresa Pública. Todos utilizan la informática para gestionar sus "negocios" de forma rápida y eficiente con el fin de obtener beneficios económicos y reducción de costos.

1.3.6 Concepto de Auditoría Informática[19]

Existen un sin número de conceptos sobre auditoría informática; pero muy pocos son aceptados, he aquí algunos conceptos muy validos sobre auditoría informática:

a) Es una función que ha sido desarrollada para la salvaguarda de los activos de los sistemas de computadoras, mantener la integridad de los datos y lograr los objetivos de la organización en forma eficaz y eficiente.

[18] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

[26] Auditoría en Informática, Lic. José Antonio Echenequi García, Pág.17-20

b) Es la verificación de los controles en las siguientes tres áreas de la organización(informática):
    - Aplicaciones (programas de producción)
    - Desarrollo de sistemas
    - Instalación del centro de proceso

c) Es la revisión y evaluación de los controles, sistemas y procedimientos de la información; de los equipos de computo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones.

1.3.7 Objetivos de la Auditoría Informática

La auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría.

a) **Objetivo General**

Su objetivo general consiste en la evaluación de un sistema informático para poder:

- Emitir una opinión sobre la fiabilidad y exactitud de los datos procesados
- Detectar y corregir errores encontrados y asegurar la continuidad del soporte automatizado de la gestión.
- Elaborar un informe de recomendaciones y plan de acción.

b) **Objetivos Específicos**

- El control de la función informática (Sistema de Información - SI y la Tecnología de la Información -TI).
- El análisis de la eficiencia de los SI y la TI.
- La verificación del cumplimiento de la Normativa General de la Organización.
- La verificación de los Planes, Programas y Presupuestos de los Sistemas Informáticos.
- La revisión de la eficaz gestión de los recursos materiales y humanos informáticos.
- La revisión y verificación de Controles Técnicos Generales y Específicos de Operatividad.
- La revisión y verificación de las Seguridades.

- De Cumplimiento de normas y estándares.
- De Sistema Operativo.
- De Seguridad de Software.
- De Seguridad de Comunicaciones.
- De Seguridad de Base de Datos.
- De Seguridad de Proceso.
- De Seguridad de Aplicaciones.
- De Seguridad Física.
- De Suministros y Reposiciones.
- De Contingencias.

- El análisis del control de resultados.
- El análisis de verificación y de exposición de debilidades y disfunciones.

1.3.8 Alcance de la Auditoría Informática

El alcance ha de definir con precisión el entorno y los límites que van a desarrollarse en la auditoría informática, se complementan con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. Ejemplo: ¿Se someterán los registros grabados a un control de integridad exhaustivo? ¿Se comprobará que los controles de validación de errores son adecuados y suficientes*? La indefinición de los alcances de la auditoría compromete el éxito de la misma.

1.3.9 Síntomas de Necesidad de una Auditoría Informática[20]

Las empresas acuden a las auditorías externas cuando existen síntomas bien perceptibles de debilidad. Existe una gran variedad de síntomas, a continuación se mencionan algunos de los más comunes:

- Controlar el uso de las computadoras, que cada día se vuelven más importantes y costosas.
- No coinciden los objetivos de la Informática de la Compañía y de la propia Compañía.

[20] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

- Los estándares de productividad se desvían sensiblemente de los promedios conseguidos habitualmente.
- Puede ocurrir con algún cambio masivo de personal, o en una reestructuración fallida de alguna área o en la modificación de alguna Norma importante.
- Síntomas de mala imagen e insatisfacción de los usuarios:
  - No se atienden las peticiones de cambios de los usuarios. Ejemplos: cambios de Software en los terminales de usuario, refrescamiento de paneles, variación de los ficheros que deben ponerse diariamente a su disposición, etc.
  - No se reparan las averías de Hardware ni se resuelven incidencias en plazos razonables. El usuario percibe que está abandonado y desatendido permanentemente.
  - No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de Aplicaciones críticas y sensibles.
- Síntomas de debilidades económico-financieras:
  - Incremento desmesurado de costos.
  - Necesidad de justificación de Inversiones Informáticas (la empresa no está absolutamente convencida de tal necesidad y decide contrastar opiniones).
  - Desviaciones Presupuestarias significativas.
  - Costos y plazos de nuevos proyectos (deben auditarse simultáneamente a Desarrollo de Proyectos y al órgano que realizó la petición).
- Síntomas de Inseguridad: Evaluación de nivel de riesgos
  - Seguridad Lógica
  - Seguridad Física
  - Confidencialidad

1.3.10 Control Interno y Auditoría Informática[21]

a) **Control**

Consiste en verificar si todo ocurre de conformidad con lo adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como fin señalar las debilidades y errores a fin de rectificarlos e impedir que se produzcan nuevamente.

[21] Auditoria Informática, Un enfoque practico. Mario G. Piattini, Pág. 25-40

b) **Control Interno**

Es el plan de organización de todos los métodos y procedimientos que son relativos y que están directamente relacionados principalmente con la salvaguarda de los activos y la confiabilidad de los registros financieros.

c) **Control Interno Informático**

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la Organización y/o la Dirección de Informática. Control interno informático suele ser un órgano staff de la Dirección del departamento de informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden.

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad.
- Asesorar sobre el conocimiento de las normas
- Colaborar y apoyar el trabajo de Auditoría informática, así como de las auditorias externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático.

Tipos de Controles Internos

Históricamente, los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- *Controles preventivos*: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema

- *Controles detectivos*: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

- *Controles correctivos*: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

Control Interno y Auditoría Informática: Campos Análogos

La evolución de ambas funciones ha sido espectacular durante la última década. Muchos controles internos fueron una vez auditores. Aunque ambas figuras tienen objetivos comunes, existen diferencias que conviene matizar:

Las similitudes y diferencias entre el control interno y la auditoría informática se puede observar en la Tabla 2.2.

	CONTROL INTERNO INFORMATICO	AUDITOR INFORMATICO
SIMILITUDES	• Personal interno • Conocimientos especializados en tecnología de la información • Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección general para los sistemas de información	
DIFERENCIAS	• Análisis de los controles en el día a día • Informa a la Dirección del departamento de Informática • Solo personal interno • El alcance de sus funciones es únicamente sobre el departamento de Informática	• Análisis de un momento informático determinado • Informa a la Dirección general de la Organización • Personal interno y/o externo • Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización

Tabla 2.2. Similitudes y Diferencias del Control Interno y Auditoría Informática[22]

[22] Auditoria Informática, Un enfoque practico. Mario G. Piattini, Pág. 30

1.3.11 Herramientas y Técnicas para la Auditoría Informática[23]

El auditor informático al igual que el auditor financiero hace uso de herramientas que ayudan la gestión de examinar la eficiencia y eficacia a los controles establecidos sobre el objeto que se evalúa, entre las herramientas más utilizadas por el auditor informático tenemos:

- Cuestionarios.
- Entrevistas.
- Formularios Checklist.
- Formularios Virtuales,
- Pruebas de Consistencias.
- Inventarios y Valorizaciones.
- Historias de cambios y mejoras.
- Reporte de Bases de Datos y Archivos
- Reportes de Estándares.
- Compatibilidades y Uniformidades.
- Software de Interrogación:
- Certificados, Garantías, otros del Software.
- Fotografías o Tomas de Valor (Imágenes).
- Diseño de Flujos y de la red de Información.
- Planos de Distribución e Instalación (Para Estudio y Revisión).
- Listado de Proveedores.
- Otros.

1.3.12 Metodología, Fases y Plan de una Auditoría Informática

Según el Diccionario de la Lengua de la Real Academia Española, METODO es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra METODOLOGIA como "conjunto de métodos que se siguen en una investigación científica o en una exposición

[23] http://perso.wanadoo.es/idmb/a_ing/temas/auditoría_informatica.htm

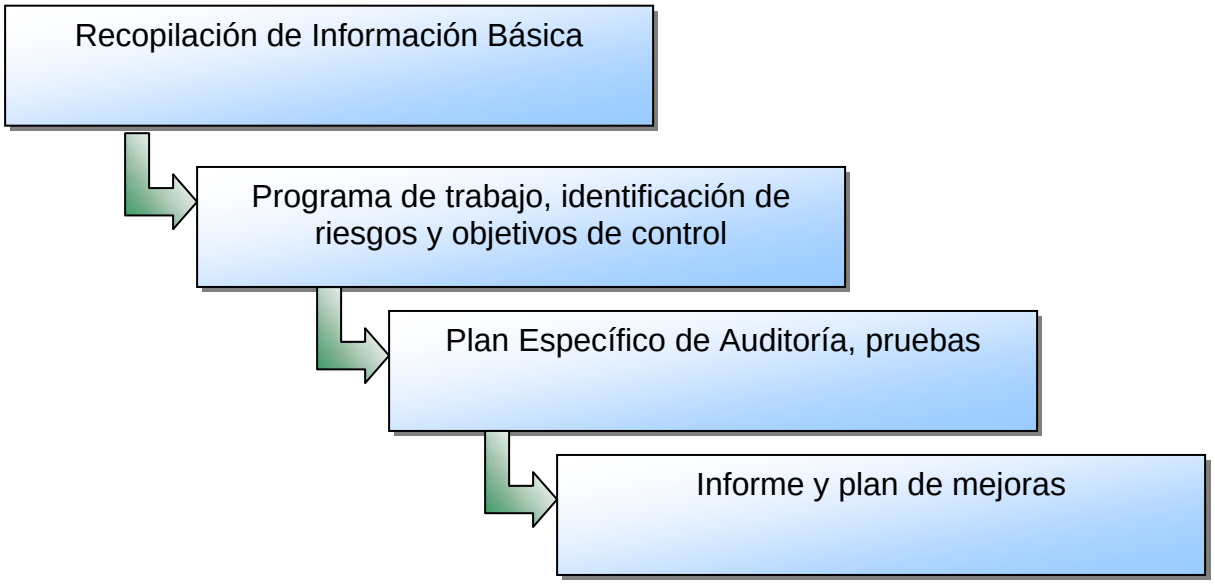
doctrinal". Esto significa que cualquier proceso científico debe estar sujeto a una disciplina de proceso definida con anterioridad que llamaremos Metodología.

Por lo que a continuación se presenta la metodología para llevar a cabo una auditoría informática:

- Diseño del Plan y método de trabajo.
- Alcance y Objetivos de la Auditoría Informática.
- Estudio inicial del entorno u medio auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del plan y de los Programas de Trabajo.
- Actividades propiamente dichas de la auditoría.
- Confección y redacción del Informe Final.
- Determinación de las Conclusiones y recomendaciones.
- Fijación del Pliego de Responsabilidades y valoración de Gestión.
- Redacción de la Carta del Informe final

a) **Fases y Planificación de una Auditoría Informática**

Para hacer una adecuada realización de la auditoría informática, hay que seguir una serie de fases previas:



b) **Plan para Realizar una Auditoría Informática** [24]

Para la realización de una auditoría informática se deben completar las siguientes fases y planificación de actividades:

- **Toma de contacto**

  Primera toma de contacto con la empresa auditada para conocer características generales de la misma: sector industrial, organización y organigrama, relaciones externas, volumen de negocio, etc.

- **Definición del alcance**

  Se ha de definir con precisión el área y objetivos perseguidos por la auditoría.
  Se ha de indicar que parte del servicio de informática va a ser auditado así como hacer constar que elementos de éste van a quedar fuera de la auditoría.
  Deben quedar recogidas, si existieran, excepciones que se deben tener cuenta al efectuar la revisión.
  Desde el punto de vista de los objetivos, debe quedar reflejado cuales son los motivos y fines que persigue la auditoría.

- **Recursos y tiempo**
  - Recursos personales (equipo auditor)
  - Recursos materiales.
  - Calendario de actuaciones.

- **Plan de trabajo. Recopilación de la información**

  Análisis de la información básica obtenida en la primera toma de contacto con la organización.
  Conclusiones que se deducen.

---

[24] http://www.monografias.com/trabajos/maudisist/maudisist.shtml

Establecimiento del programa de trabajo a realizar para ampliar y completar la información necesaria para la realización de la auditoría informática. Esta recopilación de información se puede realizar de varias formas: entrevistas personales, cuestionarios, observación de las actividades.

Se establece el orden, cronología y personal asignado a cada una de las anteriores tareas. Posteriormente se realizará un análisis y resumen con los conceptos fundamentales obtenidos en dichas entrevistas.

- **Identificación de los riesgos potenciales**

Con toda la información obtenida en las fases anteriores, el equipo de auditoría estará en condiciones de identificar los riesgos potenciales que pueden existir en el servicio informático, teniendo en cuenta el alcance que se ha definido para la realización de la auditoría.

- **Definición de pruebas**

El equipo de auditoría debe realizar pruebas para verificar la consistencia de los controles existentes o bien para medir el riesgo existente.

Toda opinión o evaluación de un auditor debe estar basada en pruebas realizadas de acuerdo con una normativa profesional.

Las pruebas pueden ser de cumplimiento, se utilizan para comprobar si el riesgo potencial es real.

- **Obtención de resultados de las pruebas**

Los resultados de cada prueba deben valorarse para obtener una conclusión, siempre teniendo en cuenta los objetivos y el alcance de la auditoría.

- **Obtención de resultados de las pruebas**

Las conclusiones obtenidas deben comentarse y discutirse con los responsables directos del área afectada por las razones que se expresan a continuación:

- Puede haber limitaciones en la realización de las pruebas.
- Puede haber controles alternativos que no hayan detectado en el proceso

Todas las deficiencias o riesgos deben ser objeto de comentarios individuales y deben incluir:

- Descripción de la situación.
- Riesgo existente y deficiencia a solucionar.
- Si es preciso, sugerencia de solución.

- **Revisión y cierre de papeles de trabajo**

Tiene por objeto preparar la documentación del trabajo realizado y se debe realizar de acuerdo con unas normas básicas de auditoría que expresen:

- La metodología utilizada.
- Cobertura del objetivo de la auditoría.
- Pruebas realizadas y criterios utilizados.
- Resultado de las pruebas.

Antes de pasar a la realización del borrador del informe, los papeles de trabajo deben ser revisados, tratando de identificar:

- Las limitaciones en las tareas realizadas.
- Deficiencias en pruebas realizadas, que puedan requerir alguna extensión especial de la revisión.
- Falta de consistencia o claridad en las conclusiones.
- Documentación de todas las conclusiones obtenidas.

- **Preparación del borrador del informe**

El borrador del informe, es un resumen del trabajo efectuado durante la realización de la auditoría y debe incluir:

- El alcance y objetivo de la auditoría.
- La metodología utilizada.
- Las posibles limitaciones y conclusiones.

- **Discusión del informe**

Es importante que el informe, antes de su emisión definitiva, sea comentado y discutido con los responsables del área auditada y en caso de discrepancia de opiniones con el área auditada, estas deberán ser incluidas en el texto final del informe.

- **Emisión y distribución del informe**

Finalizada la realización de la auditoría informática, se redactará el informe final y posteriormente se enviará a la dirección de la empresa.

- **Plan de mejoras o recomendaciones**

El informe puede ir acompañado de un plan de mejoras donde para cada uno de los problemas detectados se ofrezca un conjunto de posibles soluciones.

Estas soluciones pueden dividirse en tres tipos:

- Medidas a corto plazo (formación, cumplimiento de calendario)
- Medidas a medio plazo (mayor cantidad de recursos, mejoras en la estructura organizativa)
- Medidas a largo plazo (cambio de política en el ser. Informática, objetivos, etc).

1.4 NORMA ISO/IEC 17799

1.4.1 Introducción Sobre la Norma ISO/IEC 17799[25]

Los gerentes de seguridad de la información han esperado mucho tiempo a que alguien tomara el liderazgo para producir un conjunto de normas de seguridad de la información que estuviera

[25] http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1261.html

sujeto a auditoría y fuera reconocido globalmente. Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la Organización Internacional de Normas en Diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

1.4.2 El Origen de ISO/IEC 17799

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado parámetros globales a las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de la información.

Finalmente en 1995, el BSI publicó la primera norma técnica de seguridad, BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el e-commerce. En 1995, problemas como el Y2K y el la Unidad Monetaria Europea (EMU por su sigla en inglés) prevalecieron sobre otros. Para empeorar las cosas, la norma BS 7799 se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces.

Cuatro años después en mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la norma BS 7799, la que fue una revisión más amplia de la primera publicación. Esta edición sufrió muchos mejoramientos y perfeccionamientos desde la versión de 1995. En este momento la ISO se percató de estos cambios y comenzó a trabajar en la revisión de la norma técnica BS 7799.

En Diciembre de 2000, la Organización Internacional de Normas Técnicas (ISO) adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799. Alrededor de la

misma época, se adoptó un medio formal de acreditación y certificación para cumplir con la norma técnica. Los problemas Y2K y EMU y otros similares se habían solucionado o reducido a 2000 y la calidad total de la norma técnica había mejorado considerablemente. La adopción por parte de ISO de la Parte 1 - los criterios de la norma técnica - de BS 7799 recibió gran aceptación por parte del sector internacional y fue en este momento que un grupo de normas técnicas de seguridad tuvo amplio reconocimiento.

1.4.3 Marco de las Recomendaciones

La norma ISO 17799 no incluye la segunda parte de BS 7799, que se refiere a la implementación. ISO 17799 hoy en día es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector. La norma técnica fue redactada intencionalmente para que fuera flexible y nunca indujo a las personas que la cumplían para que prefirieran una solución de seguridad específica. Las recomendaciones de la norma técnica ISO 17799 son neutrales en cuanto a la tecnología y no ayudan a evaluar y entender las medidas de seguridad existentes. Así, la norma discute la necesidad de contar con cortafuegos, pero no profundiza sobre los tres tipos de cortafuegos y cómo se utilizan, lo que con lleva a que algunos detractores de la norma digan que ISO 17799 es muy general y que tiene una estructura muy imprecisa y sin valor real.

La flexibilidad e imprecisión de ISO 177999 es intencional por cuanto es difícil contar con una norma que funcione en una variedad de entornos de tecnología de la información y que sea capaz de desarrollarse con el cambiante mundo de la tecnología. ISO 177999 simplemente ofrece un conjunto de reglas a un sector donde no existían.

La ISO 17799 está redactada bajo la forma verbal "should" (DEBERIA), un término presente en otras normas ISO y también del IETF que, por convención, expresa una forma condicional a modo de recomendación y no de imposición. Es así como la norma hace precisamente *recomendaciones* y no establece requisitos cuyo cumplimiento pudieren certificarse.

Lamentablemente, errores en algunas traducciones han traído confusión en el verdadero alcance de esta norma.

Ocurre que la ISO 17799 deriva de la norma británica BS 7799-1 (Parte 1 de la BS 7799) y en realidad prácticamente es igual a la misma. (Figura 2.7)

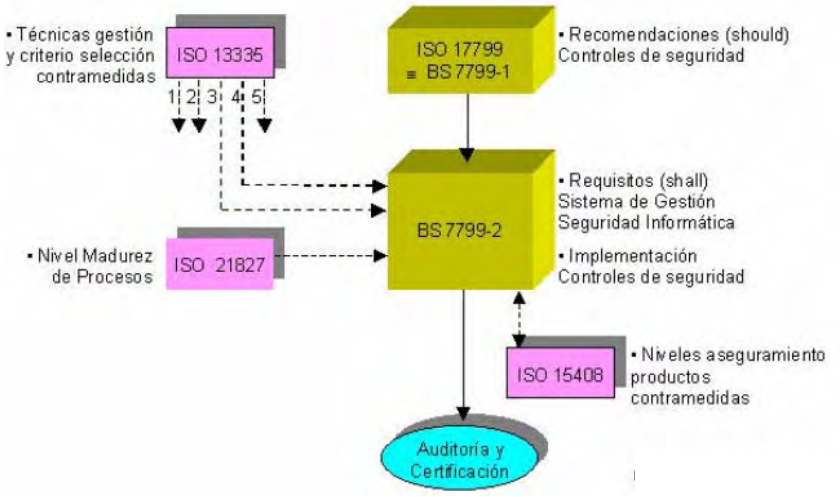


Figura 2.7. Diagrama de relación entre norma BS 7799-1 y ISO 17799

Pero la norma británica tiene dos partes. La última versión de la Parte 2, es del 2002 denominándose entonces BS 7799-2:2002, aunque por simplicidad en lo sucesivo la mencionaremos simplemente como BS 7799-2.

La BS 7799-2 usa la expresión "shall" (DEBE), otro término habitual en ciertas normas, en este caso para expresar mandato u obligación. De esta manera la BS 7799-2 especifica los *requisitos* para establecer un plan de seguridad constituido por un *Sistema de Gestión de Seguridad Informática* (SGSI o ISMS, por su nombre en inglés) dentro del contexto de los riesgos totales de negocios de una empresa.
Estas especificaciones y la implementación correspondiente hacen que tanto la auditoría como la certificación se hagan con referencia a la BS 7799-2, toda vez que no hay una versión ISO equivalente de esta segunda parte de la BS 7799.

1.4.4 Estructura de la Norma ISO/IEC 17799

La norma esta compuesta de áreas, objetivos y controles.

- Cada área o dominio tiene asociados uno o varios objetivos de seguridad

- Para cada objetivo se definen, a su vez, uno o más controles de seguridad cuya implantación debe traducirse en la consecución del objetivo de seguridad asociado.

10 Áreas

36 Objetivos

127 Controles

En la Tabla 2.3 se puede apreciar un ejemplo de cómo se organiza un área, sus objetivos y sus controles.

ÁREA	OBJETIVOS	CONTROLES
5. Seguridad física y lógica	5.1 Áreas seguras	5.2.1 Instalación y protección de los equipos
	5.2 Seguridad de los equipos	5.2.2 Suministro eléctrico
	5.3 Controles generales	5.2.3 Seguridad del cableado
		5.2.4 Mantenimiento de equipo
		5.2.5 Seguridad de los equipos fuera de las instalaciones de la Organización
		5.2.6 Seguridad en la reutilización o eliminación de equipos

Tabla 2.3 Ejemplo de estructura de la Norma

1.4.5 Objetivos de la Norma ISO/IEC 17799 [26]

Dentro de los objetivos de la norma encontramos:

a) **Objetivo General**

La finalidad principal es implantar en las empresas de la sociedad de la información una cultura de gestión, seguridad y calidad basada en los aspectos específicos de su actividad y que les permita afrontar las demandas de su sector y crecer competitivamente. Mejorando las empresas de la sociedad de la información, (cuyos servicios a empresas y particulares están

[26] http://alerta-antivirus.red.es/docs/seguridad_empresas.pdf Pág.21-27

cada vez más extendidos, son más críticos como recurso base para otros negocios y cuya influencia es cada vez mayor), se mejorará la actividad de sus clientes, empresas y organizaciones y se ganarán adeptos a la sociedad de la información.

b) **Objetivos Específicos**

- Aumentar la seguridad objetiva de los sistemas de información y de las comunicaciones que constituyen una de las infraestructuras claves de la sociedad actual.
- Mejorar la seguridad de la información percibida y aumentar el grado de confianza de empresas, ciudadanos y administraciones en las tecnologías de la información y de las comunicaciones para facilitar el desarrollo de la Sociedad de la Información.
- Mejorar el grado de protección de activos humanos, de información y materiales frente a accidentes y agresiones.
- Garantizar la integridad, confidencialidad y disponibilidad de la información por su gran valor estratégico.
- Protección de los datos personales, la seguridad en el comercio electrónico y en los pagos a través de Internet, la confidencialidad de las comunicaciones, la autentificación de los usuarios y la protección frente a virus informáticos y ataques de hackers.
- Mejorar la competitividad, crecimiento económico, mejoras en la productividad, creación de riqueza y empleo en los próximos años.
- Mantener relaciones de negocio tanto interiores como exteriores, sin limitaciones por falta de seguridad o certificación en los Sistemas de Gestión de la Seguridad de la Información.
- Conseguir en todo momento un rápido acceso a los datos y un oportuno empleo de los Sistemas de Seguridad de la Información que aumenten la competitividad de sus organizaciones.
- Poner en marcha Planes de Contingencia activos, que reduzcan los tiempos de retorno a la situación normal.
- Impulsar la confianza de empresas, consumidores y ciudadanos en general en los nuevos servicios, apoyando los sistemas de resolución extrajudicial de conflictos y la elaboración de códigos de conducta de los prestadores de servicios, así como promoviendo el uso seguro de Internet.

- La acreditación es un elemento muy valioso, de cara a que los clientes y asociados de una empresa certificada, confíen en que la información guardada en su red empresarial está segura y que la seguridad general de la empresa es confiable.

1.4.6 Las Diez Áreas de Control de ISO/IEC 17799 [27]

La ISO/IEC 17799:2000 considera la organización como una totalidad y tiene en consideración todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que puedan producirse. Como ya se menciono, esta formada de 10 dominios en los que cada uno de ellos hace referencia a un aspecto de la seguridad de la organización (Ver Figura 2.8):

Fig.2.8 Áreas de la Norma ISO 17799

[27] http://www.symantec.com/region/mx/enterprisesecurity/content/framework/LAM_1261.html

a) **Política de seguridad:** Una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte. La política también se puede utilizar como base para el estudio y evaluación en curso.
b) **Organización de la seguridad:** Diseñar una estructura de administración dentro la organización que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.
c) **Control y clasificación de los recursos de información:** Elaborar un inventario de los recursos de información de la organización y con base en este conocimiento, debe asegurar que se brinde un nivel adecuado de protección.
d) **Seguridad del personal:** Establecer un plan para educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determinar cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la compañía.
e) **Manejo de las comunicaciones y las operaciones:** Los objetivos de esta sección son:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de falla de los sistemas.
- Proteger la integridad del software y la información.
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

f) **Control de acceso:** Establecer la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.
g) **Desarrollo y mantenimiento de los sistemas:** Recordar que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

h) **Manejo de la continuidad de la empresa:** Aconsejar estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes de la empresa en caso de una falla grave o desastre.

i) **Cumplimiento:** Impartir instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma técnica ISO 17799 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

1.4.7 Beneficios de la Norma ISO/IEC 17799[28]

Una empresa certificada con la norma técnica ISO 17799 puede ganar frente a los competidores no certificados. Si un cliente potencial tiene que escoger entre dos servicios diferentes y la seguridad es un aspecto importante, por lo general optará por la empresa certificada. Además una empresa certificada tendrá en cuenta lo siguiente:

- Mayor seguridad en la empresa.
- Planeación y manejo de la seguridad más efectivos.
- Alianzas comerciales y e-commerce más seguras.
- Mayor confianza en el cliente.
- Auditorías de seguridad más precisas y confiables.
- Menor Responsabilidad civil

1.4.8 Generalidades sobre la Norma ISO/IEC 17799[29]

Actualmente ISO está revisando la norma técnica 17799 para que se adapte mejor a su amplio público. ISO 17799 es la primera norma técnica y se harán y ampliarán sus recomendaciones y sugerencias básicas en la medida que sea necesario. Por ahora, ISO 17799 es la norma técnica a seguir.

Esta norma es aplicable a cualquier empresa, sea cual sea el tamaño, la actividad de negocio o el volumen del mismo, esto es lo que se denomina el principio de proporcionalidad de la norma, es

[28] http://alerta-antivirus.red.es/docs/seguridad_empresas.pdf Pág.45-46
[29] http://www.virusprot.com/Art41.htm

decir que todos los aspectos que aparecen en la normativa deben ser contemplados y tenidos en cuenta por todas las organizaciones a la hora de proteger sus activos, y la diferencia radicará en que una gran organización tendrá que utilizar más recursos para proteger activos similares a los que puede poseer una pequeña organización. De la misma forma, dos organizaciones que tengan actividades de negocio muy diferentes, no dedicarán los mismos esfuerzos a proteger los mismos activos/informaciones. En pocas palabras, esta norma debe tenerse como guía de los aspectos que deben tener controlados y no quiere decir que todos los aspectos que en ella aparecen tienen que ser implementados con los últimos avances, eso dependerá de la naturaleza de la propia organización.

1.5 ANTECEDENTES TECNOLÓGICOS RELACIONADA CON EL PROYECTO

El presente proyecto para su implementación hará uso de tecnología de vanguardia, como lo es Internet, entorno Web y aplicaciones de servidor. A continuación se presenta una breve información sobre esta tecnología.

1.5.1 Internet

Internet puede ser definida como ***"Una red de redes de computadoras"*** que se encuentran interconectadas a lo largo del mundo, nadie es dueño de Internet simplemente cada usuario paga su conexión hasta llegar a la red.

Para darse una idea de cómo Internet se incorpora a la sociedad se debe recordar que la radio demoró 28 años en llegar a 40 millones de personas y la televisión solo tardo 10 años en llegar a la misma cantidad de gente, hoy dichos medios tiene una llega masiva.

Internet apenas tardo 3 años en llegar al mismo número de personas y pronto será un elemento de comunicación más en la vida cotidiana.

Ventajas Que Ofrece Internet

Son muchas las ventajas que Internet nos ofrece, podríamos llenar páginas enteras de bondades, pero trataremos de citar las principales.

Acceso Global: Uno ingresa a la red a través de una llamada telefónica o una línea alquilada directa a Internet y el acceso a la información no posee un costo de comunicación extra para la información donde se encuentre, que puede ser localmente o en otro país.

Acercamiento con los clientes: Mediante Internet y el correo electrónico, se tiene llegada a personas e información dentro y fuera de las empresas que para realizarlo por medio de otras tecnologías en algunos casos se tornaría imposible

Relaciones mediante hiperlinks: Con el solo clic de un botón paso de un servidor de información a otro en forma transparente y gráfica.

Compatibilidades tecnológicas: Puedo acceder de equipos corriendo sistemas operativos gráficos como Windows 98/NT o Mac, a sistemas operativos tipo carácter como algunas versiones de Unix y otros en forma transparente, ya que la red se encarga de resolver esta compatibilidad.

1.5.2 URL (Uniform Resource Locator)

Es decir, localizador uniforme de recurso. El URL es la cadena de caracteres con la cual se asigna dirección única a cada uno de los recursos de información disponibles en Internet. Existe un URL único para cada página de cada uno de los documentos de la World Wide Web.

El URL de un recurso de información es su dirección en Internet, la que permite que el navegador la encuentre y la muestre de forma adecuada.

El formato general de un URL es: "servicio://dirección_de_la máquina:puerto/directorio/fichero",

Por ejemplo: http://www.ufg.edu.sv

1.5.3 La World Wide Web (www)

La WWW convierte el acceso a la Internet en algo sencillo para el público en general, lo que da a ésta un crecimiento explosivo. Es relativamente sencillo recorrer la Web y publicar información en ella, las herramientas de la WWW crecieron a lo largo de los últimos tres años hasta ser las más populares.

Permite unir información que está en un extremo del planeta con otro en un lugar distante a través de algo que se denomina hipervínculo, al hacer clic sobre éste nos comunica con el otro sector del documento o con otro documento en otro servidor de información.

Que es una página Web?

Una aplicación Web consta de una o más páginas conectadas entre sí. Un buen punto de partida sería decir que una página Web es un archivo de texto que contiene lenguaje de marcas de hipertexto (**HTML**), etiquetas de formato y vínculos a archivos gráficos y a otras páginas Web.

El archivo de texto se almacena en un servidor Web al que pueden acceder otras computadoras conectadas a ese servidor, vía Internet o una LAN. Al archivo se puede acceder utilizando exploradores Web que no hacen otra cosa que efectuar una transferencia de archivos e interpretación de las etiquetas y vínculos HTML, y muestran el resultado en el monitor.

Otra definición sería que una página Web es un formulario interactivo que utiliza una red de computadoras.

Hay dos propiedades de las páginas Web que las hacen únicas: que son interactivas y que pueden usar objetos multimedia. El término multimedia se utiliza para describir archivos de texto, sonido, animación y video que se combinan para presentar la información, por ejemplo, en una enciclopedia interactiva o juego.

1.5.4 Exploradores o Navegadores Web

Todos los exploradores Web interpretan y muestran los archivos codificados en HTML.

Los navegadores (Browser) mas utilizado en el mundo de la Internet tenemos:

- Internet Explorer (Microsoft)
- Netscape (Netscape)
- Firefox (Mozilla)

Los fabricantes de exploradores Web han creado extensiones fuera del estándar. Esto ha sido positivo para la Web en término de avances, pero también ha creado grandes problemas en

términos de compatibilidad. Algunas de las extensiones son compatibles entre sí pero otras funcionan solamente en sus respectivos exploradores, las principales diferencias ocurren con la tecnología Java y ActiveX.

1.5.5 Servidores Web

Un **servidor Web** es un programa que implementa el *protocolo HTTP* (hypertext transfer protocol). Este protocolo está diseñado para transferir lo que llamamos hipertextos, páginas web o páginas HTML (hypertext markup language): textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de sonidos.

Cabe destacar el hecho que la palabra *servidor* identifica tanto al programa como a la máquina en la que dicho programa se ejecuta. Existe, por tanto, cierta ambigüedad en el término, aunque no será difícil diferenciar a cuál de los dos nos referimos en cada caso. En este artículo nos referiremos siempre a la aplicación.

Un servidor Web se encarga de mantenerse a la espera de *peticiones HTTP* llevada a cabo por un *cliente HTTP* que solemos conocer como *navegador*. El navegador realiza una petición al servidor y éste le responde con el contenido que el cliente solicita. A modo de ejemplo, al teclear *www.ufg.edu.sv* en nuestro navegador, éste realiza una petición HTTP al servidor de dicha dirección. El servidor responde al cliente enviando el código HTML de la página; el cliente, una vez recibido el código, lo interpreta y lo muestra en pantalla..

Los servidores web más populares son: Http Apache y IIS de Microsoft

- **HTTP Apache** es un servidor HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etcétera), Windows y otras, que implementa el protocolo HTTP/1.1 (RFC 2616) y la noción de sitio virtual. Cuando comenzó su desarrollo en 1995 se basó inicialmente en código del popular NCSA HTTPd 1.3, pero más tarde fue reescrito por completo. Su nombre se debe a que originalmente Apache consistía solamente en un conjunto de parches a aplicar al servidor de NCSA. Era, en inglés, *a patchy server* (un servidor *parcheado*).

El servidor Apache se desarrolla dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Apache presenta entre otras cosas mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido, pero fue criticado por la falta de una interfaz gráfica que ayude en su configuración.

En la actualidad (2005), Apache es el servidor HTTP más usado, siendo el servidor HTTP del 68% de los sitios web en el mundo y creciendo aún su cuota de mercado (estadísticas históricas y de uso diario proporcionadas por Netcraft

- **Internet Information Server** (o Services), IIS, es una serie de servicios para los ordenadores que funcionan con Windows. Originalmente era parte del *Option Pack* para Windows NT. Luego fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP Profesional incluye una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS.

El servidor web se basa en varios módulos que le dan capacidad para procesar distintos tipos de páginas, por ejemplo Microsoft incluye los de Active Server Pages (ASP) y ASP.NET. También pueden ser incluidos los de otros fabricantes, como PHP.

1.5.6 Aplicaciones de Usuario y de Servidor en Internet

Sobre el servicio Web *clásico* podemos disponer de aplicaciones Web. Éstas son fragmentos de código que se ejecutan cuando se realizan ciertas peticiones o respuestas HTTP. Hay que distinguir entre:

- *Aplicaciones en el lado del cliente:* el cliente web es el encargado de ejecutarlas en la máquina del usuario. Son las aplicaciones tipo Java o Javascript: el servidor proporciona el código de las aplicaciones al cliente y éste, mediante el navegador, las ejecuta. Es necesario, por tanto, que el cliente disponga de un navegador con capacidad para ejecutar aplicaciones (también llamadas *scripts*). Normalmente, los navegadores permiten ejecutar aplicaciones escritas en lenguaje *javascript* y *java*, aunque pueden añadirse mas lenguajes mediante el uso de *plugin*s

- *Aplicaciones en el lado del servidor:* el servidor web ejecuta la aplicación; ésta, una vez ejecutada, genera cierto código HTML; el servidor toma éste código recién creado y lo envía al cliente por medio del protocolo HTTP.

Las aplicaciones de servidor suelen ser la opción por la que se opta en la mayoría de las ocasiones para realizar aplicaciones web. La razón es que, al ejecutarse ésta en el servidor y no en la máquina del cliente, éste no necesita ninguna capacidad adicional, como sí ocurre en el caso de querer ejecutar aplicaciones javascript o java. Así pues, cualquier cliente dotado de un navegador web básico puede utilizar éste tipo de aplicaciones.

Como aplicaciones de servidor más populares tenemos: ASP, PHP, .NET, JSP

- **Active Server Pages** (**ASP**) es una tecnología del lado servidor de Microsoft para páginas web generadas dinámicamente, que ha sido comercializada como un anexo a Internet Information Server (IIS).

ASP ha pasado por cuatro iteraciones mayores, ASP 1.0 (distribuido con IIS 3.0), ASP 2.0 (distribuido con IIS 4.0), ASP 3.0 (distribuido con IIS 5.0) y ASP.NET (parte de la plataforma .NET de Microsoft). Las versiones pre-.NET se denominan actualmente (desde 2002) como ASP *clásico*.

- **PHP** (acrónimo de "PHP: Hypertext Preprocessor") es un lenguaje de programación de scripts, concebido en el tercer trimestre de 1994 por Rasmus Lerdorf. Se utiliza principalmente para la programación dinámica de páginas web, destaca por su capacidad de ser embebido en el código HTML. Además, existe un compilador comercial (el Zend Optimizer).

Es parte de las tecnologías de código abierto (Open Source), y es uno de los más utilizados hoy en día para aplicaciones Web con soporte nativo con muchas bases de datos y otros servicios de servidor como: correo electrónico, ftp. Además puede trabajar en diferentes plataformas de S.O. como: Windows, Linux, Unix, OS2, Solaris, Mac, etc y Servidores Web como: Apache, IIS, Lotus Notes, etc.

Su estructura a nivel de módulos le permite ir creciendo a la par de nuevas tendencias tecnológicas, la comunidad de expertos alrededor del mundo enriquecen su funcionamiento, actualmente se encuentra en la versión 5.

- **.NET** La tecnología .NET de Microsoft es la respuesta al creciente mercado de los negocios en entornos Web. Es una plataforma que provee una serie de herramientas orientadas a simplificar el trabajo en la red, desde el punto de la validación de datos y la programación portable en múltiples lenguajes de programación que soporten el uso de sus librerías. Muchas personas lo encuentran como la competencia del lenguaje de programación Java en entornos corporativos.
- **Java Server Pages (JSP)** es la tecnología para generar páginas Web de forma dinámica en el servidor, desarrollado por Sun Microsystems, basado en scripts que utilizan una variante del lenguaje java.

La tecnología JSP, o de JavaServer Pages, es una tecnología Java que permite a los programadores generar dinámicamente HTML, XML o algún otro tipo de página web. Esta tecnología permite al código Java y a algunas acciones predefinidas ser empotradas en el contenido estático. En las jsp, se escribe el texto que va a ser devuelto en la salida (normalmente código HTML) empotrando código java dentro de él para poder modificar o generar contenido dinámicamente. El código java se incluye dentro de las marcas de etiqueta <% y %>.

1.5.7 Motores de Bases de Datos para Internet

Las definiciones de base de datos son numerosas. Todas coinciden que es un conjunto de datos almacenados en un soporte de acceso directo. Los datos están interrelacionados y estructurados de acuerdo a un modelo que sea capaz de recoger el máximo contenido semántico.

El Web es un medio para localizar/enviar/recibir información de diversos tipos, aun con las bases de datos. En el ámbito competitivo, es esencial ver las ventajas que esta vía electrónica proporciona para presentar la información, reduciendo costos y el almacenamiento de la información, y aumentando la rapidez de difusión de la misma.

Internet provee de un formato de presentación dinámico para ofrecer campañas y mejorar negocios, además de que permite acceder a cada sitio alrededor del mundo, con lo cual se incrementa el número de personas a las cuales llega la información.

Alrededor de 14 millones de personas alrededor del mundo hacen uso de Internet, lo cual demuestra el enorme potencial que esta red ha alcanzado, con lo cual se puede decir que en un futuro no muy lejano, será el principal medio de comunicación utilizado para distintos fines.

Los usuarios de Internet o Intranet pueden obtener un medio que puede adecuarse a sus necesidades de información, con un costo, inversión de tiempo, y recursos mínimos. Asimismo, las bases de datos serán usadas para permitir el acceso y manejo de la variada información que se encuentra a lo largo de la red.

A continuación se presentan breves descripciones de los motores de bases más populares en el ambiente Web.[30]

- **MySQL** es una de las bases de datos más populares desarrolladas bajo la filosofía de código abierto. La desarrolla y mantiene la empresa MySql AB pero puede utilizarse gratuitamente y su código fuente está disponible.

Entre sus características principales tenemos:

- Amplio subconjunto del lenguaje SQL. Algunas extensiones son incluidas igualmente.
- Disponibilidad en gran cantidad de plataformas y sistemas.
- Diferentes opciones de almacenamiento según si se desea velocidad en las operaciones o el mayor número de operaciones disponibles.
- Transacciones y claves foráneas.
- Conectividad segura.
- Replicación.
- Búsqueda e indexación de campos de texto.

[30] http://es.wikipedia.org Enciclopedia libre

- **Microsoft SQL Server** es una herramienta de gestión y administración de bases de datos relaciones basada en el lenguaje SQL, que incluye también un potente entorno gráfico de administración, que permite el uso de comandos DLL y DML gráficamente.

Permite trabajar en modo cliente-servidor donde la información y datos se alojan en el servidor y las terminales o clientes de la red sólo accedan a la información.

Además permite administrar información de otros servidores de datos, también maneja de forma fácil la seguridad en cuanto al acceso a las bases de datos.

- **PostgreSQL** es un servidor de base de datos relacional libre, liberado bajo la licencia BSD. Es una alternativa a otros sistemas de bases de datos de código abierto (como MySQL, Firebird y MaxDB), así como sistemas propietarios como Oracle o DB2.

Algunas de sus principales características son:

- Claves ajenas
- Disparadores (*triggers*)
- Vistas
- Integridad transaccional
- Acceso concurrente multiversión (no se bloquean las tablas, ni siquiera las filas, cuando un proceso escribe)
- Capacidad de albergar programas en el servidor en varios lenguajes.
- Herencia de tablas
- Tipos de datos y operaciones geométricas

- **Oracle** es un sistema de administración de base de datos (o RDBMS por el acrónimo en inglés de Relational Data Base Management System), fabricado por Oracle Corporation.

Se considera a Oracle como el sistema de bases de datos más completo que existe, destacando su:

- Soporte de transacciones.
- Gran estabilidad.
- Gran seguridad.

- Escalabilidad.
- Es multiplataforma.
- Soporta PL/SQL.

Su mayor defecto es su enorme precio, que es de varios miles de dólares (según versiones y licencias).

Aunque su dominio en el mercado de servidores empresariales ha sido casi total hasta hace poco, recientemente sufre la competencia del Microsoft SQL Server de Microsoft y de la oferta de otros RDBMS con licencia GNU como MySql. Las últimas versiones de Oracle han sido certificadas para poder trabajar bajo Linux.