"AUDITORIA DE LA SEGURIDAD DE UNA RED DE DATOS"

Marjorie Alexandra Chalén Troya[1], Luis Andrés Mideros Romero[2], Washington Caraguay Ambuludi[3]
Ing. José Escalante[(4)]
[(1)(2)(3)]Facultad de Ingeniería en Electricidad y Computacion,
[(4)] Director de Tesis
Escuela Superior Politécnica del Litoral
Campus "Gustavo Galindo V.", Km 30.5, Vía Perimetral, 593, Guayaquil, Ecuador
mchalen@ceibo.fiec.espol.edu.ec, lmideros@ceibo.fiec.espol.edu.ec,
wcaragua@ceibo.fiec.espol.edu.ec
Ingeniera en Electrónica y Telecomunicaciones, Escuela Superior Politécnica del Litoral

Resumen

Actualmente existe un desarrollo significativo de las Tecnologías y Medios de Comunicación, principalmente cuando se trata de transmitir información; siendo ésta la parte más importante en el mundo de los negocios. Sin embargo, paralelamente al incremento de nuevas tecnologías, equipos y medios de comunicación, se presentan día a día nuevas formas de acceder a la información y se presentan vulnerabilidades que se deben prevenir. Por lo tanto, se requiere tomar las medidas necesarias para su protección. Se considera una red LAN, SOHO, donde se realiza la auditoria de la seguridad de la información dirigida hacia la red interna de la empresa. Se debe tener presente que existen diversas maneras de obtener seguridad en una red; el análisis presentado se base en la Norma ISO 17799, mediante un procedimiento que se divide en fases para lograr la aplicación de la auditoria, de acuerdo a las políticas de una organización específica; identificando los riesgos y debilidades que posee, por consiguiente proponer recomendaciones para fortalecer los controles de la seguridad.

Palabras Claves: *información, tecnologías, comunicación, auditoria, seguridad.*

Abstract

Nowadays, there is a significant development of Technology and the Media, mainly information transmission, being this latter the most important in business world. However, in parallel with the increase of new technologies, equipment and media, every day new ways to access information and vulnerabilities to be prevented are presented. Therefore, it is required to take the necessary measures for their protection. It is considered a LAN, SOHO, which conducts the audit of the information security directed toward the internal network of the company. We must keep in mind that there are various ways to get into a network security; the analysis is based on ISO 17799, in a manner which is divided into phases for the implementation of the audit, according to the policies of an organization specific identifying the risks and weaknesses that have thus propose recommendations for strengthening controls security.

Cue Words: *information, technology, communication, audit, security.*

1. Introducción.

Se realizó un estudio de las tecnologías y análisis de las herramientas y equipos de comunicación que brindan seguridad en una red para la implementación dedicada de una red SOHO, en base a los requerimientos de una determinada empresa.

Se analiza el nivel de seguridad interna que la empresa debe poseer en base a sus políticas, recalcando y confirmando que la información hoy en día es un activo importante en una entidad de negocio. Por lo tanto, es necesario ofrecer la debida atención y consideración en cuanto a la seguridad de este activo.

2. Protocolos de Red

Para lograr la transferencia de la información se requiere el conocimiento de los conceptos básicos como las interfases, protocolos de comunicación, para entender la transmisión de los datos en los diferentes tipos de redes. En nuestro análisis se considera el tipo LAN.

Un protocolo es una descripción formal de un conjunto de reglas y procedimientos que rigen la transmisión de datos y comunicación de dispositivos.

También se requiere considerar las bondades y requerimientos que los sistemas operativos ofrecen para la implementación de la red; predominando en nuestro medio Windows XP, Windows NT, Windows Server 2003.

3. Auditoria de la Seguridad

3.1. Fases y Tipos de Auditoria

Identificación del Sistema

El sistema comprende la empresa en la que se realiza la auditoría, en donde se observan las personas y las aplicaciones para las cuales se utiliza la red. Se debe considerar las políticas de la empresa, lo cual es fundamental para el momento de la evaluación; es la referencia para verificar el tipo de control que se posee. Se identifica el sistema, la distribución de la empresa; es decir organigrama de las áreas en el sistema, las funciones que poseen las personas que comprenden el sistema.

Análisis de procesos y recursos en la red

Consiste en identificar los procesos y dependiendo del tamaño del sistema, subprocesos, en base a los flujogramas que determinan el recorrido de los procesos y de la información; esto es manejado por los administradores de la red. Cuando se habla de recursos en la red, pues se trata de los dispositivos que se emplean en la red y las funciones que realizan.

Análisis de riesgos y amenazas

Se identifican los riesgos que presentan en la red, lo cual incluye el riesgo con respecto a la integridad de los dispositivos y pérdida de recursos; lo que afecta amenaza directamente a la seguridad de la información. Esto provoca que las operaciones y procesos que se realizan sean ineficientes. En esta parte se procura verificar cuales son los errores que existen con el manejo de la información.

Análisis y evaluación de controles

Se debe controlar a los grupos que utilizan los recursos, codificando a cada grupo de acuerdo a los recursos que maneje. Debe haber uno o más controles sobre los recursos, los riesgos y las amenazas. El análisis de los controles procura determinar si los controles aplicados al manejo de la información son los adecuados.

Informes de Auditoria y Recomendaciones

Una vez identificado el tipo de red, los recursos, las aplicaciones, los riesgos, las amenazas; se realiza un informe detallado cuales son las partes débiles de la red que están siendo amenazadas, y los riesgos que representan para la seguridad e integridad de la información.

La última parte que se presenta en una auditoría, es el seguimiento de las recomendaciones que se indicaron- Se detalla un informe de dicho seguimiento y se evalúan los resultados de acuerdo a los controles que se implementaron luego de indicar las recomendaciones.

Tipos de Auditoria

Existen dos tipos generales: Auditoría de Seguridad Interna y Auditoría de Seguridad Perimetral.

La Auditoría de Seguridad Interna, procura identificar la seguridad de la información así como su nombre lo indica, a nivel interno; verificando los controles internos que estén de acuerdo a las políticas de la empresa. Se verifican accesos a nivel de usuarios, seguridad con respecto a los respaldos de la información.

La Auditoría de Seguridad Perimetral plantea la revisión de controles de accesos de entrada y salida de una red corporativa.

3.2. Técnicas, Métodos y Herramientas para proteger una red

Escaneo de Red

Emplea un puerto de escaneo para detectar todos los computadores, servidores empleados en la red, como ftp y http, y el tipo de aplicación específica que está utilizando.

Escaneo de Vulnerabilidad

Actúa de la misma manera que el escaneo de puerto, identificando los computadores y puertos abiertos; además identifica los daños existentes en un sistema operativo ó una aplicación. Por ejemplo, si una versión de software está vencida, la actualización de un sistema operativo.

Craqueo de Claves

Son programas que verifican que los usuarios utilicen claves fuertes que sean difíciles de descifrar. Los ataques más comunes son el ataque de diccionario y el híbrido, pero el método más poderoso en craqueo de claves es el llamado fuerza bruta. Éste genera aleatoriamente claves y las funciones de correspondencia asociadas a estas.

Revisiones de Registro de usuarios

Básicamente lo que se intenta identificar es que cada usuario tenga el acceso que requiera de acuerdo a las funciones que desempeña y a las políticas de la empresa.

Evaluación de Integridad de los Archivos

Se realiza un análisis de los archivos y se almacena el checksum de cada archivo y establece una base de datos de checksum de los archivos. Esto suele estar incluido en el sistema de detección de intrusos.

Detector de virus

Esta herramienta escanea los discos duros mediante un algoritmo aplicado a diferentes fuentes al mismo tiempo, y si detecta este tipo de amenazas las pone en cuarentena ó las remueve.

4. Proyecto.- Implementación y Aplicación de la Auditoría en una red

4.1 Procedimiento para Evaluar un Sistema de Seguridad en una Red de Comunicaciones

En base a la norma ISO 17799 se desarrolló un procedimiento para evaluar la seguridad de la información en una red de datos. Por lo tanto, se aplicó dicho procedimiento para evaluar una red en particular. Se expone lo siguiente:

<u>Identificación del Sistema</u>

La empresa se dedica a la distribución de lubricantes, llantas y aditivos, y servicios automotrices. Donde se define que se tiene una persona encargada del área de sistemas quien se encarga de todas las actividades del Área de IT. No presenta otras sucursales, sólo tiene una localidad; posee un contrato con tvcable para el servicio de internet.

Análisis de Procesos y Recursos en la Red

El Departamento de Ventas se encarga de la venta de productos y servicios; los privilegios que posee son:

- Acceso al sistema para revisar inventarios, costos, cuentas por cobrar
- Comunicaciones mediante correo electrónico.

El Departamento de Operaciones maneja la facturación, la logística; es decir, la compra, almacenamiento y transporte de productos hasta las instalaciones de los clientes; y maneja también el taller de servicio. Los privilegios que posee son:

- Facturación, acceso al sistema y modificación de inventario.
- Ingreso de Compras al Inventario, acceso al sistema y modificación de inventario
- Control de Inventarios.
- Comunicaciones mediante correo electrónico.

El Departamento de Sistemas brinda soporte técnico a la red y gestiona privilegios en el sistema interno. Los privilegios que posee son:

- Acceso mediante VNC a cada usuario de la red.
- Monitorea y controla mediante firewall y analizador de protocolos los servicios y aplicaciones empleados por los usuarios.
- Acceso a la red externa, Internet.
- Actualización de aplicaciones, servidores y firmware de equipos de comunicación.
- Comunicaciones mediante correo electrónico.

El Departamento Financiero se encarga de las funciones de Crédito, de Caja y Bancos, y de Contabilidad e Impuestos. Los privilegios que posee son:

Acceso al sistema con privilegio para realizar; asientos de Pagos realizados por los clientes, análisis de crédito y definición de cupo de crédito de los clientes, pagos a proveedores y pagos de gastos, control de Caja y Bancos, Tributación, y asientos contables y estados financieros

- Comunicaciones mediante correo electrónico.
- Acceso limitado a la red externa, Internet; sitios Web de bancos, Sitio Web del SRI y demás sitios donde sea requerido el acceso.

El Departamento de Gerencia monitorea las actividades que se efectúan en el sistema y realiza los cambios que se requieran. Los privilegios que posee son:

- Acceso total a la información de los servidores que contiene el sistema.
- Posee acceso total a la red externa, Internet.

<u>Análisis de Riesgos y Amenazas</u>

- Existe el riesgo de que personas no autorizadas manipulen los equipos. Por lo tanto, se debe verificar que los equipos de comunicación están ubicadas en un área segura; es decir área restringida.
- Riesgo de daño de equipos; se debe mantener equipos en una zona seca, lejos de la humedad y aislados de materiales inflamables.
- Interrupción física de los enlaces de comunicación, se debe verificar que estén protegidos adecuadamente; mediante canaletas. También se debe verificar periódicamente el estado del cableado.
- Interrupción en los procesos de los negocios. Puede ser provocada por pérdida de energía eléctrica o por daño en el servidor. Se requiere un UPS por equipo de comunicación y un servidor de respaldo que se deberá actualizar de manera periódica.
- Riesgo de robo ó acceso no autorizado a la información. Como medida preventiva el sistema a emplearse tendrá su base de datos en un servidor; cada usuario debe autenticarse.
- Riesgo de manipulación de la información por parte de los usuarios de la red. Se debe establecer privilegios de acuerdo a los departamentos.

<u>Análisis y Evaluación de Controles</u>

- En esta fase se analizará las medidas preventivas con respecto a los riesgos y amenazas en la red.
- Confirmar que el cuarto de sistemas esté cerrado bajo llave cuando no estén personas autorizadas dentro de él.
- Verificar que cada departamento de la empresa debe tener una codificación y privilegios de acuerdo a las actividades que les está permitido realizar. Esto estará considerado en la autenticación y división de departamentos en la configuración de los equipos de comunicación.
- Mediante un analizador de protocolos se debe monitorear la red para determinar que aplicaciones están siendo utilizadas por los usuarios.
- Se utilizará arbitrariamente aplicación de VNC para monitorear las actividades de los usuarios. Esta herramienta también será empleada para que el departamento de sistemas pueda auxiliar remotamente a los usuarios con respecto al manejo de las aplicaciones.

Informes de la Auditoría y Recomendaciones

Para proveer un informe se requiere del análisis de los datos antes mencionados, se debe exponer detalladamente lo que se ha realizado, explicando el objetivo de cada implementación realizada y cual es el resultado obtenido. Se obtendrá un informe final mediante el uso del Firewall ISA Server

4.2 Proyecto.- Descripción e Implementación de un Red

La red a implementarse se ajusta a las políticas y necesidades de la empresa.

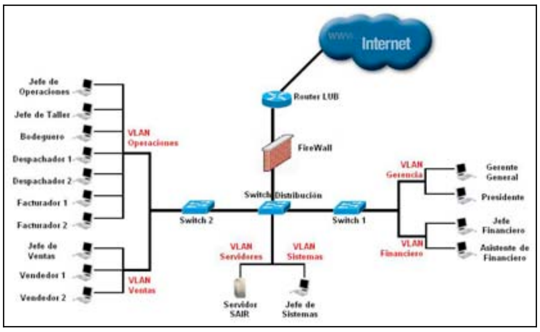

Figura 1. Diagrama esquemático de la Red.

Se puede observar en la Figura 1 la distribución del personal de la empresa correspondiente a su respectiva área de trabajo.

Se analizan tanto el sistema operativo como la configuración cada equipo. Entre éstos tenemos: 3 switches CISCO C2960, router CISCO 2801, servidor con OS WINDOWS SERVER 2003 y computadores con OS WINDOWS XP.

En la configuración de switches y routers se define que el acceso a estos equipos se maneje de forma segura; se crean listas de acceso en la interface del router, logrando que sólo se utilicen puertos específicos de acuerdo a los requerimientos establecidos y las políticas de la seguridad de la empresa.

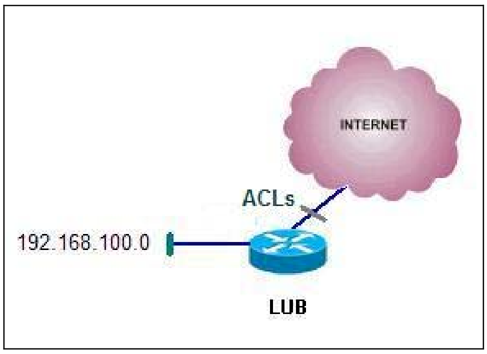

Figura 2. Esquema indicativo de ubicación de ACLs.

Configuración del Firewall

El Firewall usado es el Microsoft ISA Server 2004 y esta alojado en un servidor con el sistema operativo Windows Server 2003. El acceso a este servidor esta encriptado con una contraseña conocida solo por el jefe de sistemas y el gerente general de la compañía.

En el firewall se configuran las políticas que establecen los permisos y accesos que poseen los usuarios, una función del firewall es que tiene la capacidad de generar un reporte del comportamiento de la red. Mediante dicho reporte se pueden observar la utilización del ancho de banda de cada usuario, las páginas web más visitadas, y que usuario las visita con mayor frecuencia.

Las Directivas de Firewall se configuran desde lo más específico hasta lo más general

La manera como se ejecutan las reglas del firewall, es verificando una a una de manera jerárquica, de menor a mayor. Por lo tanto, si coincide una de las peticiones de algún usuario con una de las reglas establecidas, la ejecuta y no verificará las siguientes.

Configuración de directivas de los usuarios en Windows XP

Cada usuario Windows XP se le ha creado 2 cuentas uno como administrador y otra como usuario este con el nombre del cargo que desempeña y con sus respectivas restricciones. Tanto el acceso a la cuenta administrador como la de usuario están encriptados con contraseñas. El derecho al acceso a la cuenta administrador y por ende el conocimiento de la contraseña la tiene el jefe de sistemas y el gerente general de la empresa. La contraseña de acceso como usuario es única por computador y solo debe de ser conocida por la persona encargada de ese puesto de trabajo.

Antivirus

Cada estación de trabajo y cada servidor cuenta con la protección de un antivirus, NOD32. Tiene como principal ventaja un bajo consumo de recursos al momento de ejecutar su análisis,

Configuraciones del Software de Facturación

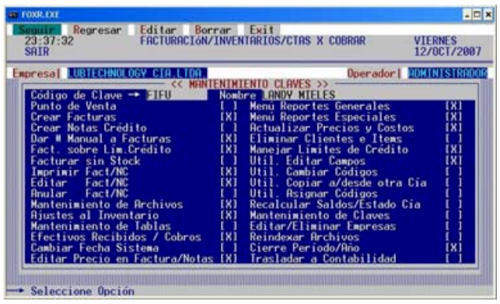

Figura 3. Privilegios por usuario en el sistema SAIR

La empresa utiliza un software de facturación llamado SAIR, que permite dar accesos a los usuarios mediante claves y realizar consultas sobre los productos, afectar directamente los inventarios; cuya contraseña sólo la tiene el Gerente General.

Revisión y comprobación de los enlaces

El Firewall también permite realizar pruebas de conectividad con respecto a los equipos conectados a la Red.

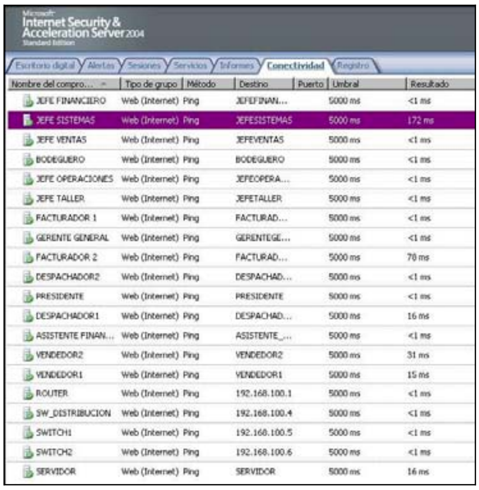

Figura 4. Pruebas de conectividad del ISA Server de los equipos conectados a la Red.

4.3 Evaluación de la Seguridad en una

La realización de la evaluación de la seguridad se basó en el reporte del ISA Server antes de implementar las reglas mencionadas en el subcapítulo anterior. Se reportaron las siguientes debilidades:

1. No se tiene un control adecuado. Las páginas web visitadas no tienen relación alguna con las actividades de la empresa. La red se congestiona casi a toda hora del día. Se observa un número alto de peticiones.
2. Se identifica que personal de alto y bajo nivel en la escala del organigrama empresarial cuentan con los mismos privilegios de acceso de Internet. No existen una definición de perfiles de usuarios.
3. Se identifica que no existen controles con respecto a la utilización de un explorador de manera unificada, por lo tanto se puede inferir que no se posee las licencias de los mismos.
4. No existe un estándar a nivel de plataforma de usuario.
5. No se refleja un control en la utilización de protocolos, varios protocolos utilizados son empleados para acceso a centros de Chat.
6. Se observa una variedad de aplicaciones tipo ejecutable no locales que influyen en el funcionamiento de la red, las cuales no

son actividades propias de la empresa. Se detectan conexiones simultáneas altas.

Estas debilidades fueron superadas con la implementación de las reglas descritas en el subcapítulo anterior.

CONCLUSIONES

Las redes de comunicaciones pueden implementarse de diversas maneras, cuyo factor más significativo es la información. Para una organización es de vital importancia la integridad, confidenciabilidad y disponibilidad de la información; va ligado a la norma ISO 17799.

La Auditoria de la Seguridad de una red de datos analiza las vulnerabilidades que se presentan con respecto al manejo de la información, con el objetivo de identificar el nivel de seguridad que se posee en la red. Se verifica que los procesos se efectúen de acuerdo a las políticas de seguridad de la organización, lo que es manejado por una tercera persona, el auditor ó la empresa auditora, de tal forma que el resultado sea imparcial.

Existen diversas herramientas, que pueden ser de tipo hardware, software ó una combinación de ambas, para atacar las vulnerabilidades que se presentan en la seguridad de una red de datos. Estas herramientas pueden requerir licencias que tienen un costo de acuerdo a su aplicación; por esto se debe analizar lo que realmente es adecuado para el control que se desea.

Luego de evaluar detenidamente distintos métodos de seguridad; en este trabajo se ha considera una herramienta tipo software, firewall ISA Server 2004 para el control de accesos y de monitoreo de una red SOHO. La principal ventaja al utilizar el ISA Server es que realiza una inspección minuciosa de protocolos de Internet, como el Protocolo de transferencia de hipertexto (HTTP, Hypertext Transfer Protocol), que le permite detectar numerosas amenazas que se escapaban a los servidores de seguridad tradicionales.

Es de suma importancia que el administrador de la red esté pendiente de la seguridad de la LAN en todo momento; aunque se haya configurado el firewall para que controle dicha seguridad, es necesario que se vigile su funcionamiento. Esto sirve en caso de que surja algún problema, sea detectado inmediatamente.

La seguridad no sólo depende de la herramienta que se emplee para la ejecución de los controles pertinentes a la seguridad de la información; un factor que posee un alto nivel de importancia, es el usuario. Por lo tanto, en una organización se debe capacitar a cada empleado con respecto al manejo de los equipos terminales, de cuales son los accesos y el tipo de información que manejan; también deberán ser notificados de las sanciones que se impondrán en caso de violar las políticas de seguridad.

Se debe considerar que para cubrir las diferentes áreas con respecto a seguridad, existen varios caminos a seguir. Sin embargo, para lograr la protección adecuada de la información, se requiere el análisis pertinente y dirigido a lo que realmente requiere la organización. Es decir, no se trata de utilizar cualquier herramienta con el fin de indicar que hay cierta protección, sino de identificar cual es la más apropiada.

Conforme a lo expuesto anteriormente, a la información recopilada y en base a la norma ISO 17799 se desarrolló un procedimiento para la realización de la auditoría, el mismo que se divide en fases; esto se logra con la investigación realizada y presentada en el capítulo 2. Es aconsejable seguir una metodología y un procedimiento al momento de analizar una red, considerando todos los procesos y las aplicaciones que se empleen para flujo de la información. El orden es esencial al realizarse auditoría.

Con respecto a la empresa Lubtechnology, se aplicaron controles a las comunicaciones por medio del ISA Server 2004, estableciendo reglas en base a las políticas de la empresa, mediante lo cual se logró mejorar el desempeño de la red y la disponibilidad de la información. Además se monitorea la red mediante la comprobación de los enlaces, en caso de presentar alguna anomalía, se busca la identificación del problema. Se controla el acceso de los usuarios mediante el sistema operativo, de manera que los ingresos se realicen de acuerdo a los perfiles de usuarios por área y por cargo.

BIBLIOGRAFÍA

[1] Cisco Networks. CCNA Módulo 1, 2 y 3

[2] Network Security Bible. Chapter 11. Network Protocols. Página 370

[3] Auditoría de la Red Interna, disponible en: http://www.isecauditors.com/es/auditoria-interna.html

[4] Network Security Bible. Chapter 17. Intrusion Detection and Response. Página 567

[5] Forward Error Correction (FEC) techniques for optical communications, disponible en: http://grouper.ieee.org/groups/802/3/10G_study/public/july99/azadet_1_0799.pdf

[6] Redes de Área Amplia (WAN), disponible en: http://www.textoscientificos.com/redes /area-amplia

[7] Teorema del Muestreo, disponible en: http://www.ifent.org/Lecciones/digitales/secuenciales/Teorema_Muestreo.asp

[8] Control de acceso al medio IEEE 802.3 CSMA/CD, disponible en: http://www.textoscientificos.com/redes/ethernet/control-acceso-medio-csma-cd

[9] Internet Security and Acceleration (ISA) Server TechCenter, disponible en: http://www.microsoft.com/technet/isa/default.mspx

[10] Auditor, disponible en: http://es.wikipedia.org/wiki/Auditor

[11] Redes. Topología, disponible en: http://vgg.uma.es/redes/topo.html

[12] Capítulo 9: Implementación de la infraestructura de seguridad para LAN inalámbricas, disponible en: http://www.microsoft.com/latam/technet/articulos/wireless/bgch09.mspx

[13] Tema5: Redes de Conmutación de Circuitos, disponible en: http://www.it.uniovi.es/docencia/Telecomunicaciones/arss/material/arssTema5-Conmutacioncircuitos.pdf

[14] Multiplicación y acceso múltiple, disponible en: http://www.eie.fceia.unr.edu.ar/ftp/Comunicaciones/MUX.pdf

[15] Auditoria, disponible en: http://www.monografias.com/trabajos6/audi/audi.shtml

[16] Control de Flujo y errores, disponible en: http://www.it.aut.uah.es/juanra/docencia/fundamentosdetelematica/materiales/ARQ.pdf

[17] Capa de enlace Punto a Punto, disponible en: http://www.fi.uba.ar/materias/7543/m7543t/datalink.pdf

[18] Auditoria en redes telemáticas, disponible en: http://www.coitt.es/antena/pdf/162/06B_Reportaje_Auditorias.pdf

[19] Auditoria de Sistemas, disponible en: http://www.hispasec.com/corporate/auditoria.html

[20] Gestión de proyectos de Auditoria de Seguridad, disponible en: http://www.fistconference.org/data/presentaciones/gestiondeauditoriasdeseguridad.pdf

[21] Consideraciones de Seguridad en Sistemas de Información, DB y Web, disponible en: http://www.amereiaf.org.mx/3reuniondeverano/materiales/Departamento_de_Seguridad_de_Computo_de_la_UNAM.pdf

Firma Autorizada

ING. José Escalante

DIRECTOR DE TESIS