Capítulo 6
Contenidos desarrollados

Los temas que se desarrollan en este capítulo se basan en la realización de un análisis exhaustivo de los programas de estudio correspondientes a las asignaturas de Seguridad Informática I y II, dando como resultado la actualización del material de apoyo que se brinda a los alumnos de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México.

Es necesario destacar que el mundo de la seguridad informática es muy amplio y complejo, por ello se contemplaron incluir estos temas ya que beneficiará al buen aprendizaje de ambas asignaturas, logrando así cumplir con los objetivos de cada una de éstas.

Los temas propuestos para actualizar el material de apoyo se ven reflejados a continuación, de manera que se muestra el índice modificado del libro ya mencionado (Fundamentos de Seguridad Informática) destacando con letra cursiva y en negritas los temas que se le han agregado a éste.

"Fundamentos de Seguridad Informática"
CONTENIDO

CAPÍTULO 1
CONTEXTO DE LA SEGURIDAD
1.1 Panorama general
1.2 Metodología
1.3 Perfiles de protección
    1.3.1 Estructura de los perfiles de protección
    1.3.2 Administración de la seguridad

CAPÍTULO 2
NORMATIVIDAD
2.1 Definiciones
2.2 Niveles de seguridad
    2.2.1 Criterios comunes
    2.2.2 Estándar ISO 17799
    2.2.3 Familia de Normas ISO/IEC 27000
    2.2.4 Identificación de los factores de riesgo
    2.2.5 Metodologías para el análisis de riesgos

CAPÍTULO 3
AMENAZAS Y VULNERABILIDADES
3.1 Clasificación general de amenazas
    3.1.1 De humanos
    3.1.2 Errores de hardware
    3.1.3 Errores de la red
    3.1.4 Problemas de tipo lógico
    3.1.5 Desastres
3.2 Clasificación general de vulnerabilidades
3.3 Clasificación general de amenazas o ataques inherentes a las redes
    3.3.1 Ataques pasivos
    3.3.2 Ataques activos
3.4 Métodos de ataque
    3.4.1 Preparación y planteamiento
    3.4.2 Activación
    3.4.3 Ejecución
    3.4.4 Ataques en escudos

CAPÍTULO 4
SERVICIOS DE SEGURIDAD
4.1 Definición
4.2 Clasificación
- 4.2.1 Confidencialidad
- 4.2.2 Autenticación
- 4.2.3 Integridad
- 4.2.4 No repudio
- 4.2.5 Control de acceso
- 4.2.6 Disponibilidad

CAPÍTULO 5
POLÍTICAS DE SEGURIDAD
5.1 Misión de la organización (sus objetivos)
5.2 Definición de política
- 5.2.1 Principios fundamentales

5.3 Definición de modelos
- 5.3.1 Criterios
- 5.3.2 Modelos de control de acceso
- 5.3.3 Modelos de flujo de información
- 5.3.4 Modelos de integridad

5.4 Identificación y establecimiento de políticas de seguridad

CAPÍTULO 6
ANALISIS DEL RIESGO
6.1 Definiciones
6.2 Tipos de análisis del riesgo
- 6.2.1 Análisis cuantitativo del riesgo
- 6.2.2 Análisis cualitativo del riesgo

6.3 Cómo establecer los requerimientos y riesgos de seguridad
6.4 Pasos del análisis del riesgo
6.5 Consideraciones adicionales durante el análisis del riesgo

CAPÍTULO 7
HERRAMIENTAS DE SEGURIDA
7.1 Introducción
7.2 Principales Herramientas
- ***7.2.1 Monitoreo***
- ***7.2.2 Auditoría***
- ***7.2.3 Criptografía***
- ***7.2.4 Escaneo***
- ***7.2.5 Filtrado***
- ***7.2.6 Detección de Intrusos***
  - ***7.2.1 Tipos de Intrusos***
  - ***7.2.2 Composición de los IDS***

7.2.3 Clasificación de los IDS
7.3 Autenticación

CAPÍTULO 8
AUDITORIA
8.1 Definición
8.2 Auditoría interna y auditoría externa
8.3 Características de la Auditoría informática
8.4 Tipos y clases de auditorías
8.5 Fases de una auditoría
8.6 Auditoría de la seguridad de la información
8.7 Enfoques de la Auditoría Informática
8.8 Herramientas y técnicas para la auditoría informática
8.9 Perfil Profesional del auditor informático

CAPITULO 9
SEGURIDAD EN REDES INALAMBRICAS
1.1 Definición de la seguridad inalámbrica
1.2 Implementación de los atributos de seguridad
1.3 Servicios de seguridad en redes inalámbricas
1.3.1 Confidencialidad
1.3.2 Autenticación
1.3.3 Integridad de datos en redes inalámbricas
1.3.4 Disponibilidad en redes inalámbricas
1.3.5 No repudio (rendición de cuentas)
9.4 Principales amenazas de seguridad en las redes inalámbricas

CAPÍTULO 10
SEGURIDAD EN BASES DE DATOS
10.1 Introducción
10.2 Confidencialidad de la BD
10.2.1 Deducción de información confidencial de una BD
10.3 Disponibilidad de la BD
10.4 Integridad de la BD
10.5 Mecanismo de seguridad en SGBD

CAPITULO ***11***
ÉTICA INFORMÁTICA
11.1 Concepto de ética
11.2 Código deontológico
11.3 Ética profesional
11.3.1 Código de ética profesional del ingeniero mexicano
11.3.2 Código de ética y ejercicio profesional de la ingeniería de software del Institute of Electrical and Electronics Engineer (IEEE)
11.3.3 Código de ética universitario a la comunidad universitaria
11.4 La formación ética

11.5 Contenidos de la ética informática
11.6 Código deontológico
11.7 Objetivos del código deontológico
11.8 Funciones del código deontológico
11.9 Código deontológico de los ingenieros informáticos

*CAPITULO **12***
LEGISLACIÓN Y DELITOS INFORMÁTICOS
12.1 Panorama mundial
    12.1.1 Antecedentes externos
    12.1.2 Ley modelo sobre comercio electrónico
    12.1.3 Comisión de las Naciones Unidas para la ley del comercio internacional
12.2 Contexto nacional
    12.2.1 Reorientación de la política informática
    12.2.2 Normatividad en informática
    12.2.3 Foros de consulta
12.3 Delitos informáticos
12.4 Tipos de delitos informáticos
12.5 Legislación Internacional

GLOSARIO
BIBLIOGRAFÍA

Es imprescindible que los futuros ingenieros conozcan las diferentes metodologías que existen para el análisis de riesgos y así mismo los estándares de la Familia ISO/IEC 27000, ya que les permitirá adquirir una visión más amplia sobre lo importante que se vuelve, principalmente para las organizaciones el hecho de tener como base estos estándares, los cuales se desarrollan a continuación:

6.1 Familia de Normas ISO / IEC 27000

Desde 1901 y como primera entidad de normalización a nivel mundial, BSI (British Standars Institution) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 – ahora ISO 9001
- 1992 Publicación BS 7750 – ahora ISO 14001
- 1996 Publicación BS 8800 – ahora OHSAS (Occupational Healt and Safety Assessment Series) 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa (británica o no) un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7788-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO sin cambios sustanciales como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión, de manera que para el año 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de

Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información. En la Figura 6.1 se puede observar de manera resumida lo antes mencionado.

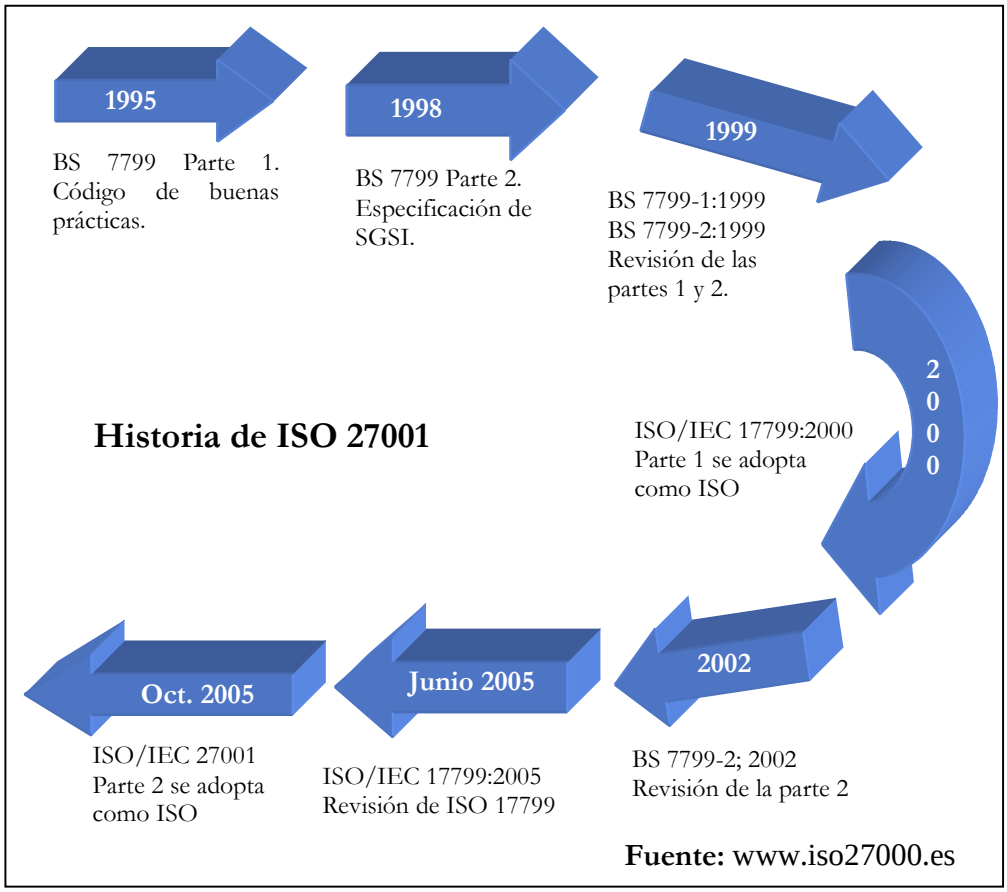

Figura 6.1 Historia de ISO 27001

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), esta serie contiene las mejores prácticas recomendadas para la Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), hasta principios de febrero de 2011 la mayoría de estas normas se encuentran en preparación e incluyen:

a) **ISO/IEC 27000:** Publicada el 1 de Mayo de 2009. Esta norma proporciona una visión general de las normas que componen la serie 27000, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción del proceso Plan-Do-Check-Act y términos y definiciones que se emplean en toda la serie 27000[23].

b) **ISO/IEC 27001:** Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

c) **ISO/IEC 27002**: 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.

d) **ISO/IEC 27003:** Publicada el 1 de Febrero de 2010. No certificable. Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001:2005. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de obtención de aprobación por la dirección para implementar un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

e) **ISO/IEC 27004:** Publicada el 7 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para

[23] http://www.iso27000.es/iso27000.html

determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.

f) **ISO/IEC 27005**: Publicada el 4 de Junio de 2008. No certificable. Proporciona las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

g) **ISO/IEC 27006**: Publicada el 1 de Marzo de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

h) **ISO/IEC 27007**: En fase de desarrollo, consistirá en una guía de auditoria de un SGSI, como complemento a lo especificado en ISO 19011.

i) **ISO/IEC 27008**: En fase de desarrollo. Consistirá en una guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI.

j) **ISO/IEC 27010:** En fase de desarrollo. Es una norma en 2 partes, que consistirá en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.

k) **ISO/IEC 27011**: Publicada el 15 de Diciembre de 2008. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002. Está publicada también como norma ITU-TX.1051. ITU (Unión Internacional de Telecomunicaciones).

l) **ISO/IEC 27012:** En fase de desarrollo. Consistirá en un conjunto de requisitos (complementarios a ISO/IEC 27001) y directrices (complementarias a ISO/IEC

27002) de gestión de seguridad de la información en organizaciones que proporcionen servicios de e-Administración.

m) **ISO/IEC 27013:** En fase de desarrollo. Consistirá en una guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

n) **ISO/IEC 27014:** En fase de desarrollo. Consistirá en una guía de gobierno corporativo de la seguridad de la información.

o) **ISO/IEC 27015:** En fase de desarrollo. Consistirá en una guía de continuidad de SGSI para organizaciones del sector financiero y de seguros.

p) **ISO/IEC 27031**: En fase de desarrollo, consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

q) **ISO/IEC 27032**: En fase de desarrollo, consistirá en una guía relativa a la ciberseguridad.

r) **ISO/IEC 27033:** Norma dedicada a la seguridad de redes, consiste en 7 partes: 27033-1, conceptos generales; 27033-2, directrices de diseño e implementación de seguridad en redes; 27033-3, escenarios de redes de referencia; 27033-4, aseguramiento de las comunicaciones entre redes mediante gateways de seguridad; 27033-5, aseguramiento de comunicaciones mediante VPNs; 27033-6, convergencia IP; 27033-7, redes inalámbricas.

s) **ISO/IEC 27034:** En fase de desarrollo, consistirá en una guía de seguridad en aplicaciones informáticas.

t) **ISO/IEC 27035:** En fase de desarrollo, consistirá en una guía de gestión de incidentes de seguridad informática.

u) **ISO/IEC 27036**: En fase de desarrollo, consistirá en una guía de seguridad en outsourcing (externalización de servicios).

v) **ISO/IEC 27037:** En fase de desarrollo, consistirá en una guía de identificación, recopilación y preservación de las evidencias digitales.

w) **ISO/IEC 27799:** Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO/IEC 27002 y es un complemento de esa norma. ISO 27799:2008

especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, videos e imágenes médicas), sea cual fuere el medio utilizado para almacenar(de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para el transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida.

Beneficios de la familia de normas 27000

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través de medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, entre otros).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

6.2 Metodologías para el análisis de riesgo

En el mundo de la seguridad informática no sólo se disponen de normas de análisis de riesgos, también existen metodologías ampliamente conocidas y de uso generalizado. Las Principales son MAGERIT, EBIOS, CRAMM y OCTAVE, las cuales se detallan a continuación:

MAGERIT: Es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas y fue elaborado por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales (SSITAD), del Consejo Superior de Informática.

Se trata de una metodología para conocer el riesgo al que está sometida una información y qué tan segura (o insegura) está.

Objetivos de MAGERIT:

- **Estudiar los riesgos** que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un **análisis de los riesgos** que implica la evaluación del *impacto* que una violación de la seguridad tiene en la organización; señala los *riesgos* existentes, identificando las *amenazas* que acechan al sistema de información y determina la *vulnerabilidad* del sistema de prevención de dichas amenazas, obteniendo unos resultados.

- Los resultados del análisis de riesgos permiten a la ***gestión de riesgos*** **recomendar las medidas** apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.
- Como **objetivo a más largo plazo,** MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información (ITSEC, Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información).

La Aplicación de MAGERIT permite:

- *Aportar racionalidad en el conocimiento del estado de seguridad* de los Sistemas de Información y en la introducción de medidas de seguridad.
- *Ayudar a garantizar una adecuada cobertura en extensión*, de forma que no haya elementos del sistema de información que queden fuera del análisis, y *en intensidad*, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- *La incrustación de mecanismos de seguridad en el corazón mismo de los sistemas de información:*
  a) Para paliar las insuficiencias de los sistemas vigentes.
  b) Para asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento.

El análisis y Gestión de Riesgos es el "corazón" de toda actuación organizada en materia de seguridad y de la gestión global de la seguridad. Influye en las Fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la oportunidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento). Así cómo se muestra en la figura 6.2.

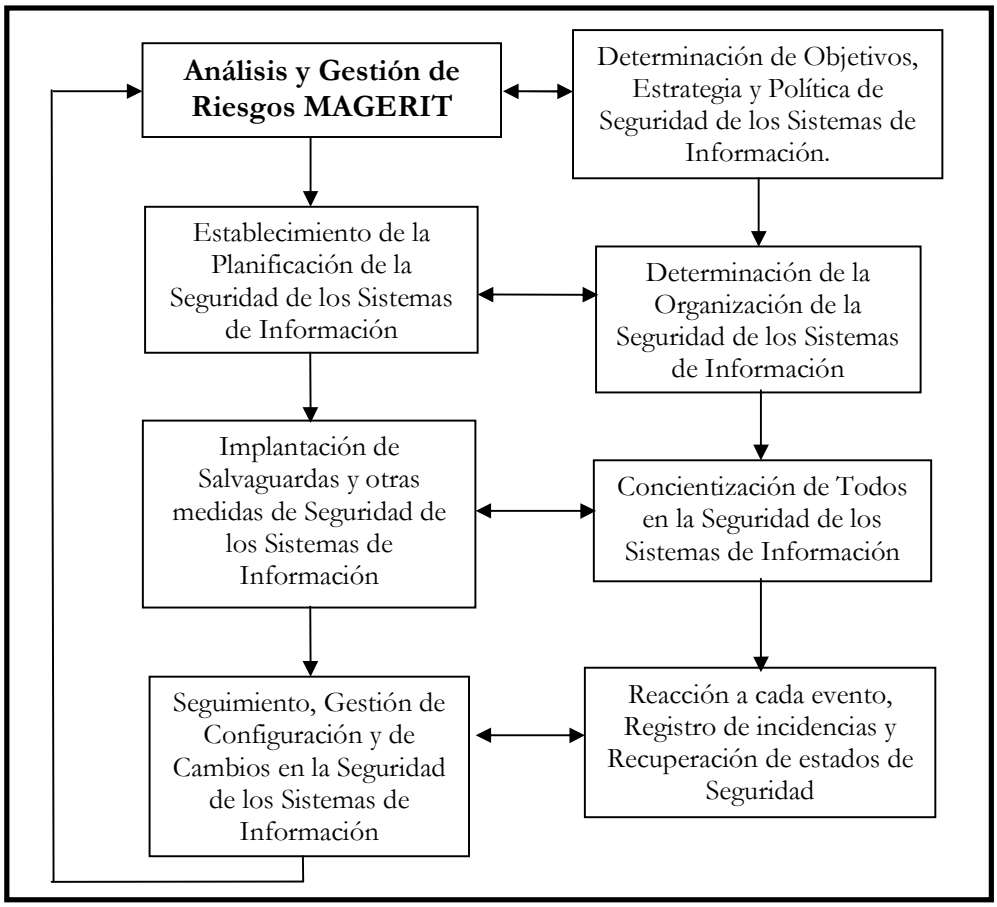

Figura 6.2 Análisis y Gestión de Riesgos de MAGERIT

Tipos de proyectos

MAGERIT responde a las necesidades de un amplio espectro de intereses de usuarios con un enfoque amplio de adaptación a cada organización y a sensibilidades diferentes en Seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:

- **Situación:** dentro del "ciclo de estudio"; marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos, determinación de mecanismos específicos de salvaguarda.
- **Envergadura:** complejidad e incertidumbre relativas del dominio estudiado, tipo de estudio más adecuado a la situación (corto, simplificado, entre otros), granularidad adoptada.

- **Problemas específicos que se deseen solventar:** Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos, Auditorías de seguridad.

Estructura de MAGERIT: El modelo normativo de MAGERIT se apoya en tres submodelos (así como se muestra en la figura 6.3):

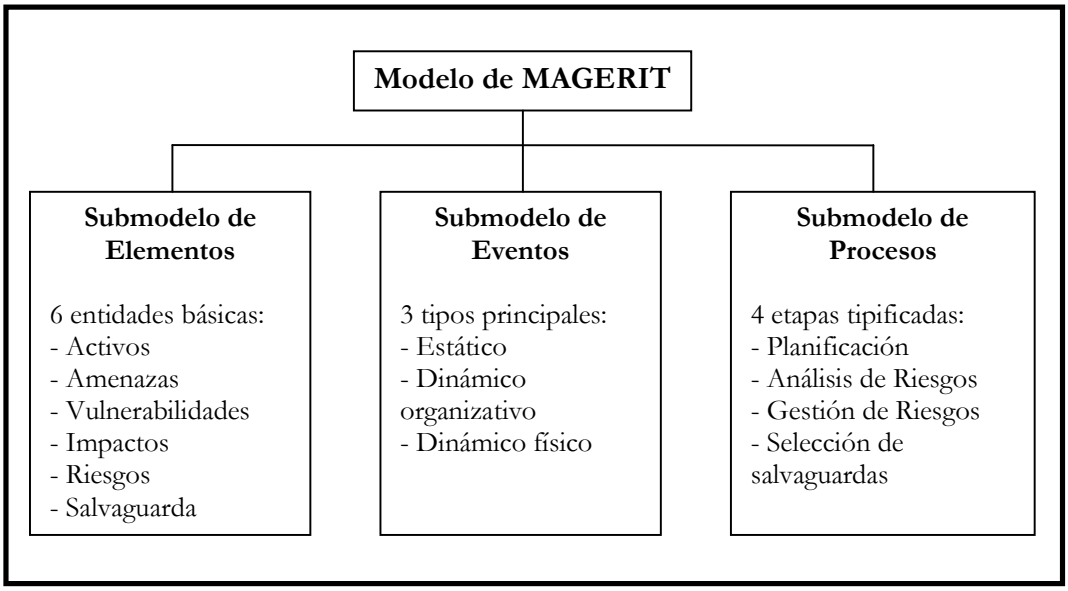

Figura 6.3 Modelo MAGERIT

El *Submodelo de Elementos* proporciona los "componentes" que el *Submodelo de Eventos* va a relacionar entre sí y con el tiempo, mientras que el *Submodelo de Procesos* será la descripción funcional ("el esquema explicativo") del proyecto de seguridad a construir.

El submodelo de procesos de MAGERIT comprende 4 etapas (así como se muestra en la figura 6.4):

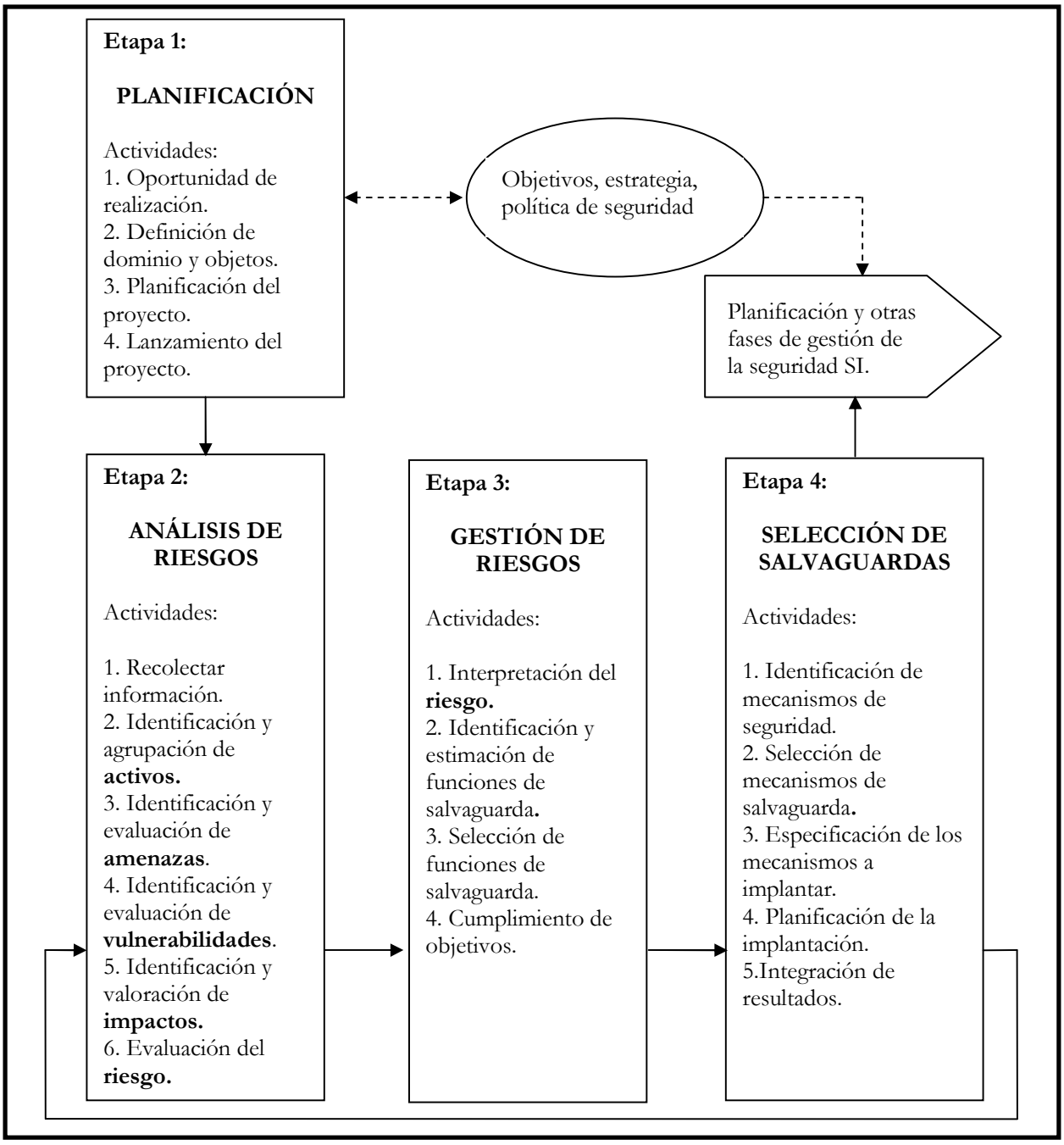

Figura 6.4 Etapas del Submodelo de procesos MAGERIT

1. **Planificación del Proyecto de Riesgos:** Como consideraciones iniciales para arrancar el proyecto de Análisis y Gestión de Riesgos (AGR), se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.
2. **Análisis de riesgos:** Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.
3. **Gestión de riesgos:** Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.
4. **Selección de salvaguardas:** Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del Análisis y Gestión de Riesgos (AGR), para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

Para lograr construir proyectos específicos de seguridad, MAGERIT posee interfaces de enlace con METRICA v2.1. MAGERIT permite añadir durante el desarrollo del sistema, la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento.
Estas interfaces tienen ventajas inmediatas, cómo: analizar la seguridad del sistema antes de su desarrollo así como la incorporación de defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

Tipos de Técnicas usadas en MAGERIT

Cada una de las tareas del Submodelo de Procesos en la Guía de Procedimientos indica las técnicas empleadas para realizarla. MAGERIT tipifica las técnicas recomendadas como: Técnicas Comunes con METRICA v2.1 y con EUROMÉTOCO – Técnicas características

de MAGERIT, tales como matriciales, algorítmicas y de lógica difusa – Técnicas Complementarias.

MAGERIT consta de 7 guías:

1. **Guía de Aproximación:** Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por personal no especialista y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.
2. **Guía de Procedimientos:** Representa el núcleo del método que se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente, puesto que basta su contenido para comprender la terminología para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información.
3. **Guía de Técnicas:** Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.
4. **Guía para Responsables del Dominio Protegible:** Explica la participación de los directivos "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.
5. **Guía para Desarrolladores de Aplicaciones:** Está diseñada para ser utilizada por los desarrolladores de aplicaciones y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica v2.1
6. **Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos:** La interfaz para intercambio de datos posibilita que un usuario de MAGERIT establezca la comunicación con otras aplicaciones y sistemas facilitando la incorporación de sus productos a la herramienta MAGERIT y viceversa.
7. **Referencia de Normas legales y técnicas:** Lista de normas en materia de seguridad.

EBIOS (Expresision des Besoins et Identification des Objectifs de Sécurité - Expresión de las necesidades e identificación de los objetivos de seguridad): El método EBIOS es una herramienta de gestión de riesgos para los sistemas de seguridad informática, fue creada por la Dirección Central de Seguridad de los Sistemas de Información de Francia DCSSI.

El método EBIOS permite tratar los riesgos relativos a la seguridad de los sistemas de información (SSI), facilita la comunicación dentro y fuera del organismo para contribuir al proceso de la gestión de los riesgos SSI y ayuda a la toma de decisiones.
Este método toma en cuenta todas las entidades técnicas (software, hardware, redes) y no técnicas (organización, aspectos humanos, seguridad física).

Las características de EBIOS son:

- Es compatible con normalizaciones internacionales.
- Es utilizado para estudiar tanto sistemas por diseñar como sistemas ya existentes.
- Presenta y describe los tipos de entidades, métodos de ataque, vulnerabilidades, objetivos de seguridad y requerimientos de seguridad.

Los pasos del método EBIOS son:

1. **Estudio del contexto:** Durante este proceso se realiza un análisis de los activos de la organización, estos pueden ser distintos tipos como: hardware, software, redes, personal, entre otros.
2. **Expresión de las necesidades de seguridad:** En este proceso se realiza un estudio de las necesidades de seguridad para los activos determinados en el paso anterior.
3. **Estudio de las amenazas:** Al considerar que cada organismo se encuentra expuesto a diversos peligros, es importante realizar un estudio de las amenazas y vulnerabilidades a las que se encuentra expuesta la organización.
4. **Expresión de los objetivos de seguridad:** Este proceso consiste principalmente en cubrir las vulnerabilidades a las que la entidad se encuentra expuesta, es decir disminuir los riesgos.

5. **Determinar los requerimientos de seguridad:** Durante este proceso el equipo encargado del desarrollo del sistema de seguridad informática será el responsable de determinar las funcionalidades de seguridad esperadas, así como también el cumplimiento de los objetivos de seguridad.

CRAMM (Risk Analysis and Method Management): Es una metodología de análisis de riesgos desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA). Comenzó a desarrollarse en la década de 1980. En la figura 6.5 se muestra el modelo de análisis y gestión de riesgos de CRAMM el cual consiste en:

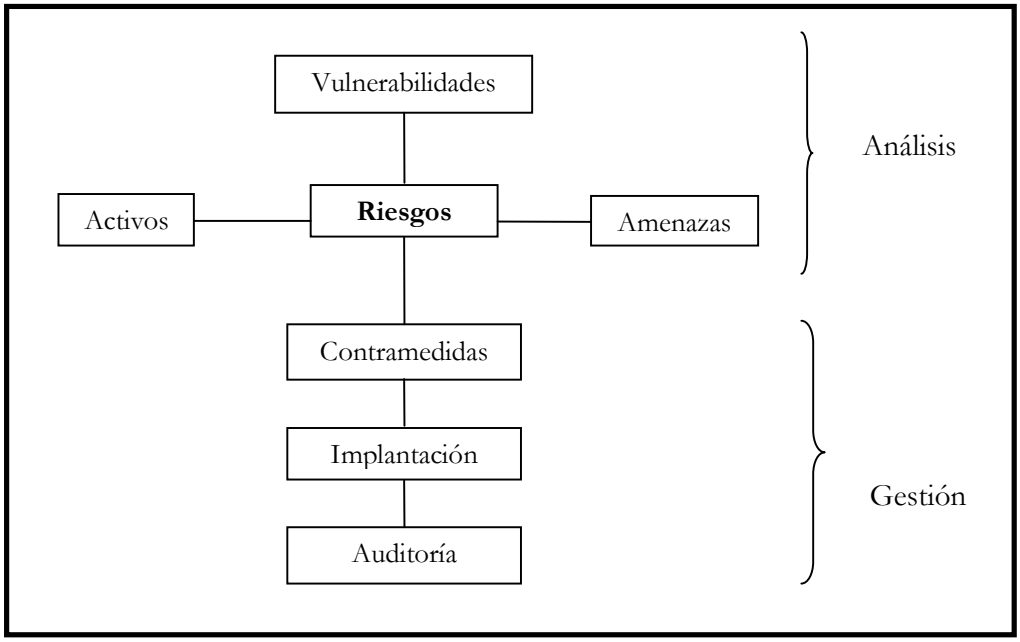

Figura 6.5 Modelo de análisis y gestión de riesgos de CRAMM

Uno de los aspectos principales de CRAMM es el soporte que proporciona la herramienta informática con una base de datos de:

- Más de 400 tipos de activos
- Más de 25 tipos de impacto
- 38 tipos de amenaza
- 7 tipos de medida del riesgo
- Más de 3,500 salvaguardas

CRAMM soporta 3 tipos de revisiones:

- CRAMM Express
- CRAMM Expert
- BS7799

Adicionalmente existen variantes para la gestión de riesgos en proyectos de desarrollo, con una interfaz al ciclo de vida estándar utilizado por la Administración Pública británica: SSADM (Structured System Analysis and Design Method).
La metodología CRAMM define tres fases para la realización del análisis de riesgos.

Fase 1: Establecimiento de objetivos de seguridad

Esta fase consiste en llevar a cabo los siguientes aspectos.

- Definir el alcance del estudio.
- Definir el valor de la información entrevistando a los usuarios sobre los impactos potenciales para el negocio que podrían producirse por la indisponibilidad, destrucción, divulgación o modificación.
- Identificar y evaluar los activos físicos que forman parte del sistema.
- Identificar y evaluar los activos de software que forman parte del sistema.

Fase 2: Análisis de riesgos

Consta de:

- Identificar y valorar el tipo de nivel de las amenazas que pueden afectar al sistema.
- Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas.
- Combinar las valoraciones de amenazas y vulnerabilidades para calcular la medida de los riesgos.

Fase 3: Identificación y selección de salvaguardas

Los principales productos de la metodología CRAMM son:

- Documento de inicio del proyecto.
- Informes de análisis de riesgos.

- Informes de gestión de riesgos, cimentados en una base de datos de más de 3,500 salvaguardas técnicas y organizativas.
- Plan de implantación.

Las principales actividades del proceso de análisis y gestión de riesgos CRAMM se resumen en la siguiente figura (6.6):

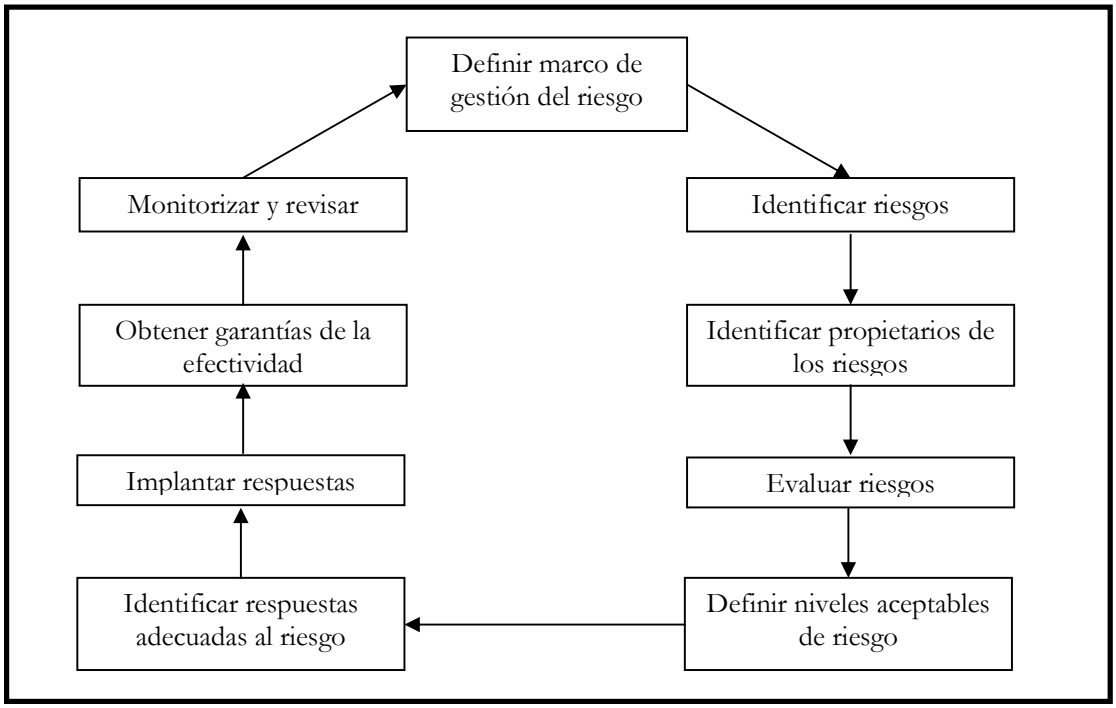

Figura 6.6 Principales actividades de análisis y gestión de riesgos de CRAMM

OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability Evaluation*)**:** Es una técnica efectiva de evaluación de riesgos creada por la oficina de patentes y negocios de los Estados Unidos.

OCTAVE es una técnica de planificación y consultoría estratégica en seguridad basada en el riesgo, esta técnica está en contra de la consultoría enfocada en el campo tecnológico, que tiene como objetivo los riesgos tecnológicos y en los temas tácticos, OCTAVE se

enfoca en el riesgo organizacional y su objetivo principal son los temas relativos a la estrategia y a la práctica.

OCTAVE equilibra los siguientes aspectos:

- Riesgos operativos
- Prácticas de seguridad
- Tecnología

Lo cual permite a las compañías tomar decisiones de protección de información en los riesgos de confidencialidad, integridad y disponibilidad de los bienes relacionados a la información crítica.

Características:

- Es diferente de los análisis tradicionales enfocados a la tecnología
- Es autodirigido
- Flexible

Los objetivos de OCTAVE son:

- Permitir la comprensión del manejo de los recursos
- Identificación y evaluación de los riesgos que afectan la seguridad dentro de una organización.
- Exige llevar la evaluación de la organización y del personal de la tecnología de información.

Este método se enfoca en tres fases para examinar los problemas organizacionales y tecnológicos, los cuales son:

Fase I: Durante esta fase se identifica la información de la organización. Los procesos que se realiza en esta fase son:

- Establecer criterios de evaluación de impacto
- Identificar sus criterios de seguridad
- Identificar sus amenazas
- Analizar los procesos tecnológicos relacionados

Fase II: En esta fase se examina la infraestructura tecnológica y se realizan los siguientes procesos:

- Examinar rutas de acceso
- Analizar procesos tecnológicos

Fase III: Durante esta fase se realiza la identificación de los riesgos, así como también se realizan estrategias de mitigación y planes de protección. Los procesos que intervienen en esta fase son:

- Evaluar el impacto de las amenazas
- Evaluar la probabilidad de ocurrencia de amenazas
- Seleccionar formas de mitigación de riesgos
- Desarrollar planes de mitigación de riesgos

6.3 Herramientas de Seguridad

Las herramientas de seguridad informática son una parte fundamental para el desarrollo de cualquier sistema de seguridad de redes de computadoras, por ello es muy importante conocer los tipos de herramientas tanto de software como de hardware existentes y a su vez clasificarlos acorde a las necesidades de cada usuario. Si bien es cierto que a lo largo del tiempo, se han desarrollado diversas aplicaciones cuyo objetivo es prevenir y mitigar los posibles ataques a los que se están expuestos todos los días, desafortunadamente existen personas que desafían a las herramientas, logrando burlar la seguridad y cumplir sus objetivos. Por este y otros motivos se debe de procurar estar actualizados ante los nuevos avances tecnológicos y una forma para ayudar a lograrlo es incluir en el capítulo 7 titulado Herramientas de Seguridad los siguientes temas (**Monitoreo, Paswords, Auditoría, Criptografía, Código Malicioso, Escaneo, Filtrado, Detección de Intrusos y Autenticación),** los cuales se desarrollan a continuación:

6.3.1 Monitoreo

El término monitoreo de red describe el uso de un sistema que constantemente monitorea una red de computadoras para detectar sistemas lentos o en mal funcionamiento y que notifica al administrador de la red en caso de falla vía correo electrónico, beeper u otras alarmas. Sirven para el control sobre algunos eventos que van sucediendo en un sistema de computación, que puede ser desde un sistema aislado, hasta una red de computadoras muy compleja. Su principal objetivo es analizar los eventos conforme suceden a fin de detectar condiciones anómalas o indeseadas y generar las alarmas correspondientes.

Los aplicativos de monitoreo del estado de red permiten:

- **Revisar los signos vitales de la red en tiempo real:** Mientras un sistema de detección de intrusos monitorea una red de amenazas del exterior, un sistema de monitoreo de red vigila la actividad en la red en busca de problemas debidos a servidores, conexiones de red u otros dispositivos sobrecargados y/o fuera de servicio para informar al administrador de la red.

Existe un gran número de herramientas de monitoreo en el mercado y éstas se pueden dividir en dos tipos:

A. Herramientas de control y seguimiento de accesos: Estas herramientas permiten obtener información (mediante ficheros de trazas) de todos los intentos de conexión que se produzcan en el sistema o sobre otro que se indiquen, así como intentos de ataque de forma sistemática a puertos tanto de TCP como de UDP.

Este tipo de herramientas permiten tener control sobre todos los paquetes que entran por la interfaz de red de la máquina: IP (TCP, UDP) e ICMP, o analizando paquetes a nivel de aplicaciones como:

- **Telnet:** Abre una sesión en una máquina remota.
- **FTP:** Transfiere archivos desde una máquina remota.
- **SMTP (Simple Mail Transfer Protocol):** Utilizado para enviar y recibir correo electrónico.

Estas herramientas pueden ser utilizadas junto con otras que permitan definir desde qué máquinas se permiten ciertas conexiones y de cuáles se prohíben.

Algunas de éstas pueden tener un doble uso, es decir, ofrecer protección ante posibles ataques, pero también podrían ser utilizadas para intentar comprometer sistemas. Por eso es importante que el uso de estas herramientas esté restringido de manera que el personal no autorizado no pueda utilizarlas de forma aleatoria y se oculte realmente un ataque. También podrán ser utilizadas para hacer seguimientos en la red cuando se sospeche que alguna de las máquinas en la red ha sido comprometida.

Sin embargo, estas herramientas son muy inseguras ya que a su paso por Internet existen programas que pueden identificar todo el flujo de información de manera textual desde una máquina hacia otra incluyendo el nombre y la contraseña del usuario. Para evitarlo, se crearon las siguientes herramientas:

- **Achilles:** Es una herramienta designada parar comprobar la seguridad de aplicaciones web. Achilles es un servidor Proxy que actúa como una persona en el medio (main in the middle) durante una sesión de http. Un Proxy de http típico para paquetes hacia y desde el explorador de web cliente y un servidor de web. Esta herramienta intercepta los datos en una sesión de http en cualquier dirección y le da al usuario la habilidad de alterar datos antes de ser transmitidos.
- **AirSnort:** Herramienta de crackeo del cifrado WEP de 802.11. Es una herramienta para LANs inalámbricas (WLAN) que recupera las llaves de cifrado. Fue desarrollada por el Shmoo Group y opera monitoreando pasivamente las transmisiones, computando la llave de cifrado cuando suficientes paquetes han sido recolectados.
- **Brutus:** Cracker de autenticación para redes. Este cracker es sólo para Windows, se extiende sobre servicios de red de sistemas remotos tratando de averiguar passwords utilizando un diccionario y permutaciones de éste. Soporta http, POP3, FTP, SMB, TELNET, IMAP, NTP, entre otros.

- **Cain & Abel:** Es una herramienta de recuperación de passwords para los sistemas operativos de Microsoft. Permite una fácil recuperación de varias clases de password, escuchando (sniffing) la red, crackeando los passwords cifrados utilizando ataques por diccionarios, decodificando passwords codificados (scrambled) y revelando cuadros de diálogo del tipo password.
- **Código Malicioso:** Existen herramientas generales que suelen brindar protección en "tiempo real" y otras contra determinado código malicioso (vacunas). También hay herramientas contra Spyware como el Norton Antivirus y Trend, Titanium/Enterprise.
- **DSniff:** Es un juego de herramientas de auditoría y pruebas de penetración de redes. Incluye dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf y webspy que monitorean pasivamente una red en busca de datos (passwords, e-mail, archivos, entre otros.)
- **Ethereal:** Es un analizador de protocolos de red para Unix y Windows. Permite examinar datos de una red viva o de un archivo de captura en algún disco.
- **Ettercap:** Es un interceptor sniffer registrador para LANs con Ethernet basado en terminals. Soporta direcciones activas y pasivas de varios protocolos.
- **Firewall:** software que se instala en una computadora la cual es el intermediario entre la red local (correspondiente a la organización) y la red externa que por lo general es Internet, aunque también pueden existir firewall entre diferentes redes dentro de una organización si así se desea.
- **Firewalk:** Analiza las respuestas a paquetes IP para determinar mapas de redes y filtros de listas de control de acceso (ACL) empleadas por gateways.
- **Fport:** Reporta todos los puertos TCP/IP y UDP abiertos en la máquina en la que se está ejecutando y muestra qué aplicación abrió cada puerto y sus aplicaciones asociadas.
- **GFI LANguard:** Esta herramienta escanea redes y reporta información como el nivel de "service pack" de cada máquina, faltas de parches de seguridad, recursos compartidos, puertos abiertos, servicios / aplicaciones activas en la computadora, datos del registro, passwords débiles, usuarios y grupos; y más.

- **Hping2:** Esta herramienta ensambla y envía paquetes de ICMP/UDP/TCP hechos a medida y muestra la respuesta. Fue inspirado por el comando ping, pero ofrece mucho más control sobre lo enviado.
- **IDS (Intrusion Detection System):** Sistema para detectar intrusiones al sistema[24].
- **ISS Internet Scanner:** Esta herramienta consiste en la evaluación de vulnerabilidades a nivel de Aplicación.
- **John the Ripper:** Su propósito principal es detector passwords.
- **Kismet:** Es un sniffer para redes inalámbricas, detecta bloques de IP automáticamente por medio de paquetes UDP, ARP y DHCP.
- **Kerberos:** es un protocolo de seguridad para realizar servicios de autenticación en la red, usa la criptografía basada en claves secretas para proporcionar la seguridad de las contraseñas en la red, por consiguiente, el cifrado de contraseñas con kerberos ayuda a evitar que los usuarios no autorizados intercepten contraseñas en la red, esto representa un método de seguridad del sistema. Es un proceso en el que diferentes elementos colaboran para conseguir identificar a un cliente que solicita un servicio ante un servidor que lo ofrece; asegura que las contraseñas nunca se envíen de manera clara a través de la red. Un uso correcto de kerberos erradica la amenaza de analizadores de paquetes que interceptan contraseñas en la red. Cada usuario tiene una clave y cada servidor también, por lo tanto, se tiene una base de datos que las contiene a todas. En el caso de ser de un usuario, su clave se deriva de su contraseña y está cifrada, mientras que en el caso del servidor, la clave se genera aleatoriamente. Los servicios de red que requieren autenticación y los usuarios que requieren estos servicios, se deben registrar con kerberos. Como éste conoce todas las claves privadas, puede crear mensajes que convencen a un servidor de que un usuario es realmente quien dice ser y viceversa.
- **NBTScan:** Recolecta información de NetBIOS de redes de Windows.
- **Netcat:** Es una herramienta para Unix que lee y escribe datos a través de conexiones de red usando los protocolos TCP o UDP.

[24] Un intruso es alguien que trata de destruir el sistema desde dentro o darle un mal uso. Por darle un mal uso se entiende desde robar información confidencial hasta usar un correo para enviar correo spam.

- **Netfilter:** Es un filtro de paquetes el cual es implementado en el Kernel de Linux estándar.
- **Network Stumbler:** Es utilizada para encontrar "acces point" inalámbricos abiertos ("wardriving").
- **NGrep:** Busca y muestra paquetes.
- **Nikto:** Es un escáner de web de mayor amplitud. Busca más de 2000 archivos / CGIs potencialmente peligrosos y problemas en más de 200 servidores.
- **Nmap:** Existe para el escaneo de puertos, éste permite a los administradores de sistemas el escaneo de grandes redes para determinar qué servidores se encuentran activos y qué servicios ofrecen.
- **N-Stealth:** Escáner de servidores Web.
- **NTop:** Es un monitor de uso de tráfico de red.
- **OpenSSH (Open secure shell):** Se encarga de cifrar el tráfico incluyendo las contraseñas, para eliminar de un modo efectivo el espionaje, los secuestros de las conexiones y otros ataques a nivel de red, de tal manera que permite realizar la comunicación y transferencia de información de forma cifrada pues proporciona fuerte autenticación sobre un medio inseguro. OpenSSH ofrece amplias posibilidades para la creación de túneles seguros, aparte de una variedad de métodos de autenticación.
- **Parches (patch):** Es conveniente su colocación en el sistema, ya que diariamente surgen nuevos ataques a través de agujeros no protegidos por el sistema y al poner estos parches se pueden contrarrestar las posibles incursiones de los atacantes informáticos además de que éstos permiten actualizar y mejorar la operatividad del sistema.
- **Passwords:** Se utilizan para mejorar el tratamiento de los passwords, brindando un mayor grado de seguridad a los recursos de los usuarios. Una posible clasificación es la siguiente:
    - **De Crackeo:** Ayuda a la detección de passwords débiles.
    - **Generadores:** Ayudan a obtener passwords buenos. Se basan en distintos algoritmos.
    - **Ocultamiento:** Ayuda a esconder los archivos de passwords del sistema.

- **PEM (Privacy Enhaced Mail):** Da soporte a la criptografía, autenticación e integridad de mensajes de correo electrónico ya que permite cifrar de manera automática los mensajes antes de enviarlos. PEM realiza las siguientes funciones:
    - Especifica los formatos de mensajes para pedir y revocar certificados.
    - Especifica la jerarquía de las autoridades certificadoras (AC).
    - Especifica la jerarquía de los algoritmos de criptografía.
- **Portsentry:** Programa que cuenta con un archivo de los puertos más vulnerables del sistema, también se pueden agregar a esa lista otros que no se consideran pertinentes para la seguridad del sistema, esta herramienta identifica si alguien quiere entrar por alguno de esos puertos impidiéndole la entrada.
- **SAINT (Security Administrator's Integrated Network Tool):** Herramienta de red integrada para el administrador de seguridad. Funciona únicamente sobre UNIX.
- **Sam Spade:** Herramienta de consulta de redes.
- **SARA:** Asistente de Investigación para El Auditor de Seguridad (Security Auditor's Researchs Asistant). Es una herramienta de evaluación de vulnerabilidades.
- **Sniffer:** Herramienta para la revisión de una red, se puede observar en forma clara conexiones no encriptadas, también permite verificar varios servicios como el correo por su puerto 25, la web por su puerto 80 y todos los servicios que se desean revisar en cada momento.
- **Snort:** Es un sistema de detección de intrusos de red capaz de realizar análisis de tráfico en tiempo real y registro de paquetes en redes con IP.
- **SSL (Secure socket layer):** Sistema de protocolos de carácter general diseñado en 1994 por la empresa Netscape Communications Corporation, está basado en la aplicación conjunta de criptografía simétrica, criptografía asimétrica, certificados digitales y firmas digitales para conseguir un canal o medio seguro de comunicación a través de Internet, es idóneo para transferir información personal o relacionada con transacciones financieras a través de Internet de forma segura y privada. SSL implementa un protocolo de negociación para establecer una comunicación segura a nivel de socket, de forma transparente al usuario y a las aplicaciones que lo usan. Actualmente es el estándar de comunicación segura en los navegadores más importantes como Netscape Navigator e Internet Explorer.

- **SuperScan:** Es un escáner de puertos de TCP. Puede manejar escaneos por ping y escaneo de puertos utilizando rangos de IP específicos.
- **THC-Amap:** Es un escáner de identificación de aplicaciones y servicios.
- **Tripwire:** Monitor de la integridad de los archivos, esta herramienta rastrea cambios en los permisos de los archivos y ligas, tamaños en archivos, tamaños en directorios y cambios en los identificadores de grupos (groupid) y usuarios (userid).
- **TCPDump / WinDump:** Es un analizador de paquetes de red basado en texto. Puede ser utilizado para mostrar los encabezados de los paquetes en un interfaz de red que concuerden con cierta expresión de búsqueda. Se puede utilizar para rastrear problemas en la red o para monitorear actividades de la misma.
- **Whisker/Libwhiske:** Whisker es un escáner que permite poner a prueba servidores de HTTP con respecto a varios agujeros de seguridad conocidos, particularmente, la presencia de peligrosos scrips que utilicen CGI.
- **Windows Privacy Tools (Herramientas de privacidad para Windows):** Colección de aplicaciones multilingües para facilitar el cifrado de contenidos –como el correo electrónico–, la firma digital y la gestión de claves. Se basa en GnuPG, que es compatible con aplicaciones que soportan OpenPGP (como PGP) y además es gratis para uso comercial y personal, bajo la licencia GPL.
- **XProbe2:** Herramienta que sirve para determinar el sistema operativos de un host remoto.

B. Herramientas que verifican la integridad del sistema

Estas herramientas ayudan a proteger el sistema. Algunas se basan en el chequeo a los ficheros y otras alertan de posibles modificaciones de ficheros y de programas “sospechosos” que puedan estar ejecutándose en la máquina de manera oculta, algunas de estas herramientas son:

- **Crack:** Es una herramienta que consiste únicamente en crackear passwords.
- **Chklastlog:** Software para detectar modificaciones en el archivo de log para Unix.
- **Chkwtmp:** Software para detectar modificaciones en el archivo wtmp de Unix.

- **Cmp (Check Promiscuous Mode):** Este programa se encarga de revisar la interfaz de red de la máquina descubriendo si está siendo utilizada en modo promiscuo (escuchando todo el tráfico de la red).
- **COPS (Computer Oracle and Password System):** Esta herramienta se encarga de revisar las posibles vulnerabilidades y agujeros de seguridad existentes.
- **Ifstatus:** Es una herramienta que facilita de forma gráfica y en tiempo real, lo que está haciendo la tarjeta de real.
- **LSOF (List Open Files):** Es una herramienta de diagnostico específica de UNIX, la cual lista la información acerca de cualquier archivo abierto por procesos que estén actualmente ejecutándose en el sistema. También puede listar sockets de comunicaciones abiertos por cada proceso.
- **Noshell:** Este software permite al administrador obtener información adiciona sobre intentos de conexión a cuentas canceladas en una máquina.
- **Osh (Operator Shell):** Este software es de dominio público, es una shell restringida que permite indicar al administrador mediante un archivo de datos qué comandos puede ejecutar cada usuario.
- **Spar:** Software de dominio público diseñado por CSTC (Computer Security Technology Center) que realiza una auditoría de los procesos del sistema, mucho más flexible y potente que el comando lastcomm de UNIX.
- **Tiger:** Es un software que está conformado por un conjunto de shell scripts y código C que chequean el sistema para detectar problemas de seguridad de forma parecida a COPS.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **SolarWinds:** Ayuda a empresas de cualquier tamaño a monitorizar y gestionar sus redes corporativas con una eficiencia en costos, con productos fáciles de usar, rápidos de implementar y muy efectivos. (www.solarwinds.net)
- **Iris:** El servicio de seguridad de RedIRIS tiene como finalidad la detección de problemas que afecten a la seguridad de las redes de centros de redIRIS, así

como la actuación coordinada con dichos centros para poner solución a estos problemas. También se realiza labor preventiva, avisando con tiempo de problemas potenciales, ofreciendo asesoramiento a los centros, organizando actividades de acuerdo con los mismos y ofreciendo servicios complementarios. www.eeye.com

- **Ethereal:** Es una potente herramienta que incluye todas las funciones necesarias para ejecutar análisis exhaustivos de protocolos en redes Ethernet. www.ethereal.com
- **MS Operations Manager:** Es una herramienta de monitoreo que permite la administración de manera eficaz y eficiente de las alarmas y eventos que se realizan en un sistema que se esté controlando, presentando una interfaz de usuario muy amigable, integrándose apropiadamente con el Directorio Activo y permite fusionarse adecuadamente con otras herramientas de administración y monitoreo de otros fabricantes. www.microfosft.com
- **Core Wisdom:** Es un conjunto de herramientas diseñadas para facilitar la auditoría segura de sistemas informáticos. Esta solución centraliza y garantiza la integridad de la información del sistema y optimiza la auditoría, procesando y representando la información en diferentes modos gráficos. La suite posibilita en análisis sobre información histórica al mismo tiempo que reproduce los eventos en tiempo real, permitiendo alta disponibilidad de los sistemas. http://www1.corest.com/

6.3.2 Auditoría

La utilización de herramientas de auditoría permite la detección de puntos débiles en el sistema, así como el seguimiento de determinadas actividades y/o de usuarios. Así mismo, brinda un panorama acerca del perfil de funcionamiento del sistema en condiciones normales.

Así, este tipo de herramientas sirven para verificar en diferido el funcionamiento normal de un sistema o la ocurrencia de determinados hechos basándose en información recolectada con tales fines. Las más comunes son aquellas que hacen el análisis de los archivos de logs, tanto del sistema operativo como de aplicaciones específicas.

Existen otras herramientas, tales como los antivirus, que proveen sus propias funcionalidades de auditoría. En ocasiones, el resultado producido por las herramientas de auditoría sirve como entrada a otros sistemas de protección, como es el caso de los IDS y de los escaneadores de vulnerabilidades.

Algunas de las herramientas más comunes son:

- **Bastille:** Un script de fortalecimiento de seguridad Para Linux, MacOS X, y HP-UX.
- **Cheops / cheops-ng:** Nos provee de una interfaz simple a muchas utilidades de red, mapea redes locales o remotas e identifica los sistemas operativos de las máquinas.
- **Crack / Cracklib:** El clásico cracker de passwords locales de Alec Muffett.
- **Dig:** Una útil herramienta de consulta de DNS que viene de la mano con Bind.
- **Etherape:** Monitor de red gráfico para Unix basado en etherman.
- **Fping:** Programa para el escaneo con ping en paralelo.
- **IpTraf:** Software para el monitoreo de redes de IP.
- **LibNet:** Es una API (toolkit) de alto nivel permitiendo al programador de aplicaciones construir e inyectar paquetes de red.
- **OpenBSD:** El sistema operativo preventivamente seguro.
- **Shadow Security Scanner:** Una herramienta de evaluación de seguridad no libre
- **Tcpreplay:** Herramienta para reproducir (replay) archivos guardados con tcpdump o con snoop a velocidades arbitrarias.
- **TCPTraceroute:** Es una implementación de traceroute que utiliza paquetes de TCP.

- **Tcp wrappers:** Su función radica en que autentica las redes, es decir, reconoce que la Ip de una red en realidad pertenece a dicha red. Esto se debe a que alguien que sabe la aceptación de una Ip para ingresar a un sistema, puede poner en una red inventada esa Ip –a esto se le llama spoofing– y así ingresar a cierto sistema.
- **pwdump3:** Permite recuperar las hashes de passwords de Windows localmente o a través de la red aunque syskey no esté habilitado.
- **The Coroner's Toolkit (TCT):** Colección de herramientas orientadas tanto a la recolección como al análisis de información forense en un sistema Unix.
- **Visual Route:** Obtiene información de traceroute/whois y la grafica sobre un mapa del mundo.
- **Winfingerprint:** Escáner de enumeración de Hosts/Redes para Win32.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **BindView:** Es una herramienta que ofrece el acceso y análisis de los datos fundamentales para el administrador de la red de forma sencilla y gráfico desde un único interface. www.bindview.com
- **DumpSec:** Es un programa de auditorías de seguridad para Microsoft Windows NT/XP/200X. vuelca los permisos (DACL –Lista de control de acceso direccional-) y la configuración de auditoría (SACL –Auditoría de acceso a objetos-) para el sistema de archivo, registro, impresoras y recursos compartidos en un formato conciso, legible, de modo que los agujeros en la seguridad del sistema son evidentes. www.somasoft.com

6.3.3 Criptografía

Las herramientas criptográficas son usadas en diferentes ambientes o partes de los sistemas como:

- Contraseñas
- File System

- Canales de comunicación
- Correo electrónico
- PKI

En general soportan varios algoritmos de cifrado.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **GNUPG**: Programa de encriptación que ayuda a proteger la información de curiosos y otros riesgos.
- **PGP (Pretty Good Privacy):** Aplicación ampliamente utilizada en todo el mundo, sobre todo por usuarios particulares, ya que se trata de un programa de cifrado de datos que incluye múltiples funciones de seguridad adicionales y de gestión de claves, permite intercambiar archivos y mensajes con seguridad y comodidad. Está basado en un conjunto de comandos muy sencillos y en la criptografía de clave pública. PGP puede utilizarse para firmar un mensaje, como un certificado de autenticidad y para enviar archivos a través de correo electrónico codificados en formato ASCII, esto proporciona servicios de autenticación y confidencialidad, tanto para el correo electrónico como para el almacenamiento de archivos. (www.pgp.com)
- **Steganos:** Herramienta diseñada para proteger la computadora de los diferentes códigos maliciosos que atacan desde Internet. (www.steganos.com)
- **Tripwire:** Esta herramienta se utiliza para comprobar la integridad de archivos y directorios. Ayuda a administradores y usuarios de sistemas monitoreando alguna posible modificación en algún set de archivos. Si se usa regularmente en los archivos de sistema, tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, para que se puedan tomar medidas de control de daños a tiempo. (www.tripwire.org)

6.3.4 Escaneo

Estas herramientas basan su funcionamiento en realizar un "recorrido" a través de un conjunto de host (un rango de direcciones IP, un dominio, entre otros.) para revisar sus estatus de seguridad. En este barrido, interrogan a cada host respecto a cómo está preparado ante las vulnerabilidades conocidas.

Un tipo de herramienta muy utilizada por los administradores de redes es el escáner de puertos, éste se encarga de revisar e identificar cuáles puertos están abiertos en un host para detectar los servicios que están disponibles.

Algunos productos son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **GFILanguard:** Es un escáner de red y de seguridad. Escanea la red y puertos para detectar, evaluar y corregir vulnerabilidades de seguridad con mínimo esfuerzo administrativo.(www.gfi.com)
- **Nessus:** Herramienta de evaluación de seguridad "Open Source" → de mayor renombre. Nessus es un escáner de seguridad remoto para Linux, BSD, Solaris y otros Unix. Está basado en plug-in(s), tiene una interfaz basada en GTK y realiza más de 1200 pruebas de seguridad remotas. Permite generar reportes en HTML, XML, LaTeX y texto ASCII; también sugiere soluciones para los problemas de seguridad. (www.nessus.org)
- **Retina:** Su función es escanear todos los host en una red y reportar cualquier vulnerabilidad encontrada.(www.eeye.com)

6.3.5 Filtrado

Son herramientas que funcionan bajo reglas para permitir o denegar tráfico de acuerdo a criterios tal como direcciones IP, puertos y protocolos entre otros.

La mayoría de estas herramientas funcionan de modo automático a partir de las reglas configuradas, pero también existen otras de funcionamiento manual, las cuales ante determinadas alertas y con base en las políticas de seguridad de la organización hacen que el administrador decida si deja pasar o no, cierta conexión. Las herramientas más comunes son los firewalls.

Firewall

Entre las comunicaciones que pueden protegerse mediante un firewall están las que se muestran en la figura 6.7.

1

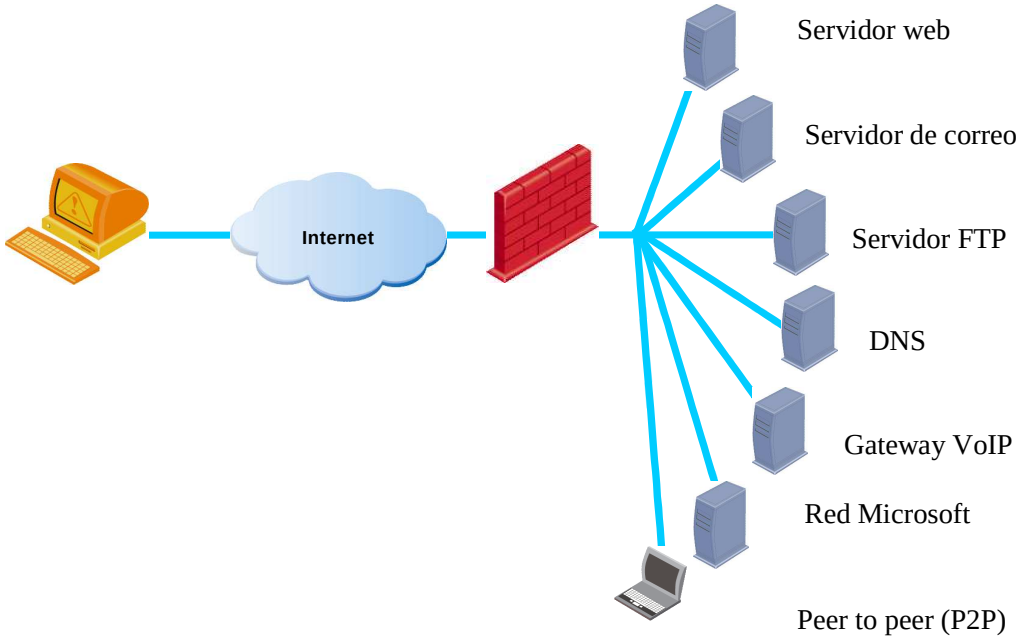

Figura 6.7 Esquema de protección mediante un firewall

Los firewalls funcionan bajo alguna de las dos siguientes filosofías:

- Dejar pasar a todas las redes exceptuando a las que no se desea.
- Negar el acceso a todas las redes y sólo permitir a las que se desea.

La selección de la filosofía también depende directamente de las necesidades identificadas y de las políticas que al respecto (control de acceso) se hayan escrito.
En la máquina donde se instale el firewall sólo debe existir ese software activo y no usarla para otras aplicaciones, ya que el firewall sólo es el puente de comunicación entre las redes local y externa y no debe haber otro trabajo realizándose ni ninguna otra información guardada, ya que en caso de que llegara a ser accedida por alguna persona no autorizada, sólo podría dañar al firewall, el cual no contiene información importante de la organización y podría reponerse de inmediato tapando el agujero por donde se infiltró el perpetrador.

Un Firewall o cortafuegos es una combinación de elementos de hardware y software que se ubica principalmente entre dos redes, tal como una red interna y un ISP (Internet Service Provider) así cómo se muestra en la figura 6.8.

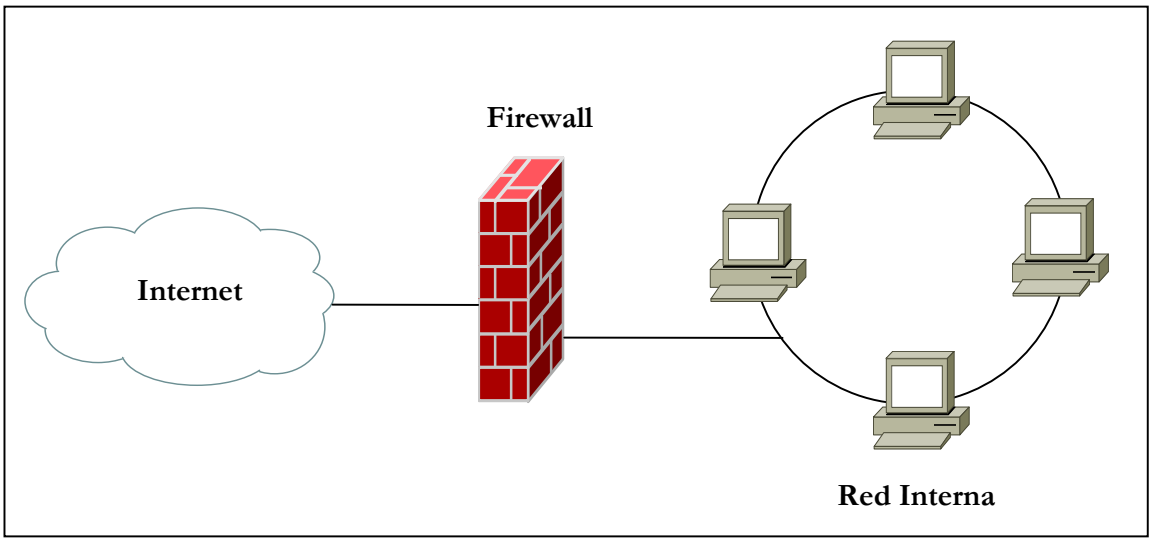

Figura 6.8 Firewall

Sin embargo es necesario hacer notar que también se puede ubicar dentro de una misma red para separar segmentos restringidos donde se procesa o se ubican los servidores con la información sensible de la organización.

El Objetivo del firewall es proteger a la red interna, evitando que usuarios externos no autorizados tengan acceso a la red. También se puede usar para que los usuarios internos no envíen tráfico destinado a determinados receptores fuera de la red.

Para que un firewall sea eficiente se deben garantizar los siguientes aspectos:

- Que todo el tráfico entrante y saliente pase a través de él.
- Que deje pasar sólo el tráfico autorizado por la política de seguridad (se implementa mediante reglas).
- Que sea inmune a ataques dirigidos a él.

Existen básicamente 2 tipos de firewall:

a) Packet filter: El filtrado se realiza para cada paquete que entra o sale de la red. Las reglas de filtrado se basan en:

- Dirección IP origen
- Dirección IP destino
- Puerto Origen
- Puerto Destino

Este tipo de filtrado es estático, para realizar algún cambio sobre éste se deben de cambiar las reglas. Algunas ventajas de packet filter son:

- Simple: Se puede implementar en routers con ACL
- Bajo costo
- Alto rendimiento

Desventajas:

- **Filtrado estático:** Para cambiar algo, se deben de cambiar las reglas.
- **Susceptibles de spoofing**

b) Statefull inspection: Posee una especie de “filtrado inteligente”. El firewall permite o deniega sesiones (entrantes o salientes) tomando en cuenta el estado de las conexiones a partir del análisis de cada uno de los paquetes para obtener información acerca de la sesión. El filtrado se hace sobre la sesión. Algunas ventajas son:

- Filtrado dinámico
- Bajo costo
- Más seguro que packet filter
- Buena capacidad de jogging

Algunas desventajas son:

- No todos los routers lo soportan
- La configuración de reglas es más compleja que el packet filter

Por lo tanto se puede concluir que los firewalls de filtrado:

- Mejoran la seguridad de la red interna frente a los ataques externos.
- No proveen autenticación de usuarios: si se requiere, se deberá implementar en algún servidor de la red interna.
- La configuración de las reglas de filtrado es una tarea bastante compleja.
- Permiten conexiones directas end-to-end.
- Una debilidad: una vez que un atacante ganó acceso a la red interna, podrá acceder directamente a cualquier host con vulnerabilidades (principalmente los que están mal configurados.)
- No brindan protección a ataques internos (excepto que se use algún firewall interno).
- No tienen capacidad para evitar ataques que se basan en servicios autorizados.

Proxy

El proxy es un servidor conectado normalmente al servidor de acceso de la www de un proveedor de acceso que va almacenando toda la información que los usuarios reciben de la web, por lo tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.[25]

El proxy funciona en un host ubicado como "conector" de una red interna con servidores externos a la misma. Los usuarios de la red interna solicitan servicios de

[25] http://www.definicion.org/proxy

Internet a través del Proxy y éste se ocupa de establecer una nueva conexión hacia el sistema destino, así como se muestra en la siguiente figura 6.9.

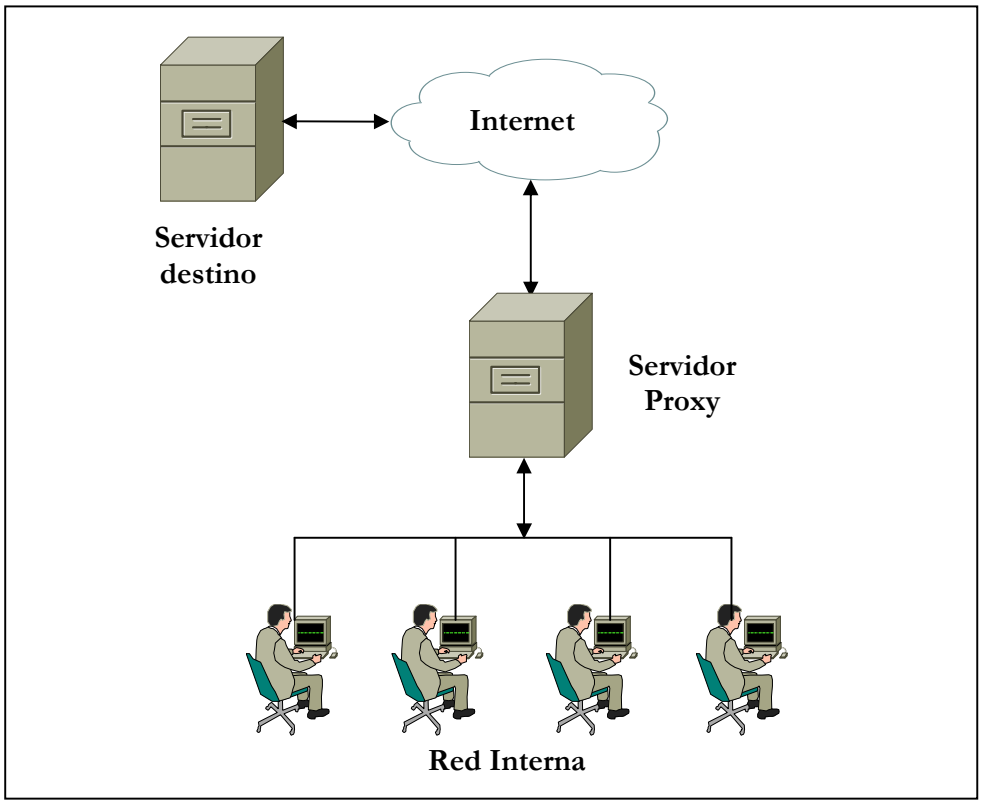

Figura 6.9 Proxy

Algunas características del Proxy:

- Emplea software para capturar, analizar y realizar la inspección de seguridad para cada conexión en cada protocolo.
- Cuando aprueba un requerimiento lo redirige hacia el servidor externo que corresponda, es decir, que actúa como servidor y como cliente.
- Para los clientes, el Proxy es transparente.
- Tiene la capacidad de autenticar usuarios finales.
- Suministran servicios de buffer: por ejemplo, pueden mantener un conjunto de páginas almacenadas en su disco local de modo que si son nuevamente referenciadas por algún cliente, la conexión se pueda establecer rápidamente sin necesidad de acceder al exterior para traerlas.

- Pueden monitorear lo que está pasando en la red interna.

Ventajas del Proxy:

- Proporcionan un buen nivel de seguridad.
- No permiten conexiones directas end-to-end.
- Tienen un buen registro de actividad.
- Proveen autenticación de usuarios.
- Son simples de administrar.

Desventajas del Proxy:

- Tienen un alto requerimiento de CPU.
- Requerimiento de un Proxy por cada protocolo (Proxy de aplicación).

La implementación de un firewall en una organización dependerá de varios aspectos, principalmente del grado de seguridad deseado en función de las características de la empresa y de un adecuado análisis de costos.

Muchas veces no cubren la totalidad de los equipos de la red interna (alguna conexión que "burla" los mecanismos de protección).
Algunos productos de firewall's son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **BlackIce:** Proporciona un sólido Firewall que detecta, informa y bloquea eficazmente los intentos de intrusión.
- **Firewall-1:** Esta herramienta incorpora una nueva arquitectura dentro del mundo de los cortafuegos: la inspección con estado (stateful inspection). Esta herramienta inserta un módulo denominado Inspection Module en el núcleo del sistema operativo sobre el que se instala, en el nivel software más bajo posible (por debajo incluso del nivel de res), así, desde ese nivel tan bajo, Firewall-1 puede interceptar y analizar todos los paquetes antes de que lleguen al resto del sistema; se garantiza que ningún paquete es procesado por ninguno de los

protocolos superiores hasta que Firewall-1 comprueba que no viola la política de seguridad definida. (www.checkpoint.com).

- **Pix:** Se trata de un firewall completamente hardware. PIX no se ejecuta en una máquina UNIX, sino que incluye un sistema operativo empotrado denominado Finesse que desde el espacio del usuario se asemeja más a un router que a un sistema Unix clásico. (www.cisco.com).
- **Zone alarm:** El firewall personal para Windows. Ofrecen una versión gratuita limitada. (www.zonelabs.com)

6.3.6 Detección de intrusos

Las herramientas de detección de intrusos permiten proteger a los sistemas mediante el uso de mecanismos que analizan actividades no lícitas.
Las más conocidas son las denominadas IDS (Intrusion Detection System). Una generación más actual son los Honeypots y Honeynets, que funcionan como señuelos.

6.3.6.1 Tipos de intrusos

Hay que aclarar que los intrusos son los individuos que llevan adelante los ataques y éstos pueden ser de dos tipos:

- **Externos:** Son personas no autorizadas a acceder en el sistema objeto de ataque.
- **Internos:** Son personas que tienen acceso a algunos recursos del sistema.

Los intrusos internos se clasifican en:

- **Enmascarados:** Son los que se ocultan tras la identidad de algún otro usuario legítimo con acceso a datos sensitivos. Los logs no logran detectar al verdadero atacante.

- **Clandestinos:** Son los que tienen acceso como para deshabilitar los controles de auditoría, para que no registren algunas actividades. Son los más peligrosos.

Para comprender mejor un ataque de intrusión interna se dará un ejemplo:

- "A" es un usuario legítimo con acceso al archivo de *sueldos* y "B" es un usuario también legítimo pero sin acceso al archivo *sueldos.*
- "B" compromete la contraseña de "A" (por cualquier método de los descritos anteriormente) y accede al sistema con la identidad de A y modifica el archivo *sueldos.*
- En los logs quedará registrado que "A" modificó el archivo *sueldos.*

Los más peligrosos son los sujetos que pueden deshabilitar los registros de auditoría. Su técnica consiste en:

a) Deshabilitar el registro en los logs;
b) Efectuar su acción intrusiva sin dejar registros;
c) Reactivar el registro en los logs.

Al descubrirse la intrusión no se encontrarán datos registrados que puedan ser de utilidad para investigar (origen, autor, entre otros).
Lo que sí es posible detectar es que los registros en los logs fueron deshabilitados por un cierto tiempo. En este caso se debe buscar al responsable entre los usuarios con accesos privilegiados.

6.3.6.2 Composición de los IDS (Sistemas de Detección de Intrusos)

Los IDS están compuestos por tres elementos básicos, los cuales son:

1. Fuente de Información: Proporciona los eventos del sistema. Estos eventos pueden ser:

- Logs o registros de auditoría, tanto del sistema operativo, como de las aplicaciones.

- Paquetes de red.

Estos no son excluyentes, ya que hay sistemas que los combinan para mejorar su capacidad de detección.

2. Motor de análisis: Busca evidencias de intrusiones y funciona de acuerdo con dos estrategias:

- **Detección de anomalías:** Consiste en comparar la actividad monitorizada con el uso normal del sistema.
- **Detección de mal uso:** Consiste en comparar la actividad monitorizada con el uso adecuado del sistema.

3. Mecanismo de respuesta: Actúa de acuerdo a los resultados del motor de análisis y ésta puede ser:

- **Pasiva:** El IDS emite una alarma al administrador señalando la situación detectada, pero no toma ninguna acción para detener la intrusión. Opera off-line. Analiza los logs y señala posibles intrusiones o violaciones para que el administrador tome las acciones apropiadas.
- **Activa:** Analiza los logs en tiempo real. Al detectar una posible intrusión, emite la alarma al administrador y además puede lanzar medidas inmediatas de protección en forma proactiva o reactiva.

Las medidas proactivas se toman después de que ocurrió el incidente de seguridad, con lo que se evita vuelva a suceder en el futuro. Ejemplo: Deshabilitar un servicio. Y las medidas reactivas se toman durante el momento del ataque, con lo que se evita que el mismo prospere.

Ejemplo: matar el proceso sospechoso, desconectar el usuario.

Ambos pueden ser tomados automáticamente por el propio IDS o manualmente por el administrador de seguridad ante la notificación del IDS.

6.3.6.3 Clasificación de los IDS

Los IDS se pueden clasificar en 2 tipos; según los sistemas que vigilen y según la estrategia que emplea su motor de análisis, mismos que se describen a continuación:

A. Según los sistemas que vigilen:

- **Basados en host (HIDS):** Examinan la actividad en un único equipo. Son muy simples de implementar y poco costosos, aunque su alcance es limitado, por ejemplo, si llegara a producirse una intrusión en otro host u otra parte de la red, este IDS no la detectará.
- **Basados en red (NIDS):** Monitorean todos los paquetes que circulan por la red en busca de elementos que denoten un ataque contra alguno de los sistemas ubicados en ella. Puede situarse en cualquiera de los *hosts* o en un servidor, en ambos casos su placa de red debe estar en modo promiscuo para capturar todo el tráfico y son capaces de detectar ataques provenientes del tráfico "ilícito" que dejó pasar el firewall.
- **Basados en agentes:** Están orientados a computación móvil y a sistemas distribuidos. Los agentes (programas autónomos pequeños) se ejecutan sobre el sistema que se desea proteger, monitoreando su actividad tal como en los HIDS, los datos recogidos por los agentes se envían a otras unidades del IDS donde se analizan en mayor profundidad. Algunos ejemplos de dichos sistemas son: AAFID (Autonomous Agents for Intrusion Detection) y EMERALD.

B. Según la estrategia que emplea su motor de análisis

- **Basados en detección de anomalías:** Parten de la siguiente consideración: ***"Todas las actividades de intrusión son actividades anómalas"*** Lo que significa que toda actividad anómala que detecte la va a considerar como una actividad intrusiva.

Por ello, para diferenciar los eventos anómalos de los eventos normales, el IDS se debe basar en el conocimiento previo de las actividades normales del sistema (perfil normal), así cómo, comparar cada evento contra el perfil normal. Un desvío significativo respecto a ese perfil normal será tomado como intento de intrusión.

Algunos ejemplos son:

- El usuario “mlopez” ingresa al sistema desde la estación de trabajo WSTD24 o desde WSTD25 en el horario de 8 a 16 hrs.
- La impresora LPTD190 emite listados de hasta 30 hojas.
- La estación de trabajo móvil WSM12 se conecta a la red diariamente entre las 20 y 21 hrs.

¿Pero qué pasa si?:

- El usuario “mlopez” debe trabajar un sábado a partir de las 18 hrs?
- Si se manda a imprimir a la impresora LPTD190 un documento de 50 páginas?
- Si la estación de trabajo móvil WSM12 se conecta a la red a las 23:30 hrs?

En todos esos casos el IDS detectará una intrusión.

O bien ¿Qué pasa si?:

- Otro empleado de la empresa aprovecha que “mlopez” salió a hacer un trámite y usa su estación de trabajo para mandar a imprimir por la impresora LPTD190 un documento confidencial de 23 páginas?.
- O si un objeto roba la estación de trabajo móvil WSM12 y se conecta normalmente?

En todos esos casos el IDS no detectará nada anormal. De estos ejemplos surge que: “el conjunto de actividades intrusivas no es exactamente igual al conjunto de actividades anómalas” Así como se muestra en la figura 6.10.

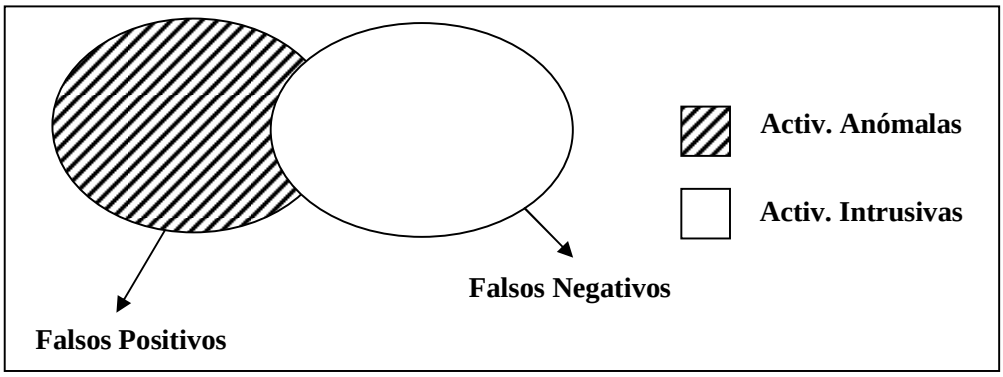

Figura 6.10 Ejemplo

Falsos Positivos: El IDS detecta actividades anómalas pero que no son intrusivas. Genera falsas alarmas, si el índice es alto, y puede resultar que el IDS sea ineficiente.

Falsos Negativos: El IDS desecha actividades intrusivas pero que no son anómalas. A mayor índice mayor riesgo tiene el sistema. Por lo tanto se puede decir, que los falsos negativos son mucho más peligrosos que los falsos positivos. El objetivo es minimizar ambos indicadores. Para ello es necesario seleccionar con cierto cuidado los aspecto del sistema que se van a monitorear y los umbrales de análisis, razón por la que es imprescindible que el administrador conozca la operatividad de la red.

- **Basados en mal uso:** Estos parten de la siguiente consideración: “Todas las actividades de intrusión se corresponden al uso incorrecto o mal uso del sistema o de algún recurso del mismo”.

Lo que significa que todo mal uso del sistema que detecte lo va a considerar como una actividad intrusiva.

Para este tipo de IDS el concepto de “mal uso” significa uso inadecuado y este uso inadecuado es el que sucede en el caso de las intrusiones o ataques. Por lo tanto para detectar “mal uso” los IDS se basan en los patrones de conducta o firmas. Por ello se deben comparar toda actividad en el sistema contra una base de datos de firmas de ataques:

- Dependiendo de su nivel de "inteligencia" son capaces de detectar variaciones de un mismo ataque aunque el mismo sea llevado a cabo con actividades diferentes.
- Pero, igual que los programas antivirus, no pueden hacer prácticamente nada en caso de un ataque desconocido, pues carecen de la firma que lo pueda identificar.
- La BD de firmas de ataques debe estar siempre actualizada.

Existen dos cuestiones importantes ligadas a la efectividad de este tipo de IDS:

- **Identificación de la firma asociada a un ataque:** No es fácil conocer todas las estrategias que emplean los atacantes para llevar a cabo un determinado ataque. A veces los ataques intercalan actividades correctas e inofensivas con las verdaderas actividades intrusivas, otras veces, realizan los ataques por etapas.
- **Distinción entre un ataque y una actividad no intrusiva:** Algunas actividades comunes tiene un patrón similar al de ciertos ataques: por ejemplo, un administrador escaneando la red mediante el comando *ping* se puede asemejar a la preparación de un ataque donde el intruso busca cuáles hosts están respondiendo.

C. Híbridos

Combinan aspectos de ambos tipos: detección de anomalías y detección de mal uso. Trabajan con una base de datos de firmas de ataques y también aprenden de ataques analizando el tráfico normal de la red. Si bien, poseen las ventajas de los dos modelos y son más eficientes y complejos de administrar.

Según la técnica que emplean los IDS se pueden clasificar en:

- **Basados en uso normal:** Se basan en comparaciones simples con los datos de registro generados por el sistema sin aplicar ningún tipo de "inteligencia", también, son los más comunes y los más simples de

implementar. Un dato interesante es que los primeros IDS utilizaban este modelo.

- **Basados en modelos estadísticos:** Este tipo de modelo incorpora algún grado de análisis a partir de los datos registrados en el sistema y establecen los posibles perfiles normales o uso adecuado mediante análisis estadísticos de los datos obtenidos de la fuente de información.
- **Basados en regla (predictivos):** Son más complejos ya que incorporan reglas a su motor de análisis para predecir posibles comportamientos anómalos o posibles usos indebidos. La mayor complejidad se basa en establecer las reglas.
- **Basados en razonamiento:** Una variante con respecto a los que se han mencionado anteriormente es que aplican técnicas de inteligencia artificial para razonar de acuerdo a reglas establecidas en un motor de inferencia, pudiendo llegar a detectar (y detener) ataques en progreso.
- La complejidad está dada no solo por las reglas sino por el motor de inferencia. Actualmente la mayoría de los IDS implementan este tipo de técnica.
- **Basados en transición de estados:** Se basan en analizar los estados resultantes como producto de las acciones realizadas, más que de analizar las secuencias de acciones en si mismas, de este modo pueden detectar ataques aunque se encuentres enmascarados en acciones legítimas.

Algunos productos de firewall’s son los que se listan a continuación junto con la dirección electrónica donde se puede obtener más información de cada uno de ellos:

- **Prelude:** Es un IDS híbrido que trabaja junto con otras herramientas. (www.prelude-ids.org)
- **RealSecure:** Es un sistema de detección de intrusos y avisos automatizado en tiempo real, que detecta las actividades sospechosas y responde a los ataques a la red. (www.iss.com)

- **Snort**: Esta herramienta es un sniffer de paquetes y un detector de intrusos basado en red (se monitoriza todo un dominio de colisión). Es un software muy flexible que ofrece capacidades de almacenamiento de sus bitácoras tanto en archivos de texto como en bases de datos abiertas como MySQL. Esta herramienta implementa un motor de detección de ataques y barrido de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida.(www.snort.org)

Como se mencionó anteriormente, también están los Honeypots y los Honeynets, que funcionan como señuelos y se describen a continuación:

- **Honeypots**

Los Honeypots son sistemas señuelo que se usan para detectar y analizar intrusiones, así mismo, se implementan en una red para que puedan ser explorados y atacados mediante flujos de seguridad, preparados para atraer a los intrusos. Por esta razón pueden ser considerados cómo un tipo de IDS.
La idea de los Honeypots es que un atacante descubra un sistema "atacable" y efectúe su intrusión, comprometiendo los mecanismos de seguridad. El intruso cree que su ataque es efectivo sin darse cuenta de que en realidad fue realizado sobre un sistema aislado de la red.

Algunas de las características de los Honeypots son:

- Un honeypot no tiene utilidad desde el punto de vista de producción; por lo tanto, toda interacción con él es una intrusión o un intento de ésta.
- Es especialmente útil para estudiar las técnicas que emplean los intrusos y para aprender sobres nuevas técnicas de ataque.
- Esto permite reforzar el sistema verdadero y tomar medidas de seguridad anticipadas.

Existen dos tipos de *honeypots* de acuerdo al nivel de actividad que le permiten tener al atacante:

- **De baja interacción:** Operan únicamente emulando servicios y sistemas operativos, con lo que presentan al intruso una interacción restringida a lo que se esté emulando.
- **De alta interacción:** Operan en sistemas reales ofreciendo servicio y aplicaciones reales (no son emuladas), obviamente aislados de la red.

Ventajas:

- **Logs más pequeños:** Solo registran la actividad proveniente del exterior.
- **Nuevas herramientas y tácticas:** Permiten analizar herramientas o técnicas de ataque no vistas anteriormente.
- **Cifrado:** Operan bien en entornos cifrados como IPv6.

Desventajas:

- **Visión limitada:** Sólo pueden rastrear y capturar actividad que interactúen directamente con ellos.
- Los atacantes expertos y que verdaderamente tienen la intención de atacar pueden darse cuenta fácilmente de su existencia y pasarlo por alto.
- Tienen vulnerabilidades porque trabajan con las tecnologías existentes.

- **Honeynets**

Se define como un conjunto de Honeypots altamente interactivos, diseñados para la investigación y obtención de información sobre atacantes.
Un Honeynet es una arquitectura, no un producto de software determinado, su objetivo es hacerle creer al atacante que está ante una red “real”, entonces se deben añadir los distintos elementos que conforman una arquitectura de red.

La mayoría de los sistemas de seguridad han sido siempre de carácter defensivo, por ejemplo los IDS, firewalls y demás soluciones, se basan el a defensa de los sistemas de la organización y cuando un ataque o vulnerabilidad es detectado de inmediato se procede a corregirlo.

Con los Honeynets se obtienen nuevos patrones de comportamiento así como métodos de ataque cuyo objetivo es prevenirlos en los sistemas reales, sin éstos, cada vez que se produzca un ataque "nuevo" y exitoso a un sistema real existente, este dejará de dar servicio y se verá comprometido. Por el contrario con los Honeynets, un ataque exitoso o nuevo, no tiene porqué afectar a ningún sistema real.

6.3.7 Autenticación

Las redes y los servicios que prestan los servidores son cada vez más complejos. La red de una organización ya no se restringe a un único lugar físico, sino que puede estar distribuida en muchos ambientes geográficos con servidores ubicados en distintos lugares.

Frente a esta realidad es necesario garantizar que los servidores presten los servicios a clientes legítimos.
Las herramientas de autenticación surgen como una necesidad para garantizar la identidad de clientes ante servidores. La más común es Kerberos.

Kerberos fue creado en 1983 por el MIT para el proyecto Athena, éste tenía como objetivo crear un entorno de trabajo educacional compuesto por estaciones gráficas, redes de alta velocidad y servidores.
Un dato interesante es que en la mitología griega, kerberos es el nombre de un perro de tres cabezas que vigila la puerta de entrada al infierno.

Antes de kerberos, existían 2 modelos de autenticación:

1. Una vez que un usuario se autenticaba e ingresaba al sistema, podía usar todos los servicios que éste le ofrecía.
   El nivel de seguridad proporcionado era muy bajo, ya que el cliente adquiría demasiado poder sobre el servidor.

2. Cada vez que un cliente solicitaba un servicio, se debía volver a identificar y autenticar ante el servidor (por ejemplo, usar contraseñas para cada servicio de la red).

   Se obligaba al usuario a teclear su clave repetidamente; de tal forma que la contraseña viajaba muchas veces por la red, lo que hacía más probables los ataques exitosos.

Kerberos mejora estos esquemas porque exige que un cliente tenga autorización para comunicarse con un servidor y por que elimina la necesidad de demostrar el conocimiento de la contraseña.

Cuando un cliente solicita un servicio a un servidor, éste le exigirá al cliente un ticket de autorización antes de darle el servicio, este ticket, que es entregado por un servidor kerberos, a pedido del cliente, indicará que kerberos autorizó al cliente a pedirle un servicio al servidor.
Los ticket son entregados por kerberos después de que el cliente haya demostrado ser quien decía ser, si el cliente posee el ticket apropiado, el servidor supone que el cliente es legítimo.

Funcionamiento de Kerberos:

1. Un cliente inicia una sesión en la red.
2. Se autentica por única vez contra un servidor Kerberos.
3. Solicita servicios de un servidor “S”:
   i. Le pide a Kerberos un ticket que lo autentique ante el servidor “S”.
   ii. Luego se conecta al servidor “S”, le presenta el ticket y finalmente le solicita el servicio.

El paso número 3 será realizado cada vez que el cliente solicite un servicio. Un servidor Kerberos se denomina KDC (Key Distribution Center), y provee dos servicios fundamentales:

- **Autenticación (AS):** Autentica inicialmente al cliente proporcionándole un ticket especial (TGT – Ticket Grating Ticket), que posteriormente le servirá para demostrarle a Kerberos (más precisamente al Servicio de Concesión de Ticket) que ya fue autenticado.
- **Concesión de ticket (TGS):** Le proporciona al cliente los ticket que este debe presentar ante los servidores cuando solicite algún servicio.

Características principales de Kerberos:

- Se basa en la criptografía simétrica
- Requiere relojes sincronizados
- Debe conocer todas las claves privadas

El mecanismo de autenticación en Kerberos es un proceso que se realiza en tres grandes etapas (así cómo se muestra en la figura 6.11):

- **Login:** Procedimiento por el que un cliente se identifica y autentica ante un servidor Kerberos.
- **Obtención de ticket:** Procedimiento para solicitar al servidor Kerberos la provisión de tickets para acceder a los servidores.
- **Petición de servicios:** Solicitud de servicios a los servidores.

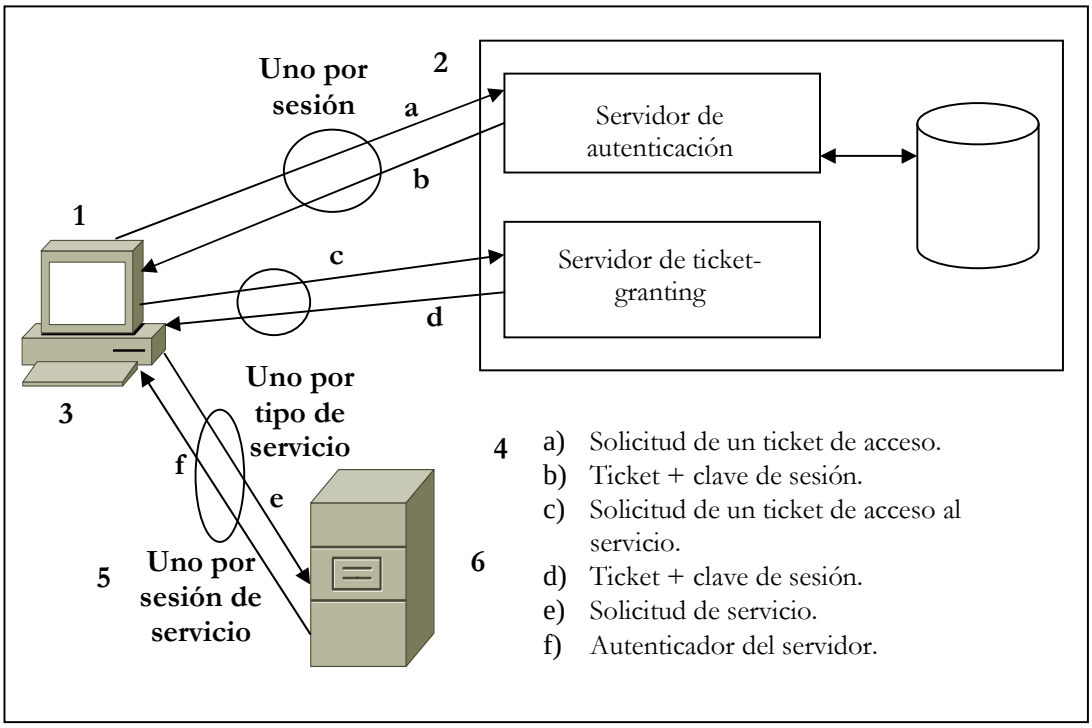

Figura 6.11 Mecanismo de autenticación en Kerberos

La arquitectura de Kerberos se basa en tres objetos de seguridad:

- **Clave de sesión:** Clave creada dinámicamente por kerberos durante una sesión para ser usada en la comunicación entre el cliente y un servidor.
- **Ticket:** Credencial que Kerberos le entrega a un cliente para que éste pueda demostrar que ha sido autenticado recientemente. Hay 2 clases de ticket: TGT (ticket para pedir ticket) y TS (ticket para pedir servicios).
- **Autenticador:** Elemento construido por el cliente con su nombre y la hora, cifrado con una clave de sesión entre el cliente y el TGS, que utiliza el TGS en verificar la identidad del cliente para poder extender los TS que éste solicita.

TGT: Es la credencial que el servicio de autenticación de Kerberos (AS) le entrega al cliente para que lo presente ante el servicio de concesión de ticket (TGS) cuando solicite credenciales para algún servicio.

TS: Es la credencial que el TGS le entrega al cliente para que lo presente ante el servidor al que le solicita servicios.

Cabe destacar que Kerberos es un sistema para garantizar la autenticidad, pero también proporciona integridad y confidencialidad.

Por ejemplo:

- Integridad: Cada paquete de datos se envía con un checksum cifrado con la clave de sesión.
- Confidencialidad: Cada paquete viaja cifrado con la clave de sesión.

Resulta que kerberos es el modelo más generalizado de aplicación del concepto *Single Sign On (SSO)* que consiste en que los clientes disponen de un único punto de identificación y autenticación en un entorno de red muy complejo, con muchos servicios distribuidos entre múltiples servidores.

Las principales desventajas son:

- Modelo centralizado.
- Necesidad de sincronización de los relojes de todas las máquinas que ejecuten servicios autenticados.
- Toda la red debe estar "Kerberizada".

Por lo tanto, se puede concluir que los Kerberos se encuentran disponibles para la mayoría de sistemas UNIX y es el sistema de autenticación elegido por Microsoft para Windows 2000, también incursiona en algunos conceptos avanzados de seguridad, tales como:

- Delegación
- Autenticación entre dominios
- Confianza transitiva
- Uso de claves públicas

Como se ha podido observar, existe una gran serie de herramientas que se pueden emplear para implantar el esquema de seguridad desarrollado, y aun cuando éstas no son todas ni las únicas que existen, sí son una amplia gama de posibilidades a estudiar y elegir aquellas que sean necesarias para el entorno (véase figura 6.12).

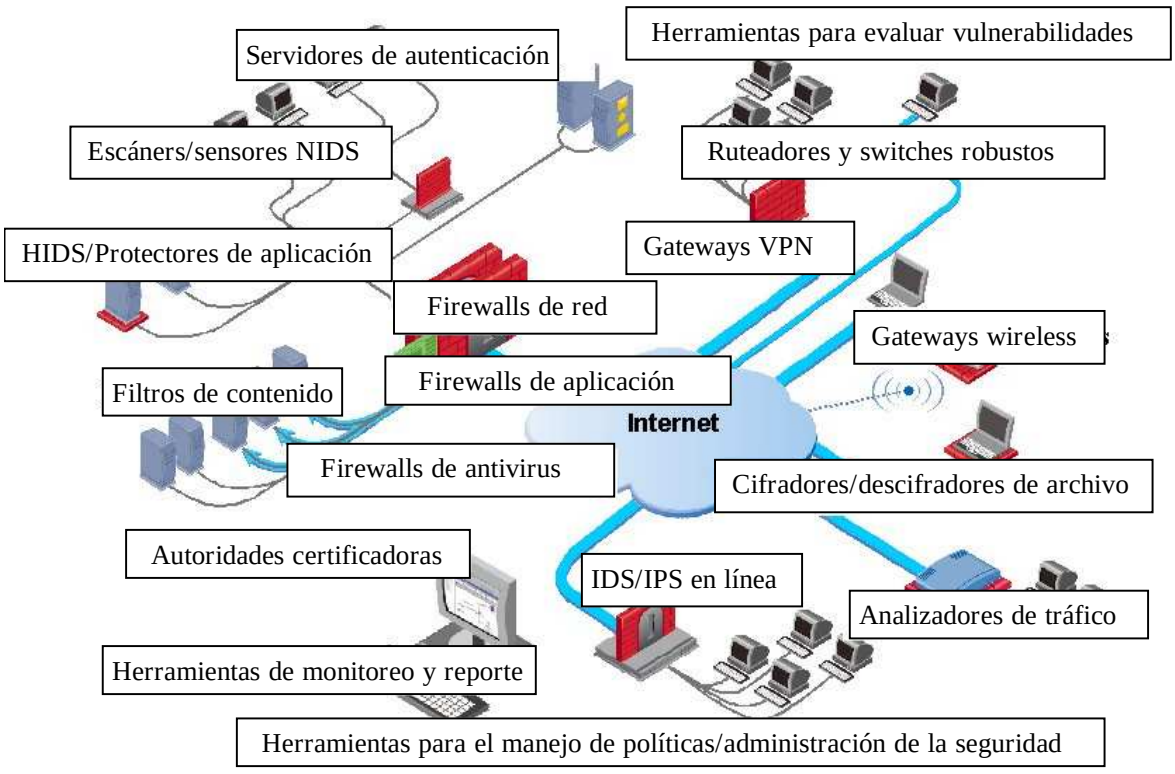

Figura 6.12 Uso de herramientas de seguridad

6.4 Auditoría

La auditoría resulta ser un tema de gran interés ya que con esta herramienta es posible identificar y corregir diversas vulnerabilidades existentes que suelen presentarse en las estaciones de trabajo, en las redes o en los servidores. Por ello es imprescindible conocer más a fondo los tipos de auditoría que existen así como las fases y los diversos estándares, los cuales se desarrollan a continuación.

La proliferación de metodologías en la auditoría y el control informático se observan en los primeros años de la década de los 80’s, paralelamente al nacimiento y comercialización de determinadas herramientas metodológicas (como el software de análisis de riesgos).

6.4.1 Definición

Una auditoría de seguridad informática es el estudio que comprende el análisis y gestión de sistemas para identificar y posteriormente corregir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables, quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas, aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

Algunos de los objetivos de la auditoría informática son:

- *El control de la función informática*
- *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*

La auditoría informática sirve para mejorar las actividades informáticas en las empresas así como su eficiencia, eficacia, rentabilidad y seguridad.

Algunos de los objetivos específicos de la auditoría informática son:

- *El cumplimiento de controles de la transferencia de aplicaciones del entorno de desarrollo al entorno de explotación*
- *La concientización de la Dirección y de los usuarios en la seguridad de los SI*
- *El cumplimiento de la legislación vigente*
- *La remuneración de los recursos humanos del departamento de SI*

- *Los procedimientos del Centro de Información*

6.4.2 Auditoría interna y auditoría externa

La Auditoría interna es realizada por una entidad funcional perteneciente a la propia estructura organizativa de la empresa y como contraprestación reciben una remuneración económica. La principal ventaja de la auditoría interna es que quienes son los responsables de llevarla a cabo pertenecen a la propia empresa, y que, por tanto, conocen directamente su problemática. Por otra parte el costo será menor puesto que los recursos utilizados emanan de la propia organización.

Por otro lado la Auditoría externa se realiza por personas ajenas a la empresa. La empresa contrata un servicio profesional para auditar su sistema de información por expertos externos a la empresa. La principal ventaja es el alto grado de objetividad que se consigue en comparación con la anterior. El principal inconveniente viene dado por el alejamiento de la problemática de la empresa de quienes asumen la responsabilidad de llevar a cabo la auditoría. No obstante, la profesionalidad y la experiencia de quienes asumen la auditoría debe superar estos inconvenientes para llevar a cabo un trabajo profesional. La auditoría externa desde el punto de vista económico es más costosa que la interna.

6.4.3 Características de la Auditoría informática

La Auditoría informática no suele realizarse de forma periódica en las organizaciones, sino que surge como consecuencia de problemas reales o potenciales, excepto cuando alguna normativa legal obliga, periódicamente o no, a su realización.
Agrupando por áreas esos problemas, las causas que pueden originar la realización de una Auditoría Informática son:

- **Desorganización / Descoordinación**
    - No coincidencia de objetivos del sistema de Información (SI) con los objetivos de la Organización

  - Los circuitos de información no son los adecuados
  - Duplicidad de información
  - No disponibilidad de la información o de resto de los recursos de la SI
- **Insatisfacción de usuarios**
  - No resolución de incidencias y averías
  - No atención de peticiones de cambios
  - Inadecuado soporte informático
  - Incumplimiento en los plazos de entrega de resultados periódicos
- **Debilidades económico – financieras**
  - Incremento inadecuado de las inversiones
  - Aumento constante de los costos
  - Desviaciones presupuestarias significativas
  - Incremento de recursos en el desarrollo de proyectos
- **Inseguridad de los SI**
  - Escasa confidencialidad de la información
  - Falta de protección física y lógica
  - Inexistencia de planteamientos en cuanto a la continuidad del servicio
- **Cumplimiento de la legalidad**
  - Protección de datos de carácter personal
  - Cumplimiento en TI por la ley Sarbanes - Oxley[26]

6.4.4 Tipos y clases de auditorías

El departamento de informática posee una actividad proyectada al exterior, al usuario, aunque el "exterior" siga siendo la misma empresa, por lo tanto, de ahí surge la *Auditoría Informática de Usuario.* Ésta se distingue para contraponerla a la Informática

[26] La ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor.
http://forodeseguridad.com/artic/segcorp/7217.htm

Interna, en donde se hace la informática cotidiana y real. En consecuencia, existe una *Auditoría de Actividades Internas.*

Por otra parte, el control del funcionamiento del departamento de informática referente al exterior, con el usuario se realiza por medio de la Dirección, ya que ésta es capaz de interpretar las necesidades de la Compañía. Por ello, una informática eficiente y eficaz requiere el apoyo continuo de su Dirección frente al "exterior". Revisar estas interrelaciones constituye el objeto de la *Auditoría Informática de Dirección.* Estas tres auditorías, más la auditoría de Seguridad, son las cuatro Áreas Generales de la Auditoría Informática más importantes, dentro de éstas se establecen las siguientes divisiones de auditoría informática: Explotación, Desarrollo de Proyectos, Sistemas, Comunicaciones y Seguridad, las cuales se muestran en la tabla 6.1

Tabla 6.1 Divisiones de Auditoría Informática

Áreas Específicas	Áreas Generales			
	Interna	Dirección	Usuario	Seguridad
Explotación				
Desarrollo de Proyectos				
Sistemas				
Comunicaciones				
Seguridad				

Cada área específica puede ser auditada desde los siguientes criterios generales:

- Su propio funcionamiento interno
- El apoyo que recibe la dirección y en sentido ascendente, del grado de cumplimiento de las directrices de ésta.
- La perspectiva de los usuarios, destinatarios reales de la informática.
- El punto de vista de la seguridad que ofrece la informática en general o la rama auditada.

Estas combinaciones pueden ser ampliadas y reducidas según las características de la empresa auditada.

6.4.5 Fases de una auditoría

Los servicios de auditoría constan de las siguientes fases:

Fase I: Conocimientos del sistema

- *Aspectos Legales y Políticas Internas:* Sobre estos elementos está construido el sistema de control y por lo tanto constituyen el marco de referencia para su evaluación.
- *Características del Sistema Operativo.*
  - Organigrama del área que participa en el sistema.
  - Manual de Funciones de las personas que participan en los procesos del sistema.
  - Informes de auditorías realizadas anteriormente.
- *Características de la aplicación de computadora.*
  - Manual técnico de la aplicación del sistema.
  - Funcionarios (usuarios) autorizados para administrar la aplicación.
  - Equipos utilizados en la aplicación de computadora.
  - Seguridad de la aplicación (claves de acceso).
  - Procedimientos para generación y almacenamiento de los archivos de la aplicación.

Fase II: Análisis de transacciones y recursos

- *Definición de las transacciones:* Dependiendo del tamaño del sistema, las transacciones se dividen en procesos y estos en subprocesos. La importancia de las transacciones deberá ser asignada con los administradores.
- *Análisis de las transacciones.*
  - Establecer el flujo de los documentos.

  En esta etapa se hace uso de los flujogramas (representación gráfica de la secuencia de actividades de un proceso[27]) ya que facilita la visualización del funcionamiento y recorrido de los procesos.
- *Análisis de los recursos:* Consiste en identificar y codificar los recursos que participan en los sistemas.

[27] http://www.infomipyme.com/Docs/GENERAL/Offline/GDE_04.htm

- *Relación entre transacciones y recursos.*

Fase III: Análisis de riesgos y amenazas

- La *Identificación de riesgos* consiste en identificar los siguientes aspectos:
    - Daños físicos o destrucción de los recursos
    - Pérdida por fraude o desfalco
    - Extravío de documentos fuente, archivos o informes
    - Robo de dispositivos o medios de almacenamiento
    - Interrupción de las operaciones del negocio
    - Pérdida de integridad de los datos
    - Ineficiencia de operaciones
    - Errores
- *Identificación de las amenazas.*
    - Amenazas sobre los equipos
    - Amenazas sobre documentos fuente
    - Amenazas sobre programas de aplicaciones
- *Relación entre recursos, amenazas y riesgos.*

La relación entre estos elementos deberá establecerse a partir de la observación de los recursos en su ambiente real de funcionamiento.

Fase IV: Análisis de controles

- *Codificación de controles.*

Los controles se aplican a los diferentes grupos utilizadores de recursos, donde la identificación de los controles debe contener una codificación la cual identifique el grupo al que pertenece el recurso protegido.

- *Relación entre recursos, amenazas y riesgos.*

La relación con los controles debe establecerse para cada tema (recursos, amenazas y riesgos) identificado. Para cada tema debe establecerse uno o más controles.

- *Análisis de cobertura de los controles requeridos.*

Este análisis tiene como propósito determinar si los controles que el auditor identificó como necesarios proveen una protección adecuada de los recursos.

Fase V: Evaluación de controles

- *Objetivos de la evaluación.*

Consiste en:

  - Verificar la existencia de los controles requeridos.
  - Determinar la operatividad y suficiencia de los controles existentes.

- *Plan de pruebas de los controles.*
  - Incluye la selección del tipo de prueba a realizar.
  - Deben solicitarse al área respectiva todos los elementos necesarios de prueba.
- *Pruebas de controles.*
- *Análisis de resultados de las pruebas.*

Fase VI: Informe de auditoría

- *Informe detallado de recomendaciones.*
- *Evaluación de las respuestas.*
- *Informe resumen para la alta gerencia.*

Este informe debe prepararse una vez obtenidas y analizadas las respuestas de compromiso de las áreas y debe contemplar los siguientes aspectos:

- **Introducción:** Objetivo y contenido del informe de auditoría.
- **Objetivos** de la auditoría.
- **Alcance:** cobertura de la evaluación realizada.
- **Opinión:** con relación a la suficiencia del control interno del sistema evaluado.
- **Hallazgos**
- **Recomendaciones**

Fase VII: Seguimiento de las Recomendaciones.

- *Informes del seguimiento.*
- *Evaluación de los controles implantados.*

6.4.6 Auditoría de seguridad de la información

La auditoría de seguridad de la información tiene por objetivo verificar que se cumplan los controles estipulados por la organización. Esto puede hacerse bien en un "documento de seguridad", a través de unas Políticas de Seguridad, en un Plan de Seguridad o mediante unos Objetivos de Control de carácter sectorial o general.

Existen diferentes tipos de auditoría de seguridad, los cuales son:

- **Auditoría de seguridad física:** Se refiere a la ubicación de la organización, evitando ubicaciones de riesgo y en algunos casos no revelando la situación física de ésta. También se refiere a las protecciones externas (vigilantes, arcos de seguridad, entre otros) y protecciones del entorno.
- **Auditoría de seguridad lógica:** Comprende los métodos de autenticación de los sistemas de información.
- **Auditoría de seguridad en el desarrollo de las aplicaciones:** comprende la revisión de las metodologías utilizadas y el control interno de las aplicaciones. En la primera se analizan las metodologías, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de las mismas. En la segunda se revisan las fases que se deben seguir acorde al área de desarrollo, por ejemplo:
  - **Estudio de viabilidad de la aplicación:** para aplicaciones largas, complejas y caras.
  - **Definición lógica de la aplicación:** Se analizan las posturas lógicas de actuación, en función de la metodología elegida y la finalidad que persigue el proyecto.
  - **Desarrollo técnico de la aplicación:** Se verifica que éste sea ordenado y correcto.
  - **Diseño de programas:** Deberán poseer la máxima sencillez, modularidad y economía de recursos.
  - **Métodos de pruebas: Se** realizan de acuerdo a las normas de instalación.
  - **Documentación:** Debe cumplir con la norma establecida en la instalación, tanto en la de Desarrollo como en la de Aplicaciones a Explotación.

- **Equipo de programación:** Se deben fijar las tareas de análisis puro, de programación y las intermedias.

- **Auditoría de seguridad en el área de producción:** Se refiere a los errores que pueden ocurrir así mismo cómo accidentes y fraudes.
- **Auditoría de seguridad en los datos:** Se refiere a la clasificación de los datos, estudio de las aplicaciones y análisis de los diagramas de flujo.
- **Auditoría de las bases de datos:** Se refiere a los controles de acceso, de actualización
- **Auditoría de seguridad en comunicaciones y redes:** Hace referencia a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- **Auditoría de la gestión:** Referido a la contratación de bienes y servicios, documentación de los programas, entre otros.
- **Auditoría legal del reglamento de protección de datos:** Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento desarrollo de la "Ley Orgánica de Protección de Datos"

Como áreas sobre las que ha de actuar la auditoría informática se pueden considerar las siguientes:

a) **Fundamentos de la seguridad:** Políticas, planes, funciones, existencia y funcionamiento de algún comité relacionado, objetivos de control, presupuesto, así como que existen sistemas y métodos de evaluación periódica de riesgos.
b) **Desarrollo de las políticas:** Procedimientos, posibles estándares, normas y guías.
c) **Amenazas físicas externas:** Inundaciones, incendios explosiones, cortes de líneas de comunicaciones, terremotos, terrorismo y huelgas.
d) **Control de accesos adecuado tanto físicos como lógicos:** De manera que cada usuario pueda acceder a los recursos para los que esté autorizado y asimismo pueda realizar solo las funciones permitidas.

e) **Protección de datos:** Según lo que regula la ley orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal y el reglamento 994/1999
f) **Comunicaciones y redes:** Topología y tipo de comunicaciones, uso de cifrado y protecciones ante virus.
g) **Entorno de Producción:** Entendiendo como tal la explotación más Técnica de Sistemas.
h) **Desarrollo de aplicaciones en un entorno seguro.**
i) **Continuidad de las operaciones.**

6.4.7 Enfoques de la Auditoría Informática

Los enfoques asignados a la Auditoría informática son: Auditoría alrededor de, a través de, y auditoría con la computadora.

Auditoría alrededor de la computadora: En este enfoque de auditoría, los programas y los archivos de datos no se auditan.
La auditoría alrededor de la computadora enfoca sus esfuerzos en la entrada de datos y en la salida de la información. Es el más cómodo para los auditores de sistemas, por cuanto únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina. También se examinan los controles desde el origen de los datos para protegerlos de cualquier tipo de riesgo que atente contra la integridad, exactitud y legalidad.

Los objetivos de este tipo de auditoría son:

- Verificar la existencia de una adecuada segregación funcional.
- Comprobar la eficiencia de los controles sobre seguridades físicas y lógicas de los datos.
- Asegurarse de la existencia de controles dirigidos a que todos los datos enviados a proceso estén autorizados.

- Comprobar la existencia de controles para asegurar que todos los datos enviados sean procesados.
- Cerciorarse que los procesos se hacen con exactitud.
- Comprobar que los datos sean sometidos a validación antes de ordenar su proceso.
- Verificar la validez del procedimiento utilizado para corregir inconsistencias y la posterior realimentación de los datos corregidos al proceso.
- Examinar los controles de salida de la información para asegurar que se eviten los riesgos entre sistemas y el usuario.
- Verificar la satisfacción del usuario. En materia de los informes recibidos.
- Comprobar la existencia y efectividad de un plan de contingencias, para asegurar la continuidad de los procesos y la recuperación de los datos en caso de desastres.

Auditoría a través de la computadora: Este enfoque está orientado a examinar y evaluar los recursos del software y surge como complemento del enfoque de auditoría alrededor de la computadora, en el sentido de que su acción va dirigida a evaluar el sistema de controles diseñados para minimizar los fraudes y los errores que normalmente tienen origen en los programas.

Los objetivos de esta auditoría son:

- Asegurar que los programas procesan los datos, de acuerdo con las necesidades del usuario o dentro de los parámetros de precisión previstos.
- Cerciorarse de la no-existencia de rutinas fraudulentas al interior de los programas.
- Verificar que los programadores modifiquen los programas solamente en los aspectos autorizados.
- Comprobar que los programas utilizados en producción son los debidamente autorizados por el administrador.

- Verificar la existencia de los controles eficientes para evitar que los programas sean modificados con fines ilícitos o que se utilicen programas no autorizados para los procesos corrientes.
- Cerciorarse que todos los datos sean sometidos a validación antes de ordenar su proceso correspondiente.

Auditoría con la computadora: Este enfoque va dirigido especialmente, al examen y evaluación de los archivos de datos en dispositivos de almacenamiento, con la ayuda de la computadora y de software de auditoría generalizados a la medida.

Los paquetes de auditoría permiten desarrollar operaciones y prueba, tales como:

- Recálculos y verificación de información, como por ejemplo, relaciones sobre nómina, montos de depreciación y acumulación de intereses, entre otros.
- Demostración gráfica de datos seleccionados.
- Selección de muestras estadísticas.
- Preparación de análisis de cartera por antigüedad.

Estos tres enfoques de auditoría mencionados son complementarios así como se muestran en la figura 6.13. Ninguno de los tres es suficiente para auditar aplicaciones en funcionamiento.

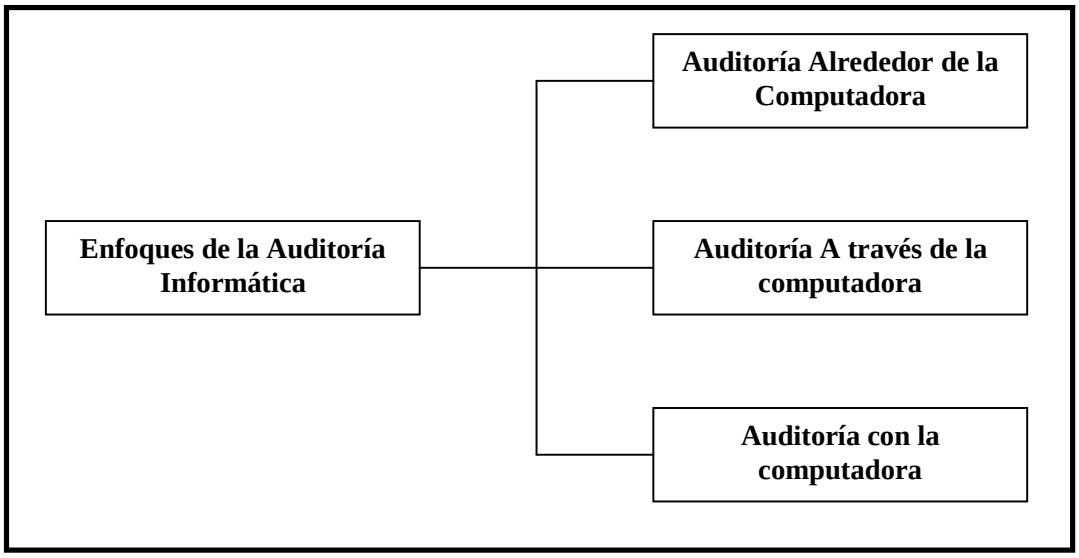

Figura 6.13 Enfoques de la auditoría informática.

6.4.8 Herramientas y técnicas para la auditoría informática

Cuestionarios

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos.

Para esto, suele ser habitual que se comience por solicitar el cumplimiento de cuestionarios preimpresos, que se envían a las personas que el auditor considera que son las adecuadas.

Estos cuestionarios no deben ser repetidos, sino que deben ser específicos para cada situación.

Entrevistas

El auditor comienza a realizar entrevistas con el personal de la empresa y lo hace de tres maneras:

1. Mediante la petición de documentación sobre alguna materia de su responsabilidad.
2. Mediante “entrevistas” en las que no se sigue un plan determinado ni un método estricto de sometimiento a un cuestionario.
3. Por medio de entrevistas en las que el auditor sigue un método preestablecido y busca finalidades concretas.

La entrevista entre el auditor y el auditado se basa en el concepto de interrogatorio y el auditor sigue en forma cuidadosa un sistema previamente establecido haciendo que la conversación sea lo menos tensa posible para que el auditado conteste de manera clara y sencilla.

Checklist

En esta etapa el auditor reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro lo que necesita saber y por qué. Sus cuestionarios son espacios vitales para el trabajo de análisis.

Ejemplo de un checklist:

Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y dentro de ella, se analiza el control de los accesos de personas y cosas al centro de cálculo. Podrían formularse las siguientes preguntas:

- ¿Existe personal específico de vigilancia externa al edificio?
  Re: No, solamente un guardia por la noche que atiende además otra instalación adecente.

<Puntuación: 1>

- Para la vigilancia interna del edificio, ¿hay al menos un vigilante por turno en los aledaños del Centro de Cálculo?
  Re: Si, pero sube a las otras 4 plantas cuando lo necesita.
  <Puntuación: 2>
- ¿Hay salida de emergencia además de la habilitada para la entrada y salida de máquinas?
  Re: Si, pero existen cajas apiladas en dicha puerta. Algunas veces las quitan.
  <Puntuación: 2>

Así como estas preguntas, existen otras qué dependiendo de lo que se esté auditando, es cómo se resuelven los cuestionarios que realiza el auditor.

6.4.9 Perfil Profesional del auditor informático

A continuación en la tabla 6.2 se muestran algunas ocupaciones con sus respectivos perfiles que se deben cubrir para ser un auditor informático.

Tabla 6.2 Perfil Profesional del auditor informático

Ocupación	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el marcado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas	Con experiencia en el mantenimiento de bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación.
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Experto en Subsistemas de teleproceso.
Técnico de Organización.	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costos	Economista con conocimiento de informática. Gestión de costos.

De lo anteriormente mencionado se puede decir que para ser un auditor en materia de seguridad informática se requiere tener conocimientos especializados en las diversas ramas que existen. Por ello es de suma importancia que los futuros profesionistas, tengan la preparación adecuada, de tal manera que les sea posible cubrir las necesidades que las organizaciones demandan.

Se puede concluir que la auditoría informática juega un papel muy importante en las organizaciones, ya que se debe garantizar en la medida de lo posible, que la información que éstas manejan, sea íntegra, confiable y sobre todo que se encuentre disponible cuando ésta se requiera. Por ello, se tienen que realizar auditorías de manera

periódica, para asegurarse de que las normas que se establecieron al diseñar los sistemas de seguridad, cumplan y mantengan las normas establecidas.

6.5 Seguridad en redes inalámbricas

En los últimos años las redes inalámbricas han tomado un papel muy importante y día con día son más los usuarios que disponen de éstas. Hoy en día la mayoría de las personas que disponen de una computadora o laptop se conectan por medio de su tarjeta inalámbrica en diversos puntos de acceso, como lo son; las escuelas, bibliotecas, restaurantes, cafés, espacios públicos, entre otros.

El auge de las redes inalámbricas ha surgido debido a la facilidad que hay para conectarse a Internet, por ejemplo, ahora ya no se requieren de cables para conectarse a esta red, debido a que son fáciles de instalar, son flexibles, es decir, es posible instalar nuevas WLAN o cambiarlas, y también tienen la característica de ser escalables (se puede realizar una instalación empezando por pequeñas “redes ad-hoc” de unas pocas estaciones, e ir ampliándolas hasta hacerlas muy grandes por medio de la utilización de puentes inalámbricos).
Por ello se vuelve importante mantener un nivel de seguridad que permita que la información viaje de manera segura logrando cumplir con los principios básicos de la seguridad; integridad, confiabilidad y disponibilidad.

6.5.1 Definición de la seguridad inalámbrica

La palabra seguridad abarca un amplio rango de campos dentro y fuera del ámbito de la computación. Se habla de seguridad cuando se describe por ejemplo una nueva plataforma de cómputo y que se dice que ésta es segura. Por ello se puede decir que el término “seguridad inalámbrica” se encuentra dentro del contexto de la seguridad de la información, es decir, cuando se hace referencia a la seguridad inalámbrica se está

hablando de la seguridad de la información que se mueve a través de las redes inalámbricas.

Para entender el significado de la seguridad informática es necesario entender la manera en que el término ha evolucionado a lo largo del tiempo. Hasta finales de los años 70's, esta área de seguridad fue referida como "Seguridad de Comunicaciones" o COMSEC, por un acrónimo en inglés definido por la U.S. National Security Telecomunications and Information Systems Security Instruction (NSTISSI) como: "Medidas y controles que se toman para negar el acceso no autorizado de personas a información derivada de las telecomunicaciones y augurar la autenticidad de tales telecomunicaciones".

Se incluyeron cuatro áreas como partes de las actividades de seguridad COMSEC y son:

1. Criptoseguridad.
2. Seguridad de transmisiones.
3. Seguridad de emisiones.
4. Seguridad física.

La seguridad en COSMEC incluyó dos atributos los cuales son: *Confidencialidad y Autenticación.*

La *confidencialidad* consiste en asegurar que la información no sea divulgada a personas, procesos o dispositivos no autorizados.
La *Autenticación* es la medida de seguridad diseñada para establecer la validez de una transmisión, mensaje o remitente, o un medio para verificar la autorización de un individuo para recibir categorías específicas de información (verificación de emisor).

En los 80's con el crecimiento de las computadoras personales se inició una nueva era: Computación personal y la seguridad aplicada a este campo (COMPUSEC), ésta fue definida por NSTISSI como: *"Medidas y controles que aseguran la confidencialidad,*

integridad y disponibilidad de sistemas de información incluyendo hardware, software, firmware e información que está siendo procesada, almacenada y comunicada".
COMPUSEC introdujo dos atributos de seguridad adicionales, los cuales son: *Integridad y Disponibilidad.*

La *Integridad* es la calidad de un sistema de información que refleja el correcto funcionamiento y confiabilidad del sistema operativo, la coherencia del hardware y software que implementan los sistemas de protección y la consistencia de las estructuras de datos de la información almacenada.

La *Disponibilidad* se refiere al acceso oportuno y confiable a datos y servicios de información para usuarios autorizados.
Finalmente en los 90's, las dos eras de la información, COMSEC y COMPUSEC, fueron integradas para formar Seguridad en Sistemas de Información (INFOSEC); ésta incluyó los cuatro atributos: Confidencialidad, Autenticación, Integridad y Disponibilidad, pero también se agregó un nuevo atributo: No repudio (non repudiation).

El *No repudio (rendición de cuentas)* consiste en asegurar que el remitente de la información es provisto de una prueba de envío y que el receptor es provisto de una prueba de la identidad del remitente, de manera que ninguna de las partes puede negar el proceso de dicha información.

Seguridad de la información y las WLAN

La NSTISSI define el concepto de Seguridad de Sistemas de información como *"la protección de los sistemas de información contra el acceso no autorizado o la modificación de la información, ya sea en el medio de almacenaje, procesamiento o tránsito y contra la negación de servicio a los usuarios autorizados, o la provisión de servicio a usuarios no autorizados incluyendo las medidas necesarias para detectar, documentar y contabilizar esas amenazas"*.

Por ello, la seguridad inalámbrica se presenta desde el punto de vista de la "seguridad de los sistemas de información" o INFOSEC.

6.5.2 Implementación de los atributos de seguridad

El modelo de referencia OSI (Interconexión abierta de sistemas), creado por la ISO (organización internacional de estándares), es una descripción abstracta para el diseño de protocolos de redes de computadoras. El modelo divide las diferentes funciones de comunicación en siete capas que pueden funcionar de manera independiente una de otra.

Los estándares de redes inalámbricas se refieren normalmente a las capas 1 y 2 de la pila de protocolos OSI, conservando el paquete IP sin cambios. Los paquetes IP transportan sobre protocolos del nivel físico y de enlace de datos que son específicamente de carácter inalámbricos. Por ejemplo si se considera la "confidencialidad del tráfico de datos" entre dos puntos de acceso, se pueden lograr resultados similares (protección de la información) actuando en tres capas diferentes:

1. La capa de aplicación (mediante Transport Layer Security/Secure Sockets Layer).
2. La capa IP (mediante IPSEC).
3. La capa de enlace (mediante cifrado).

Hay que recordar que cuando se habla de seguridad inalámbrica, sólo se están examinando los mecanismos de seguridad concernientes a las capas 1 y 2, es decir, del cifrado nivel de enlace. Otros mecanismos de seguridad presentes a nivel 3 y superiores son parte de la seguridad implementada en las capas de red o de aplicación.

- **Cifrado a nivel de enlace**: El cifrado en el nivel de enlace es el proceso de asegurar los datos cuando son transmitidos entre dos nodos sobre el mismo enlace físico (puede ser también el caso de dos enlaces diferentes mediante un repetidor, ejemplo

un satélite). Con cifrado a nivel de enlace, cualquier otro protocolo o aplicación de datos que se ejecuta sobre el enlace físico queda protegida de cualquier intercepción.

El cifrado requiere una clave secreta compartida entre las partes en contacto y un algoritmo previamente acordado. Cuando el transmisor y receptor no comparten un medio de transporte de datos en común, los datos deben ser descifrados y nuevamente cifrados en cada uno de los nodos en el camino al receptor.
El cifrado en el nivel de enlace se usa en caso de que no se aplique un protocolo de mayor nivel.

- **Cifrado a nivel de enlace en el estándar IEEE 802.11:** El algoritmo de cifrado mejor conocido para el estándar IEEE 802.11 es el llamado en inglés Wired Equivalent Privacy (WEP). Está Probado que WEP es inseguro, y otras alternativas, como el protocolo WiFi Protected Acces (WPA), es considerado como el estándar recomendado. El nuevo estándar IEEE 802.11i incluye una extensión de WPA, llamada WPA2.

El cifrado a nivel de enlace no provee **seguridad de extremo a extremo,** fuera del enlace físico y sólo debe ser considerada una medida adicional en el diseño de la red. Este cifrado requiere más recursos de hardware en los puntos de acceso y medidas especiales de seguridad en la administración y distribución de claves.

6.5.3 Servicios de seguridad en redes inalámbricas

6.5.3.1 Confidencialidad

La confidencialidad en las redes inalámbricas es de suma importancia debido a que los datos que viajan en un medio poco seguro o no seguro requiere de mecanismos que garanticen de manera satisfactoria la transmisión de datos, por ello existen protocolos de seguridad diseñados para este tipo de transmisión los cuales son WEP, WPA y WPA2.

- **WEP o no WEP:** Se define la confidencialidad en redes inalámbricas como el acto de asegurar que la información transmitida entre los puntos de acceso y los clientes no sea revelada a personas no autorizadas. La confidencialidad debe asegurar que, ya sea la comunicación entre un grupo de puntos de acceso en un sistema de distribución inalámbrico (WDS por sus siglas en inglés), o bien entre un punto de acceso (AP) y una estación o cliente, se conserva protegida contra intercepciones.

  La confidencialidad en redes inalámbricas ha sido asociada tradicionalmente con el término "privacidad equivalente a enlaces alambrados" o WEP, el cual fue parte del estándar IEEE 802.11 original, de 1999.

  El propósito del WEP fue brindar, a las redes inalámbricas, un nivel de seguridad comparable al de las redes alambradas tradicionales. La necesidad de un protocolo como WEP fue obvio, las redes inalámbricas usan ondas de radio y son más susceptibles de ser interceptadas.

  La vida del WEP fue muy corta, debido a un mal diseño y por ser poco transparente condujo a ataques muy efectivos o a su implantación y tan sólo unos meses de que el WEP fuera publicado, el protocolo fue considerado obsoleto. Aunque la llave que tenía era de longitud limitada por las restricciones de exportación, se pudo comprobar que el protocolo era débil independientemente de ese hecho.
  No fueron sólo las fallas de diseño las que hicieron que WEP fuera obsoleto, sino también la falta de un sistema de manejo de claves como parte del protocolo, de manera que WEP no tuvo incluido sistema alguno de manejo de claves, así que, el sistema de distribución de claves fue tan simple como teclear manualmente la misma clave en cada dispositivo de la red inalámbrica.

WEP fue seguido por varias extensiones de carácter propietario que resultaron también inadecuadas, por ejemplo WEP+ de Lucent, y WEP2 de Cisco.

WEP y sus extensiones (WEP+, WEP2) son al día de hoy obsoletas. WEP está basado en el algoritmo de cifrado RC4, cuyas implementaciones en el estándar IEEE 802.11 se consideran inadecuadas debido a que es un protocolo vulnerable contra ataques a sus mecanismos de seguridad violando la privacidad, autenticidad e integridad de la información.

Existen varios ataques y programas para hacer sucumbir el WEP (Airsnort, wepcrack, kismac, y aircrack entre otros). Algunos de los ataques están basados en la limitación numérica de los vectores de inicialización del algoritmo de cifrado RC4, o la presencia de la llamada "debilidad IV" en un datagrama.

- **WPA y WPA2:** Luego del deceso del WEP, en 2003 se propone el Acceso Protegido a Wi-Fi (WPA, por sus iniciales en inglés) quedando certificado como parte del estándar IEEE 802.11i, con el nombre de WPA2 (en el 2004) WPA y WPA2 son protocolos diseñados para trabajar con y sin un servidor de manejo de claves. Si no se usa un servidor de claves, todas las estaciones de la red utilizan una "llave previamente compartida" (PSK – Pre-Shared-Key). El modo PSK se conoce como WPA o WPA2 – Personal.

  Por otra parte, mientras se emplea un servidor de claves, al WPA2 se le conoce como WAP2 – Corporativo (o WPA2 - Enterprise). En el WPA2 se usa un servidor IEEE 802.1x para distribuir las claves.
  Una mejora notable en el WPA sobre el antiguo WEP es la posibilidad de intercambiar claves de manera dinámica mediante un protocolo de integridad temporal de claves (TKIP – Temporal Key Integrity Protocol).

- **WPA2 – Acceso protegido a Wi-Fi:** WPA2 es la versión certificada de WPA y es parte del estándar IEEE 802.11i.

  Hay dos cambios principales en WPA2 y WPA, los cuales son:

  1. El reemplazo del algoritmo Michael por un código de autenticación conocido como el protocolo "Counter-Mode/CBC-Mac" (CCMP), que es considerado criptográficamente seguro.
  2. El reemplazo del algoritmo RC4 por el "Advanced Encryption Estándar (AES)" conocido también como Rijndael.

Se recomienda para la confidencialidad de datos que:

- Si se necesita confidencialidad mediante el cifrado a nivel de enlace, la mejor opción es WPA2 en modo corporativo (WPA2-Entreprise)
- En caso de usarse una solución más simple como la WPA2-Personal, deben tomarse precauciones especiales al escoger una contraseña (clave pre-compartida, PSK).

  Por lo tanto, el protocolo WEP y sus variantes WEP+ y WEP2, deben ser descartados.

6.5.3.2 Autenticación

En el caso de las redes LAN, la autenticación es la medida diseñada para establecer la validez de una transmisión entre puntos de acceso y/o estaciones inalámbricas. En otros términos, la autenticación inalámbrica significa "el derecho a enviar hacia y mediante el punto de acceso".

Para entender la "Autenticación" en redes inalámbricas es necesario entender qué sucede en el inicio de la sesión de comunicación entre un punto de acceso y una estación inalámbrica. El inicio de una comunicación comienza por un proceso llamado "asociación."

Cuando el estándar IEEE 802.11b fue diseñado, se introdujeron dos mecanismos de "asociación":

1. *Autenticación abierta:* Implica la **NO** seguridad y cualquiera puede hablarle al punto de acceso.

Por ejemplo; la firma Lucent Tecnhologies desarrolló en el año 2000 una variación del esquema de Autenticación abierta llamado "red cerrada". Las redes cerradas se diferencian del estándar 802.11b en que el punto de acceso no difunda periódicamente las llamadas "Tramas Baliza" o "Beacon Frames".

Evitar la publicación de la SSID implica que los clientes de la red inalámbrica necesitan saber de manera previa qué SSID´s deben asociar con un punto de acceso. Esta cualidad ha sido implantada por muchos fabricantes como una mejora de "seguridad".

2. *Autenticación con clave compartida:* Se comparte una contraseña entre el punto de acceso y la estación cliente.

Por ejemplo: La autenticación con clave compartida implementada en WEP es obsoleta. Varios ataques tipo texto plano, versus texto cifrado, pueden vulnerar la Autenticación basada en WEP. Debido al hecho de que la clave de cifrado y Autenticación son el mismo secreto compartido, una vez que una resulta comprometida, la otra también.

Filtrado de direcciones MAC como medida de seguridad

El filtrado de direcciones MAC utiliza esta dirección para identificar qué dispositivos pueden conectarse a la red inalámbrica. Cuando un cliente inalámbrico intenta conectarse envía la información de la dirección MAC. Si está activado el filtrado MAC, el router inalámbrico buscará la dirección MAC en una lista preconfigurada, de manera que sólo los dispositivos MAC pregrabados en la base de datos podrán conectarse, y si la dirección MAC no se encuentra en la base de datos, el dispositivo no podrá conectarse ni comunicarse a través de la red inalámbrica.

Existen algunos problemas con este tipo de seguridad, por ejemplo: se requiere que se incluyan en una base de datos las direcciones MAC de todos los dispositivos que tendrán acceso a la red antes de que se intente la conexión. Por

lo tanto, no podrá conectarse un dispositivo que no esté identificado en la base de datos; pero es posible que el dispositivo de un atacante clone la dirección MAC de otro dispositivo que tenga el acceso.

6.5.3.3 Integridad de datos en redes inalámbricas

Se define a la integridad de datos como la capacidad de un protocolo inalámbrico para determinar si la información transmitida ha sido alterada por personas no autorizadas.

En 1999 el protocolo WEP buscó proveer integridad de tráfico de datos, pero desafortunadamente el mecanismo de integridad seleccionado el cual fue CRC (Código de Redundancia Cíclica), resultó inseguro. El diseño fallido de WEP permite la alteración del código CRC del tráfico, sin la necesidad de saber la llave WEP, es decir que el tráfico puede ser alterado sin que se note.

Los protocolos WPA y WPA2 resolvieron el problema de la integridad de datos en WEP mediante la inclusión de un mensaje de código de autenticación más seguro y la inclusión de un contador de segmentos (frames), que previene los "ataques por repetición" (replay attack). En un ataque de repetición el atacante registra la conversación entre un cliente y un punto de acceso para obtener un acceso no autorizado. Al responder una conversación "antigua" el atacante no necesita saber la clave secreta WEP.

Por lo tanto se recomienda que se implemente WPA o WPA2 para lograr integridad de datos inalámbrica mediante el cifrado en la capa de enlace.
WPA fue diseñado como un paso intermedio hacia WPA2 (estándar IEEE 802.11i). WPA sólo incluye un subconjunto de las características del estándar IEEE 802.11i y se enfoca en preservar la compatibilidad con adaptadores que funcionan con el estándar IEEE 802.11b.

WPA abordó las fallas encontradas en WEP e incrementó la longitud y el número de las claves en uso, así mismo, agregó un nuevo mensaje de código de autenticación.

6.5.3.4 Disponibilidad en redes inalámbricas

Se define disponibilidad como la capacidad de la tecnología que asegura un acceso confiable a servicios de datos e información para usuarios autorizados, cada que se requiera y cuantas veces sea necesario.

Se considera que no es tan sencillo detener a alguien que busca interferir con su señal de radio ya que las redes inalámbricas operan en canales predefinidos que cualquiera puede usar para enviar señales de radio. Por ello, la prevención de la interferencia por parte de los usuarios no autorizados es prácticamente imposible. Lo único que se puede hacer es monitorear cuidadosamente los enlaces para identificar las fuentes potenciales de interferencia.

Negación de servicio

Las redes inalámbricas son vulnerables a los ataques de Negación de servicio mediante interferencia de radio. Se considera un escenario donde otro operador de red decide configurar sus dispositivos de radio en el mismo canal en el que opera una red.
Para evitar esta clase de ataques, intencionales o no, se debe considerar el rastreo periódico de frecuencias de radio y para evitar la interferencia con otras redes, no hay que sobrecargar la potencia de los enlaces.

Existen varias razones para que un enlace se desempeñe de manera deficiente o no esté disponible, por ejemplo, la presencia de nodos escondidos puede afectar el desempeño de la familia de protocolos IEEE 802.11. Virus, software de intercambio de archivos, “spam”, etc., pueden inundar la red con tráfico y

limitar el ancho de banda disponible para las conexiones autorizadas a servicios legítimos.

6.5.3.5 No repudio (rendición de cuentas)

La familia de estándares IEEE 802.11 no se hace cargo de la "rendición de cuentas" en el tráfico de datos. Los protocolos inalámbricos no tienen un mecanismo para asegurar que el emisor de datos tenga una prueba de envío de la información y que el receptor obtenga una prueba de la identidad del emisor.

En este sentido, cabe destacar que el no repudio es un servicio de seguridad que ofrece protección a un usuario frente a otro que rechace haber realizado cierta emisión de datos o niegue la recepción de un mensaje que le haya sido enviado; esta protección se efectúa por medio de una colección de evidencias irrefutables que regularmente son colectadas por los dispositivos que procesan la transmisión de los datos.

6.5.4 Principales amenazas de seguridad en redes inalámbricas

Resulta interesante conocer el tipo de amenazas a las que se enfrentan las organizaciones hoy en día, por ello en la tabla 6.2 se presentan las principales amenazas de seguridad más relevantes en redes inalámbricas con algunas recomendaciones para cada una de éstas.

Tabla 6.3 Las 10 amenazas más relevantes

	Tipo de Amenaza	Descripción	Solución
1	**Confidencialidad**	Riesgo de interferencia, usuarios no autorizados pueden obtener acceso al tráfico de datos en su red.	- Usar cifrado en la capa de enlace en sus enlaces inalámbricos (WPA2). - Recomendar a sus usuarios el uso de "cifrado" en protocolos de alto nivel (SMTP seguro,

			HTTPS).
2	**Confidencialidad**	Riesgo de arrebato de tráfico y riesgo de un ataque tipo de intermediario.	- Recomendación 1 + - Monitorear la SNR, la SSID y la dirección MAC de su conexión.
3	**Autenticación**	Riesgo de acceso no autorizado a la red inalámbrica	- Implementar IEEE 802.1X (WPA2). - No depender solo de un esquema de autenticación basado en direcciones MAC. - No publicar la SSID.
4	**Autenticación**	Riesgo de acceso no Autorizado a la red inalámbrica y a Internet.	- Implementar IEEE 802.1X - Implementar un portal cautivo.
5	**Integridad**	Riesgo de alteración de tráfico en la red inalámbrica.	- Se recomienda a los usuarios el uso de cifrado en las capas superiores (HTTPS, SMTP seguro). - Usar cifrado en el enlace inalámbrico.
6	**Disponibilidad**	Riesgo de interferencia. Negación de servicio (Congestionamiento)	- Monitorear periódicamente el espectro de radio. - No sobrecargar la potencia de los enlaces.
7	**Disponibilidad**	Riesgo de no disponibilidad de ancho de banda debido a retransmisiones de radio	- Buscar nodos ocultos y fuentes de interferencia- - Monitorear retransmisiones de capa de enlace en puntos de acceso.
8	**Disponibilidad**	Riesgo de no disponibilidad de ancho de banda debido a software malicioso	- Monitorear tráfico IP, especialmente de tipo ICMP y UDP. - Incluir detectores de intrusión.
9	**Autenticación**	Riesgo de acceso no	- Implementar la red inalámbrica fuera de algún firewall.

	Rendición de cuentas	autorizado a Internet.	- Implementar una red privada virtual y permitir conexiones solo vía el concentrador VPN.
10	**(Acceso a la red) Rendición de cuentas**	Riesgo de uso no autorizado de recursos de la red.	- Implementado en IEEE 802.1X - Implementar un portal cautivo basado en firmas digitales.

Es importante generar conciencia sobre la necesidad que existe hoy en día para mantener protegida la información que se encuentra almacenada en los equipos de cómputo. Ya que si bien es cierto, la cantidad de usuarios de Internet ha aumentado considerablemente según un estudio publicado por AMIPCI (Asociación Mexicana de Internet), el cual revela que del año 2007 al 2009 hubo un incremento de internautas de 21.6 millones a 22.7 millones (únicamente tomando en cuenta la zona urbana).[28] Por ello, los usuarios deben conocer las principales amenazas a las que se está expuesto y sobre todo, tener las herramientas que permitan mitigar cualquier anomalía que se pueda presentar.

6.6 Seguridad en bases de datos

Actualmente las bases de datos son herramientas que se utilizan en cualquier aplicación basada en web permitiendo que la interfaz de estos sean dinámicos. Debido a que la información que resulta ser sensible o secreta puede ser almacenada en una base de datos, se vuelve muy importante el hecho de mantenerlas protegidas.

Se define a una base de datos como una serie de datos organizados y relacionados entre sí, los cuales son recolectados y explotados por los sistemas de información de una empresa o negocio en particular.

[28] http://estudios.amipci.org.mx:8080/mashboard/main.jsp

Entre las principales características de los sistemas de base de datos se pueden mencionar las siguientes:

- Independencia lógica y física de los datos
- Redundancia mínima
- Acceso concurrente por parte de múltiples usuarios
- Integridad de los datos
- Consultas complejas optimizadas
- Seguridad de acceso y auditoría
- Respaldo y recuperación
- Acceso a través de lenguajes de programación estándar

6.6.1 Sistema de Gestión de Base de Datos (SGBD)

Los sistemas de gestión de bases de datos (DataBase Managemen System) son un tipo de software muy específico, dedicado a servir de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan. Se compone de un lenguaje de definición de datos, de un lenguaje de manipulación de datos y de un lenguaje de consulta.

Las bases de datos (BDs) nacen con el fin de resolver las limitaciones que en algunos casos presentan los ficheros para el almacenamiento de la información. En los entornos de bases de datos, las diferentes aplicaciones y usuarios utilizan un único conjunto de datos integrado a través de un Sistema de Gestión de Bases de Datos (SGBD). De esta manera se pueden resolver problemas como duplicación de información, inconsistencia de los datos y dependencia entre programa estructura de datos.

Para conseguir un entorno de bases de datos seguro se deben de identificar las amenazas reales así como la adecuada elección de políticas de seguridad que ayuden a establecer mecanismos de prevención como por ejemplo; métodos que comprueben que no se han producido accesos ilícitos.

Una amenaza contra la seguridad de las bases de datos es un agente hostil que puede difundir o modificar información gestionada por el SGBD sin la debida autorización. Las amenazas contra la seguridad se clasifican en:

- **Accidentales:** Pueden ser errores de hardware o software y fallos humanos.
- **Fraudulentas:** Son realizadas intencionalmente por usuarios no autorizados.

Las violaciones que puede sufrir un entorno de bases de datos consisten en lecturas, modificaciones y borrado de datos. Las consecuencias son:

- Difusión de información confidencial
- Modificación no autorizada de datos
- Denegación de servicio a usuarios

6.6.2 Confidencialidad de la BD

En primer lugar el sistema de BD debe identificar y autenticar a los usuarios, además el administrador deberá especificar los privilegios de cada uno sobre los objetos, por ejemplo; utilizar una BD, consultar ciertos datos o actualizarlos.

Para facilitar la administración de los SGBD se suelen incorporar el concepto de perfil, rol o grupo de usuarios que agrupa una serie de privilegios por lo que el usuario que se asigna a un grupo hereda todos los privilegios del grupo.
Por lo tanto, el mecanismo de control de acceso se encarga de denegar o conceder el acceso a los usuarios.

Existen 3 tipos de autorización y son:

1. **Autorización Explícita vs. Implícita:** La primera consiste en almacenar qué sujetos pueden acceder a ciertos objetos con determinados privilegios. La segunda consiste en que una autorización definida sobre un objeto puede deducirse a partir de otras.

2. **Autorización Fuerte vs. Débil:** En la fuerte no se pueden invalidar las autorizaciones implícitas mientras que en la débil se permiten excepciones sobre ellas.
3. **Autorización Positiva vs. Negativa:** La primera indica la existencia de autorización y la segunda indica la denegación de una autorización.

El tipo de autorización que se adopte dependerá entre otras cosas de las políticas de control y de los modelos de datos.
Un punto importante a considerar es que con el cifrado también se obtiene confidencialidad.

6.6.2.1 Deducción de información confidencial de una BD

Las BDs como almacén de gran cantidad de información estructurada pueden ser víctimas de accesos no autorizados con el fin de difundir información confidencial. Existen dos formas de obtener datos de manera ilegal:

1. Consiste en deducir información confidencial utilizando datos que son accesibles (interferencia).
2. La información secreta se consigue combinando varios datos no confidenciales (agregación).

Para proteger las BD de inferencias es conveniente conocer la información de la que se vale el atacante. Dicha información es dependiente de la BD y la aplicación es difícil de obtener. Una regla básica a aplicar es que *el SGBD no debe proporcionar información adicional al atacante.* Así mismo, la BD debe estar organizada de manera que no ayude al atacante, para esto se ha de identificar para cada BD la información a proteger y ajustar los niveles de seguridad requeridos.

Existe otro tipo de deducción y es la *inferencia estadística*, este tipo de deducción se realiza al intentar acceder a las bases de datos estadísticas con el

propósito de obtener datos individuales. Estas bases de datos mantienen información sobre grupos de individuos y deben ser sólo accesibles a través de operaciones estadísticas por ejemplo; media, varianza, entre otros. Sin embargo programadores hábiles pueden intentar acceder a la información individual. Para evitar esto existen dos tipos de protección:

- **Perturbación de los datos:** Se realiza directamente sobre la información protegida. Una vez que se ha identificado y agrupado la información que es considerada de carácter confidencial se reemplazan los datos reales por microestadísticas que conservan el valor global de la BD sin almacenar datos privados. También es posible hacer alteraciones aleatorias entre las tuplas.
- **Control de las preguntas:** La mayor parte de los controles de este tipo se basa en el número de registros a devolver como respuesta a la pregunta. La idea consiste en satisfacer únicamente demandas de información cuyo resultado se encuentra entre unos límites de tamaño con el objetivo de que no se pueda inferir información individual. Esto, aunque ideal, se traduce en un proceso caro y difícil de manejar. Por ejemplo se podría pedir a una BD que nos diese la media de sueldos de los trabajadores de una plantilla (poniendo restricciones: gafas, barba y número de hijos, entre otras.) si sólo hay uno ya se sabe el valor. Pero resulta que la limitación de devolver datos estadísticos si el conjunto al que se refiere es menor que N tampoco es la solución. No lo es porque la combinación de preguntas puede permitir el deducir cosas. Así, si hay 2N empleados siempre se pueden hacer otras preguntas que vayan refinando la información (dame el sueldo de toda la plantilla menos el director) y obtener los valores de los otros 2N-1.

6.6.3 Disponibilidad de la BD

Los SGBD deben asegurar la disponibilidad de los datos a aquellos usuarios que tienen derecho a ello, por lo que proporcionan mecanismos que permiten recuperar las bases de datos contra fallos lógicos o físicos que destruyan la información.

Por lo tanto es conveniente contar con facilidades ajenas al SGBD como, por ejemplo, máquinas tolerantes a fallos, sistemas de alimentación ininterrumpida, entre otros.

Se vuelve importante asegurar la consistencia de los datos tras realizar cambios a la base de datos, para ello, se crean transacciones; éstas se encuentran en un estado consistente antes de que se comience a ejecutar una transacción y también lo deberá estar cuando la transacción termine. Las propiedades principales que debe poseer una transacción son; atomicidad, preservación de la consistencia, aislamiento y persistencia.

- **Atomicidad:** La atomicidad de una transacción garantiza que todas sus acciones sean realizadas o ninguna sea ejecutada, por ejemplo, en el caso de una transacción bancaria o se ejecuta tanto el "depósito-deducción" o ninguna acción será realizada.
- **Preservación de la consistencia:** Muy similar a la "atomicidad", la consistencia garantiza que las que hayan sido declaradas para una transacción sean cumplidas, por ejemplo, (con respecto a una transacción bancaria), suponiendo que cada vez que se realice una transferencia interbancaria de $100,000 sea necesario notificar a la sucursal del tarjeta habiente, si no es posible comunicarse y actualizar la información en la sucursal del cliente, toda la transacción será abortada.
- **Aislamiento:** Garantiza que las transacciones que se estén realizando en el sistema sean invisibles a todos los usuarios hasta que éstas hayan sido declaradas finales. Tomando en cuenta el ejemplo anterior, en la transacción bancaria es posible que el sistema esté programado para intentar en 5 o 10 ocasiones más antes de abortar una transacción por completo, a pesar que este último paso no ha sido finalizado, ya existen otras modificaciones en el sistema, este aislamiento garantiza que los usuarios del sistema no observen estos cambios intermedios hasta que sea finalizada la última acción de actualización.
- **Persistencia:** La durabilidad de una transacción garantiza que al instante en el que se finaliza la transacción ésta perdure a pesar de otras consecuencias, esto es,

si el disco duro falla, el sistema aún será capaz de recordar todas las transacciones que han sido realizadas en el sistema.

Para conseguir anular y recuperar transacciones, el método más extendido suele ser la utilización de un fichero denominado diario (log) en el que se va guardando toda la información necesaria para deshacer o rehacer las transacciones. Normalmente se obliga a que los registros que se modifican se escriban antes en el fichero diario que en la base de datos, para poder anular así, en caso de necesidad, las transacciones y evitar problemas.

Cabe mencionar que si bien los logs son una herramienta de apoyo para la seguridad de la información dado que permiten identificar el tipo de operación realizada sobre las bases de datos, la fecha de realización, el usuario o proceso responsable de dicha acción, entre otros; puede tornarse en un lastre si no se configuran correctamente, esto es, se vuelve necesario realizar un análisis de riesgos a fin de determinar las posibles amenazas a las bases de datos y con base en ello el tipo de información que se debe almacenar en los logs, por otra parte, decidir que todo debe guardarse atenta contra la capacidad de almacenamiento del sistema para este fin, por ejemplo, cuando una contingencia se presenta, se recurre a la revisión de los logs para deslindar responsabilidades y determinar la fuente del ataque, pero el hecho de tener que revisar grandes volúmenes de información sin saber con certidumbre qué buscar, ni en donde, resulta ser un trabajo sin beneficio alguno, provocando así que los ataques se vuelvan a llevar a cabo ya que no se sabe con certeza el origen de éste.

Por otra parte, en la disponibilidad de la BD se puede recurrir a la recuperación de ésta de dos formas:

1. **Recuperación en caliente:** Al ocurrir un fallo que dé lugar a la pérdida de memoria volátil, es preciso realizar la operación de recuperación en caliente, en la que el sistema consulta el fichero diario para determinar las transacciones que hay que deshacer y rehacer.

2. **Recuperación en frío:** En caso de un fallo de memoria secundaria que afecte a la base de datos, se lleva a cabo una recuperación en frío, que consiste en utilizar una copia de seguridad de la BD. La copia de seguridad permitirá, junto con los ficheros diarios que se han ido produciendo desde que se realizó, llevándola de forma consistente a la situación anterior a que se produjera el fallo.

El *error fatal* se produce cuando se pierde el fichero diario grabado en un soporte. En este caso resulta imposible recuperar la base de datos a su estado actual. La mejor solución para evitar este problema es la que ofrecen algunos SGBD, que permiten la gestión de copias de fichero diario en dispositivos independientes, también se puede duplicar la base de datos. En general todas las técnicas de duplicación se conocen como espejo o duplexación.

La técnica espejo requiere de dos servidores de bases de datos que estén comunicados entre sí. En la figura 6.14 se observa la idea básica que muestra dos bases de datos, una primaria y un espejo o copia de la primaria. La primaria es la base de datos operativa sobre la que se ejecutan todas las transacciones, sin embargo a través de procesos automatizados hay un envío constante de los archivos de la bitácora a la base de datos espejo de tal forma que al ocurrir una falla que ponga fuera de operación a la base de datos primaria, se habilite la espejo de forma transparente para los usuarios.

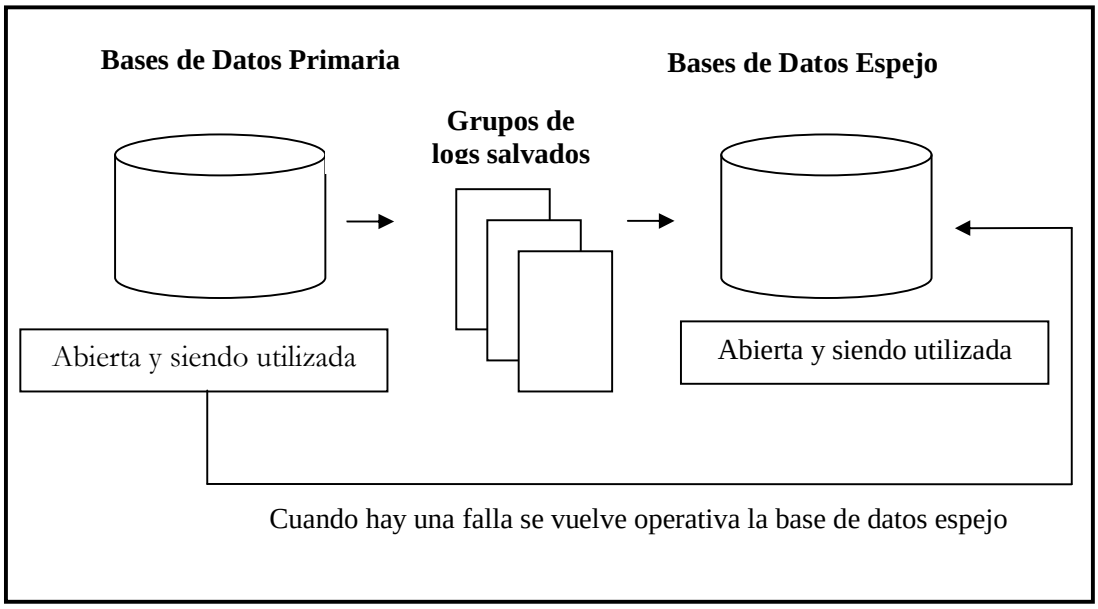

Figura 6.14 Bases de datos espejo

Este ambiente es de alta inversión ya que se necesitan, al menos, dos servidores con las mismas características para albergar las dos bases de datos iguales y una red eficiente que garantice la comunicación 7x24 entre ambos equipos ya que, de otra forma, al haber una falla se estaría igual que en un ambiente normal.

6.6.4 Integridad de la BD

Las vulnerabilidades de la integridad de la BD permiten la modificación, adición o borrado de información de la BD. La integridad se debe garantizar también frente a errores del sistema, virus y sabotajes que puedan dañar los datos almacenados. Este tipo de protección se consigue mediante controles del sistema apropiados, procedimientos de respaldo y recuperación así como procedimientos de seguridad *ad hoc.*

En general se pueden diferenciar dos peligros que requieren tratarse de diferente forma. Por una parte se tiene el problema de la consistencia de los datos debido a errores en el

sistema y por otra los usuarios que pretenden realizar modificaciones no autorizadas en la BD.

Por lo tanto el SGBD debe mantener la consistencia de los datos incluidos en la BD frente a los peligros como la caída del sistema y bloqueo mutuo entre procesos que realizan accesos concurrentes.

Los accesos para realizar modificaciones en la BD son tareas delicadas que la puede dejar inconsistente, por ejemplo, si mientras se está modificando un registro de la BD hay un corte de fluido eléctrico, no se puede tener la seguridad de que se haya quedado grabado en la BD.

Para mantener la consistencia, la SGBD trabaja con **transacciones,** que son unidades de programa que realizan una única función lógica en una aplicación de la BD. Estas transacciones deben de cumplir dos requisitos:

1. Ser atómicas, es decir, todas las operaciones asociadas a una transacción deben ejecutarse por completo o ninguna de ellas.
2. Deben ser correctas, es decir, cada transacción debe ser un programa que conserve la consistencia de la BD.

Por lo tanto, si se produce algún incidente durante la ejecución de una transacción que deje la BD inconsistente, el SGBD debe recuperar el estado previo a dicha transacción.

Los procedimientos de respaldo y recuperación tienen cómo objetivo recuperar un estado anterior de la BD. Para ello, mantienen en un fichero (fichero LOG o bitácora de la BD) información sobre las transacciones que se realizan. Si por cualquier razón se detecta que se pierde la consistencia en la BD el sistema de recuperación deshace las modificaciones realizadas por las últimas transacciones hasta dejar la BD consistente.

Para asegurar la integridad operativa de la BD se ha de controlar la consistencia lógica de los datos cuando se producen transacciones concurrentes. Por ejemplo, cuando un agente desea modificar un registro mientras otro lo está leyendo. Cuando se pueden producir accesos simultáneos a un mismo objeto de la BD la práctica común consiste en bloquear el objeto accedido al tiempo que dure la operación y liberarlo una vez completada.

En cuanto a los intentos de acceso no autorizados para de modificar las BD, las políticas de integridad se basan en limitar los privilegios a los usuarios en cada momento, de tal forma que cada usuario sólo pueda acceder a los datos que precisa para su trabajo, utilizando únicamente las operaciones estrictamente necesarias, por ejemplo:

- Limitar el número de intentos de acceso
- Bloquear la cuenta o el permiso para acceder a la BD si se alcanza el límite máximo de intentos de acceso permitido.
- Enviar una alerta al administrador de la BD

Las restricciones de privilegios no sólo se aplican a departamentos dentro de una organización, sino también a grupos de usuarios con tareas comunes. Una mejora para realizar esto de forma ordenada consiste en utilizar los roles que permiten agrupar usuarios que comparten los mismos privilegios.

Así, el SGBD puede controlar fácilmente las actividades de los usuarios y detectar los cambios en los privilegios otorgados a cada rol (así como se muestra en la figura 6.15). Además, el administrador de la BD puede fácilmente modificar los privilegios a grupos de usuarios cambiando un único rol.

Roles	**Actualizar registro**	**Borrar registro**	**Añadir registro**
Personal	**X**	**X**	**X**
Contabilidad	**X**		
Dirección	**X**	**X**	

Privilegios	**Personal**	**Contabilidad**	**Dirección**
Julen	X		
Martha			**X**
Martín		**X**	

Figura 6.15 Ejemplo de control de acceso basado en roles

6.6.5 Mecanismo de seguridad en SGBD

El SGBD juega un papel crucial en cuanto a la seguridad en una organización. El sistema operativo debe proporcionar ciertos mecanismos de protección básicos; por ejemplo, el sistema operativo ha de garantizar la identidad del usuario y la protección de los ficheros físicos sobre los que está soportada la BD. Por otra parte, el SGBD debe hacerse cargo de restricciones de seguridad dependientes de las aplicaciones y los requerimientos de seguridad principales deben hacer frente a los siguientes aspectos:

a) Acceso a diferentes niveles de gradualidad: En un entorno de BD se puede acceder a los datos a diferentes niveles (BD, colección de relaciones, una relación, conjunto de columnas de una relación, algunas filas de una relación). El SGBD debe establecer controles de acceso a cada nivel de gradualidad.

b) Varios modos de acceso: Los controles de acceso deben ser distintos según la operación a realizar. Por ejemplo; select, insert, update, delete en sql.

c) Diferentes tipos de control de acceso: El acceso se puede regular mediante diferentes tipos de controles: control basado en el nombre del objeto a acceder, control basado en el contenido del objeto a acceder, control dependiente del contexto (ejemplo; permitir o denegar el acceso dependiendo de ciertas variables de entorno como el día, hora o terminal), control dependiente de los procedimientos auxiliares.

d) Autorización dinámica: El SGBD debe ser capaz de modificar las autorizaciones de los usuarios dinámicamente mientras la BD sea operativa.

e) Protección multinivel: Con este método se etiqueta cada objeto de la BD con un nivel de seguridad. Teniendo en cuenta los diferentes niveles de gradualidad dentro de una BD, se puede tener una relación etiquetada con un nivel de seguridad y los atributos de dicha relación tienen su propio nivel de seguridad.

e) Auditoría: Los eventos importantes o sospechosos que se produzcan durante operaciones con la BD deben ser almacenados para su posterior análisis en busca de acciones no autorizadas. Las secuencias de acciones realizadas por un mismo usuario pueden ser utilizadas para detectar posibles inferencias. Esta práctica puede ser un agente disuasorio contra los usuarios que tengan malas intenciones. El

problema de la auditoría consiste en la cantidad de información que se ha de almacenar si se desea controlar las operaciones a un bajo nivel de gradualidad.

Además de estos requerimientos, el SGBD debe asegurarse de que no existan canales ocultos a través de los cuales se pueda divulgar información confidencial así cómo puertas traseras que permitan acceder a usuarios no autorizados. También se debe de controlar el flujo de la información.

Normalmente, el recurso que se utiliza para restringir el acceso a las BD son las vistas, éstas son una forma de proporcionar a cada usuario un modelo personalizado de la BD. Una vista puede ocultar al usuario los datos que no necesita ver y de la misma forma, los datos que tienen el acceso negado. El objetivo de la seguridad se logra si se dispone de un mecanismo que limite a los usuarios a utilizar vistas personales.

Otra medida de seguridad interesante es guardar las tablas de la BD y no dejarlas disponibles a terceros que puedan extraer información de su estructura que luego les sirva para realizar deducciones de la BD. La mejor forma de ocultarlas es mediante cifrado.

Finalmente, un aspecto importante a considerar en los sistemas de información es la eficiencia. Los controles de seguridad conllevan un costo computacional adicional por lo que se debe de generar un compromiso entre mantener el tiempo de respuesta de la BD en límites razonables y la BD segura.

6.7 Ética Informática

La *ética informática* se considera como la disciplina que analiza problemas éticos que son creados por la tecnología de los equipos de cómputo o también los que son transformados o agravados por la misma, es decir, por las personas que utilizan los avances de las tecnologías de la información.

Según Moor la ética informática (EI*) es el análisis de la naturaleza y el impacto social de la tecnología informática y la correspondiente formulación y justificación de políticas para*

un uso ético de dicha tecnología. La tarea de la EI es aportar guías de actuación cuando no hay un reglamento o cuando la que existe se encuentre obsoleta.

Otra definición de la ética informática según Terrel Bynum la define como *la disciplina que identifica y analiza los impactos de las tecnologías de la información en los valores humanos y sociales.* Un ejemplo de este tipo de valores son; la salud, la riqueza, el trabajo, la libertad, la democracia, el conocimiento, la privacidad, la seguridad o la autorrealización personal.

En este concepto la EI quiere incluir términos, teorías y métodos de disciplinas como la ética aplicada, la sociología de las computadoras, la evaluación social de las tecnologías o el derecho informático.
Es importante crear conciencia en nuestra sociedad sobre la tecnología informática y también ayudar a los usuarios que la utilizan, no sólo con eficiencia sino con criterios éticos, cuyo objetivo es tomar decisiones sobre temas tecnológicos de manera consistente con la afirmación de los propios valores o con los derechos humanos en general.

Para ello, esta disciplina plantea algunos objetivos:

- Determinar en qué medida son agravados, transformados o creados por la tecnología informática.
- Analizar y proponer un marco conceptual adecuado y formular principios de actuación para determinar qué hacer en las nuevas actividades ocasionadas por la informática en las que no se perciben con claridad líneas de actuación.
- Realizar análisis éticos de casos realistas y significativos.

- Para realizar lo anterior la EI pretende tener en cuenta dos aspectos:

- Utilizar la teoría ética para clarificar los dilemas éticos y detectar errores en el razonamiento ético.

- Colaborar con otras disciplinas en ese debate, siendo conscientes de los puntos de vista alternativos en las cuestiones referentes a valores y sabiendo discriminar en los distintos casos entre las consideraciones éticas y las técnicas.

6.7.1 Contenidos de la ética informática

- **Ética profesional general:** Hace referencia a problemas que son comunes a otras actividades ocupacionales, por un lado, están los criterios de moralidad personal, entendiendo como tales los criterios, obligaciones y responsabilidades personales de los profesionales. Por otro lado están los problemas interiores a la empresa: relaciones empleador – empleado, lealtad organizacional, interés público, entre otros.
- **La utilización de la información:** El principal problema es el uso no autorizado de los servicios informáticos o de la información contenida en ellos. Se plantean problemas de invasión de la privacidad, de falta de confidencialidad en la información, sobre todo de datos sensibles.
- **Lo informático como nueva forma de bien o propiedad:** Hace referencia al software informático como un bien que tiene características específicas como la piratería, el plagio, los derechos de autor, entre otros.
- **Lo informático como instrumento de actos potencialmente dañinos:** Lo informático es el medio o instrumento por medio del cual se cometen acciones que provocan daño a terceras personas. Los que proveen servicios informáticos y los que utilizan ordenadores, datos y programas han de ser responsables de la integridad y conveniencia de los resultados de sus acciones.

Se puede mencionar de las consecuencias de los errores en datos y algoritmos, los problemas que se pueden causar por la falta de protección en la seguridad de sistemas con datos sensibles o que implican riesgos en la salud de clientes, los actos de terrorismo lógico, las acciones de fanáticos, el espionaje de datos, las introducciones de virus y gusanos.

- **Dimensiones sociales de la informática:** La informática ha contribuido en el desarrollo positivo de los medios de comunicación social, las tecnologías de la información han hecho posible las comunicaciones instantáneas.

La accesibilidad, la distribución equitativa, la justicia social, el trabajo autorrealizante, el crecimiento sostenido, entre otros, son valores que están en juego en la implantación de las nuevas tecnologías.

6.7.2 Código deontológico

La deontología informática trata de la moral o la ética profesional en el manejo del activo más importante que tienen las empresas que es la información. Los profesionales de la informática y las empresas del mundo de las TIC están desarrollando código deontológico para garantizar la conducta ética en las organizaciones.

Elaborar un código de ética es una tarea laboriosa y detallista, lamentablemente muchas asociaciones profesionales y empresas creen que su tarea termina cuando consiguen presentar en sociedad un código ético propio bien elaborado mostrándose así ante sus propios países y ante la comunidad internacional como organizaciones responsables y preocupadas por la ética, sin embargo, hoy en día hay también serios intentos de hacer ver a las asociaciones profesionales que es necesario apoyar activa y continuamente a sus asociados en sus deseos de actuar con justicia en su profesión.

6.7.3 Objetivos del código deontológico

El código deontológico debe establecer las normas de comportamiento para lograr un desempeño de la profesionalidad del mayor nivel posible y dentro de las normas éticas tan necesarias en nuestra actual sociedad.

Un código deontológico intenta alcanzar los siguientes objetivos:

- Determinar las normas de comportamiento para garantizar que se utilizarán buenos modos.
- Hacer prevalecer en todo momento el interés general por delante del particular.
- Definir lo que está bien o lo que está mal.

- Configurar las actitudes mínimas exigibles.
- Canalizar la acción profesional en conformidad con el propio ideal del profesional.

Por lo tanto, el código deontológico debe cumplir las siguientes funciones:

- Servir de instrumento flexible como suplemento a las medidas legales y políticas.
- Servir como concientización pública.
- Dar identidad, estatus y una definición como profesionales.
- Servir como fuente de evaluación pública de la profesión.
- Aumentar la reputación del profesional.
- Aumentar la confianza de la gente.

6.7.4 Funciones del código deontológico

Las asociaciones de profesionales de la informática y algunas empresas relacionadas con ésta han desarrollado códigos de conducta profesional. Estos códigos tienen distintas funciones:

- El que existan normas éticas para una profesión, quiere decir que un profesional no solo es responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales.
- Sirven como instrumento flexible como suplemento a las medidas legales y políticas, ya que éstas en general van muy lentas, comparadas con la velocidad del desarrollo de las TI.
- Sirven para crear conciencia en los usuarios.
- Tienen una función sociológica ya que dan una identidad a los informáticos como grupo que piensa de una determinada manera; es símbolo de su estatus profesional y parte de su definición como profesionales.
- Sirven como fuente de evaluación pública de una profesión y es un llamado a la responsabilidad, para que la sociedad tenga conocimiento de lo que ocurre en dicha profesión.

- En las organizaciones internacionales estas normas permiten armonizar legislaciones o criterios divergentes existentes en cada país.

6.7.5 Código Deontológico de los Ingenieros Informáticos

Los códigos deontológicos de los Ingenieros informáticos, son códigos de conducta desarrollados por las asociaciones de profesionales de la informática y algunas empresas relacionadas con ésta.

Estos códigos consisten en los siguientes aspectos:

- Un informático no sólo es responsable de los aspectos técnicos del producto, sino también de las consecuencias económicas, sociológicas y culturales del mismo.
- Los códigos sirven de ayuda a los cuerpos legislativos, administrativos y judiciales.
- Sirven como concientización a los usuarios, ya que al crear normas, hace que éstos estén conscientes de los problemas y estimula un debate para designar responsabilidades.
- Es símbolo de su estatus profesional y parte de su definición como profesionales.
- Aumenta la reputación del profesional y la confianza de los usuarios.
- En las organizaciones internacionales estas normas permiten armonizar legislaciones o criterios divergentes existentes (o ausentes, en su caso) en los países individuales.

Por lo antes mencionado, se puede decir que los códigos deontológicos son un paso importante para crear conciencia en las organizaciones y en la sociedad sobre el gran avance tecnológico y de esa manera utilizar la tecnología de manera segura y eficiente puesto que cuenta ya con normas que la respaldan.

6.8 Legislación y delitos informáticos

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino también como medio eficaz para obtener y conseguir información, lo que las ha ubicado en un nuevo medio de comunicación de uso masivo, cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

Este es el panorama del nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que, la informática es hoy una forma de poder social, ya que está disponible tanto para los gobiernos como a los particulares, debido a su rapidez, así como el ahorro de tiempo y energía. Desafortunadamente los usuarios participan en una dinámica sobre lo lícito e ilícito y es ahí donde entra de manera particular el Derecho, para que regule los efectos que pueda provocar una determinada situación y exista un orden dentro de la sociedad.

Por lo antes mencionado, se sabe que los delitos relacionados con los sistemas informáticos han aumentado en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representando así una amenaza para la economía de los países y también para las sociedades. Por ello es necesario que se conozcan las legislaciones de cada país y así enfrentar de la mejor manera posible los delitos informáticos que se efectúen.

6.8.1 Delitos Informáticos

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983, *el término delito informático se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.*[29]

[29] Téllez Valdés, Julio, Derecho Informático, 3ª Ed., México, McGraw-Hill, 2004, p.163

El desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia como la manipulación fraudulenta de las computadoras con fines de lucro, así como la destrucción de programas o datos, el acceso y la utilización indebida de la información, entre otros, son algunas de las estafas relacionadas con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Desafortunadamente los delitos informáticos son difíciles de detectar debido a que los delincuentes en muchas ocasiones no dejan huella de los hechos cometidos para llevar a cabo su objetivo, en ese sentido, la informática reúne algunas características que la convierten en un medio idóneo para la ejecución de diversos delitos, en especial los de carácter patrimonial (estafas, apropiaciones indebidas, entre otros). Esto es debido a la gran cantidad de datos que se acumulan, por consiguiente resulta fácil acceder a ellos y manipularlos.

Los Delitos informáticos que se cometen con mayor frecuencia son:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, entre otros).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de los delitos convencionales (robo, homicidio y fraude).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los programas.

- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.
- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (como por ejemplo pago de rescate).
- Acceso no autorizado: Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
- Destrucción de datos: Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
- Infracción al copyright de bases de datos: Uso no autorizado de información almacenada en una base de datos.
- Interceptación de e-mail: Lectura de un mensaje electrónico ajeno.
- Estafas electrónicas: A través de compras realizadas haciendo uso de la red.
- Transferencias de fondos: Engaños en la realización de este tipo de transacciones.

Por otro lado, la red de Internet permite dar soporte para la ejecución de otro tipo de delitos, cómo lo son:

- **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
- **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

- **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
- **Otros delitos:** Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

Actualmente, los flujos de información o fuentes, como redes de información y medios de radiodifusión, han trascendido y actúan en forma débil cuando deben responder a los principios éticos y morales.

El delito informático implica actividades criminales que los países han definido cómo robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, cabe destacar que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras, por ello se vuelve necesario tener una norma por parte del Derecho que lo regularice.

6.8.2 Tipos de Delitos Informáticos

La Organización de Naciones Unidas (ONU) reconoce los siguientes tipos de delitos informáticos:

- Fraudes cometidos mediante manipulación de computadoras.
- Manipulación de los datos de entrada.
- Daños o modificaciones de programas o datos computarizados.

Delincuente y Víctima

- **Sujeto Activo:** Los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible.

- **Sujeto Pasivo:** El sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo. En el caso de los delitos informáticos las victimas pueden ser individuos, instituciones crediticias, gobiernos u otros que utilicen las tecnologías de información.

5.7.3 Legislación Internacional

A continuación se dan a conocer las diferentes legislaciones que existen en algunos países como Alemania, Austria, Chile, China, España, Estados Unidos, Francia, Holanda e Inglaterra, de tal manera que se haga frente a la delincuencia informática y evitar en la medida de lo posible que se disminuyan este tipo de delitos.

Alemania

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica.

Esta ley reforma el Código Penal (Art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos (202a).
- Estafa informática (263a).
- Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).
- Alteración de datos (303a) es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático (303b).

- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito (266b).
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita. Esta solución fue también adoptada en los Países Escandinavos y en Austria.

Austria

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

- Destrucción de datos (Art. 126) no solo datos personales sino también los no personales y los programas.
- Estafa informática (Art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos Informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del Boletín Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema, la prisión se establecería entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. Esta ley es muy similar a la inglesa aunque agrega la protección a la información privada.

China

El Tribunal Supremo Chino castigará con la **pena de muerte** el espionaje desde Internet, según se anunció el 23 de enero de 2001.

Todas las personas "implicadas en actividades de espionaje", es decir que "roben, descubran, compren o divulguen secretos de Estado" desde la red podrán ser condenadas con penas que van de diez años de prisión hasta la muerte.

La corte determina que hay tres tipos de actividades donde la vigilancia será extrema: secretos de alta seguridad, los secretos estatales y aquella información que dañe seriamente la seguridad estatal y sus intereses. Se consideran actividades ilegales la infiltración de documentos relacionados con el Estado, la defensa, las tecnologías de punta, o la difusión de virus informático.

El Tribunal ha hecho especial énfasis al apartado del espionaje desde la red. A los llamados "criminales", además de tener asegurada una severa condena (la muerte), también se les puede confiscar los bienes.

España

Este país quizás sea el que mayor experiencia ha obtenido en casos de delitos informáticos, en Europa.

Su actual Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP) aprobada el 15 de diciembre de 1999, la cual reemplaza una veintena de leyes anteriores de la misma índole, contempla la mayor cantidad de acciones lesivas sobre la información.

Se sanciona en forma detallada la obtención o violación de secretos, el espionaje, la divulgación de datos privados, las estafas electrónicas, el hacking maligno o militar, el phreacking, la introducción de virus, etc.; aplicando pena de prisión y multa, agravándolas cuando existe una intención dolosa o cuando el hecho es cometido por parte de funcionarios públicos.

Así mismo su nuevo Código Penal establece castigos de prisión y multas "a quien por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos".

Estados Unidos

El primer abuso de una computadora se registró en 1958 mientras que en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Mineapolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, centros de investigación y transferir datos, las redes debían (y deben) ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

Esta ley fue la base para que Florida, Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Act de 1986.

Éste se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero sólo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación de los virus (computer contaminant) conceptualizándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El aumento en la cantidad de casos de hacking y la sensación de inseguridad permanente que generaron (fomentada por la difusión de los hechos en programas especiales de televisión y artículos de revistas especializadas), cambiaron la percepción de las autoridades con respecto a los hackers y sus ataques. Los casos que demostraron

ese cambio fueron los del "Cóndor" Kevin Mitnicky y los de "ShadowHawk" Herbert Zinn hijo.

El FCIC (Federal Computers Investigation Committee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales, los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

Además existe la Asociación Internacional de Especialistas en Investigación Computacional (IACIS), quien investiga nuevas técnicas para dividir un sistema en sus partes sin destruir las evidencias. Sus integrantes son "forenses de las computadoras" y trabajan, además de los Estados Unidos, en el Canadá, Taiwán e Irlanda.

Francia

Aquí, la Ley 88/19 del 5 de enero de 1988 sobre el fraude informático contempla:

- Acceso fraudulento a un sistema de elaboración de datos. Se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.
- Sabotaje Informático. Falsificar el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos. Se sanciona a quien intencionalmente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos, suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados. Se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

Holanda

Hasta el día 1 de marzo de 1993, día en que entró en vigencia la Ley de Delitos Informáticos, Holanda era un paraíso para los hackers. Esta ley contempla con artículos específicos sobre técnicas de Hacking y Phreacking.

El sólo hecho de entrar en una computadora en la cual no se tiene acceso legal ya es delito y puede ser castigado hasta con seis meses de cárcel. Si se usó esa computadora hackeada para acceder a otra, la pena sube a cuatro años aunque el crimen, a simple vista, no parece ser peor que el anterior. Copiar archivos de la máquina hackeada o procesar datos en ella también conlleva un castigo de cuatro años en la cárcel. Publicar la información obtenida es ilegal si son datos que debían permanecer en secreto, pero si son de interés público es legal.

El daño a la información o a un sistema de comunicaciones puede ser castigado con cárcel de seis meses a quince años, aunque el máximo está reservado para quienes causaron la muerte de alguien con su accionar. Cambiar, agregar o borrar datos puede ser penalizado hasta con dos años de prisión pero, si se hizo vía remota aumenta a cuatro.
Los virus están considerados de manera especial en la ley. Si se distribuyen con la intención de causar problemas, el castigo puede llegar hasta los cuatro años de cárcel; si simplemente se "escapó", la pena no superará el mes.

El usar el servicio telefónico mediante un truco técnico (Phreacking) o pasando señales falsas con el objetivo de no pagarlo puede recibir hasta tres años de prisión. La venta de elementos que permitan el Phreaking se castiga con un año de prisión como tope y si ese comercio es el modo de ganarse la vida del infractor, el máximo aumenta a tres. La ingeniería social también es castigada con hasta tres años de cárcel.

Recibir datos del aire es legal (transmisiones satelitales), siempre y cuando no haga falta un esfuerzo especial para conseguirlos; la declaración protege datos encriptados,

como los de ciertos canales de televisión satelital. Falsificar tarjetas de crédito de banca electrónica y usarlas para obtener beneficios o como si fueran las originales está penado con hasta seis años.

Inglaterra

Luego de varios casos de hacking surgieron nuevas leyes sobre delitos informáticos. En agosto de 1990 comenzó a regir la Computer Misuse Act (Ley de Abusos Informáticos) por la cual cualquier intento, exitoso o no de alterar datos informáticos con intención criminal se castiga con hasta cinco años de cárcel o multas sin límite.

El acceso ilegal a una computadora contempla hasta seis meses de prisión o multa de hasta dos mil libras esterlinas. El delito se divide en tres partes: hackear (ingresar sin permiso en una computadora), hacer algo con la computadora hackeada y realizar alguna modificación no autorizada.

El último apartado se refiere tanto al hacking (por ejemplo, la modificación de un programa para instalar un backdoor), la infección con virus o, yendo al extremo, a la destrucción de datos como la inhabilitación del funcionamiento de la computadora.

Otras legislaciones

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho.

Se considera que no existe una definición formal y universal de delito informático pero se han formulado conceptos respondiendo a realidades nacionales concretas: "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de "delitos" en el sentido de acciones típicas, es decir tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los

códigos penales, lo cual en nuestro país, al igual que en otros muchos no han sido objeto de tipificación aún."[30]

En 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin e luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), adoptó diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".
Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".[31]

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define **Delito Informático** como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."[32]

"Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma".[33]

[30] TÉLLES VALDEZ, Julio. Derecho Informático. 2° Edición. Mc Graw Hill. México. 1996 Pág. 103-104
[31] MOLINER, María. Diccionario de María Moliner Edición Digital. Copyright© 1996 Novel Inc.; Copyright © 1996 María Moliner.
[32] Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.
[33] CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio 2001.

Adicionalmente, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con la intención de ofrecer las bases para que los distintos países pudieran erigir un marco de seguridad para los sistemas informáticos:

1. Esta delincuencia se trata con especialistas capaces de efectuar el crimen y borrar toda huella de los hechos, resultando, muchas veces, imposible de deducir como es como se realizó dicho delito. La Informática reúne características que la convierten en un medio idóneo para la comisión de nuevos tipos de delitos que en gran parte del mundo ni siquiera han podido ser catalogados.
2. La legislación sobre sistemas informáticos debería perseguir acercarse lo más posible a los distintos medios de protección ya existentes, pero creando una nueva regulación basada en los aspectos del objeto a proteger: la información.

En este punto debe hacerse un punto y notar lo siguiente:

- No es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir.
- No es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.
- La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento.
- Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.
- La protección de los sistemas informáticos puede abordarse desde distintos perspectivas: civil, comercial o administrativa.

Lo que se deberá intentar es que ninguna de ellas sea excluyente con las demás y, todo lo contrario, lograr una protección global desde los distintos sectores para alcanzar cierta eficiencia en la defensa de estos sistemas informáticos.

Julio Téllez Valdez clasifica a los delitos informáticos con base en dos criterios:

1. Como instrumento o medio: se tienen a las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.

   Ejemplos:

   - Falsificación de documentos vía computarizada: tarjetas de créditos, cheques, entre otros.
   - Planeamiento y simulación de delitos convencionales como robo, homicidio y fraude.
   - Alteración el funcionamiento normal de un sistema mediante la introducción de código extraño al mismo: virus, bombas lógicas, entre otros.
   - Intervención de líneas de comunicación de datos o teleprocesos.

2. Como fin u objetivo: se enmarcan las conductas criminales que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

   Ejemplos:

   - Instrucciones que producen un bloqueo parcial o total del sistema.
   - Destrucción de programas por cualquier método.
   - Atentado físico contra la computadora, sus accesorios o sus medios de comunicación.
   - Secuestro de soportes magnéticos con información valiosa, para ser utilizada con fines delictivos.
   - Este mismo autor sostiene que las acciones delictivas informáticas presentan las siguientes características:
     a) Sólo una determinada cantidad de personas (con conocimientos técnicos por encima de lo normal) pueden llegar a cometerlos.

b) Son conductas criminales del tipo "cuello blanco": no de acuerdo al interés protegido (como en los delitos convencionales) sino de acuerdo al sujeto que los comete. Generalmente este sujeto tiene cierto status socioeconómico y la comisión del delito no puede explicarse por pobreza, carencia de recursos, baja educación, poca inteligencia, ni por inestabilidad emocional.
c) Son acciones ocupacionales, ya que generalmente se realizan cuando el sujeto atacado se encuentra trabajando.
d) Son acciones de oportunidad, ya que se aprovecha una ocasión creada por el atacante.
e) Provocan pérdidas económicas.
f) Ofrecen posibilidades de tiempo y espacio.
g) Son muchos los casos y pocas las denuncias, y todo ello por la falta de regulación y por miedo al descrédito de la organización atacada.
h) Presentan grandes dificultades para su comprobación, por su carácter técnico.
i) Tienden a proliferar, por lo se requiere su urgente regulación legal.

María Luz Lima, por su parte, presenta la siguiente clasificación de "delitos electrónicos"[34]:

1. **Como Método:** conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.
2. **Como Medio:** conductas criminales en donde para realizar un delito utilizan una computadora como medio o símbolo.
3. **Como Fin:** conductas criminales dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

[34] *LIMA de la LUZ, María. Criminalia N° 1-6 Año L. Delitos Electrónicos. Ediciones Porrúa. México. Enero-Julio 1984.*

Por lo tanto se puede concluir que dado el carácter transnacional de los delitos cometidos mediante el uso de las computadoras, se vuelve importante establecer tratados o acuerdos entre países que ayuden a fijar mecanismos para contrarrestar de manera eficaz los incidentes sobre los delitos informáticos. Así mismo las sociedades harán conciencia sobre lo importante que es mantener protegida la información y si se llega a abusar de ello, tener una norma que castigue los crímenes que se llegasen a cometer.