ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"Metodología de Seguridad en Redes

T.A.M.A.R.A: Testeo, Análisis y MAnejo de Redes y Accesos"

Tesina de Seminario

Previa a la obtención del Título de:

INGENIERO EN TELEMÁTICA

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por:

María Fernanda Viteri Minaya.

Pedro Enrique Orellana Zúñiga.

Guayaquil – Ecuador

2011

AGRADECIMIENTO

Agradecemos en primer lugar a Dios por bendecirnos y guiar nuestros pasos, a nuestros padres por su apoyo incondicional y a todos nuestros profesores por sus enseñanzas, en especial al Ing. Ignacio Marín por la ayuda brindada en la realización de ésta modesta Metodología.

María Fernanda Viteri Minaya.

Pedro Enrique Orellana Zúñiga.

DEDICATORIA

Dedico este trabajo a Dios; a mis padres Galo Viteri y Nancy Minaya por su comprensión y por todo su apoyo incondicional; a mis hermanos, Mariela y Galo por brindarme todo su amor, confianza, por siempre ser mi guía, y no darme por vencida antes las adversidades.

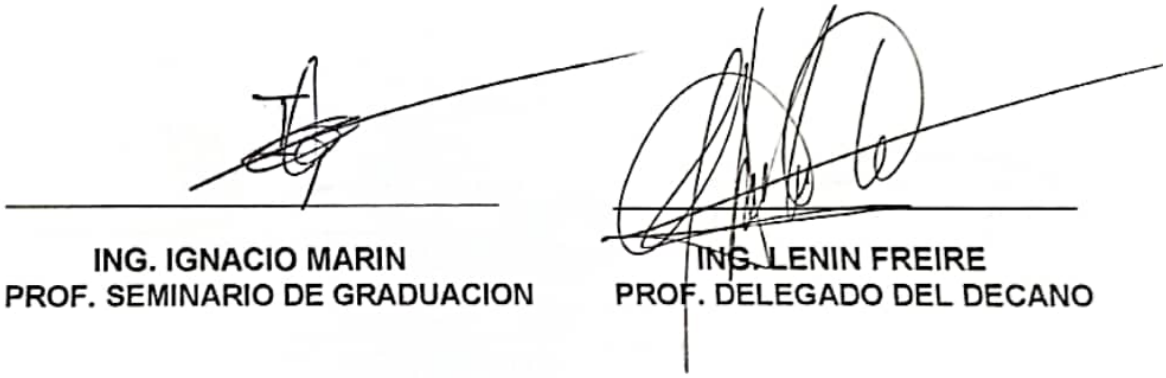
María Fernanda Viteri Minaya

A Ailyn Orellana Montecé.

Mi hijita…

Pedro Enrique Orellana Zúñiga.

TRIBUNAL DE SUSTENTACIÓN



ING. IGNACIO MARIN
PROF. SEMINARIO DE GRADUACION

ING. LENIN FREIRE
PROF. DELEGADO DEL DECANO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este proyecto de graduación nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

Pedro Orellana Zúñiga

María Viteri Minaya

RESUMEN

Debido a la necesidad de seguridad en los sistemas de información en las empresas ecuatorianas, hemos desarrollado una metodología utilizando los sistemas más comunes que se presentan en dichas empresas, como son: sistemas particulares, sistemas pequeños, sistemas medianos y grandes. Las soluciones que se brinden para cada sistema deberán ser acumulativas, es decir los sistemas pequeños deberán tener como mínimo las soluciones dadas para los sistemas particulares, y los sistemas medianos y grandes como mínimo las dos anteriores.

En el primer capítulo tratamos la seguridad en redes, tipos de seguridad, situación actual en el medio, mecanismos básicos de seguridad y por último citamos algunos tipos de ataques informáticos.

En el segundo capítulo, citamos la metodología a usar: “T.A.M.A.R.A”: Testeo, Análisis y MAnejo de Redes y Accesos, nombre de origen hebreo y que significa “Da protección, seguridad”, y que refleja el objetivo de ésta metodología, mencionamos la introducción, los objetivos y una explicación de ésta, la cual es resumida al final con un gráfico. El desarrollo total de ésta metodología está explicado en el tercer y cuarto capítulo.

Los sistemas particulares y los sistemas pequeños son tratados en el tercer capítulo, para el primer sistema brindamos consejos básicos y avanzados de

seguridad para la autoprotección. Mientras que para el segundo, nos basamos en el cumplimiento de la legislación ecuatoriana, así como también citamos cual es el organismo encargado de velar por la seguridad de la información en el Ecuador.

El cuarto capítulo, por ser el que requiere un mayor control de seguridad, está dividido en tres etapas que son: Determinar las necesidades de protección mediante un análisis de riesgos y las soluciones a este tipo de problemas, definir e implementar las políticas, medidas y procedimientos de seguridad que garantice minimizar los riesgos identificados en el punto uno y evaluar el sistema de seguridad a través de auditorías. El impacto en la organización, la visibilidad del proceso y la implementación de éstas medidas de seguridad se mencionan al final de éste capítulo.

ÍNDICE GENERAL

CAPITULO 2.

Metodología de Seguridad "T.A.M.A.R.A"

CAPITULO 3.

"T.A.M.A.R.A" en Sistemas Particulares y Pequeños.

CAPITULO 4.

"T.A.M.A.R.A" en Sistemas Medianos y Grandes.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

Pág.

Glosario de Términos

Ancho de banda: Es una medida de la capacidad de transmisión de información que posee un canal de comunicaciones. Se suele medir en bits por segundo.

Antivirus: Programa informático diseñado para detectar, aislar y eliminar virus alojados en un equipo informático.

Autentificación: También llamada Autenticación, es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

Back-up: Una copia de seguridad o back-up es una herramienta, que puede utilizarse para restaurar el documento original después de una eventual pérdida de datos.

Cifrado: Es un método que permite codificar el contenido de un mensaje o de un archivo para que sea leído solo por la persona autorizada.

Chargen: (Character generator o Generador de caracteres en español) es un programa informático para sistemas operativos basados en Unix que actúa de servidor de caracteres ofrecido por Inetd en el puerto 19 con los protocolos TCP y UDP**.**

Concentrador: Dispositivo que une las redes y permite conectarlas entre sí.

Dial-up: Ésta tecnología permite acceder al servicio Internet a través de una línea telefónica analógica y un modem.

Email Bombing: Mensaje o conjunto de mensajes utilizados para "bombardear" (llenar) una cuenta de correo.

Enrutador: (En inglés: **router**), el enrutador es un dispositivo que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Escaneadores de puertos: Son programas que permiten analizar el estado de los puertos de una máquina conectada a una red de comunicaciones. Detecta si un puerto está abierto o cerrado.

Firewall: Es un elemento de los equipos informáticos, que regula las comunicaciones, una de sus aplicaciones es la de permitir o prohibir el acceso a los puertos.

Firma Digital: Es un esquema matemático que sirve para demostrar la autoría de un mensaje digital o de un documento electrónico. Una firma digital da al destinatario la seguridad de que el mensaje fue creado por el remitente, y que no fue alterado durante la transmisión.

Firma Electrónica: Una firma electrónica es una firma digital que se ha almacenado en un soporte de hardware.

Gateway: La “puerta de enlace” es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation).

Hacker: Nombre con el cual se conoce a los expertos en informática capaces de acceder a los equipos y violar la seguridad de sus datos, en la mayoría de los casos con malas intenciones.

Internet: La Internet es una red global en la cual, cada equipo actúa como un cliente y un servidor. Actualmente conecta miles de redes para permitir compartir información y recursos a nivel mundial. Con la Internet los usuarios pueden compartir, prácticamente, cualquier cosa almacenada en un archivo.

Macintosh: Es el nombre del tipo de ordenadores creados por la marca Apple, su abreviatura popular es MAC.

Modem: Modulator-Demodulator (Modulador-Demodulador): Aparato que Modula y demodula señales en una frecuencia portadora que convierte las frecuencias de nuevo en pulsos en el lado receptor.

Denegación de servicio: En seguridad informática, un ataque de denegación de servicio, también llamado ataque **DOS** (de las siglas en inglés ***D****enial* ***o****f* ***S****ervice*), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

Nuke: Es un viejo ataque de denegación de servicio contra redes de computadoras. Dicho ataque consiste en enviar paquetes de datos ICMP fragmentados o de alguna otra forma inválidos a un objetivo, lo que se consigue usando una herramienta de ping modificada para enviar estos datos corruptos una y otra vez, ralentizando la computadora afectada hasta que deje de funcionar.

Ping: Herramienta que permite averiguar si existe comunicación entre dos equipos de cualquier parte de internet.

Protocolo: Es un conjunto de reglas usadas por dispositivos de red para comunicarse unas con otras a través de ésta.

Puerto: En la informática, un puerto es una forma genérica de denominar a una interfaz a través de la cual los diferentes tipos de datos se pueden enviar y recibir.

Punto de Acceso: Es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un WAP (wireless Access point) también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.

Rack: Es un bastidor destinado a alojar equipamiento electrónico, informático y/o de comunicaciones.

Ranura de expansión: (también llamada *slot de expansión*) es un elemento de la placa base de un ordenador que permite conectar a ésta una tarjeta adicional.

Red privada: Es una red que usa el espacio de direcciones IP especificadas en el documento RFC 1918. A los terminales puede asignársele direcciones de este espacio de direcciones cuando se requiera que ellas deban comunicarse con otras terminales dentro de la red interna (una que no sea parte de Internet) pero no con Internet directamente.

Red pública: Es una red de computadoras interconectadas, capaz de compartir información y que permite comunicar a usuarios sin importar su ubicación geográfica.

Sistema Operativo: Es el programa o conjunto de programas que efectúan la gestión de los procesos básicos de un sistema informático, y permite la normal ejecución del resto de las operaciones.

Sniffer: Es un programa para monitorizar y analizar el tráfico en una red de computadoras, detectando los cuellos de botella y problemas que existan. También puede ser utilizado para "captar", lícitamente o no, los datos que son transmitidos en la red.

Software: Comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.

Software libre: Es un software que una vez obtenido, puede ser usado, copiado, estudiado, cambiado y redistribuido libremente.

Spam: Mensaje electrónico no solicitado, normalmente enviado a muchas personas.

Spoofing: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad, de los nombres o direcciones de equipos generalmente con usos maliciosos.

Spyware: Programa espía, que funciona dentro de la categoría malware**,** que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste.

Switch: Dispositivo de conmutación genérica que permite la conexión entre una puerta de entrada y otra de salida.

SYN Flood: La "Inundación" consiste en saturar el tráfico de la red (*denegación de servicio*) para aprovechar el mecanismo de negociación de tres vías del protocolo TCP**.**

Texto plano: Son aquellos que están compuestos únicamente por texto sin formato, sólo caracteres.

Tripwire: Es un programa de computador Open Source consistente en una herramienta de seguridad e integridad de datos. Es útil para monitorizar y alertar de cambios específicos de ficheros en un rango de sistemas.

Troll: Es un vocablo de Internet que describe a una persona que sólo busca provocar intencionadamente a los usuarios o lectores, creando controversia.

Virus: Programa informático que intencionalmente modifica y altera el correcto funcionamiento de un equipo informático.

Índice de Abreviaturas

BBS: Un Bulletin Board System (Sistema de Tablón de Anuncios) es un software para redes de computadoras que permite a los usuarios conectarse al sistema (a través de internet), realizar funciones tales como descargar software y datos, leer noticias, intercambiar mensajes con otros usuarios, disfrutar de juegos en línea, leer los boletines, etc.

BS 7799: Es el estándar de seguridad de información de facto, creada por British Standards Institution (BSI) como un conjunto de controles de seguridad y de metodologías para su correcta aplicación.

DNS: (Domain Name System, en español: sistema de nombres de dominio), traduce su nombre de dominio por ejemplo: pedroorellana.com en una dirección IP.

FTP: (sigla en inglés de File Transfer Protocol - Protocolo de Transferencia de Archivos) en informática, es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

HTML: (Hypertext Mark-up languaje), Es un Lenguaje de Etiquetas de Hipertexto para programación web, visible desde un explorador.

ICMP: El Protocolo de Mensajes de Control de Internet o ICMP (por sus siglas de Internet Control Message Protocol) es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

IP: (Internet Protocol), Es una etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del protocolo TCP/IP.

IPSEC: (Abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos.

IPv6: Versión 6 del protocolo de internet (IP), diseñada para sustituir a la versión 4 ya que posee cerca de 6,7 × 10^17 (670 mil billones) de direcciones por cada milímetro cuadrado de la superficie de La Tierra.

ISO: (International Organization for Standardization), en español la Organización Internacional de estandarización, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio

y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

ITSEC: (Information Technology Security Evaluation Criteria). Es un conjunto estructurado de criterios para evaluar la seguridad informática dentro de los productos y sistemas.

ITSEM: (Information Technology Security Evaluation Manual).es un documento técnico destinado principalmente a los evaluadores, patrocinadores y certificadores. Contiene suficiente detalle acerca de los métodos de evaluación y procedimientos que permiten técnicas equivalencias de las evaluaciones realizadas en diferentes ambientes.

LAN: (Local Area Network), Redes de área local en español, Una LAN conecta varios dispositivos de red en una área de corta distancia (decenas de metros) delimitadas únicamente por la distancia de propagación del medio de transmisión [coaxial (hasta 500 metros), par trenzado (hasta 90 metros) o fibra óptica [decenas de metros].

MAN: (Metropolitan Area Network), Red de área metropolitana en español. Una MAN es una colección de redes LAN dispersas en una ciudad (decenas de kilómetros).

PAT: (Port Address Translation), La Traducción de Dirección de puerto permite que una sola dirección IP sea utilizada por varias máquinas de la intranet.

PC: Siglas de Personal Computer o Computador personal (desktop, notebook, etc.) que contiene la totalidad de las funciones en su interior.

PGP: (Pretty good Privacy),Privacidad bastante buena, es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de llave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

SMTP: Simple Mail Transfer Protocol, Protocolo Simple de Transferencia de Correo, es un protocolo de la capa de aplicación. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos.

SSH: (Secure Shell, en español: intérprete de órdenes segura) es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red.

SSL: (Secure Socket Layers) es un proceso que administra la seguridad de las transacciones que se realizan a través de Internet.

TCP: (Transmission control Protocol), Protocolo de control de transmisión. Protocolo del ámbito de Internet que forma el núcleo del funcionamiento junto a Ip, Corresponde a la capa 4 del modelo OSI, define los mecanismos para mantener la confiabilidad de las comunicaciones en la red.

TCSEC: (Trusted Computer System Evaluation Criteria). Los TCSEC tienen por objetivo aplicar la política de seguridad del Departamento de Defensa estadounidense. Esta política se preocupa fundamentalmente del mantenimiento de la confidencialidad de la información clasificada a nivel nacional.

UDP: User Datagram Protocol, protocolo del nivel de transporte basado en el intercambio de datagramas (paquetes de datos).

UPS: Un sistema de alimentación ininterrumpida, SAI (en inglés Uninterrupted Power System), UPS, es un dispositivo que gracias a su fuente de alimentación de energía, puede proporcionar energía eléctrica tras un apagón a todos los dispositivos que tenga conectados.

WAN: Wide Area Network, red de área extensa. Una WAN es una colección de LANs dispersadas geográficamente cientos de kilómetros una de otra. Un dispositivo de red llamado enrutador es capaz de conectar LANs a una WAN.

WEP: Acrónimo de Wired Equivalent Privacy o "Privacidad Equivalente a Cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11

como protocolo para redes Wireless que permite cifrar la información que se transmite.

Wlan: (Wireless Local Area Network), es un sistema de comunicación de datos inalámbrico flexible, muy utilizado como alternativa a las redes LAN cableadas o como extensión de éstas.

WPA: (Wi-Fi Protected Access, Acceso Protegido Wi-Fi) es un sistema para proteger las redes inalámbricas (Wi-Fi); creado para corregir las deficiencias del sistema previo WEP.

INTRODUCCIÓN

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada una de las ramas que la componen, es por esto que para cumplir los objetivos de las leyes y normas ecuatorianas en materia de seguridad, es necesario que las administraciones, profesionales y empresas puedan organizar su política de seguridad. Muchas organizaciones no toman de modo serio una política de seguridad "formal" debido a que las metodologías y normas existentes relacionadas con los sistemas de gestión de seguridad de la información (SGSI) no aclaran sus ámbitos de aplicación, resultando un conjunto de normas de compleja aplicación.

Según la ley orgánica de transparencia y acceso a la información pública No. 24, publicado en el Registro Oficial Suplemento 337 del 18 de Mayo del 2004 de la republica del Ecuador, en su artículo 10 denominado **custodia de la información** [1] nos dice que:

"Es responsabilidad de las instituciones públicas, personas jurídicas de derecho público y demás entes señalados en el artículo 1 de la presente Ley, crear y mantener registros públicos de manera profesional, para que el derecho a la información se pueda ejercer a plenitud, por lo que, en ningún

caso se justificará la ausencia de normas técnicas en el manejo y archivo de la información y documentación para impedir u obstaculizar el ejercicio de acceso a la información pública, peor aún su destrucción.

Quienes administren, manejen, archiven o conserven información, serán personalmente responsables, solidariamente con la autoridad de la dependencia a la que pertenece dicha información y/o documentación."

Esta metodología está enfocada a cumplir con los cuatro puntos que caracterizan a un sistema "seguro", las cuales son: Integridad, Confiabilidad, Disponibilidad y no repudiación. Con nuestra propuesta, esperamos dar soluciones a empresas de pequeña, mediana y gran escala, con el fin de aumentar la seguridad en este tipo de organizaciones, así como también para asegurar aquellos recursos que estén dispuestos para un posible ataque por parte de personas internas o externas a la entidad.

CAPITULO 1.

Seguridad en Redes

Para la mayoría de los expertos el concepto de seguridad en la informática es utópico, porque no existe un sistema 100% seguro. Para que un sistema pueda considerarse como “seguro” debe tener estas cuatro características [2]:

Tabla 1.1 Características de un sistema seguro

Integridad	Consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencionalmente), garantizando que los datos sean los que se supone que son.
Confidencialidad	La información solo puede ser legible para los autorizados.
Disponibilidad	Debe estar disponible cuando se necesita.
No repudiación	El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no debe negar dicha acción.

Se entiende por seguridad en redes, al conjunto de técnicas que tratan de minimizar la vulnerabilidad de los sistemas o de la información en ellas contenida. Toda organización debe estar a la vanguardia de los procesos de cambio, donde disponer de información continua, confiable y en tiempo preciso, constituye una ventaja fundamental, la información se reconoce como:

Crítica: Indispensable para garantizar la continuidad operativa de la organización.

Valiosa: Es un activo corporativo que tiene valor en sí mismo.

Sensitiva: Debe ser conocida por las personas que necesitan los datos.

Los usuarios de un sistema son una parte a la que no hay que olvidar ni menospreciar, "**Siempre hay que tener en cuenta que la seguridad comienza y termina con personas**".

1.1 Tipos de Seguridad Informática

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en tres tipos: Seguridad Física, Seguridad Ambiental y Seguridad Lógica.

1.1.1 Seguridad Física

Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del departamento de sistemas y equipos, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

1.1.2 Seguridad Ambiental

Son los procedimientos existentes para controlar que los efectos ambientales no perjudiquen el procesamiento, los equipamientos y el personal de una red. Algunas reglas básicas sobre la seguridad ambiental son: Protectores de pico de tensión eléctrica para el equipamiento central, protecciones eléctricas, de agua y gas, instalaciones de aire acondicionado, sistemas de refrigeración y ventilación fluida, protección ante incendios y métodos eficaces de evacuación guiados.

1.1.3 Seguridad Lógica

Nos referimos a seguridad lógica como los procedimientos existentes para controlar el acceso lógico no autorizado a la información, ya sea que se realice mientras ésta se encuentra almacenada o durante la transmisión, es decir, la seguridad a nivel de los datos, en especial los datos de la empresa, las aplicaciones e incluso los sistemas operativos de las compañías.

1.2 Situación actual en el medio empresarial

En la web de Ramón Millán, quien brinda consultoría estratégica en tecnologías de la información [3], se menciona que los problemas de seguridad en sistemas basados en redes responden a la siguiente distribución: Errores de los empleados 50%, Empleados deshonestos 15%, Empleados descuidados 15%, otros 20% (Intrusos ajenos a la Empresa 10%; Integridad física de instalaciones 10%).

Se puede notar que el 80% de los problemas, son generados por los empleados de la organización, y, éstos se podrían tipificar en tres grandes grupos: Problemas por ignorancia, haraganería y malicia. Entre éstas razones, la ignorancia es la más fácil de direccionar, la haraganería será siempre una tentación –tanto para los administradores de sistemas como para los usuarios – pero, se

encuentra que éste es un problema menor cuando los usuarios ven las metas de los sistemas de seguridad, la malicia, se debe combatir creando una cultura en la organización que aliente la lealtad de los empleados.

Por otro lado, como lo muestra la tabla 1.2 hay que tomar muy en cuenta los niveles de seguridad [4], ya que conociendo el nivel en el cual nos hallamos, será más fácil saber si nuestras políticas están funcionando o si debemos migrar a otras.

Tabla 1.2 Niveles de Seguridad.

Nivel de seguridad (%)	Aspectos	Consideración
0-25	No presentan políticas de seguridad.	**inaceptable**
26-50	Presenta pero no son las adecuadas.	**Poco aceptable**
51-75	Presenta algunas políticas aceptables pero necesita de otras.	**Medianamente aceptables**
76-100	La mayoría de las políticas son adecuadas, sin decir que se llegó a la excelencia.	**Aceptable**

1.3 Mecanismos Básicos de Seguridad

Los mecanismos básicos de seguridad, sin importar que tecnología sea utilizada son: autenticación, autorización, administración, auditoria y mantenimiento de la integridad de los datos. Cualquiera de los cinco mecanismos son llevados a cabo por medio del uso de técnicas de seguridad, las cuales si van a depender de la tecnología utilizada.

1.3.1 Autenticación

Es la verificación de la identidad del usuario, generalmente cuando ingresamos a la red, a una base de datos, o a muchos sitios. Típicamente para ingresar a un sistema se utiliza una contraseña, aunque es posible autenticarse, básicamente, de tres maneras: Por lo que uno sabe (una contraseña), Por lo que uno tiene (una tarjeta magnética), Por lo que uno es (las huellas digitales).

En primera instancia, nos referiremos a la autenticación mediante contraseñas, la fortaleza de este método está determinada por las características de la contraseña, cuanto más grande y difícil de adivinar esta sea, mas difícil será de burlar el mecanismo, como una medida complementaria se

debe sugerir el cambio de contraseña de manera periódica (30-60 días). Por ejemplo el Banco del pacífico en su web intermatico, obliga al cambio de claves cada 60 días.

1.3.2 Autorización

Es el proceso de determinar que, como y cuando, un usuario autenticado puede utilizar los recursos de la empresa. El grado de autorización puede variar dependiendo de que sea lo que se esté protegiendo, es importante que las autorizaciones queden registradas para ser controladas posteriormente. Es posible otorgar autorizaciones transitorias o modificar las anteriores otorgadas a medida que las necesidades de ese usuario varíen.

1.3.3 Administración

La administración incluye los procesos de definir, mantener y eliminar las autorizaciones de los usuarios del sistema, los administradores son los responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.

1.3.4 Auditoría

Es el proceso de recolectar información y analizarla, lo cual permite a los administradores u otros especialistas verificar que las técnicas de autenticación y autorización empleadas se realizan según lo establecido cumpliendo los objetivos fijados por la empresa. Ésta se puede realizar con una periodicidad acorde a la criticidad de la información protegida y al nivel de riesgo.

1.3.5 Mantenimiento de la Integridad

Mantener la información integra refiere a los procedimientos establecidos para evitar o controlar que los archivos permanezcan sin sufrir cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada. El mantenimiento de la integridad también involucra la prevención de cambios accidentales, lo cual generalmente se maneja por medio de códigos de manejo de errores.

1.4 Tipos de Ataques y Vulnerabilidades

Son todas aquellas acciones que suponen una violación de la seguridad de nuestro sistema, atentando contra la confidencialidad, integridad o disponibilidad de nuestra información con propósitos

desconocidos por el operador del sistema [5], y que por lo general, causan un daño (Anexo A). Se pueden clasificar según los efectos causados, como:

Interrupciones: Cuando un recurso del sistema es destruido o se vuelve no disponible.

Intercepciones: Alguien no autorizado consigue acceso a un recurso.

Modificaciones: Alguien no autorizado consigue acceso a una información y es capaz de manipularla.

Fabricaciones: Cuando se insertan objetos falsificados en el sistema.

Los ataques también se dividen según su forma de actuar, como por ejemplo:

Ataques de exploración: Ésta técnica consiste en buscar brechas de seguridad como puertos abiertos etc., y fijarse en los que puedan ser receptivos o de utilidad.

Ataques de autentificación: Cuando un atacante suplanta a una persona quien posee autorización.

Ataques de denegación de servicio (DOS): Consiste en saturar un servidor con pedidos falsos hasta dejarlo fuera de servicio.

Ingeniería social: Consiste en la obtención de información sensible y/o confidencial de un usuario cercano a un sistema u organización explotando ciertas características que son propias del ser humano, ya sea por ignorancia, negligencia o coacción, pueden permitir a un atacante obtener acceso no autorizado, quien, de esta manera, podrá eludir los complejos esquemas y tecnologías de seguridad que se hayan implementado en la organización.

CAPITULO 2.

Metodología de Seguridad "T.A.M.A.R.A"

La viabilidad de los proyectos y negocios sustentados en sistemas de información no está determinada por las bondades de la tecnología que se usa, puesto que también el desarrollo de éstas ofrece un nuevo campo de acción a conductas antisociales y delictivas, otorgando la facilidad de cometer delitos tradicionales en formas no tradicionales, atentando contra la confidencialidad, disponibilidad, seguridad de la infraestructura y los datos [6]. En consecuencia, esto ocasiona un aumento en el grado de vulnerabilidad e incertidumbre sobre la eficacia de los sistemas que guardan y protegen la información, lo cual ha convertido a la seguridad en una preocupación prioritaria para cualquier empresa.

FIGURA 2.1 INTRUSION EN LA RED

Por tal motivo hemos creado esta metodología de Seguridad Informática denominada **"T.A.M.A.R.A: Testeo, Análisis y MAnejo de Redes y Accesos"** seleccionado por su origen **hebreo** y que significa **"Da protección, brinda seguridad"**, la cual se fundamenta en los principios básicos de seguridad: confidencialidad, disponibilidad, integridad, y no repudiación, en ésta tratamos la implantación de controles o mecanismos de seguridad, basados en las políticas generales de la empresa, particularmente en las políticas y procedimientos de seguridad, con lo que se busca minimizar las vulnerabilidades expuestas y aumentar la seguridad de la información.

2.1 Objetivo de la Metodología

Ésta metodología tiene como objetivo poner en conocimiento de todas las personas que hacen uso de programas, sistemas o aplicaciones de propiedad de las empresas que la adopten, las consideraciones mínimas de seguridad para garantizar la integridad y buen recaudo de la información guardada, procesada, transmitida y

propagada por estas aplicaciones. A fin de preservar la confidencialidad, integridad y disponibilidad de la información, las disposiciones contenidas en esta Metodología deberán ser respetadas ya que el incumplimiento total o parcial de alguna de las políticas de ésta metodología estará sujeto a sanciones y/o acciones disciplinarias.

2.2 Explicación de la Metodología

Una vez conocido lo que es seguridad en términos de las redes, los tipos de seguridad, métodos básicos de seguridad, y las necesidades de seguridad que se dan en las empresas entre otros temas, es necesario emplear la metodología anteriormente expuesta para poner en práctica todos los pasos necesarios para cuidar de nuestros sistemas, reduciendo las vulnerabilidades e intrusiones. Primero observaremos que tipo de sistema queremos proteger: Sistema particular, pequeño, mediano o grande, Si el sistema es **particular** (Laptop o desktop que usamos en nuestra casa o en nuestra oficina y que no es de uso comercial ni público), lo que debemos verificar es si está o no conectada a internet, **si no hay una conexión a internet**, se deja a criterio personal las medidas de seguridad, pero se recomienda tener actualizada la base de firma de virus del antivirus que nos guste emplear o del que creamos es el mejor, las

actualizaciones de la PC ayudan, como así también tener activado el firewall de Windows (si se usa este sistema operativo), a mas de los criterios de seguridad que tengan los usuarios de cada equipo. Pero por el contrario, **si hay una conexión a internet**, debemos citar algunos principios de seguridad que son: simplicidad, adecuación, centrarse en los puntos débiles, economía y no reinventar la rueda.

También se citarán unas series de medidas que se consideran indispensables si hay una conexión a internet, las hemos denominado básicas y avanzadas. Las básicas son de implantación obligatoria y las avanzadas serán de implantación deseada.

En el caso de ser un sistema **pequeño** (Llámese así al cibercafé de la esquina de nuestras casas o a una pequeña red LAN) debemos tomar en cuenta las leyes y normas ecuatorianas para este nivel, ya que a medida que los sistemas se hacen más grandes necesitamos de éstas para no irrespetar las leyes y a la vez defendernos en caso de alguna irregularidad. También se cita quien es el organismo encargado de velar por la seguridad de la información en el Ecuador.

Por el contrario, si el sistema es **mediano** o **grande** (Empresa con más de 20 estaciones de trabajo), con el fin incrementar la seguridad se hace necesario realizar un análisis de riesgos, para identificar

aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad. De este modo, el estudio de estos riesgos debe abarcar varios frentes de seguridad, reduciendo al mínimo la efectividad de los ataques que pueden aprovechar los mismos, también mencionamos las lista de controles, que es un conjunto de ítems referentes a lo que habría de chequear en el funcionamiento del sistema, dependiendo del nivel de riesgo, se implementan las políticas de seguridad y luego se evalúa. Todo lo antes expuesto se resume en el siguiente gráfico:

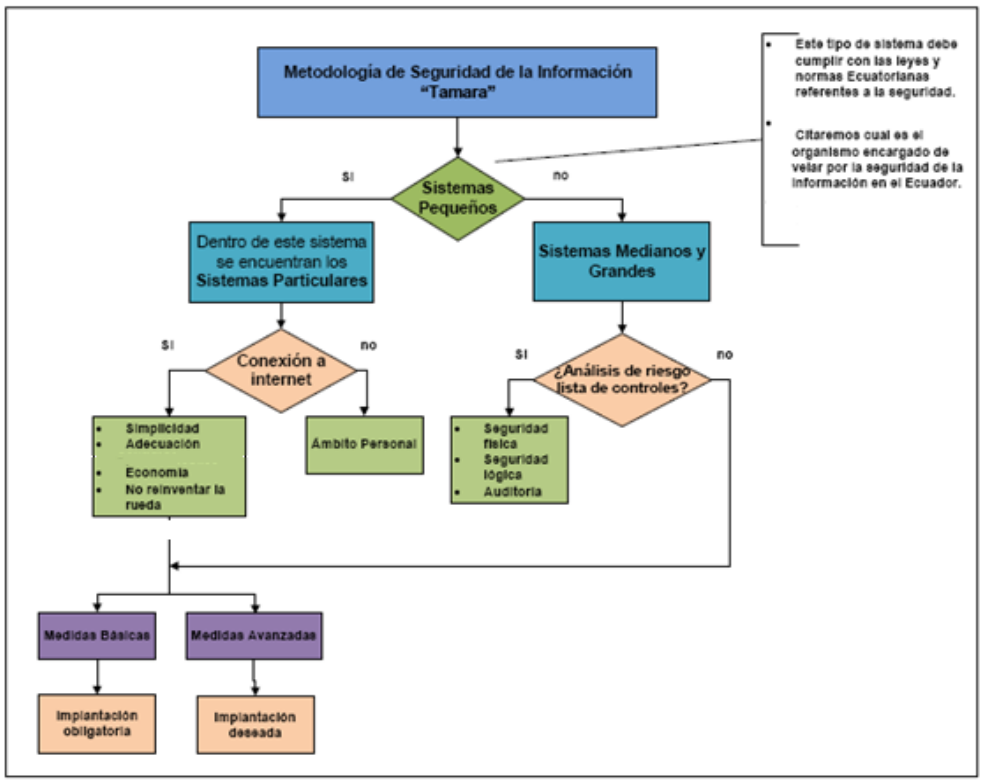


FIGURA 2.2 METODOLOGIA DE SEGURIDAD TAMARA

Teniendo en cuenta los diferentes aspectos anteriormente mencionados, solo las empresas con suficiente capital podrían implementar una solución de seguridad que contemple todos los temas necesarios; por tal motivo se ha hecho necesaria la elaboración de ésta metodología de seguridad apropiada para las empresas que no poseen estos recursos, la metodología creada busca satisfacer esta necesidad, con el fin de brindar y mejorar los ambientes de seguridad a un bajo costo, dándole, de esta manera, un enfoque social.

Hemos tratado en lo posible de no usar términos técnicos ni complicados en ésta metodología, esto es porque deseamos que sea legible tanto para el usuario común como para los administradores o gente de sistemas.

2.3 Ventajas y Desventajas de “T.A.M.A.R.A”

Ventajas:

La principal ventaja de ésta metodología es que de ser bien manejada, podremos mantener la integridad, disponibilidad, confidencial y no repudiación dentro del marco previsto de seguridad. Los usuarios solo tendrán acceso a lo que le corresponda al manejar las cuentas con privilegios, nos evitamos que algún usuario

descuidado provoque la intromisión de algún tipo de virus o algo peor.

Es de fácil lectura y comprensión, ya que no ahondamos en detalles técnicos ni proponemos términos difíciles para el usuario común. Nos proveerá de recursos para mantenernos informados sobre lo que pasa en nuestra PC, nos permite conocer nuestro sistema operativo y así hacer uso de utilidades de seguridad.

Nos permitirá saber qué hacer en caso de un ataque, ya sea en nuestra PC o en la de nuestra empresa. Es importante saber que hacer, ya que hay personas que piensan que nunca van a ser víctimas de fraude o ataques, pero están equivocadas, hay que recordar que todos somos vulnerables.

Desventajas:

La principal desventaja de ésta y de todas las metodologías de seguridad, es que se depende mucho de las personas (usuarios), ya que como se explicó en el primer capítulo, el 80% de los errores se produce dentro de las mismas empresas.

La ingeniería social, ésta es una de las formas más interesantes que tienen los hackers y no hackers para descubrir alguna vulnerabilidad a través de ti, ósea el usuario, es la forma más fácil de descubrir la clave de tu cuenta de correo, la de tu tarjeta, solo depende de ti el no dar información valiosa.

Debido a que en esta metodología proponemos algunas restricciones a los usuarios, éstos podrán tomarla de mal manera, pero deberán entender y hacer conciencia que es para el bien de ellos y la empresa donde se trabaja.

CAPITULO 3.

“T.A.M.A.R.A” en sistemas particulares y pequeños

En este capítulo aplicamos T.A.M.A.R.A a los sistemas particulares y pequeños, siendo los sistemas particulares aquellos que no tengan un uso comercial o público, Un ejemplo sería el ordenador de casa, o una laptop para uso personal [7]. Estos sistemas no están sujetos a normativas legales.

En cambio, los sistemas pequeños son los que tienen un uso comercial o público, como puede ser un cyber café, o pequeñas redes LAN. A continuación se detalla más a fondo cada sistema.

3.1 Sistemas Particulares

Creemos conveniente dividir los sistemas particulares en los que tienen una conexión a internet y los que no figura 3.1, ésta división nos facilitará la aplicación de medidas dependiendo el caso.

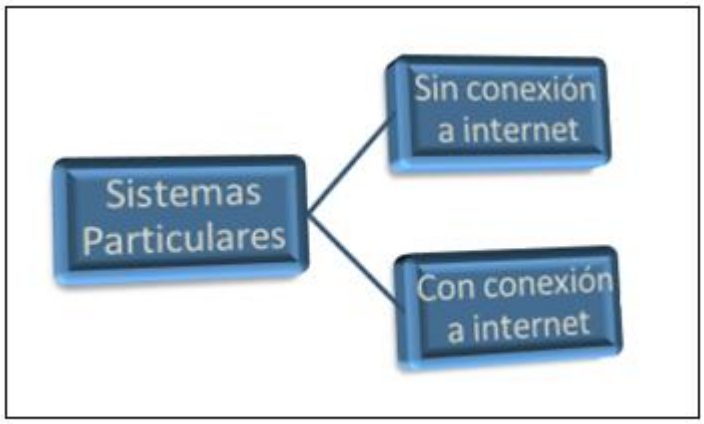


FIGURA 3.1 SISTEMAS PARTICULARES

Si el ordenador no está conectado a internet, el riesgo de pérdida de información, o de falta de confidencialidad es una decisión que solo afecta al ámbito personal, la situación cambia radicalmente si el ordenador está conectado a internet, aquí la falta de protección puede facilitar la expansión de virus, o los ataques de negación de servicio, al ser utilizado el ordenador para ataque sobre servicios claves de la red.

Los principios de seguridad deben de ser:

Simplicidad: Lo primero que se debe hacer es prestar atención para detectar el peligro y usar el sentido común para evitarlo.

Adecuación: Proporcionada al bien a proteger. No matar mosquitos a cañonazos.

Economía: El costo de las medidas de seguridad debe ser inferior al costo del bien a proteger. No Infravalorar los costes de los riesgos, ni supervalorar los costes de las salvaguardas.

No reinventar la rueda: Parte del trabajo seguro ya está hecho. Los sistemas incorporan muchas medidas de seguridad no utilizadas.

3.1.1 Medidas a usar

Hay una serie de medidas de salvaguarda que consideramos imprescindibles a este nivel, las clasificamos en “Básicas” y “Avanzadas”. Las básicas las consideramos de implantación obligatoria y las avanzadas serían de implantación deseadas (Anexo B).

3.2 Sistemas Pequeños

Éstos deberían de cumplir con las normas y leyes de acuerdo a cada País. El porqué fue explicado en el capítulo 2.

3.2.1 Cumplimiento de la Legislación

Estas instalaciones deben cumplir las medidas expuestas en el punto 3.2 y como mínimo las leyes nacionales, por ejemplo la **ley de comercio electrónico, firmas electrónicas y**

mensajes de datos publicada en el registro oficial 735 del 31 de Diciembre del 2002 en la República del Ecuador, que en su título V menciona el tema de las infracciones informáticas [8], así como también **el perfil de los delitos informáticos en el Ecuador** de la Fiscalía general del estado [9].

En Ecuador, el organismo encargado de velar por la seguridad de la información en el área de informática según el registro oficial nº 139 del día miércoles 1^{ero} de agosto del 2007 es la **Subsecretaría de Informática** [10], en el apartado de documentación se pone a disposición todos los aspectos del siguiente tipo: Legal y Normativa, Técnica de sistemas informáticos, Procedimientos subsecretaria informática. En el apartado de software se presenta: Software liberado por la subsecretaria informática, Software libre en general.

Por otro lado, existe una guía de buenas prácticas que describe los controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios, ésta fue publicada en Ecuador como NTE INEN-ISO/IEC 27002:2009 (Anexo C) desde el 4 de Mayo del 2007.

CAPITULO 4.

“T.A.M.A.R.A” en sistemas Medianos y Grandes

Como se mencionó en el primer capítulo, en los sistemas medianos o grandes (La empresa donde trabajamos o cualquier otra), con el fin incrementar la seguridad se hace necesario realizar un análisis de riesgos, para identificar aquellas brechas de seguridad que se encuentran expuestas hacia el exterior o el interior de la organización, así como facilitar la toma de decisiones sobre las formas de proteger sus bienes y los servicios que prestan a la comunidad.

4.1 Análisis de riesgos

Al crear una política de seguridad de la información, es importante entender que la razón para crear tal política es, en primer lugar, asegurar que los esfuerzos invertidos en la seguridad son

costeables. Esto significa que se debe entender cuáles recursos de la red vale la pena proteger y también entender que algunos recursos son más importantes que otros. Es decir se deberá identificar la fuente de amenaza de la que se protege a los recursos [11].

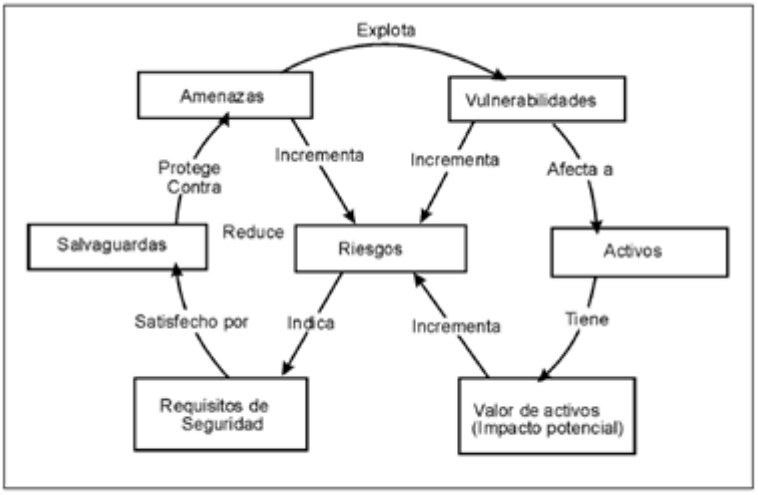


FIGURA 4.1 ANALISIS DE RIESGOS

El análisis de riesgos implica determinar lo siguiente: ¿Qué se necesita proteger?, ¿De quién protegerlo? Y ¿Cómo protegerlo? , los riesgos se clasifican por el nivel de importancia y por la severidad de la pérdida. No se debe llegar a una situación donde se gasta más para proteger aquello que es menos valioso.

En el análisis de los riesgos, es necesario determinar los siguientes factores:

Pi= Estimación del riesgo de pérdida del recurso.

W1= Estimación de la importancia del recurso.

Como un paso hacia la cuantificación del riesgo de perder un recurso, es posible asignar un valor numérico. Por ejemplo, al riesgo Pi de perder un recurso, se le asigna un valor de cero a diez, donde cero, significa que no hay riesgo y diez es el riesgo más alto. De manera similar, a la importancia de un recurso W1 también se le puede asignar un valor de cero a diez, donde cero significa que no tiene importancia y diez es la importancia más alta.

La evaluación general del riesgo será entonces el producto del valor del riesgo y su importancia (también llamado el peso WPi **= $\boldsymbol{W} * \boldsymbol{Pi}$**)

Dónde:

WPi**:** Es el peso del riesgo del recurso “i”

Pi**:** Es el riesgo del recurso “i”

Wi**:** Es la importancia del recurso “i”

Como podemos ver en el ejemplo práctico de CNEL Regional Milagro (Anexo D), nos damos cuenta que el recurso que debemos proteger más es el Servidor (Anexo E) ya que su riesgo ponderado es muy alto. Hay que tener muy en cuenta que, al realizar el análisis de riesgo, se deben identificar todos los recursos (por más triviales que parezcan) cuya seguridad está en riesgo de ser quebrantada, ahora bien, ¿cuáles son los recursos? Los recursos que deben ser considerados al estimar las amenazas a la seguridad son solamente seis:

Hardware: Procesadores, tarjetas, teclados, terminales, estaciones de trabajo, Computadoras personales, impresoras, unidades de disco, líneas de comunicación, cableado de la red, servidores de terminal, routers, bridges.

Software: Programas fuente, programas objeto, programas de diagnóstico, sistemas operativos, programas de comunicaciones.

Datos: Durante la ejecución, almacenados en línea, archivados fuera de línea, back-up, bases de datos.

Gente: Usuarios, personas para operar los sistemas.

Documentación: Sobre programas, hardware, sistemas, procedimientos administrativos locales.

Accesorios: Papel, formularios, cintas, información grabada.

La pregunta que cabe formular, luego de haber hecho el trabajo anterior, es ¿cómo protegemos ahora nuestros recursos? Tal vez, ésta sea la pregunta más difícil de responder, pues, según el recurso del que se trate, será el modo de protegerlo, pero primero, deberemos saber quiénes son los que van a hacer uso de los recursos. Es decir se debe contar, previamente, con un conocimiento cabal de todos los usuarios que tenemos en el sistema. Al realizar la lista de usuarios, debemos separarlos por grupos y sus necesidades en el sistema. Una vez identificados los usuarios (o grupos de usuarios), se puede realizar la determinación de los recursos de que harán uso y de los permisos que tendrán. Esto es sencillo de realizar con una tabla como la siguiente:

Tabla 4.1. Determinación de los Recursos

Recurso del Sistema		Identificación del usuario	Tipo de acceso	Permisos otorgados
Número	Nombre			
1	Base Datos	Auditores	Local	Lectura
2	Router	Grupo de mantenimiento de comunicaciones	Local y Remoto	Lectura y escritura

Este modelo, nos permitirá disponer para cada usuario (o grupos de usuarios), la información de qué se les está permitido hacer y qué no. El otro problema que nos presentamos, es el de las intromisiones clandestinas. Aquí, es preciso tener en cuenta el tipo de recurso a proteger. En base a ello, estará dada la política de seguridad.

Daremos, a continuación, algunos ejemplos acerca de a qué nos estamos enfrentando: ¿Cómo aseguramos que no están ingresando a nuestro sistema por un puerto desprotegido o mal configurado? (Anexo F). ¿Cómo asegurarnos no se estén usando programas del sistema operativo para ingresar al sistema en forma clandestina? , ¿Cómo aseguramos de que, ante un corte de energía eléctrica, el

sistema seguirá funcionando?, ¿Cómo nos aseguramos de que los medios de transmisión de información no son susceptibles de ser monitoreados?, ¿Cómo actúa la organización frente al alejamiento de uno de sus integrantes?, La respuesta a éstas interrogantes reside en la posibilidad de conseguir dicha seguridad por medio de herramientas de control y seguimiento de accesos, utilizando listas de controles (Anexo G) para comprobar puntos importantes en la configuración y/o funcionamiento de los sistemas y por medio de procedimientos que hacen frente a las distintas situaciones

4.2 Implementación del sistema de seguridad que minimiza los riesgos

Es conveniente citar en esta sección el área física y también la parte lógica (software, sistemas operativos etc.) para poder establecer las políticas y procedimientos de seguridad [12].

4.2.1 Área Física

La seguridad física es una de las vías fundamentales para minimizar los riesgos al interior de la empresa. Para la metodología creada, la fase de aseguramiento físico se enfocó en 4 temas principales (Anexo H):

FIGURA 4.2 CUARTO DE SERVIDORES

4.2.2 Seguridad Lógica

Dentro de las herramientas que se utilizan a diario en una organización se encuentra el sistema operativo, el cual controla el acceso y uso de los recursos de una maquina, siendo uno de los elementos más apetecibles para intentar explotar cualquier vulnerabilidad, por lo tanto, en un sistema operativo se debe contemplar: Identificación y autentificación de los usuarios, Control de acceso a los recursos del sistema, Monitorear las acciones realizadas por los usuarios, Auditoria de los eventos de posible riesgo, Garantía de integridad de los datos almacenados, Garantía de la disponibilidad de los recursos.

La mayoría de los problemas de seguridad comienzan por una mala configuración de los servicios, los cuales son dispuestos

con sus configuraciones por defecto, lo cual hace que, para un atacante, sea mucho más sencillo el tener control de estos.

En consecuencia dentro de la metodología se elaboraron una serie de recomendaciones y lista de chequeo, con las cuales la organización se puede ayudar para la eliminación de las vulnerabilidades que se encuentran presentes en los dispositivos tales como firewalls e IDS principalmente, los cuales ayudan a la protección de las redes organizacionales, pero que por sí solos no constituyen la solución final a todos los problemas de seguridad; sistemas operativos, servidores y demás, que hacen parte de la arquitectura de red de la compañía. De la misma manera se encuentran las herramientas de apoyo, como lo son los escaneadores de puertos y sniffers, brindan un gran soporte para la comprobación de las configuraciones previamente establecidas.

4.2.3 Evaluación del sistema de seguridad

Una vez implementada la metodología y aseguradas todas las áreas que se tuvieran en cuenta en el plan de seguridad, se procede con la auditoria de sistemas, con el fin de verificar el

éxito de la implementación y el buen desempeño de los sistemas de información, ya que se determina si estos salvaguardan los activos, mantienen la integridad de los datos y utilizan eficientemente los recursos. Dentro de las principales áreas que hacen parte de la auditoria de sistemas, se encuentran (Anexo I):

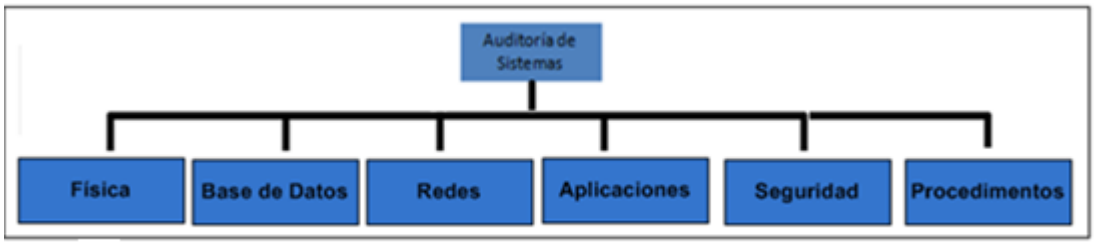


FIGURA 4.3 AUDITORIA DE SISTEMAS

4.3 Impacto en la Organización

La implementación de políticas de seguridad, trae aparejados varios tipos de problemas que afectan el funcionamiento de la organización. ¿Cómo pueden impactar si se implementan para hacer más seguro el sistema? En realidad, la implementación de un sistema de seguridad conlleva a incrementar la complejidad en las operaciones de la organización, tanto técnica como administrativa.

Por ejemplo, en el punto de seguridad administrativa (Área Física) se toman algunas medidas como deshabilitar los puertos USB, no se permitirá ingresar CDs etc. Esto va llevar que los usuarios tomen ciertas medidas de rechazo, ya que no podrán instalar ni almacenar nada si no es con la autorización del personal responsable, pero deben entender que estas son medidas de la empresa, para así poder lograr tener nuestra información segura sin que se produzcan infiltraciones.

Por otro lado, al poner en funcionamiento una nueva norma de seguridad, ésta traerá una nueva tarea para la parte técnica (por ejemplo, cambiar los derechos de algunos usuarios y cosas por el estilo) y administrativamente, se les deberá avisar por medio de una nota de los cambios realizados y en qué les afectará.

4.3.1 Visibilidad del Proceso

La visibilidad es permitir el aporte de las personas de la organización y, dar a conocer las acciones tomadas. Es decir que, cuando se deben producir cambios en las políticas no es necesario que se decidan unilateralmente.

Es altamente deseable que se formen grupos de trabajo para discutir y/o conocer el alcance y el tipo de medidas a llevar a cabo. Esto, además de llevar algunas veces a obtener soluciones que son más efectivas que las que se pensaban tomar, hace que aquellos que sean tocados por las modificaciones no se sientan recelosos de los cambios realizados y se comprometan con el cambio. Luego, una vez tomada la decisión, se debe comunicar a los involucrados de los cambios realizados por medio de notas o boletines informativos

4.3.2 Implementación

La implementación de medidas de seguridad, es un proceso técnico-administrativo. Como este proceso debe abarcar toda la organización, sin exclusión alguna, ha de estar fuertemente apoyado por el sector gerencial, ya que sin ese apoyo, las medidas que se tomen no tendrán la fuerza necesaria.

Será necesario hacer un balance cuidadosamente entre la ganancia en seguridad respecto de los costos administrativos y

técnicos que se generen. También, como hemos mencionado anteriormente, es fundamental no dejar de lado la notificación a todos los involucrados en las nuevas disposiciones y, darlas a conocer al resto de la organización con el fin de otorgar visibilidad a los actos de la administración.

CONCLUSIONES:

1. Con esta metodología podemos brindar a más de seguridad, control y administración de los accesos a las empresas y a sus respectivas áreas tecnológicas.

2. El nivel de aceptación de las metodologías y normas de seguridad depende de un factor social, el mismo que está totalmente desligado de un tema técnico (el cual también viene a ser un factor muy importante al momento de implementar dicha metodología o norma). En Ecuador específicamente en el área de seguridad de la información informática se han presentado situaciones las cuales dejan mucho que desear, esto se debe porque al momento de implementar una metodología o norma, la aceptación por parte de las personas o usuarios ha sido nula, ocasionando de esta manera que los sistemas de accesos queden vulnerables a personas mal intencionadas o simplemente “curiosas” como por ejemplo cuando se comparte contraseñas o se pide ayuda al hacer una transferencia .Con esto se concluye que los sistemas de gestión de seguridad de la información dependen directamente de los factores técnico y social.

3. Previo al planteamiento de soluciones ante los problemas que se presentan en las empresas y porque no decirlo en vuestros hogares, fue necesario establecer claramente cuáles son las falencias más comunes, realizando un proceso investigativo, se descubrió que hay personas que no saben proteger sus PCs, otras que no sabían de leyes etc. Esto se lo trata en el capítulo 2, el capítulo 3 lo dejamos para las empresas medianas y grandes donde se tratan temas de accesos y controles, en todos estos sistemas podemos concluir diciendo que "siempre hay que tener en cuenta que la seguridad comienza y termina con personas".

4. Viviendo experiencias en época de pasantías (CNT Regional Los Ríos, CNEL Regional Guayas-Los Ríos) se pudo observar que las políticas de seguridad definidas en las respectivas áreas de sistemas eran muy básicas (o muy pobres), lo que ocasionaba que la empresa sea vulnerable en algunos casos, puesto que personas no autorizadas (pasantes) tenían acceso libre al cuarto de servidores, obteniendo algún tipo de información confidencial de la empresa. Aquí se menciona lo citado en el capítulo 3, que los errores de los empleados son un 50% y los empleados deshonestos un 15%. Podemos concluir diciendo que no se debe permitir libre acceso a lugares de suma importancia, solo personas capacitadas y autorizadas.

5. Todo mecanismo de protección de la información en una empresa debe estar enmarcado dentro de una política de seguridad adecuada. El seguimiento de una política consistente evita que las medidas de protección se vuelvan un obstáculo para el trabajo habitual de los empleados con los sistemas de información y garantiza la calidad y confidencialidad de la información presente en los sistemas de la empresa. Podemos concluir diciendo que esta metodología tiene un alto compromiso con la organización que la adopte, primero identificando las falencias para luego superarlas, logrando el nivel de seguridad requerido ya que "la seguridad absoluta no existe" pero si podemos hacer lo posible para que nuestras vulnerabilidades sean cada vez menores.

RECOMENDACIONES:

1. Crear manuales de configuración y administración para todos los dispositivos que forman parte de la infraestructura de las redes: switches, Puntos de Acceso, servidores de autenticación, servidores Active Directory, administrador y monitor de la red inalámbrica WCS. Esto sirve para que las personas que los administren a futuro, tengan a mano las configuraciones y como dar seguridad a estos equipos y así nos podemos evitar algunos errores.

2. Informar a los usuarios de los servicios y beneficios que nos proveen las redes, así como de su funcionamiento; además solicitar que se enmarquen en las políticas de seguridad establecidas. También se debe dar capacitación técnica al administrador de la red alámbrica o inalámbrica, dentro y fuera de la empresa, para que éste pueda dar un mejor mantenimiento a las redes y un mejor soporte a los usuarios.

3. Se recomienda monitorear periódicamente el funcionamiento de los equipos tales como enrutadores, conmutadores, cortafuegos mediante la interfaz web, o con algún software de monitoreo ya que de esta manera se preverá inconvenientes en la red.

4. Es recomendable documentar adecuadamente todas las modificaciones y correcciones que se realicen por los administradores de la red, esto sirve para analizar la factibilidad de nuevos cambios, en el caso de ser necesario.

5. Se debe mantener actualizado el software del equipo de seguridad perimetral, para así mejorar el nivel de software del equipo, y por tanto el mejorar el nivel de la seguridad perimetral de la empresa. También se recomienda seguir los siguientes consejos (Anexo J).

ANEXOS

ANEXO A

ATAQUES Y VULNERABILIDADES

ATAQUES

Todas aquellas acciones que suponen una violación de la seguridad de nuestro sistema, confidencialidad, integridad o disponibilidad. Con propósitos desconocidos por el operador del sistema y que, por lo general, causan un daño.

Se pueden clasificar según los efectos causados, como:

- Interrupción: cuando un recurso del sistema es destruido o se vuelve no disponible.
- Intercepción: una entidad no autorizada consigue acceso a un recurso.
- Modificación: alguien no autorizado consigue acceso a una información y es capaz de manipularla.
- Fabricación: cuando se insertan objetos falsificados en el sistema.

Según la forma de actuar:

- Escaneo de puertos: esta técnica consiste en buscar puertos abiertos, y fijarse en los que puedan ser receptivos o de utilidad.
- Ataques de autentificación: cuando un atacante suplanta a una persona con autorización.
- Explotación de errores: suceden en el momento que se encuentran agujeros de seguridad en los sistemas operativos, protocolos de red o aplicaciones.
- Ataques de denegación de servicio (DOS): consiste en saturar un servidor con pedidos falsos hasta dejarlo fuera de servicio.
- Ingeniería social
- Por ignorancia o a causa de un engaño, el usuario, genera una vulnerabilidad en el sistema al brindar información al pirata informático

PIRATAS

¿Qué es un hacker?

El término hacker se usa con frecuencia para referirse a un pirata informático.

Diferentes tipos de piratas:

- Los hackers de sombrero negro
- Los hackers de sombrero blanco
- Crackers
- Hacktivistas

VULNERABILIDAD

Vulnerabilidad es definida como un fallo en el proyecto, implementación o configuración de un software o sistema operativo que, cuando es descubierta por un atacante, resulta en la violación de la seguridad de un computador o un sistema computacional

Tipos de puntos vulnerables:

- Aumento de privilegios. Los más terribles permiten tomar el control de los programas ejecutados con privilegios de administrador
- Generación de error de sistema. El objetivo de algunos puntos vulnerables es saturar un programa informático para que se bloquee.

TIPOS DE ATAQUES

PHISHING

¿Qué es el Phishing?

El Phishing es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo, todos los datos posibles para luego ser usados de forma fraudulenta.

¿En qué consiste?

Consiste en engañar al estafado suplantando la imagen de una empresa o entidad pública de esta manera hacen creer a la posible víctima que realmente los datos solicitados proceden del sitio Oficial cuando en realidad no lo es.

WEB FALSA DE RECARGAS

Es una variante del Phishing que solo busca un propósito, robar datos bancarios a los usuarios. Detrás de llamativas ofertas prometiendo recargas más económicas se puede esconder una estafa, que lo único que busca es hacerse con información del usuario.

SCAM

Es la captación de personas por medio de correos electrónicos, anuncios en web de trabajo, chats, etc. donde empresas ficticias le ofrecen trabajar

cómodamente desde casa y cobrando unos beneficios muy altos. Sin saberlo, la víctima esta blanqueando dinero obtenido por medio del Phishing.

Siempre le piden que tenga o abra una cuenta bancaria. Su trabajo consiste en recibir transferencias bancarias a su cuenta bancaria, sacar este dinero posteriormente para enviarlo a países extranjeros por medio de empresas tipo Western Union, Money Gram. Mandan un contrato (falso) para hacer más creíble la oferta.

PHISHING-CAR

¿Qué es el Phishing-Car?

Captación de compradores de coches a un coste muy bajo, la venta nunca se efectúa, esta persona realiza un pago como seña, se queda sin dinero y sin coche.

PHARMING

¿Qué es el PHARMING?

Es una técnica para llevar a cabo estafas online, consiste en manipular las direcciones DNS que utiliza el usuario, con el objetivo de engañarle y conseguir que las paginas que visite el usuario no sean realmente originales aunque su aspecto sea idéntico.

LOTERIAS FALSAS

Falso premio de loterías, el usuario recibe un correo electrónico donde le notifican que tiene un premio de lotería, si un usuario contesta a este correo le solicitara a continuación todos datos bancarios para un falso ingreso del premio. En otros casos se le solicita un parte del premio que tendrá que enviarlo a un país para poder cobrar el premio completo. En todos los casos el premio es falso.

XPLOITS

Es el nombre con el que se identifica un programa informático malicioso, o parte del programa, que trata de forzar alguna deficiencia o vulnerabilidad de otro programa.

El fin puede ser la destrucción o inhabilitación del sistema atacado, aunque normalmente se trata de violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.

Tipos de xploits:

- Xploits de postales (Tuparada/TarjetasBubba/más).
- Xploits de Nuevo Virus informático
- Xploits de pornografía.
- Xploits de reactivar cuenta Hotmail.

TROYANOS

Infecta basándose en la ingeniería social (dependerá de ti que te infecten o no, una vez infectados tendrán un control completo sobre tu ordenador), los troyanos normalmente suelen venir en archivos ejecutables (.exe) y escondidos, por ejemplo en juegos.

KEYLOGGERS

El keylogger es un diagnóstico utilizado en el desarrollo de software que se encarga de registrar las pulsaciones que se realizan sobre el teclado, para memorizarlas en un fichero o enviarlas a través de Internet

PROGRAMAS DE FUERZA BRUTA

En criptografía, se denomina ataque de fuerza bruta a la forma de recuperar una clave probando todas las combinaciones posibles hasta encontrar aquella que permite el acceso.

¿Cómo funcionan?

Suelen utilizar las palabras clave más comunes en los passwords o ir probando con todas las letras alfabéticamente ej.: aaaaaa, aaaaab, aaaaac.

SPYWARE

Cualquier aplicación informática que recolecta información valiosa de la computadora desde donde está operando. Es un tipo de malware que por lo general se introduce y opera en las PCs sin que el usuario lo advierta.

También hay espías que entran en las computadoras cuando el usuario acepta las condiciones de uso de un programa al instalarlo, por lo general ese texto es obviado en la instalación.

Además de verse vulnerada la privacidad de los usuarios, los spyware pueden producir pérdidas económicas pues pueden recolectar números de tarjetas de crédito y claves de accesos.

También pueden producir gran deterioro en el funcionamiento de la computadora tales como bajo rendimiento, errores constantes e inestabilidad general.

ROBO DE COOKIE

Una cookie es un fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas.

Dado que las cookies pueden contener información sensible (nombre de usuario, un testigo utilizado como autenticación, etc.), sus valores no deberían ser accesibles desde otros ordenadores. Sin embargo, las cookies enviadas sobre sesiones HTTP normales son visibles a todos los usuarios que pueden escuchar en la red utilizando un sniffer de paquetes. Estas cookies no deben contener por lo tanto información sensible.

El proceso que permite a una parte no autorizada recibir una cookie se llama robo de cookies, y la encriptación no sirve contra este tipo de ataque.

DATOS DE INTERÉS:

Argentina se ubicó en 2008 a nivel regional segundo en producir spam y bot (ataques encubiertos), y tercero en actividad maliciosa. Pero a nivel mundial clasificó en el cuarto puesto como lugar de origen de ataques informáticos, y en el duodécimo entre los productores de bot.

Programas/Páginas para hackear:

John the Ripper (fuerza bruta)

foro.portalhacker.net

Www. elhacker.org

ApSniffer: Es un scanner wireless cuyo objetivo es conseguirnos acceso a redes WLAN obteniendo todas las redes Wireless dentro de nuestro radio de alcance.

Credit Wizard v1.1 b1: Permite generar fakes de tarjetas de crédito pero de un modo profesional. Permite ingresar información y datos personales para personalizar la generación de tarjetas de crédito. También incorpora un genial generador de datos aleatorios, lo cual simplifica notablemente la tarea de realizar fakes.

Consejos para defenderse de ataques:

Mantener el sistema operativo y las aplicaciones actualizadas.

Un buen firewall con el que evitaremos el escaneo de puertos y el acceso no autorizado a nuestro ordenador.

Un antivirus que apoye el trabajo del firewall.

Cambiar las contraseñas que viene por defecto en el sistema operativo.

Poner especial cuidado a la hora de compartir archivos y recursos

Coloque listas de acceso en los routers. Esto reducirá su exposición a ciertos ataques de negación de servicio.

Instale parches a su sistema operativo contra Flooding. Esta acción permitirá reducir sustancialmente su exposición a estos ataques aunque no pueda eliminar el riesgo en forma definitiva. Incluya como parte de su rutina, el examen de su seguridad física. Considere, entre otras cosas, los servidores, routers, terminales desatendidas, puertos de acceso de red y los gabinetes de cableado. Invalide cualquier servicio de red innecesario o no utilizado. Esto puede limitar la capacidad de un hacker de aprovecharse de esos servicios para ejecutar un ataque de negación de servicio Utilice una clave mínima de 8 caracteres alfanuméricos, esto ayudara en su seguridad como muestra la siguiente tabla.

Tabla 1.1. Manejo de caracteres en contraseñas

Longitud en caracteres	26 Letras (minúsculas)	36 Letras y dígitos	52 (Mayúsculas y minúsculas)	96 Todos los caracteres
6	50 minutos	6 horas	2.2 días	3 meses
7	22 horas	9 días	4 meses	23 años
8	24 días	10.5 meses	17 años	2287 años
9	21 meses	32.6 años	881 años	219000 años
10	45 años	1159 años	45838 años	21 millones años

Como puede apreciarse, resulta importante utilizar más de 8 caracteres y cuantos más símbolos intervengan, menos probabilidades habrán de encontrar la password.

ANEXO B

Medidas Básicas y Avanzadas

Hay una serie de medidas de salvaguarda que consideramos imprescindibles a este nivel, las clasificamos en “Básicas” y “Avanzadas”. Las básicas las consideramos de implantación obligatoria y las avanzadas serían de implantación deseadas.

Medidas Básicas

- Instalación de un sistema operativo seguro (Control de acceso y permisos).
- Programa de antivirus actualizado.
- Cortafuegos personales de libre distribución (seguridad perimetral).
- Instale un bloqueador de Spyware gratuito. Manténgalo actualizado por lo menos una vez a la semana, usar herramientas de limpieza semanales.
- Programa de mantenimiento del registro de Windows (En el caso de utilizar este tipo de sistema operativo).
- Copias de seguridad (Para evitar pérdidas de información).
- Normas de uso del correo seguro (Véase Anexo K)
- Normas de navegación segura (Véase Anexo L)
- Si su conexión es a través de una red inalámbrica, active todas las opciones de seguridad disponibles, use el filtrado de MAC y use claves WPA si su hardware se lo permite.
- Si Vamos a comprar un adaptador de redes inalámbricas procuremos que sea enrutador y no solo Access point.

Medidas Avanzadas

- Sistemas de cifrado y autentificación (PGP). Utilización periódica de detectores de vulnerabilidades (Detectores de fallos de seguridad).

- No descargar “cosas Gratis”, screensavers, wallpapers, imágenes, tengamos presente que en este mundo nada es gratis y muchos de estos regalos traen sorpresas ocultas, como programas Espías.

- Las herramientas a utilizar en este caso son mayoritariamente de bajo costo y otras se pueden obtener de forma gratuita de sitios de distribución de software en Internet. Esto nos indica que no es la falta de herramientas de seguridad o su costo lo que hace que no se implemente una política de seguridad básica en los ordenadores de uso personal, Entendemos que es la falta de concienciación de los riesgos, unida a una falta de formación básica para entender estas herramientas.

ANEXO C

NTE INEN-ISO/IEC 27002:2009

Dominios (11), Objetivos de control (39) y Controles (133)

5. POLÍTICA DE SEGURIDAD.

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.

6.1 Organización interna.

6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.

6.2 Terceros.

6.2.1 Identificación de los riesgos derivados del acceso de terceros.
6.2.2 Tratamiento de la seguridad en la relación con los clientes.
6.2.3 Tratamiento de la seguridad en contratos con terceros.

7. GESTIÓN DE ACTIVOS.

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos.
7.1.2 Propiedad de los activos.
7.1.3 Uso aceptable de los activos.

7.2 Clasificación de la información.

7.2.1 Directrices de clasificación.
7.2.2 Etiquetado y manipulado de la información.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.

8.1 Antes del empleo.

8.1.1 Funciones y responsabilidades.
8.1.2 Investigación de antecedentes.
8.1.3 Términos y condiciones de contratación.

8.2 Durante el empleo.

8.2.1 Responsabilidades de la Dirección.
8.2.2 Concienciación, formación y capacitación en seguridad de la información.
8.2.3 Proceso disciplinario.

8.3 Cese del empleo o cambio de puesto de trabajo.

8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.

9. SEGURIDAD FÍSICA Y DEL ENTORNO.

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física.
9.1.2 Controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos e instalaciones.
9.1.4 Protección contra las amenazas externas y de origen ambiental.
9.1.5 Trabajo en áreas seguras.
9.1.6 Áreas de acceso público y de carga y descarga.

9.2 Seguridad de los equipos.

9.2.1 Emplazamiento y protección de equipos.
9.2.2 Instalaciones de suministro.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de los equipos.
9.2.5 Seguridad de los equipos fuera de las instalaciones.
9.2.6 Reutilización o retirada segura de equipos.
9.2.7 Retirada de materiales propiedad de la empresa.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.

10.1 Responsabilidades y procedimientos de operación.

10.1.1 Documentación de los procedimientos de operación.
10.1.2 Gestión de cambios.
10.1.3 Segregación de tareas.
10.1.4 Separación de los recursos de desarrollo, prueba y operación.

10.2 Gestión de la provisión de servicios por terceros.

10.2.1 Provisión de servicios.
10.2.2 Supervisión y revisión de los servicios prestados por terceros.
10.2.3 Gestión del cambio en los servicios prestados por terceros.

10.3 Planificación y aceptación del sistema.

10.3.1 Gestión de capacidades.
10.3.2 Aceptación del sistema.

10.4 Protección contra el código malicioso y descargable.

10.4.1 Controles contra el código malicioso.
10.4.2 Controles contra el código descargado en el cliente.

10.5 Copias de seguridad.

10.5.1 Copias de seguridad de la información.

10.6 Gestión de la seguridad de las redes.

10.6.1 Controles de red.
10.6.2 Seguridad de los servicios de red.

10.7 Manipulación de los soportes.

10.7.1 Gestión de soportes extraíbles.
10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.

10.8 Intercambio de información.

10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.

10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.

11. CONTROL DE ACCESO.

11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE

INFORMACIÓN.

12.1 Requisitos de seguridad de los sistemas de información.

12.1.1 Análisis y especificación de los requisitos de seguridad.

12.2 Tratamiento correcto de las aplicaciones.

12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.

12.3 Controles criptográficos.

12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.

12.4 Seguridad de los archivos de sistema.

12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.

12.5 Seguridad en los procesos de desarrollo y soporte.

12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.

12.6 Gestión de la vulnerabilidad técnica.

12.6.1 Control de las vulnerabilidades técnicas.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

13.1 Notificación de eventos y puntos débiles de seguridad de la información.

13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.

13.2 Gestión de incidentes y mejoras de seguridad de la información.

13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la continuidad del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sistemas de información

ANEXO D

Ejemplos Práctico

Ejemplo #1.

Supongamos una red simplificada con un router, un servidor y un bridge.

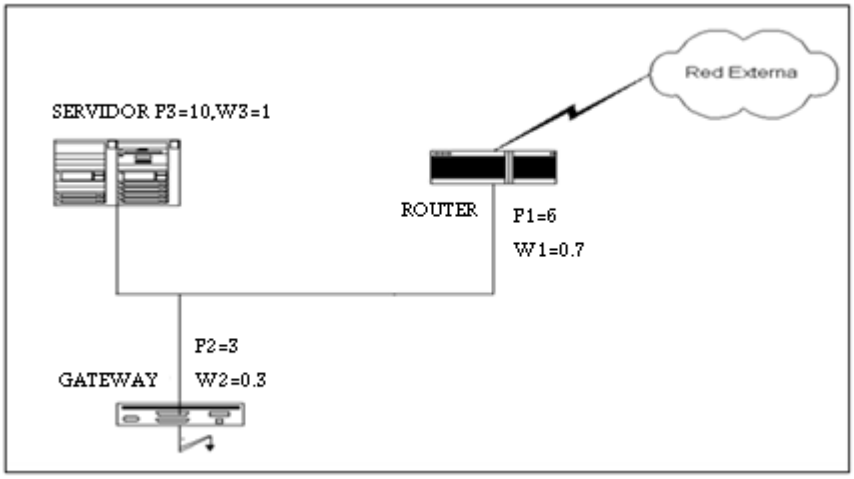


FIGURA 1. RED SIMPLIFICADA

El administrador de la red en la CNEL Regional Milagro ha producido las estimaciones siguientes para el riesgo y la importancia de cada uno de los dispositivos que forman la red:

Como se ve, a cada uno de los componentes de los sistemas, se le ha asignado un cierto riesgo y una cierta importancia. Hay que destacar que estos valores son totalmente subjetivos, dependen exclusivamente de quien ó quienes están realizando la evaluación.

Tenemos, entonces:

Router:	Bridge:	Servidor:
P1 = 6	**P2** = 6	**P3** = 10
W1 = 3	**W2** = **7**	**W3 = 10**

El cálculo de los riesgos evaluados, será, para cada dispositivo:

Router:
WP1 = P1 * W1 = 6 * 7 = 42

Bridge:
WP2 = P2 * W2 = 6 * 3 = 1.8

Servidor:
WP3 = P3 * W3 = 10 * 10 = 100

La tabla que sigue a continuación, nos muestra cómo podríamos llevar a cabo esta tarea de una manera ordenada y los valores que contiene son los que hemos tratado:

Recurso del Sistema		Riesgo (Pi)	Importancia (Wi)	Riesgo Evaluado (Pi*Wi)
Número	Nombre			
1	Router	6	7	42
2	Bridge	6	3	18
3	Servidor	10	10	100

Tabla.1 Niveles de Riesgos (Recursos Involucrados)

Ejemplo #2. **Efectividad de las Políticas**

Efectividad de las Politicas de Seguridad							
Amenaza	**Aspecto considerado en CNEL Regional Milagro**	**No Existe**	**Sin Efecto**	**Poco Efectíva**	**Efectíva**	**Muy Efectíva**	**Funcio_ nalidad(%)**
Falla de Servicio de Comunicaciones	*Falla del Proveedor de Internet*	x					0
	Caída de la Red Interna			x			30
Incumplimiento Legal	*Algún software sin licencia?*			x			30
Error de los Usuarios	*Eliminación de archivos del sistema*			x			30
	Des configuración de Impresoras					x	100
Error de los Adminis_ tradores de Red	*Actualización de Antivirus*					x	100
	Falla mantenimiento de Computadoras				x		60
	Mala configuración de Aplicaciones				x		60
Error de Monitorización	*Sniffer de Firewall*				x		60
Difusión de Software Dañino	*Instalación de Software sin licencia*			x			30
	No escaneo de flash memory		x				15
Vulnerabilidades de Programas	*Vulnerabilidades en Zeus Zimbra o Base de Datos*	x					0
Exceso Tráfico Multimedia	*Acceso a Páginas de Entretenimiento*			x			30
	Descarga de Archivos			x			30
	Ingreso al Messenger			x			30
Ataque en la Red	*Escaneo de Puertos*		x				15
	Ataques DOS		x				15
	TOTAL EFECTIVIDAD DE LAS POLÍTICAS SOBRE AMENAZAS DETECTADAS						635

Políticas Minimas implementadas	Efectividad				
	Sin Efecto	Poco Efectiva	Efectivo(%)	Muy Efectivo(%)	Funcionalidad
Protección de antivirus				x	100
Distribución de ancho de banda		x			15
Administración de grupos de usuarios				x	100
Distribución ade_ cuada equipos de interconexión				x	100
Ubicación ambien_ tal de servidores y firewall.			x		60
Uso adecuado del proxy				x	100
TOTAL EFECTIVIDAD					475

IMPACTO	VALORES DE LA EFECTIVIDAD (%)
No Existe	0
Sin Efecto	15
Poco Efectiva	30
Efectiva	60
Muy Efectiva	100

Efectividad de Políticas sobre Amenazas Detectadas	**635**
Efectividad Políticas existentes	**475**
Total Efectividad Políticas en la Red	**1110**

Número de amenazas detectadas	**9**
Número de amenazas que ya posee una política de seguridad	**6**
Total amenazas	**15**

$$NIVEL\ DE\ SEGURIDAD = \frac{TOTAL\ DE\ EFECTIVIDAD\ DE\ POLITICAS\ EN\ LA\ RED}{TOTAL\ AMENAZAS}$$

$$NIVEL\ DE\ SEGURIDAD = \frac{\mathbf{1110}}{\mathbf{15}} = \mathbf{74\%}$$

ANEXO E

Seguridad en Servidores y Firewalls

Servidores

Seguramente algunos administradores, responsables de sistemas, gerentes y directores, han vivido la experiencia de ver en peligro a sus servidores ya sea por un externo o peor aún por un interno. Ahora más que nunca es indispensable tener mejor controlados nuestros equipos y por ende, es necesario contemplar en el presupuesto todos los sistemas de seguridad que garanticen la disponibilidad del negocio.

Ahora nos enfocaremos hacia los servidores, ya que citaré los métodos más eficientes para la protección de estos equipos:

Seguridad perimetral: Chapas seguras, cámaras detectoras de movimiento, letreros de acceso limitado, son algunos de los métodos más comunes, podemos agregar chapas de combinación o sistemas biométricos, en cuanto a las cámaras pueden ser IP, de las que envían por correo cualquier evento en el punto y bien es importante poner letreros en donde se especifica de manera clara que solo personal autorizado puede entrar a este lugar.

Seguridad ambiental: El área debe de estar alejada de la humedad, calor extremo, zonas con cargas eléctricas fuertes o campos magnéticos altos, lugares de paso constante, instalaciones eléctricas improvisadas o en malas condiciones, es muy importante contar con sistemas contra incendios en las áreas de servidores que estén basadas en sistemas en seco ya sean polvos o gases y sistemas de medición de temperatura y humedad.

Control de acceso: Nos referimos al acceso a la información, nadie ajeno debe ver las carpetas de la empresa o la información de nuestros compañeros, para esto se tienen varias medidas a tomar el primero es cerrar todos los puertos del servidor dejando solo los indispensables, todos los elementos compartidos tienen que estar restringidos a los usuarios del dominio que estén registrados, debe contar con antivirus y firewall, en algunas ocasiones se ponen equipos dedicados a este fin, los cuales son muy buenos, además llevan el control de acceso a usuarios.

Bases firmes: Los sitios designados para instalar los servidores deben estar bien anclados, ya sean racks o charolas, es importante asegurarse que estén aterrizados, sujetos al piso y muros, perfectamente armados y que no tengan juego alguno, el piso de preferencia debe ser antiestático, y modular para hacer cableados limpios, al igual que el techo de preferencia modular y de materiales antiestáticos y ligeros.

Energía garantizada: En el caso de los servidores es mejor contar con sistemas redundantes en el caso de las fuentes de poder, en cuanto a la energía es bueno contar con un buen par de respaldos de energía que soporten la carga de los equipos, y que uno tenga una de las fuentes y el otro la otra fuente, después de este sistema es bueno tener el UPS de la empresa y al final de la cadena una planta de energía, si no se cuenta con el presupuesto para un sistema tan robusto, por lo menos contar con la planta y los respaldos de los servidores.

Sistemas de notificación: Es vital contar con sistemas de notificación vía SMS, correo electrónico, telefónicamente e incluso sistemas audibles en caso de una falla, esto apoyará para que sea posible detectar a tiempo algún problema, estos sistemas de notificación cada vez son más comunes, sobre todo en los sistemas profesionales, algunos de estos reportan desde fallas de energía hasta acceso de personal no autorizado.

Sistemas de respaldo: Pero ahora nos referimos a los datos, un buen sistema de respaldo es como un seguro de vida, es indispensable, los datos tienen que tener un ciclo de vida, no se deben perder nada y todo se debe salvar en cuestión de minutos, ya sean unidades de cinta, DVD o discos duros siempre debe de existir un respaldo de la información más importante del negocio.

Firewall

¿Qué es un firewall?

Un firewall es software o hardware que comprueba la información procedente de Internet o de una red y, a continuación, bloquea o permite el paso de ésta al equipo, en función de la configuración del firewall.

¿Por qué necesito un firewall?

Un firewall puede ayudar a impedir que piratas informáticos o **software malintencionado** (como **gusanos**) obtengan acceso al equipo a través de una red o Internet. Un firewall también puede ayudar a impedir que el equipo envíe software malintencionado a otros equipos.

Aunque crea que en el equipo no hay nada que pueda interesar a otras personas, un gusano puede deshabilitar por completo el equipo, o alguien puede usar el equipo para diseminar gusanos o **virus** a otros equipos sin su conocimiento.

¿Contra qué tipo de cosas no ofrece protección un firewall?

- Virus del correo electrónico

  Los virus del correo electrónico se adjuntan a los mensajes de correo electrónico. Un firewall no puede detectar el contenido del correo electrónico, de manera que no puede protegerlo contra los virus de ese tipo. Debe usar un programa antivirus para examinar y eliminar los archivos adjuntos sospechosos de un mensaje de correo electrónico antes de abrirlos. Aunque tenga un programa antivirus, no debe abrir un archivo adjunto de un mensaje de correo electrónico si no tiene absoluta certeza de que es seguro. Para obtener más información, consulte **Evitar los virus propagados por correo electrónico**.

- Estafas mediante suplantación de identidad (Phishing)

  La suplantación de identidad (Phishing) es una técnica que se utiliza para inducir a los usuarios de equipos, mediante engaños, para que revelen información personal o financiera, como una contraseña de una cuenta bancaria. Un engaño de suplantación de identidad (Phishing) habitual comienza con un mensaje de correo electrónico que parece proceder de un origen de confianza pero que realmente ordena a los destinatarios que proporcionen información a un sitio web fraudulento. Un firewall no puede detectar el contenido del correo electrónico, de manera que no puede protegerlo contra este tipo de ataque.

Si tengo un enrutador que tiene un firewall incorporado, ¿puedo activar también el Firewall de Windows?

Sí, porque los firewalls basados en **enrutadores** únicamente proporcionan protección frente a los equipos de Internet, no frente a los equipos de su red doméstica. Por ejemplo, si un equipo móvil o invitado se conecta a otra red, se infecta con un gusano informático y luego se conecta a su red local, el firewall del enrutador no podrá evitar la diseminación del gusano. Por otro lado, un firewall que se ejecute en cada equipo de la red puede ayudar a controlar la diseminación de gusanos.

¿Qué más necesito para proteger mi equipo, aparte de un firewall?

- Activar las Actualizaciones automáticas de Windows y comprobar que las **actualizaciones** se instalen automáticamente en el equipo.
- Conseguir un buen programa antivirus y mantenerlo actualizado
- Usar Microsoft Windows Defender u otro programa anti spyware. Estos programas pueden ayudarle a proteger el equipo contra **spyware** y otro software malintencionado.

ANEXO F

Seguridad en los Puertos

¿Que son los puertos?

Los puertos son las vías de comunicación que usan las computadoras para conectarse entre sí, para aclarar un poco más si nosotros nos conectamos al internet y pedimos ver una página web, nuestra maquina tendrá que habilitar un puerto (Vía de comunicación) para acceder al servidor web, el servidor web a retribución de esto nos abrirá un puerto y nos pedirá nuestra información (Ip) para identificar quien ingresa.

Como ya dije un puerto es el canal necesario para conectarse o comunicarse con otra computadora, y aunque poca gente sabe existe una cantidad impresionante de puertos. La computadora abre y cierra puertos según la necesidad de comunicación, como ejemplo puedo resaltar que para jugar en red un juego como Fifa2004 abre un puerto especifico para conectarse con la otra máquina.

Ahora que ya tenemos un pequeño concepto de que es un puerto de PC, creo que es necesario decir un poco en que nos afectan, los puertos son como las puertas o ventanas de nuestras casas, nosotros podemos salir y entrar por la puerta principal de ella pero eso no evita que un mendigo ladrón nos entre por la ventana, o peor aun que aproveche el menor descuido posible y hasta se entre con nosotros por la puerta principal sin darnos cuenta. Los puertos sin una seguridad buena, pueden ser usados para observar nuestras computadoras, robarnos información, espiarnos, etc.

Lista de Puertos

* 21 (Puerto de Ftp)
* 4661,4662 (Puertos usados para Conexiones P2P como Emule y otros)
* 47624 (Puerto para juegos de en red por lo general)
* 25 (Puerto de conexión de smtp)
* 80 (Puerto del Http)
* 119 (Puerto nntp)
* 139 (El famoso puerto de NetBIOS)
* 445 (Móvil Ip)
* 531 (Puerto IRC)
* 1521 (Puerto para Oracle y SQL)
* 3306 (Puerto para Mysql)
* 40193 (Puerto para Novell)

Como defendernos

Bueno para empezar creo que lo más urgente siempre es cerrar el famoso puerto 139 de NetBIOS de Windows.

Lo que primero debemos hacer es ir a panel de control ---> Conexiones en Red ---> Elegimos el Grupo de red al que pertenecemos ---> Propiedades ---> Elegimos el protocolo TCP / IP ---> Propiedades ---> Presionamos el botón de Opciones avanzadas ---> Elegimos la pestaña WINS ---> Elegimos Deshabilitar NetBIOS ---> Reiniciamos la PC.

Ahora si deseamos tener más seguridad de que no se pueda ingresar a nuestra maquina por este medio buscamos el archivo vnbt.386 que se encuentra en la carpeta SYSTEM o en la SYSTEM32 depende que versión de Windows se use, luego lo que hay que hacer es cambiarle el nombre, le colocamos una letra extra por ejemplo vnbta.386, reiniciamos la computadora y listo.

Ahora para saber que otros puertos debemos cerrar podemos escanear la máquina y así encontrar los puertos abiertos en la misma, bueno para no quedar como flojo explicare como pueden cerrar o abrir manualmente cada uno de los puertos que ustedes elijan:

Panel de Control ---> Conexiones de Red ---> Propiedades ---> Elegimos la viñeta Avanzadas ---> hacemos clic en la opción Proteger mi equipo ---> Presionamos el botón Configuración.

Aparecerá otra ventana donde están enlistados los puertos habilitados en la computadora, si queremos modificar o eliminar uno de ellos solo basta elegir el puerto y elegir el botón que corresponda de eliminar o modificarlo, acá encontrarán también el Botón Agregar, al hacer clic en él, deberán llenar en el primer espacio que les aparecerá en la ventana el comentario respecto al puerto, el segundo campo se debe colocar el nombre del equipo, en el tercer y cuarto campo debemos colocar el puerto para abrir internamente y externamente, luego debemos elegir al tipo de puerto que corresponde si es TCP o UDP y luego colocamos aceptar

¿Cómo puedo cerrar un puerto?

Atención: Un puerto abierto no es necesariamente peligroso! Estas en riesgo solo si el programa que usa el puerto tiene códigos dañinos. En realidad, sin tener puertos abiertos, simplemente no funcionaría internet!

Un puerto abierto no es un objeto autónomo, y no debería ser considerado como algo que puede ser destruido al cerrarlo. Si un puerto está abierto en tu ordenador, significa que hay un programa activo usando dicho número de

puerto para comunicarse con otros ordenadores en la web. Un puerto no es abierto por el sistema operativo, es abierto por un programa específico queriendo usarlo.

Para cerrar un puerto, usualmente solo es necesario cerrar el programa ó servicio que mantiene dicho puerto abierto. En algunos puertos basta con decirle a un programa o servicio que el puerto no debe estar abierto. Un buen ejemplo son los Servicios de Información de Internet de Microsoft, en Windows 2000 y Windows XP. Si son instalados, abren tres puertos automáticamente: 21, 25 y 80. El puerto 21 es el servidor FTP; el puerto 25 el servidor SMTP (servidor de email); y el puerto 80 el servidor web para HTTP.

El servidor FTP habilita a otros usuarios de internet a descargar archivos compartidos desde tu sistema. Pueden también subir archivos a tu sistema, si eliges permitirlo. El servidor SMTP es usado para enviar emails directamente a la casilla de correo del recipiente sin usar un servidor de correo externo. El servidor de correo te permite correr un sitio web en tu PC. Pero esto es solo alcanzable en tu dirección de IP. Si deseas hacer esto accesible al público, necesitas un nombre de dominio que redireccione a una dirección de IP estática.

Sin embargo, si no necesitas todos estos servidores, simplemente ciérralos y los puertos serán cerrados automáticamente. Abre el administrador de servicios en el panel de control - administrador de tareas. Servicios y programas que son abiertos automáticamente cuando se inicia el sistema sin ninguna ventana visible. Estos trabajan tras bambalinas (en el fondo).

Busca "servicio de publicación WWW" en la lista y haz clic en el icono Detener Servicio en la parte superior. El puerto 80 no estará más en uso, estará cerrado. Puedes hacer lo mismo con el "servicio de publicación FTP" y el "protocolo simple de transporte de Correo (SMTP)".

Sin embargo, no es siempre sencillo el averiguar porque un puerto está abierto. Un ejemplo es el puerto 5000 el cual es abierto de forma predeterminada por Windows ME y XP. Para esto, no hay servicio que puedas apagar, que cierre el puerto. Para cerrar este puerto, es necesario desinstalar cierto componente del sistema. El puerto 5000 es usado para "plug and play" con dispositivos de redes. Si cierras este puerto, la red "plug and play" (conecta y juega) no estará más disponible.

ANEXO G

Lista de Controles

Las listas de controles, como su nombre lo indica, son listas con un conjunto de ítems referentes a lo que habría que chequear en el funcionamiento del sistema. Ejemplos:

- Asegurar el entorno. ¿Qué es necesario proteger? ¿Cuáles son los riesgos?
- Determinar prioridades para la seguridad y el uso de los recursos.
- Crear planes avanzados sobre qué hacer en una emergencia.
- Trabajar para educar a los usuarios del sistema sobre las necesidades y las ventajas de la buena seguridad.
- Estar atentos a los incidentes inusuales y comportamientos extraños.
- Asegurarse de que cada persona utilice su propia cuenta.
- ¿Están las copias de seguridad bien resguardadas?
- No almacenar las copias de seguridad en el mismo sitio donde se las realiza.
- ¿Los permisos básicos son de sólo lectura?
- Si se realizan copias de seguridad de directorios/archivos críticos, usar chequeo de comparación para detectar modificaciones no autorizadas.
- Periódicamente rever todo los archivos de “booteo” de los sistemas y los archivos de configuración para detectar modificaciones y/o cambios en ellos.
- Tener sensores de humo y fuego en el cuarto de computadoras.
- Tener medios de extinción de fuego adecuados en el cuarto de computadoras.
- Entrenar a los usuarios sobre qué hacer cuando se disparan las alarmas.
- Instalar y limpiar regularmente filtros de aire en el cuarto de computadoras.
- Instalar UPS, filtros de línea, protectores gaseosos al menos en el cuarto de computadoras.
- Tener planes de recuperación de desastres.

- Considerar usar fibras ópticas como medio de transporte de información en la red.

- Concientizar a los usuarios de pulsar la tecla ESCAPE antes de ingresar su login y su password, a fin de prevenir los “Caballos de Troya”.

- Considerar la generación automática de password.

- No crear cuentas por defecto o invitado para alguien que está temporariamente en la organización.

- No permitir que una sola cuenta esté compartida por un grupo de gente.

- Deshabilitar las cuentas de personas que se encuentren fuera de la organización por largo tiempo.

- Deshabilitar las cuentas “dormidas” por mucho tiempo.

- Limitar el acceso físico a cables de red, routers, repetidores y terminadores.

- Los usuarios deben tener diferentes passwords sobre diferentes segmentos de la red.

- Monitorear regularmente la actividad sobre los Gateway.

ANEXO H

Área Física

Ubicación física, seguridad ambiental y disposición del centro de cómputo:

Este es uno de los puntos de mayor cuidado y atención, puesto que aquí se encuentra la infraestructura central de la información y de comunicaciones de las cuales depende la compañía para sus labores diarias.

Medidas:

- Todos los servidores deben encontrarse en Racks con puertas de seguridad para mantener los equipos lejos del alcance de personal no autorizado y tener control de los mismos. Así mismo protegerlos de agentes adversos del ambiente (polvo, humedad, etc.), estos deberán contar con los mecanismos de ventilación apropiados garantizando niveles óptimos de temperatura.

- Los equipos electrónicos contarán con un sello de seguridad (PC, servidores, UPS, switch, etc.) para garantizar que no sean manipulados por personas ajenas al departamento de sistemas, la verificación de la existencia de estos precintos es de responsabilidad de los administradores y del personal del área de Informática según corresponda. Y para evitar que los equipos puedan ser afectados por inundaciones se deben colocar los CPUs encima de los escritorios o en soportes colocados en la parte inferior de los mismos.

- El Centro de Computo y/o la sala de maquinas de todas las agencias debe contar con sistemas de aire acondicionado, un detector de humos y un extintor. También se tiene prohibido conectar a la red eléctrica de cómputo, cualquier dispositivo ajeno, por ejemplo (Electrodomésticos, Cargadores de baterías, etc.).

- En caso de corte de fluido eléctrico público, los UPSs deberán garantizar un tiempo de autonomía mínimo de 20 minutos aproximadamente. Tiempo en el cual se deberá activar el generador eléctrico (cada empresa debería tener uno), éste deberá tener la capacidad necesaria para proporcionar alimentación a los sistemas informáticos, Dependiendo de la empresa, se debe contar con un pozo a tierra, el cual deberá recibir mantenimiento para no tener sorpresas con descargas eléctricas y fenómenos parecidos.

- En algunos tipos de instituciones, donde sea necesario, las cámaras estarán dispuestas en zonas estratégicas monitoreando las operaciones en las ventanillas, en zonas de extrema seguridad (bóveda). Estos sistemas de vigilancia ayudan a minimizar el riesgo de asaltos o intentos de fraude en las ventanillas por el temor de ser fácilmente detectados.

Control de acceso físico:

Esta etapa refuerza la anterior, debido a que en ésta se dan parámetros para controlar el acceso de personas ajenas o no autorizadas a la organización.

Medidas:

- Toda persona que se acuda a las instalaciones, debe de identificarse y decir que actividad va a realizar en el área de recepción donde se les proporcionara un “Carnet de VISITANTE” a cambio de su cédula de Identidad, durante la permanencia de la persona en las instalaciones es necesario que la persona lleve el carnet visible, de no hacerlo el personal de seguridad comunicara a la persona la obligatoriedad de su uso mientras permanezca en las instalaciones. Cuando la persona finalice sus actividades devolverá el carnet y se le entregará su cédula.

- Está normado el uso obligatorio del carnet para todo el personal que labora en la empresa con el propósito de detectar personas sospechosas dentro de la institución.

- El acceso al centro de cómputo será mediante tarjetas electrónicas. Y el acceso a la sala de servidores es restringido (solo personal autorizado), se deberá llevar un registro del ingreso y salida de las personas

Seguridad administrativa:

Busca la capacitación de los empleados de la organización en cuanto al manejo y aseguramiento de los recursos en general. Como complemento a la capacitación de empleados, se podrán realizar las siguientes acciones para que las personas encargadas de las PCs no instalen programas no autorizados

Medidas:

- Eliminación de los usuarios del grupo Administradores Locales, deshabilitación de Unidades lectoras de CD, deshabilitación de unidades de almacenamiento masivo USB.

- La deshabilitación de las unidades se hace tanto física (desconectar el componente de su fuente de poder) como lógicamente (en el Setup de la PC se deshabilita), el password del Setup de las PC lo maneja el

personal de soporte y comunicaciones, es así que el usuario deberá coordinar con el Jefe de Soporte y Comunicaciones la instalación de cualquier software ajeno a su perfil.

Realización de planes de contingencia:

Se ocupa de los procedimientos de recuperación, en caso de algún incidente de seguridad.

Medidas:

- El personal de Soporte y Comunicaciones deberá contar con un Plan de Mantenimiento de equipos donde se consignan las actividades y procedimientos a seguir. Los formatos que deben de utilizar para el control de tareas, es responsabilidad del Jefe de Soporte y Comunicaciones, es recomendable cumplir con este plan de trabajo. Una vez terminada con esta fase (área física), se procede con el aseguramiento lógico.

ANEXO I

Auditoría

Auditoría física

La auditoría es el medio que va a proporcionar la evidencia de la seguridad física en el ámbito en el que se va a desarrollar la labor profesional, por lo tanto se debe asumir que esta no se limita a comprobar la existencia de los medios físicos, sino también su funcionalidad, racionalidad y seguridad, así como también el correcto uso de las políticas y procedimientos de seguridad.

Auditoría de Bases de Datos

La importancia de la auditoria del entorno de bases de datos radica en que es el punto de partida para poder realizar la auditoria de las aplicaciones que utilizan esta tecnología.

Auditoría de Redes

En este punto ha de auditarse hasta qué punto las instalaciones físicas ofrecen garantías suficientes para la seguridad de datos. De la misma manera es necesario monitorear la red, revisar los errores o situaciones anómalas que se producen y además tener establecidos los procedimientos para detectar y aislar equipos posiblemente infectados o comprometidos.

Auditoría de Aplicaciones

El objetivo de este punto consiste en ayudar a planificar, preparar y llevar a cabo auditorias de aplicaciones en funcionamiento, en cuanto al grado de cumplimiento de los objetivos para los que estas fueron creadas.

Auditoría de la seguridad

Se evalúa si los niveles de seguridad están en concordancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones.

Auditoria de procedimientos

Este tipo de auditoría examina la eficiencia de los procedimientos de seguridad que se den en la compañía, permitiendo saber en que se es más fuerte o en que se tiene falencias.

ANEXO J

Las 10 leyes inmutables de la (in) seguridad

I. Si un intruso puede persuadirlo para ejecutar un programa en su computadora, esta deja de ser suya.

Una vez que un programa se está ejecutando, puede hacer cualquier cosa, incluso lo que usted mismo puede hacer en la máquina. Puede monitorear la pulsación de las teclas que usted realiza y enviarlas a un sitio Web.

Puede abrir todos los documentos que se hallan en la máquina y cambiar la palabra “quiero” por “no quiero” en todos ellos. Puede enviar emails groseros a todos sus amigos. Puede instalar un virus. Puede crear una “puerta trasera” que le permita a alguien controlar en forma remota su máquina. Puede llamar a un ISP en Katmandu. O bien, puede simplemente reformatear su disco rígido.

Por esta razón, es importante nunca ejecutar, o ni siquiera descargar, un programa proveniente de una fuente poco confiable — y con “fuente”, me refiero a la persona que lo escribió, no la que se lo dio a usted.

II. Si un intruso puede alterar el sistema operativo en su computadora, esta deja de ser suya.

Para comprender por qué, considere que los archivos de sistemas operativos están entre los más confiables de la computadora y, generalmente, se ejecutan con privilegios de sistema-operativo. Es decir, pueden hacer absolutamente todo.

Entre otras cosas, se les confía la administración de las cuentas de usuario, los cambios de contraseña y la implementación de las reglas que rigen quién puede hacer qué en la computadora. Si un intruso puede cambiarlos, los ahora no confiables archivos obedecerán sus órdenes y no hay límites en cuanto a lo que puede hacer.

Puede robar contraseñas, convertirse en un administrador de la máquina o agregar funciones totalmente nuevas al sistema operativo. Para prevenir este tipo de ataque, asegúrese de que los archivos del sistema (y, de hecho, el registro) están bien protegidos. (Las listas de control de seguridad en el sitio web Microsoft Security lo ayudarán a hacer esto).

III. Si un intruso tiene acceso físico sin restricción a su computadora, esta deja de ser suya.

Las cosas que un intruso podría hacer si logra posar sus manos en su computadora! Aquí tiene ejemplos, que van desde la Edad de Piedra hasta la Era Espacial:

- Podría realizar un ataque “Denial” de baja tecnología y hacer añicos su computadora con un mazo.
- Podría desenchufar su computadora, sacarla a rastras del edificio y pedir rescate.
- Podría iniciar su computadora desde un disquete y reformatear su disco rígido. Pero no, usted dice, he configurado el BIOS en mi computadora para que pida contraseña al iniciarla. No hay problema, si él puede abrir el gabinete y poner sus manos en el hardware del sistema, simplemente puede reemplazar el chip del BIOS y listo. (De hecho, hay maneras más sencillas de hacerlo.)
- Podría quitar el disco rígido de su computadora, instalarlo en la de él y leerlo.
- Podría hacer un duplicado de su disco rígido y llevarlo a su guarida. Una vez allí, tendría todo el tiempo del mundo de dirigir ataques de fuerza bruta, como probar todas las contraseñas de ingreso posibles. Se puede automatizar esto en los programas +
- Y, con bastante tiempo, es casi seguro que tenga éxito. Una vez que sucede eso, se aplican las leyes #1 y #2 de arriba.
- Podría reemplazar su teclado por uno que contenga un radiotransmisor. Entonces, podría monitorear todo lo que usted tipea, inclusive su contraseña.

IV. Si usted permite a un intruso, subir un programa a su sitio web, este dejara de ser suyo.

Esto es básicamente lo inverso a la Ley#1. En esa situación, el intruso persuade a su víctima para que descargue un programa nocivo en su máquina y lo ejecute. En esta, el intruso sube un programa nocivo a una máquina y lo ejecuta él mismo. Si bien esta situación es una amenaza cada vez que usted le permite a extraños conectarse a su máquina, los sitios Web están involucrados en la gran mayoría de los casos.

Mucha gente que opera sitios Web son demasiado hospitalarios para su propio bien y les permiten a los visitantes subir programas al sitio y ejecutarlos. Como ya hemos visto anteriormente, pueden suceder cosas muy desagradables si el programa de un intruso se ejecuta en su máquina. Si usted administra un sitio Web, debe limitar las cosas que pueden realizar los visitantes. Usted sólo debería permitir un programa en su sitio si está escrito por usted o si confía en el desarrollador que lo escribió. No obstante, esto

puede no ser suficiente. Si su sitio Web es uno de varios alojados en un servidor compartido, debe ser más cuidadoso.

V. Las contraseñas débiles constituyen un atentado a la seguridad.

El propósito de tener un proceso de Inicio de Sesión es establecer quién es usted. Una vez que el sistema operativo establece quién es, puede otorgar o denegar requerimientos para recursos del sistema en forma apropiada. Si un intruso consigue su contraseña, puede iniciar sesión como usted.

De hecho, en lo que concierne al sistema operativo, él es usted. Todo lo que usted puede hacer en el sistema, él también lo puede hacer, porque él es usted. Quizá él quiera leer información delicada que usted almacenó en su computadora, como su email. Quizá usted tenga más privilegios en la red que los que tenga él y ser usted le permitirá hacer cosas que normalmente no podría realizar.

VI. Una sola máquina es segura en medida que el administrador sea fidedigno.

Todas las computadoras deben tener un administrador: alguien que pueda instalar software, configurar el sistema operativo, agregar y administrar cuentas de usuario, establecer políticas de seguridad y manejar todas las otras tareas de administración asociadas con mantener una computadora en funcionamiento.

Por definición, estas tareas requieren que tenga control sobre la máquina. Esto pone al administrador en una posición de poder incomparable. Un administrador no confiable puede invalidar cualquier todas las otras medidas de seguridad que usted haya tomado.

Puede cambiar los permisos de la máquina, modificar las políticas de seguridad del sistema, instalar software nocivo, darles el alta a usuarios falsos o hacer cualquiera de un millón de cosas más. Puede subvertir virtualmente cualquier medida de protección en el sistema operativo, porque él lo controla. Lo que es peor aún, puede cubrir su rastro. Si usted posee un administrador que no es confiable, no posee seguridad en absoluto.

VII. Los datos cifrados son seguros en la misma medida que la clave de descifrado lo sea.

Supongamos que usted instaló la cerradura más segura, fuerte y grande del mundo en su puerta principal, pero pone la llave debajo del felpudo que está delante de la puerta. No importaría cuán fuerte es la cerradura ¿verdad? El

factor fundamental sería la forma pobre en que se protegió la cerradura, porque si la encontrara un ladrón, tendría todo lo necesario para abrirla. Los datos encriptados funcionan de la misma manera — no importa cuán fuerte es el criptoalgoritmo, los datos van a estar a salvo siempre y cuando también lo esté la clave que puede desencriptarlos.

VIII. Un antivirus desactualizado sólo es parcialmente mejor que ninguno.

Los escáneres funcionan comparando los datos de su computadora con una colección de “firmas” de virus. Cada firma es característica de un virus particular. Cuando el escáner halla datos en un archivo, email o cualquier otro lugar que iguale la firma, significa que se ha encontrado un virus.

De todos modos, un escáner de virus sólo puede escanear los virus que conoce. Es vital que mantenga su archivo de firmas del escáner de virus actualizado, dado que se crean virus nuevos todos los días.

IX. La anonimicidad absoluta no es práctica, ni en la vida real ni en la web.

Si usted visita un sitio Web, el propietario, si está suficientemente motivado, puede averiguar quién es. Después de todo, los unos y ceros que conforman la sesión Web han podido hallar el camino al lugar indicado, y ese lugar es su computadora. Hay muchas medidas que usted puede tomar para ocultar los bits y cuantas más emplee, mejor ocultos estarán.

Por ejemplo, usted podría emplear la traducción de direcciones de red para enmascarar su dirección IP real, suscribirse a un servicio de anonimato que esconde los bits transmitiéndolos desde un extremo del espacio al otro y así sucesivamente.

X. La tecnología no es una panacea.

La tecnología puede hacer algunas cosas que son increíbles. Estos últimos años han sido testigos del desarrollo del hardware más poderoso y barato de todos los tiempos, software que aprovecha el hardware para abrir nuevos horizontes para los usuarios, como también avances en la criptografía y otras ciencias. Es tentador creer que la tecnología puede llevarnos a un mundo libre de todo riesgo, si sólo trabajamos lo suficientemente duro. Sin embargo, esto simplemente no es real.

ANEXO K

Normas de Uso del Correo Seguro

Se llama ***netiquette*** a las pautas de buenas maneras en la red. Normas sencillas y de sentido común sin las cuales corremos el riesgo de ser considerados, como mínimo, ignorantes, como mucho, reventadores (trolls). Estas pautas deben observarse cuando incorporamos cualquier contenido a la red, por tanto son aplicables a todas nuestras publicaciones y mensajes. Respetarlas y aplicarlas hará que se lean con interés y respeto. Vulnerarlas sistemáticamente puede implicar que nadie entre en nuestro blog o red social, o que nuestros mensajes de correo electrónico sean eliminados por el receptor sin abrirlos siquiera.

Estas son unas cuantas normas para un buen uso de esa maravillosa herramienta que es el correo electrónico:

- Con el correo electrónico ocurre lo mismo que con el resto de relaciones humanas, la primera impresión es la queda. **Es importante el uso de una gramática y tono correctos**. Debemos ser siempre conscientes de que se trata de comunicación escrita, y como tal queda registro de ella.

- **Utiliza siempre el campo "asunto"**: el destinatario puede decidir si leer o no un mensaje basándose solo en el encabezamiento. Esto facilita la lectura, clasificación y por tanto, ahorra tiempo.

- **Envía tus mensajes en texto plano, no utilices estilos ni adornos innecesarios**. Además de más seguros, los mensajes en texto puro, sin colores, tamaños, negritas, etc. son más pequeños y llegan y se descargan más rápido.

- **No escribas en mayúsculas.** Escribir en mayúsculas en Internet equivale a gritar. A no ser que realmente quieras gritar una palabra o frase, escribe de manera normal, con mayúsculas y minúsculas. Puedes utilizar las comillas, los asteriscos y guiones bajos para *enfatizar* y subrayar.

- **Cuida tu ortografía y gramática**. Si no lo haces, los demás tendrán dificultades en entender lo que quieres decir, y tus opiniones no serán valoradas. Antes de enviar un mensaje, asegúrate de que esta escrito con corrección y claridad.
- **Usa un estilo de redacción adecuado al destinatario**. La forma de redacción debe adecuarse al destinatario. Utiliza los emoticones con moderación y nunca para un mensaje formal. No utilices la arroba (@) como sustituto del doble género. Ten en cuenta siempre la diferencia de estilo que debe haber entre un mensaje personal y otro profesional, entre uno informal y otro de carácter serio.

- **Escribe por párrafos** para que el mensaje quede mejor estructurado, y sepáralos con líneas en blanco, para no cansar con su lectura, o invitar al lector a "dejarlo para después". Tampoco escribas líneas de más de 80 caracteres. Muchos monitores no permiten visualizar más en la pantalla.

- Cuando respondas a un mensaje, **incluye parte del mensaje original para situar el contexto**. De otra manera, tus interlocutores podrían no saber de que estás hablando o a qué estas contestando, especialmente si reciben mucho correo. Normalmente basta con el asunto. Muchos servidores de correo integran ya esta opción por defecto.

- **Reenvío de correos:** Si recibes un correo electrónico interesante que deseas reenviar a tus contactos: ¿te olvidas de eliminar esas líneas heredadas de los mensajes anteriores e incluso bastantes direcciones de correo también del mensaje que has recibido? ¿Por qué se debe borrar todo eso antes de reenviar, exclusivamente, el cuerpo del mensaje? Puede que alguno de los destinatarios del correo tenga un virus en su ordenador y que ese virus captura las direcciones de correo de los mensajes que se reciben para luego enviarlas a un spammer. Todas esas direcciones sufrirán ahora el molesto correo basura.

- Por el mismo motivo, **cuando envíes copias de un correo a varias personas**, pon la lista de direcciones a enviar en el campo Cco (cuentas de correo ocultas). De esa forma evitarás dar a conocer las direcciones de terceras personas, que no interesan a nadie. Es una buena medida de seguridad para evitar virus y spam.

- **No reenvíes mensajes en cadena, falsas alarmas de virus**, etc. Solo contribuirás a aumentar el correo no solicitado entre sus conocidos.

- **Evita el envío de archivos adjuntos demasiado pesados**. Mándalos solo cuando sean necesarios y advierte sobre su contenido al remitente en el cuerpo del mensaje.

COMO DESTINATARIO debes también tener algunas precauciones:

- **No respondas al correo no solicitado y de origen desconocido**. Es una forma de aumentar la cantidad de correo basura en nuestro buzón ya que indica al remitente que la cuenta es leída. Los mensajes no deseados deben borrarse lo antes posible.

- **No abras ficheros que no esperas**. Aunque procedan aparentemente de personas conocidas no debemos abrir adjuntos no esperados: pueden contener virus.

- **No proporciones tu dirección de correo** en sitios que no conozcas bien o que puedan enviarte publicidad no deseada. Es una buena idea disponer de una cuenta gratuita para registrarnos en este tipo de sitios.

- **Limita el tamaño de las firmas automáticas:** Las firmas automáticas deben ser lo más claras y breves posible. No incluyas imágenes o

información innecesaria. Nunca dejes de identificarte con nombre y apellidos cuando te dirijas a personas desconocidas.

- **Utiliza claves seguras** (más de 8 dígitos, conteniendo letras y números) y configura la pregunta secreta de una forma que no sea adivinable, ya que esta es la forma más común de robar una cuenta de otra persona.

- Cuando utilices su correo electrónico en sitios públicos, **no olvides cerrar tu correo** cuando termines de trabajar. No basta con cerrar la página: es necesario pulsar en "salir" o "cerrar sesión".

ANEXO L

Normas de Navegación Segura

- Disponer en el ordenador de un antivirus y cortafuegos actualizado. Asegurarse de que el antivirus está activado
-
- Pasar el antivirus a los nuevos disquetes o pendrive que se introduzcan en el ordenador (aunque sean de nuestros amigos).

- No divulgar información privada personal (contraseñas, teléfono, dirección del domicilio familiar, datos bancarios...) o de personas conocidas por Internet.

- No enviar fotografías sin el permiso de los padres, podrían utilizarlas otras personas para violar nuestra intimidad.

- No comprar sin la supervisión de un adulto. Y ante instrucciones poco claras, NO seguir el proceso de compra.

- No contestar e-mails que tengan contenido ofensivo o resulten incómodos y cuidar de no molestar u ofender a otros en los mensajes por e-mail, SMS o chat. No fotografiar ni grabar a nadie sin su permiso... y menos aún distribuir luego su imagen sin autorización.

- No abrir mensajes cadena.

- Ante cualquier correo que nos infunda sospechas, lo mejor es borrarlo inmediatamente.

- No concertar encuentros con personas conocidas on-line o por el móvil, las personas que se conocen on-line pueden ser muy distintas a lo que parecen (en Internet a veces las personas ocultan su verdadera personalidad)

- Si se recibe o se encuentra una información que resulte incómoda, comunicarlo a los padres.

- No abrir mensajes de desconocidos ni mensajes de los que se desconoce el contenido.

- Desconfiar de correos que hagan grandes promesas.

- No bajar programas de procedencia desconocida; podrían tener virus e infectar el ordenador.

- No bajar ni ejecutar archivos adjuntos sin comprobar que el remitente es de confianza.

- Tras conectarse desde un lugar público (cibercafé, escuela) siempre cerrar la sesión para evitar que otra persona usurpe su personalidad.

- Evitar delinquir distribuyendo a través de Internet materiales (música, imágenes, películas...) de los que no tengan permiso para ello.

- Poner como ***página de inicio*** un portal "seguro".

  Ajustar los filtros de contenidos del navegador, restringiendo el acceso a contenidos como: violencia, sexo.

- Revisar de manera periódica el "historial" y los "archivos temporales" del navegador, para conocer las páginas que los menores han visitado.

  Ajustar el nivel de seguridad del navegador, indicando los sitios que queremos que sean sitios restringidos.

- Saber **utilizar** (y configurar) **las principales herramientas de Internet** navegadores, correo electrónico, FTP, listas de distribución y grupos de noticias, charlas, videoconferencias, programas de navegación off-line.

  Saber **"bajar" información** de la Red: textos, imágenes, programas.

ANEXO M

Conexiones Seguras

¿Qué es una conexión segura?

Una conexión segura es un intercambio cifrado de información entre el sitio web que está visitando e Internet Explorer. El cifrado se ofrece a través de un documento proporcionado por el sitio web que se denomina certificado. Cuando se envía información al sitio web, se cifra en su equipo y se descifra en el sitio web. En circunstancias normales, no es posible leer ni alterar la información mientras se envía, pero es posible que alguien encuentre una forma de descifrar esta información.

Aunque la conexión entre el equipo y el sitio web esté cifrada, esto no garantiza que el sitio web sea de confianza. Su privacidad aun puede ser puesta en peligro por la forma en la que el sitio web usa o distribuye la información.

¿Las conexiones seguras son privadas?

No necesariamente. Si bien la información que se envía y recibe está cifrada (codificada), un tercero podría ver el sitio web al que está conectado. Conociendo el sitio web al que está conectado, este tercero podría tener una idea bastante aproximada de las operaciones que está realizando. Por ejemplo, si está buscando un nuevo empleo usando un equipo de la oficina, su empresa podría buscar palabras clave en los sitios web o mantener un registro de los sitios visitados. Si envía un currículum a un sitio web de empleos, el documento puede que esté cifrado, pero su empresa sabría de todos modos que está buscando un nuevo trabajo.

¿Cómo se puede saber la conexión es segura?

En Internet Explorer, verá un icono de candado en la barra de estado de seguridad. La barra de estado de seguridad se encuentra a la derecha de la barra de direcciones.

El certificado que se usa para cifrar la conexión también contiene información acerca de la identidad del propietario u organización del sitio web. Puede hacer clic en el candado para ver la identidad del sitio web.

¿Qué significan los diferentes colores de la barra de estado de seguridad?

Cuando se visita un sitio Web que usa una conexión segura, el color de la barra de estado de seguridad indica la validez de su certificado y muestra el nivel de validación realizado por la organización de certificación.

En la tabla siguiente se explica el significado de los colores de la barra de estado de seguridad.

Color	Qué significa
Rojo	El certificado está caducado, no es válido o tiene un error. Para obtener más información, consulte Acerca de errores de certificado.
Amarillo	La autenticidad de un certificado o de la entidad emisora de certificados que lo emitió no se pudo verificar. Esto podría indicar un problema con el sitio Web de la entidad emisora.
Blanco	El certificado tiene una validación normal. Indica una comunicación cifrada entre el explorador y el sitio Web. La autoridad emisora del certificado no garantiza las prácticas comerciales del sitio Web.
Verde	El certificado usa una validación ampliada. Es decir, la comunicación entre el explorador y el sitio Web está cifrada y la entidad emisora del certificado confirma que el propietario o administrador del sitio Web es una empresa constituida legalmente conforme a la jurisdicción mostrada en el certificado y en la barra de estado de seguridad. La autoridad emisora del certificado no garantiza las prácticas comerciales del sitio Web.

¿Necesito actualizar mis cuentas en línea para usar certificados de validación extendida (EV)?

No, no es necesario que actualice su cuenta o información en línea para usar certificados EV. Algunos correos electrónicos de suplantación de identidad (phishing) intentan engañarlo para que proporcione información personal o financiera afirmando que necesita actualizar su cuenta para obtener mayor seguridad con un certificado EV.

Internet Explorer admite los certificados EV de manera nativa y no es necesario que realice ninguna acción más que visitar un sitio web. Si el banco utiliza un certificado EV, la barra de dirección aparecerá de color verde. Si no ve una barra de dirección de color verde, el sitio web no utiliza un certificado de Validación extendida.

¿Qué se debe hacer si se sospecha que un sitio web presenta una identidad engañosa?

Si cree que el sitio está intentando engañarlo acerca de su identidad, debe ponerse en contacto con la entidad de certificación cuyo nombre aparece en el certificado y en la barra Estado de seguridad.

¿Si las transacciones de un sitio web son seguras, ¿significa que es seguro utilizar ese sitio?

No necesariamente. Una conexión segura (cifrada) no constituye ninguna garantía de que su uso sea seguro. Una conexión segura sólo garantiza la identidad del sitio web, basándose en la información proporcionada por la organización de certificación. Es aconsejable que sólo proporcione información personal a sitios web que conozca y en los que confíe. Para obtener más información acerca del modo de determinar si puede confiar en un sitio web, consulte Cuándo se debe confiar en un sitio web.

¿Cómo se puede incrementar la seguridad de las transacciones en línea?

Si bien no existe una garantía de seguridad en Internet, puede minimizar los problemas de seguridad y privacidad en línea usando sitios web que conoce y en los que confía. Internet Explorer no puede determinar si el propietario de un sitio web es de confianza. Intente usar sitios que ya haya utilizado previamente o sitios recomendados por familiares o amigos. También debería activar el Filtro SmartScreen de Internet Explorer para ayudarlo a identificar sitios web fraudulentos. Para obtener más información acerca del Filtro SmartScreen.

¿Qué significa que un sitio tiene contenido seguro y no seguro (mixto)?

Una página web con contenido seguro y no seguro, o contenido mixto, significa que dicha página está intentando mostrar elementos usando tanto conexiones de servidor web seguras (HTTPS/SSL) como no seguras (HTTP). Esto suele ocurrir en tiendas en línea o en sitios financieros donde se muestran imágenes, banners o scripts que provienen de un servidor no seguro.

El riesgo de visualizar contenido mixto es que una página web o script que no sean seguros pueden obtener acceso a la información del contenido seguro.

Nota

- Internet Explorer usa un protocolo cifrado denominado Capa de sockets seguros (SSL) para obtener acceso a las páginas web seguras. Esas páginas utilizan el prefijo HTTPS, mientras que las páginas web normales usan HTTP.

BIBLIOGRAFÍA:

[1] Congreso Nacional del Ecuador, Ley Orgánica de transparencia y acceso a la información pública, **http://www.transparencia.espol.edu.ec/documentos/L_acceso.pdf,** Mayo 2004

[2] Areitio J, Seguridad de la información: Redes informáticas y sistemas de la información, Paraninfo 2008, Madrid-España, Diciembre 2010

[3] Millán Ramón, Consultoría estratégica en tecnologías de la información,**http://www.ramonmillan.com/tutoriales/cortafuegos_parte1.php>**, Diciembre 2010.

[4] Llanga Diego-Torres Gabriela, Estudio e implementación de una metodología de prevención de intrusos para Redes, Riobamba-Ecuador, Enero 2011

[5] Gómez Vieites Álvaro, Tipos de ataques e intrusos en las redes informáticas, XI congreso nacional de internet y sociedad de la información, Málaga-España, 2007.

[6] Garzón Daniel, Vergara Alejandro, Metodología de análisis y vulnerabilidades para empresas de mediana escala, Universidad Javeriana, Bogotá-Colombia 2006.

[7] Fernández Barcell Manuel, Estudio de una estrategia para la implantación de los sistemas de gestión de la seguridad de la información, Cádiz-España 2003.

[8] Congreso Nacional del Ecuador, Ley de comercio electrónico, firmas electrónicas y mensajes de datos, **www.sinar.gov.ec/downloads/R_comercio.pdf**, 2002

[9] Acúrio del Pino Santiago, Perfil sobre los delitos informáticos en el Ecuador, <**http://www.fiscalia.gob.ec/**>, año 2009.

[10] Subsecretaría de Informática, **http://www.informatica.gov.ec/**, Ecuador, Agosto 2007,

[11] Hoet Leonardo, Cozzi Rodolfo, Seguel Rodrigo, Manual de Seguridad en Redes, Subsecretaría Tecnologías Informáticas, Buenos Aires-Argentina 2007.

[12] Cmac-Paita, Código de Buenas prácticas para la gestión de seguridad de la información, Piura-Perú 2009.