UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

DISEÑO DE FIREWALL PARA UNA EMPRESA ELÉCTRICA

T E S I S

QUE PARA OBTENER EL TÍTULO DE:

I N G E N I E R A E N

C O M P U T A C I Ó N

P R E S E N T A

ARACELI ELIZABETH VELASCO CÁRDENAS

DIRECTOR: M.I. José Miguel Martínez Alcaraz

MÉXICO, D. F. ENERO 2006

Dedicado a :

A Dios por haberme permitido terminar una etapa más de mi vida y por permitirme compartir este momento con mis seres queridos. Gracias por ser mi guía.

Mi padre por el esfuerzo de cada día para que nada faltara en mi educación, pero sobretodo por enseñarme a apreciar la vida.

Mi madre por estar conmigo en todo momento, mami eres mi incondicional.

Mis hermanos Félix y Marco por sus enseñanzas a lograr lo que se quiere a pesar de las circunstancias y por su apoyo en situaciones difíciles.

Mi abuelita Bertha por su cariño y apoyo.

A Roberto por su apoyo y comprensión, mi vida te quiero.

A la ACM por su enseñanza de vida.

Agradecimientos:

A la Universidad Nacional Autónoma de México, por la formación profesional que me brindó.

Mi asesor de tesis y amigo José Miguel Martínez Alcaraz.

A todos los profesores a lo largo de mi vida.

Araceli Elizabeth Velasco Cárdenas.

ÍNDICE

Introducción

Inicialmente, el principal objetivo de las redes de computadoras era el de compartir sus recursos informáticos. En ese entonces la seguridad informática no era una prioridad, mientras se mantuviera la comunicación en la red todo lo demás se consideraba un lujo. Con el crecimiento de las redes en Internet, el conocimiento en cómputo y facilidad de acceso a las computadoras también incrementan las vulnerabilidades en las redes y por tanto de la información. La empresa eléctrica en estudio no es la excepción.

Esta corporación como muchas otras tiene su red cumpliendo el primer objetivo, pero se ve en dificultades al darse cuenta de la intrusión en sus sistemas. Debido al incidente ocurrido y por no estar ajenos a la realidad de las consecuencias y riesgos que se posee al estar conectados con el mundo, surge el concepto de seguridad informática antes ajeno para la empresa eléctrica.

Debido a la poca experiencia, este concepto trae consigo que el solo hecho de utilizar tecnología de punta arreglará todos los males de la inseguridad. De forma errónea se piensa en el firewall como la panacea para proteger de la inseguridad informática.

Esta tesis describe la investigación realizada para diseñar el sistema de seguridad. Como veremos más adelante el diseño no sólo consiste en la instalación del firewall sino también de otros factores tales como identificación de procesos críticos debilidades en el manejo de la información, etc.

Ahora se hará una descripción de cada capítulo de la tesis para conocer la relación de ésta con el sistema que se presenta al final.

El capítulo 1 describe el estudio realizado para conocer la importancia de los sistemas de la empresa. Este estudio también es de utilidad para saber lo que se quiere proteger, el dar prioridad por niveles de importancia y riesgo de los sistemas de información. Este estudio se verá con más detenimiento en capítulos posteriores.

En el capítulo 2 se describen los riesgos que se tienen en las redes de computadoras, se hace una clasificación de ellos y se describe el perfil de los atacantes informáticos, así como las herramientas que usan. Se encuentra que los peligros no sólo se encuentran fuera de la empresa, sino también existen riesgos internos. El conocer esta realidad nos permite solucionarla o prevenirla. En este capítulo también se describen formas de contraatacar estos riesgos.

En el capítulo 3 se describen conceptos de seguridad informática, los cuales definen los elementos que aseguran los sistemas y los elementos a proteger; éstos son esenciales para comprender el cómo se pueden proteger los sistemas informáticos.

En el capítulo 4 se verá que la seguridad de datos en las redes corporativas no depende únicamente de dispositivos que actúan en automático. Para implementar un buen sistema de seguridad se debe planear evaluando los sistemas informáticos y

dando un peso cuantitativo a las amenazas contra la seguridad de la empresa. De este modo se delegan responsables del sistema informático de seguridad, y se dan a conocer los lineamientos que se deben tomar para prevenir incidentes y tomar líneas de acción en contra de las violaciones de estos lineamientos. Este capítulo es una guía para elaborar políticas de seguridad e indica cómo darles seguimiento.

El capítulo 5 es el inicio para implementar el sistema de seguridad. Con este se estudia y se obtiene el nivel de seguridad en el centro de control de la empresa eléctrica antes de obtener las políticas de seguridad.

El capítulo 6 es la parte fuerte para el éxito de la implantación de la seguridad en redes informáticas. Este capítulo cubrió la planeación, el análisis de riesgo, la identificación de recursos, auditorías, delegación de puestos, publicación de la política así como las acciones contra las violaciones a la red, la propuesta de las políticas de seguridad en el centro de control de la empresa eléctrica. Para llegar a este documento se buscaron los ahora responsables del sistema de seguridad. Aquí se verá un ejemplo claro de políticas de seguridad.

Dado que el firewall es la herramienta más fuerte en el cumplimiento de las políticas de seguridad, el capítulo 7 está totalmente dedicado a este componente de seguridad. En ése capítulo se explican las generalidades de los firewalls, su propósito y su clasificación para llevar a cabo la elección que más convenga a las empresas y en especifico a la eléctrica, que es uno de los objetivos planteados en esta tesis.

El capítulo 8 describe el diseño del sistema firewall, las consideraciones que debiera cumplir el firewall para ejercer su trabajo, así como, las consideraciones hechas de acuerdo a las necesidades de la empresa y los usuarios; y las consideraciones que se realizaron para interactuar con los módulos de seguridad. Se enumeran los requerimientos mínimos para la solución. Este capítulo describe la arquitectura del sistema de seguridad que se propone para la empresa eléctrica e incluye las especificaciones técnicas que deben cumplir el hardware y el software para esta solución. En esta sección también se detalla el proceso de implantación del firewall de acuerdo a la propuesta hecha, el cual incluye la configuración del sistema de seguridad. También explica el como se integran las políticas y módulos de seguridad con el firewall elegido. Se muestra la topología de diseño. Se recomienda la forma de dar mantenimiento al sistema y las consideraciones posteriores al implementar el diseño.

Finalmente se da término a la tesis con las conclusiones que surgieron del diseño y la implantación. En ellas se hacen notar los beneficios obtenidos.

En el anexo A, se incluyen las hojas de trabajo que se utilizaron dentro del diseño del firewall.

En el anexo B se incluyen las preguntas para saber el estado de seguridad inicial de la organización, éstas son también útiles en el mantenimiento de las políticas de seguridad. Este anexo contiene únicamente las preguntas sin respuesta para el uso de éstas en cualquier empresa.

El glosario contiene palabras técnicas ocupadas en la tesis, todas ellas sobre seguridad informática y redes de computadoras.

Capítulo 1
Antecedentes

Inicialmente, las redes de computadoras fueron usadas por investigadores universitarios para el envío de correo electrónico y dentro de corporaciones para compartir impresoras. La seguridad no recibió mucha atención en ese entonces. Cada vez el número de redes informáticas crece diariamente junto con las nuevas oportunidades de comercio electrónico, productividad y acceso a información, muchas de estas redes se están conectando directa o indirectamente a Internet.

Empero, la conexión de las redes informáticas tienen beneficios que se exponen a una serie de inconvenientes como lo son las visitas no deseadas. Se habla con mayor frecuencia de informes de la intrusión de una computadora o una red de computadoras en los cuales se menciona a los piratas informáticos conocidos como hackers y crackers entre otros, que han conseguido introducirse en algún sistema y pueden llevar a cabo sus propósitos: acceder a activos críticos de la compañía violando la seguridad del sistema, pueden robar información por motivos económicos u otras causas o modificar el contenido de algún sitio Web, así como se tiene el espionaje industrial, introducir virus, modificar datos, etc. También se puede pensar y protegerse sólo de lo externo cuando en ocasiones la intrusión está en el personal que labora en la misma empresa.

El intercambio de datos a través de una red se ha convertido en un hecho cotidiano. Pero, ¿cómo saber si los datos de una empresa están seguros? Desde el software maligno (como virus) hasta los fallos de sistema pasando por los desastres naturales, existen una gran cantidad de riesgos para la seguridad e integridad de datos, de los cuales algunos podrían no tenerse contemplados.

El número de personas con conocimientos suficientes para dañar instalaciones informáticas va en aumento. La solución a estos problemas no es desdeñar la tecnología del Web sino por esta tendencia, hay que poner la debida atención en la seguridad de la red y sobre todo utilizar medidas preventivas, así como establecer e implementar un sistema de seguridad informática, haciendo hincapié en el mantenimiento del mismo. No obstante, también es importante comprender los límites de cualquier sistema y planear de modo correcto contra fallas y accidentes.

En razón de lo anterior se analizan los objetivos básicos de la empresa y los sistemas críticos para la cual se hace notar la importancia de tener siempre seguros los datos de sus redes informáticas.

1.1. La empresa eléctrica

El centro de control de la empresa eléctrica es un organismo creado con la misión de:

Administrar el despacho de energía y coordinar su operación, con calidad y eficiencia económica. En la figura 1.1 se muestran los objetivos básicos del sistema eléctrico.

Figura 1. 1.- Objetivos básicos de la operación del sistema eléctrico.

Para realizar la función anterior cuenta con las áreas de control que se encuentran ubicadas en puntos estratégicos y a grandes distancias unas de otras.

En el centro de control de la empresa eléctrica, para garantizar la seguridad, calidad y economía del suministro de energía eléctrica, se deben desarrollar nuevos sistemas que aprovechen las ventajas que ofrece la tecnología moderna, vencer inercias, mejorar continuamente la calidad de servicios contando como siempre con el recurso más valioso: los hombres y mujeres que trabajan en este centro de control.

La importancia de este organismo es alta, puesto que las decisiones que sean tomadas en el centro de control de la empresa eléctrica repercuten en todo el sistema eléctrico que manejan. Por ello es importante que la información que se distribuye a las áreas que este centro de control gestiona llegue de manera oportuna (en tiempo real), verídica y completa.

Para lograr que la información llegue de manera oportuna, verídica y completa es importante proteger tanto los recursos informáticos como la información. De lo contrario las consecuencias pueden tener un gran impacto, las cuales no sólo se reflejarían en el pago de los consumidores sino en perder vidas humanas que dan mantenimiento a las redes eléctricas y hasta intangibles como lo es la reputación de la empresa eléctrica.

Así como la tecnología moderna nos ofrece ventajas, también tiene sus desventajas. Internet es uno de estos avances, el cual da acceso a datos y la habilidad de publicar información en formas maravillosas. Internet siendo un buen medio de comunicación también es un peligro porque incluso proporciona la habilidad a extraños de husmear, cambiar y destruir información. Sin embargo, no hay que espantarse de ello puesto que la misma tecnología tiene formas para que Internet e Intranets tengan el uso requerido y nos brinde así de más ventajas que desventajas, teniendo un aprovechamiento óptimo.

Para poder reducir los inconvenientes de exponer la red de la empresa eléctrica a Internet, y utilizar los beneficios que brinda Internet se debe controlar el acceso hacia y de Internet. Así una parte de la solución para la protección y seguridad de la información es el Firewall, junto con otros dispositivos para lograr un mayor control de la información. La otra parte está integrada en la buena elaboración de políticas de seguridad que son el resultado de la investigación del nivel de seguridad que la empresa requiere y la administración de las políticas de seguridad junto con la disponibilidad de los recursos humanos.

1.2. Sistemas críticos del centro de control de la empresa eléctrica

La información delicada y/o confidencial de la empresa se considera que es crítica, de ahí que los sistemas que operan con ésta sean catalogados de igual forma.

Debido a la importancia de lo que se desea proteger son enunciados a continuación:

- Sistema de administración de datos en tiempo real.
- Sistema de administración eléctrica.
- Sistema de gestión de flujo de trabajo.
- Sistema de de medición de energia (SM).
- Sistema de mercado (SMAR).

1.2.1. Sistema de administración de datos en tiempo real

La red del sistema de administración de datos en tiempo real tiene un esquema distribuido, moderno, abierto y conforme al concepto de cliente / servidor.

El sistema que está suministrando la red del sistema de administración de datos en tiempo real es un sistema de control supervisorio y de adquisición de datos SCADA (**S**upervisory **C**ontrol **A**nd **D**ata **A**dquisition). El software SCADA se ha utilizado para controlar y monitorear dispositivos remotos por varias décadas. Tiene aplicaciones

avanzadas de potencia. La arquitectura distribuida del sistema que abastece cumple con estándares que permiten las funciones SCADA/EMS (SCADA/**E**nergy **M**anagement **S**ystem) para que puedan ser distribuidas entre los diversos servidores y estaciones de trabajo de la red para nivelación de cargas, expansiones futuras o por nuevos requerimientos no planeados originalmente, así como integrar aplicaciones EMS de otros vendedores que cumplan con los mismos estándares. Los estándares que permiten las funciones anteriores son OSF (**O**pen **S**oftware **F**oundation) y DME (**D**istributed **M**anagement **E**nvironment).

En el centro de control de la empresa eléctrica, la arquitectura de procesamiento distribuido del sistema SCADA es utilizada en todos los niveles jerárquicos que conforman el sistema de administración de datos en tiempo real. Los módulos de programas (software) distribuidos entre los diversos recursos de procesamiento se intercomunican a través de las redes LAN usando el protocolo TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol). Cuando existen varios módulos de programas asignados a un mismo recurso de procesamiento (servidor o estación de trabajo), estos se comunican entre sí utilizando el protocolo TCP/IP.

El sistema SCADA dotado para la empresa eléctrica utiliza **N**odos **C**oncentradores **L**ocales autónomos, redundantes y distribuidos geográficamente para proveer un sistema independiente y descentralizado para la adquisición remota de datos y control.

La base de datos Oracle del sistema SCADA puede ser accesada vía SQL (**S**tructured **Q**uery **L**anguage) en forma eficiente y segura, permitiendo acceso a otros sistemas externos, residentes en computadoras ajenas al sistema SCADA. Los accesos remotos a la base de datos SCADA son controlados mediante usuario y clave en UNIX. Estos accesos pueden otorgarse o limitarse en una variedad de niveles, desde rechazar cualquier acceso hasta permitir acceso sin restricciones.

Analizando de forma general la red conformada por los sistemas involucrados en esta especificación, implanta niveles jerárquicos de proceso de información, de acuerdo a los niveles jerárquicos de operación y responsabilidad de cada uno de los centros de control que conforman el sistema eléctrico.

1.2.2. Sistema de administración eléctrica

El sistema de administración eléctrica provee información completa de características, operación y estadísticas del sistema eléctrico como una herramienta para la toma de decisiones que se realizan en el centro de control de la empresa eléctrica.

En el sistema de administración eléctrica se integran las aplicaciones que facilitan la operación del sistema eléctrico de la empresa y lo mantienen eficiente y competitivo en el mercado abierto de compra-venta de energía, con exigentes reformas de respeto a la ecología y precios económicos de generación y porteo.

Con la automatización para la recopilación de datos, el sistema de administración eléctrica cumple su objetivo conteniendo en sus bases de datos información para fines de planeación de recursos, así como de compra-venta de energía para proveer las necesidades del consumo. Dispone de la información de comportamiento esperado de vasos de plantas hidroeléctricas en función de pronósticos de clima y de uso de agua para actividades de la población y planear la generación hidroeléctrica dependiendo de la disponibilidad y costo del agua.

Tomando en cuenta la información antes mencionada, se prepara un plan de generación y consumo de energía que servirá para anticipar las necesidades de combustible y disponibilidad del equipo a lo largo del tiempo y según la demanda de los usuarios del sistema eléctrico.

El plan de mantenimiento preventivo se prepara en función de la generación y consumo anual pronosticado.

El plan de operación horaria más acertado para el siguiente día se detalla basándose en el pronóstico de carga y condiciones específicas de operación que se definen con un día de anticipación en cada área de control y envían al centro de control de la empresa eléctrica para su integración y optimización. Los resultados sirven al operador para iniciar el día con un plan preestablecido y preparado para dar el seguimiento a las variaciones de demanda horaria pronosticada y sin embargo, ajustarlo como las condiciones reales lo requieren. Como resultados de la planeación, el predespacho proporciona adicionalmente reservas esperadas y demandas máximas horarias.

El sistema de administración eléctrica contiene el relatorio que es una bitácora de los eventos que suceden en la red eléctrica y se reportan por teléfono al operador en turno para su conocimiento y toma de decisiones en tiempo real. Aparte de su objetivo primordial de guardar relato de lo sucedido en la red, la información del relatorio sirve para el análisis del sistema eléctrico, incidencia de fallas, disponibilidad de equipo, y diferentes estadísticas de comportamiento de elementos en la red.

Éste sistema proporciona la información meteorológica y su tendencia del día para apoyar la toma de decisiones en tiempo real, así como la planeación de predespacho para el siguiente día.

El mismo sistema despliega a través de diagramas unifilares las mediciones de tiempo real.

Con los datos históricos y actuales de la base de datos el sistema de administración eléctrica genera reportes estadísticos para los diferentes grupos de usuarios.

En el sistema de administración eléctrica se visualiza en un ambiente gráfico los resultados de las aplicaciones y sus tendencias de comportamiento así como la descripción de los componentes de la red eléctrica, equipo térmico y los vasos hidráulicos, con el fin de consultarlos en proceso de toma de decisiones y análisis.

Como se describe en esta sección la información que contiene el sistema de administración eléctrica, es de alta importancia que los datos contenidos no sean alterados, ya que depende de ello la seguridad y operación de la red eléctrica. Alguna falla en este sistema es de consecuencias críticas. Por ello se considera sumamente importante proteger la red del sistema de administración eléctrica.

1.2.3. Sistema de gestión de flujo de trabajo

El sistema de gestión de flujo de trabajo es una arquitectura cliente-servidor que permite el desarrollo y la distribución rápida de aplicaciones internas del centro de control de la empresa eléctrica. Este sistema está basado en la herramienta Lotus Notes, se pueden desarrollar e instalar aplicaciones estratégicas que permitan la comunicación, colaboración y coordinación entre los grupos e individuos, está catalogado como un tipo de tecnología de trabajo en grupo.

Dicho sistema trabaja con la infraestructura DOMINO. Esta plataforma es independiente del sistema operativo por ser multiplataforma. En la figura 1.2 se muestra el esquema cliente-servidor del sistema de gestión de flujo de trabajo.

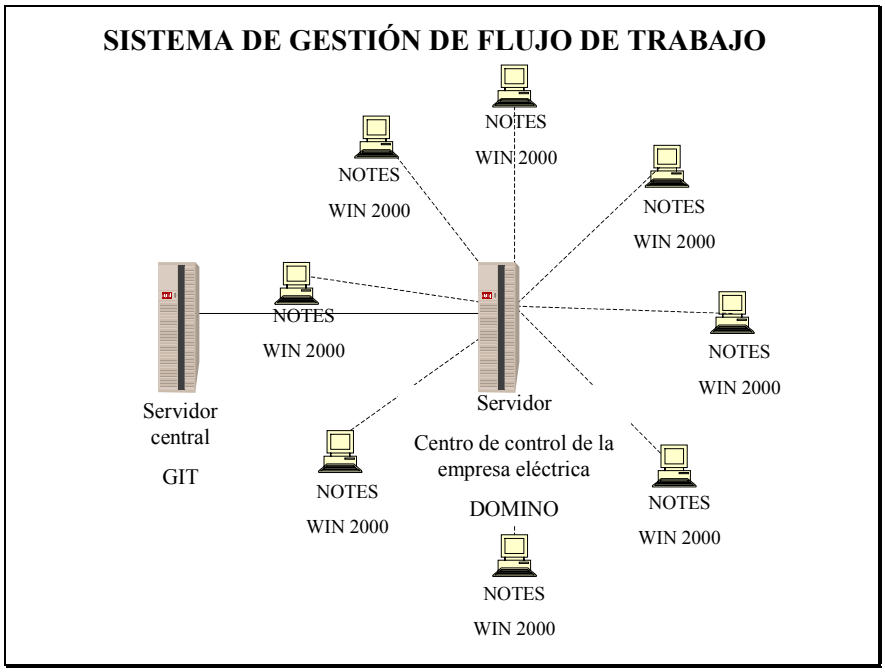

Figura 1. 2.-La infraestructura DOMINO es multiplataforma.

La infraestructura DOMINO son los elementos que forman una plataforma Lotus Notes/Domino dentro de una empresa. Dentro de este entorno se tiene:

- Al conjunto de servidores y clientes que comparten una misma libreta de direcciones.

- Una sola entidad que autoriza a los usuarios y servidores a realizar procesos de autentificación entre sí.

- Los equipos que comparten un mismo protocolo de red y conforman la red de gestión.

La mensajería constituye la plataforma de comunicación y permite la interacción entre los distintos usuarios de aplicaciones. Véase la figura 1.3.

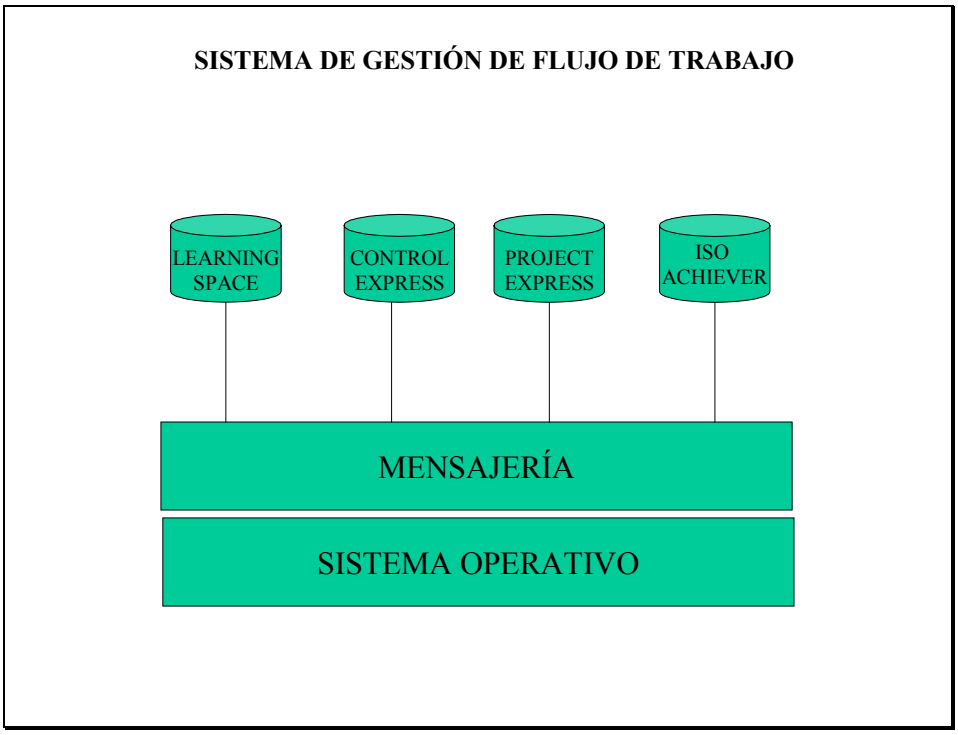

Figura 1. 3.- Plataforma de comunicación

Además de correo electrónico, permite a grupos de usuarios, seguir, compartir y organizar otros tipos de información a través de LAN, WAN y líneas telefónicas.

Entre las herramientas con que se cuenta están:

MENSAJERIA: Incluye la aplicación del correo electrónico, calendarios, agendas grupales y libreta de contactos.

La administración de tareas está clasificada en tres conceptos fundamentales:

1. Comunicación entre colegas
   Correo electrónico
   Foros electrónicos

2. Colaboración con grupos de trabajo
   - Difusión
   - Referencias

3. Coordinación de procesos estratégicos de negocios
   - Seguimiento
   - Flujos de trabajo

LEARNING SPACE: Herramienta utilizada para diseñar, desarrollar y hacer capacitación a distancia a través del uso de la computadora.

CONTROL EXPRESS: Utilizada para el control de gestión de documentos.

PROJECT EXPRESS: Aplicación para elaborar planes de trabajo y dar seguimiento a los mismos (flujos de trabajo).

ISO ACHIEVER PLUS: Es una herramienta utilizada para almacenar las definiciones de procesos, declaraciones de políticas y procedimientos. Incluye su aplicación para los procesos de certificación en las normas ISO 9000, ISO 14000 e ISO 18000. Proporciona un ambiente estructurado dentro del cual se puede crear, revisar, publicar y controlar documentos.

1.2.4. Sistema de Medición de energía(SM)

El sistema SM es un proyecto para automatizar la concentración de la medición de energía de las instalaciones centrales generadoras y subestaciones de la empresa eléctrica en servidores de datos, con el propósito de tener disponible la información en línea y ser utilizada por los diferentes procesos que la requieran.

El sistema SM es un sistema de medición que integra en una sola base de datos la información de diferentes componentes, como son: Transformadores de Instrumentos, multimedidores, cadenas de medidores, Concentradores de Información de Instalación (CII's), medios de comunicación hasta llegar a los Concentradores de Información Centrales (CIC's) que son los que reciben la información de los CII's.

La filosofía de la transferencia de información está basada en un concepto de "suscriptor-publicador", esto es, el CIC establece la primera conexión con el CII, el cual ya deberá tener configurado un buzón (definición de los datos que se enviarán al cliente o "suscriptor", así como la periodicidad de este envío) para el cliente y el servidor publicador se encargará de enviar periódicamente la información sin necesidad de solicitud posterior. De esta manera el CIC no está continuamente interrogando a los CII's solamente hace conexión una vez.

El CIC es un servidor que tiene instalada una aplicación cliente ("suscriptor") que trabaja bajo el protocolo MMS (Manufactured Message Specification) sobre TCP/IP y almacena información en el mismo servidor en una base de datos. De la misma manera que recibe información de los CII's también estos necesitan sincronizar los relojes del

sistema utilizando al CIC del centro de control de energía como servidor de tiempo mediante el protocolo NTP (Network Time Protocol).

La importancia de proteger este sistema es que la información de medición que se almacena en este servidor es confidencial y de uso exclusivo para algunos procesos de la empresa eléctrica.

1.2.5. Sistema de Mercado (SMAR)

El sistema SMAR realiza el estudio de cómo se realizaría el mercado de energía con un modelo. Mediante este modelo se obtienen las retribuciones y compensaciones a las centrales generadoras de energía. La figura 1.4 muestra este proceso.

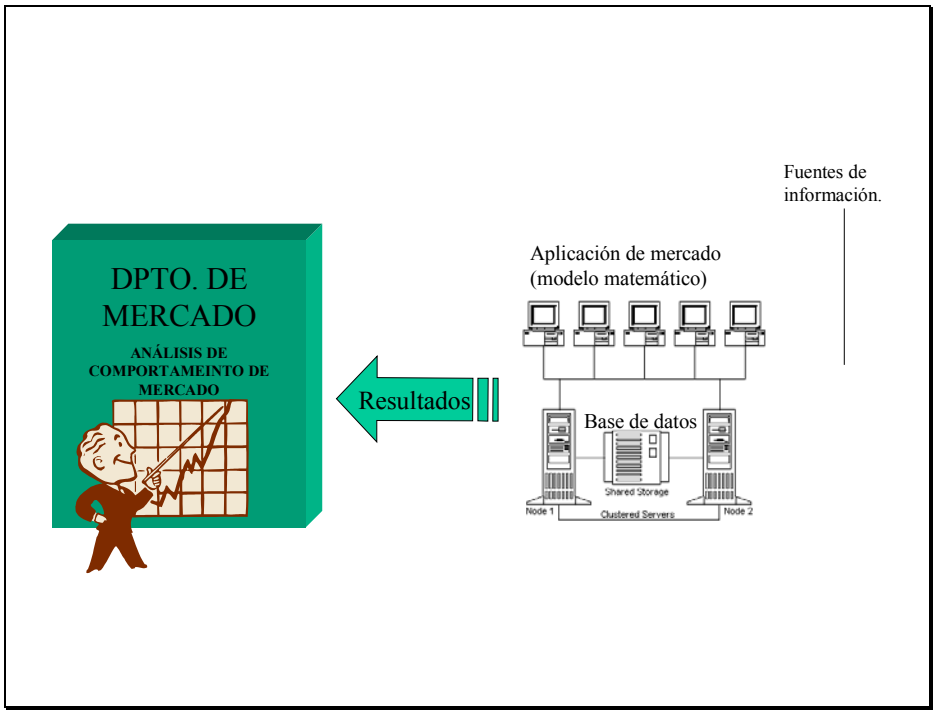

Figura 1. 4.- Procesamiento de datos de mercado de energía

En el sistema SMAR se opera el mercado interno de energía para tener un marco de modernización de la empresa eléctrica. Tiene la función de realizar operaciones de mercado y debe haber seguridad de los participantes de éste.

El sistema SMAR sirve para tener una buena gestión de mercado. De esta forma se garantiza la confiabilidad con los contratantes.

La importancia de la protección de este sistema es por el manejo monetario similar al de un banco.

Todos los resultados de mercado de energía son totalmente confidenciales.

Sólo accede a esta información el propio departamento mediante cuentas de usuarios UNIX.

1.3. Conclusiones

Conociendo los datos y la estructura de los sistemas críticos de la red en general se puede decir ahora que éstos son la parte específica a proteger en el centro de control de la empresa eléctrica de nuestro interés. Así también se ha notado la importancia de asegurar los datos que fluyen por esta red.

Dada la importancia de todo lo anterior, y además teniendo como antecedente de que ya hubo una intrusión informática conocida en la base de datos de este Centro de control, la cual fue robo y daño a la información, la empresa se ve en la necesidad de proteger la privacidad, la integridad y garantizar la disponibilidad de datos junto con el control y la consistencia de los sistemas, sobre todo la protección contra intrusos informáticos provenientes fuera de ésta y filtrar todo acceso a los datos que vienen fuera de la Intranet de la compañía eléctrica y de igual modo el no permitir la salida de la información no autorizada. Además de protegerla de los usuarios internos de la red que no tienen que ver con estos sistemas. Por lo anteriormente expuesto, es necesario contar con un sistema que protega la información del Centro por lo que se plantea el siguiente objetivo:

1.4 Objetivo

Diseñar e implementar un sistema de seguridad que permita resguardar la información crítica del centro de control de energía de la empresa eléctrica, de la intrusión de piratas informáticos y del personal interno ajeno a la información y al control del centro.

1.4.1 Objetivos específicos

- Diseñar políticas de seguridad para la empresa.
- Seleccionar un firewall.
- Implantación del firewall seleccionado.
- Documentar el proyecto para la empresa.

Otros objetivos:

- Identificar, representar y analizar las actividades de los procesos informáticos existentes.

- Realizar un diagnóstico de la seguridad del ámbito informático actual, que permita detectar riesgos y debilidades durante el flujo general de los procesos informáticos.

- Evaluar la estructura organizacional actual en cuanto a funciones de seguridad disgregadas o agregadas, realizadas y a realizar.

- Identificar los puntos de oportunidad y debilidades existente en los procesos informáticos y de administración, que permitan proponer medidas de control y reducción de riesgos.

- Determinar los procesos y actividades críticas que requieran la garantía de disponibilidad, integridad y confidencialidad de la información.

Capítulo 2
¿De qué debemos protegernos?

Cuando la LAN está conectada a Internet, existe la posibilidad de que los usuarios de ésta exploren y se comunique con el mundo exterior y con esta interacción se expone la seguridad interna de la misma.

El acceso a Internet se ha vuelto una necesidad para la operabilidad de hoy en día. Así como la necesidad del uso de Internet crece, también crecen los riesgos al usarlo, más aún cuando no se considera la seguridad informática como uno de los primeros objetivos. Por ejemplo, la organización se encuentra expuesta a que su información puede ser vista o manipulada por personas ajenas a ésta, así como el riesgo de tener una negación de servicio.

Podría pensar que la probabilidad de bajar los riesgos informáticos dentro de una empresa es el desconectarse de Internet, y así es, pero la solución en este tiempo no es factible porque no se puede estar apartado del mundo exterior. Es cierto que baja la probabilidad de riesgo, pero no se exenta éste. Esto es porque la información dentro de una empresa es manejada por muchas personas, las cuales no todas son confiables. También existen personas muy confiables, sin embargo hay que darles capacitación para que puedan protegerse de los que no lo son, así como el capacitarlos para proteger sus equipos informáticos contra software maligno y del mal uso que se puedan dar a las aplicaciones.

Con el fin de entender mejor cómo los recursos informáticos y la información son expuestos a peligros, se dan los conceptos de activo, amenaza, riesgo y vulnerabilidad, los cuales serán usados más adelante.

Activo. Es un recurso o algo (como lo puede ser la reputación de la empresa) que tiene importancia para la organización, tiene un determinado valor para la misma y consecuentemente debe ser protegido de forma acorde.

Amenaza. Es la ocurrencia potencial de un incidente que puede tener un efecto no deseable sobre un activo de la organización.

Riesgo. Es el potencial que dada una amenaza, ésta explote las vulnerabilidades del activo causando pérdidas o daños en el mismo, directa o indirectamente a la organización.

Vulnerabilidad. Es una debilidad asociada a un activo. Esta debilidad puede ser explotada por amenazas. La vulnerabilidad por sí misma no causa daño, es simplemente una condición o conjunto de condiciones que puede permitir que una amenaza afecte o cause daño al activo en cuestión.

2.1. Intrusos

Un intruso es aquel elemento no autorizado dentro de un sistema de la empresa. Los intrusos no sólo se encuentran en sitios externos sino también dentro de la misma organización.

Se tiene dos tipos de atacantes: los activos y los pasivos. Los intrusos activos son aquellos que modifican o perjudican el sistema de información. Los intrusos pasivos son aquellos que solo fisgonean, sin modificar nuestro sistema.

Se deben desarrollar políticas de seguridad para impedir, disminuir o al menos controlar el acceso a los activos de la organización.

2.2. Conocer al enemigo

La inseguridad informática es una realidad existente y por lo cual se debe considerar como el primer paso en el seguimiento de cambiarla.

Existe una gran variedad de gente que entra a sistemas informáticos sin permiso. Unos pretenden saltar medidas de seguridad del sistema, otros sólo quieren investigar y aprender, su satisfacción en ocasiones es solo el haber irrumpido a un sistema informático; su afición se encuentra en el límite que separa lo legal del delito. Aquí se describe cómo son y cómo actúan las personas que están al otro lado intentando, y consiguiendo en numerosas ocasiones, acceder a esa información que se pretende proteger.

Tipos de ataque

IP spoofing. Es el falsear la dirección IP de origen que va en los paquetitos que le llegan al servidor. De esta forma, se puede hacer creer que se están conectando desde una máquina autorizada, permitiéndose el acceso a través del firewall al interior del servidor. Esta técnica requiere un software específico así como conocer la dirección IP de alguien que esté autorizado para entrar en el servidor.

Secuestro de sesiones. Se accede al sistema a través de una sesión iniciada por un usuario autorizado, tomando el control de ésta. Se requiere software específico de acceso.

Prueba y error. Es la técnica más sencilla y tardada para el acceso a un sistema. Consiste en probar a entrar en el servidor utilizando diferentes nombres de usuarios y passwords, o claves distintas para un usuario conocido de antemano. Las contraseñas sencillas usadas por la mayoría de las personas hacen que este sistema, aunque poco útil en apariencia, sea más eficaz de lo que cabría esperar.

Fuerza Bruta. Los servidores, en la mayoría de los casos, realizan las comparaciones de passwords una vez que estos son codificados, de modo que el sistema no mantiene almacenadas las contraseñas en forma original, sino encriptadas. Un método muy

empleado para descubrir los algoritmos de encriptación es atacar al servidor con diferentes términos conocidos aprovechando los diccionarios dentro de programas, accediendo posteriormente a la tabla de resultados, comparando cada palabra con su equivalente codificada y obteniendo un patrón que puede llevar a descubrir la clave de encriptación.

Troyanos. Hace alusión al Caballo de Troya, porque al igual que en la obra literaria, se oculta el elemento intruso. Un troyano es un programa que queda residente en el sistema que modifica su función habitual para conseguir algún objetivo que le interese al intruso. Una de las utilidades más importantes de los troyanos para los intrusos, es que, una vez que se ha accedido por primera vez a un cierto sistema, el intruso introduce al troyano en el sistema y éste le deja una puerta abierta (backdoor), para que, en posteriores ocasiones, le sea más sencillo entrar. Así, los programas troyanos ocultan comportamientos del sistema, ya que el programa que parece ser no lo es, porque éste queda oculto con un nombre semejante. En la figura 2.1 podemos ver un ejemplo de una ventana del troyano conocido como Kuang2.

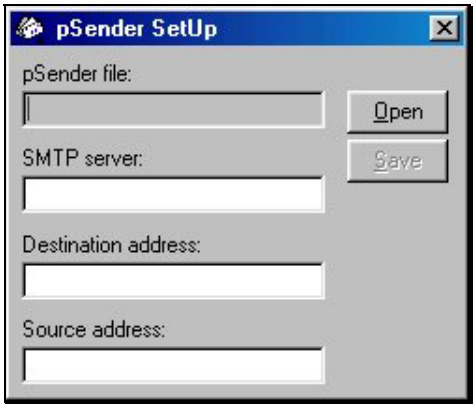

Figura 2. 1.- Kuang2 Trojan[1]

Rootkits. Es el software que permite a los intrusos depositar puertas traseras (backdoor's), para asegurar su regreso al sistema atacado.

Ping flood (tormenta de pings). Este ataque –también llamado **"pitufo" o smurf**– Consiste en enviar paquetes ICMP de "echo request" a un grupo de equipos usando una dirección grupal o broadcast pero sustituyendo nuestra dirección IP con la dirección IP de la máquina víctima. Lo que sucede entonces es que todas las máquinas que están en ese grupo le responden el ping (echo reply) a la máquina víctima, saturándola de tráfico y provocando posiblemente quede fuera de servicio o por lo menos que se degrade su tiempo de respuesta.

Sniffers (Olfateadores). Son programas que permiten "escuchar furtivamente" en redes de medios de comunicación compartidos. Se ejecuta en una máquina que está conectada a la red y captura el tráfico de todo el segmento de red. Es ahí donde un intruso puede usar un sniffer para capturar contraseñas que viajan sin cifrar en la red.

[1] Imagen tomada de http://www.megasecurity.org/trojans/kuang

Los sniffers más comunes son: linsniff, esniff, solsniff, susnsniff, sniffit, tcpdump, snoop.

Bugs. Los bugs son fallos en el software o en el hardware y que usan los hackers para entrar en sistemas y un exploit es un programa que aprovecha el agujero dejado por el bug.

Exploits. Las herramientas que utiliza el hacker para hacer explotar los bugs.

2.3. Patrones de comportamiento de los intrusos

Ésta es una descripción de forma general, el atacante puede realizar un paso más o un paso menos.

El primer paso consiste en estudiar cuidadosamente el objetivo que piensan atacar. Los intrusos reúnen información concreta acerca de la víctima, estudian todos sus sistemas de defensa, detección y respuesta para burlarlos con las contramedidas más adecuadas. Planean una forma de escape una vez que el objetivo ha sido alcanzado y evitan las medidas de seguridad con éxito sin ser descubiertos ni dejar rastro.

1. En primer lugar, el atacante debe identificar el objetivo: saber a quién atacar, es decir, servirse con la dirección IP de la máquina que se asaltará. A la hora de elegir un objetivo, el atacante tiene dos alternativas: o decidirse por un sistema concreto, o encontrar uno al azar. En muchas situaciones las víctimas son elegidas de forma totalmente aleatoria.

2. Una vez que sabe a quién atacar, es decir, conoce cuál es su dirección IP, debe recopilar la cantidad máxima de información sobre el objetivo: sistema operativo, servicios a la escucha y versión de los mismos, topología de red, información sobre la organización y sus usuarios, etc. En esta fase utilizará herramientas de exploración de puertos, como netcat, nmap o cheops, que permiten detectar qué puertos están abiertos en una máquina, o lo que es lo mismo, permiten saber qué servicios están activos.

3. Llegado a este punto, el intruso cuenta en su poder con una carpeta llena de datos sobre su objetivo: topología de la red, tipo y versión de sistema operativo instalado en los servidores y firewalls, servicios de Internet en ejecución y su versión, información de algunos usuarios, información de la organización, etc. Es el momento de estudiarla y analizarla detalladamente con el fin de identificar vulnerabilidades, puntos de acceso y puertas de escape. A partir de ahí, atacar.

4. Una vez que ha entrado en una máquina, debe obtener mayores privilegios. Del usuario anónimo, normalmente sin ningún tipo de prerrogativa, hay que intentar escalar privilegios hacia un usuario con mayores permisos, de ahí a otro, y así sucesivamente hasta llegar al objetivo: el root o administrador del sistema.

5. Conseguido el nivel de acceso apropiado, ahora se puede realizar el ataque: destrucción de archivos, robo de información, instalación de un troyano, modificación de datos, lo que sea.

6. Dependiendo del móvil del atacante, una vez realizada con éxito la penetración, puede olvidarse para siempre del objetivo o querer regresar en el futuro.

a) En el primer caso, el ataque ya ha terminado y continuará con el siguiente paso.

b) En el segundo, este primer ataque puede incurrir a la exploración para asegurar su posición y permitir el acceso prolongado. Tal vez no existe información de interés en este sistema, ya que el objetivo consiste en atacar desde él, al verdadero blanco.

7. Es el momento justo de instalar una puerta trasera, un medio que permita volver más adelante sin tener la necesidad de repetir los comprometidos pasos del ataque. Creará cuentas de usuario con nombres inocentes (puede repetir archivos del sistema con una letra más o menos, con el fin de que se parezcan los archivos y no sean extraños a los administradores), pero con privilegios de administrador; programas que se cargan al iniciar la máquina; trabajos programados para realizarse cada cierto tiempo; puertos a la escucha; rootkits; analizadores de protocolos que intercepten todo el tráfico que circula por la red interna, en busca de nombres de usuario y contraseñas; etc.

8. Si el atacante es realmente bueno, buscará además completar el ataque eliminando las evidencias del mismo y tomando todas las medidas oportunas para evitar la respuesta y salir impune. Las huellas que deja un atacante son básicamente, entradas en los archivos log del sistema: cuándo entró, qué cuenta usó, qué comandos ejecutó, qué tiempo de CPU utilizó, conexiones de red establecidas, etc.

Existen herramientas de ataque automatizadas utilizadas por los script kiddies, gente sin demasiados conocimientos que se limita a ejecutar los scripts de ataque que encuentran por Internet.

2.4. Atacantes informáticos

En esta sección se definen algunos nombres que se les ha dado a los atacantes informáticos.

Hacker. Los intrusos más conocidos son los hackers, estos se han dado fama por sí solos. Existen varias versiones sobre quienes son los hackers. Hay unos que dicen que son buenos y hay otros que dicen lo contrario. Se dice que los hackers buenos son aquellos que no actúan por perjuicio del sitio que entran, al contrario hasta lo mejoran. Aquí, se define como hacker a la persona que accede sin permiso a la información de un sitio informático sin modificarla.

Cracker. Se denomina así a una persona que entra a un sistema con fines malvados, aunque normalmente la palabra CRACKER se usa para denominar a la gente que desprotege programas, los modifica para obtener determinados privilegios, etc.

Lamer. Es una persona que no posee conocimientos técnicos, usa los programas de los hackers para entrar a un sistema y formatear un disco duro, tratan más de sorprender que el interesarse por modificar un sistema. Se dan el crédito hasta de los programas que usan.

Newbie. Es un novato (en etapa de aprendizaje) en la invasión de sistemas.

Phreaker. Se dedica a desarrollar técnicas para poder utilizar las vías de comunicación, tales como la telefónica, conexión a Internet, y modifica los servicios para que le lleguen en forma gratuita.

Pirata. Persona dedicada a la copia y distribución de software ilegal. Estos son los que se pueden dar dentro de la organización, puesto que en muchos casos se pierde el control de las licencias dentro de la misma empresa.

Script Kiddies. Gente sin demasiados conocimientos que se limita a ejecutar los scripts de ataque que encuentran por Internet.

Spammer. Son los que envían masiva e indiscriminadamente publicidad y mensajes basura sin haber sido solicitados, tanto en los grupos de noticias como en los buzones particulares.

Wanabies. Los que quieren ser, los futuros hackers, aunque por ahora no tienen ni idea. Esta definición viene de más puesto que no se ha de preocupar por quienes no hacen daño, pero así inician los chicos malos o bien así inician los grupos de seguridad.

Insiders. Otras personas que deben preocupar a la empresa son las que han quedado descontentas dentro de ésta y manejan o conocen bien los sistemas informáticos. Entre este tipo de personas se tienen los desempleados y por qué no, también personas envidiosas. La gente se puede corromper cuando necesita dinero y le ofrecen un buen pago por la información, esto lleva al robo de la información. Agregue también si el personal no está debidamente capacitado para hacer uso correcto de los sistemas de cómputo.

Las estadísticas indican que el 80% de los incidentes se producen dentro de las organizaciones.[2]

Dentro de la clasificación anterior, ellos querrían ser intrusos al sistema informático para usarlo como base para atacar a otros sistemas, por simple curiosidad, como medio de protesta, por simple satisfacción, por diversión entre otros.

[2] Congreso de Seguridad en Cómputo 2001. UNAM

2.5. Software maligno (malware)

Virus

Es un programa parásito porque ataca a los archivos o sector de arranque (boot sector) y se reproduce para continuar su esparcimiento.

Algunos se limitan solamente a reproducirse, mientras que otros pueden producir serios daños que pueden afectar a los sistemas.

Así un virus, es capaz de infectar archivos de computadoras y reproducirse una y otra vez cuando se accede a dichos archivos, por lo que dañan la información existente en la memoria o en alguno de los dispositivos de almacenamiento de la computadora.

Tienen diferentes finalidades: algunos sólo “infectan”, otros alteran datos, otros los eliminan y algunos sólo muestran mensajes. Pero el fin último de todos ellos es el mismo: propagarse.

El potencial de daño de un virus informático no depende de su complejidad sino del entorno donde actúa.

Un virus es un programa que cumple las siguientes pautas:

- Es muy pequeño.
- Ejecutable o potencialmente ejecutable.
- Se reproduce a sí mismo.
- Toma el control o modifica otros programas.
- Convierte otros objetos ejecutables en víricos.

El virus se reproduce cuando el ambiente es apropiado para “activarse” esto es: una fecha específica, a una hora determinada, por cierta cantidad de ejecuciones, por el tamaño del archivo de información o por una combinación de teclas. El virus necesita de una acción para propagarse, como el de compartir un archivo o enviar un correo electrónico.

Casi el 90% de los incidentes de virus en las redes corporativas se originan en el correo electrónico y en el tráfico web.[3]

Propiedades de los virus:

Duplicación, que es el fin en común.

Modifican el código ejecutable: de aquí el adjetivo “contagio”. Para que un virus contagie a otros programas ejecutables, debe ser capaz de alterar la organización del código del programa que va a infectar.

[3] Fuente: Estudios realizados por la International Computer Security (ICSA), 2001 e IPA/ISEC(Japón), 2001.

Permanecen en la memoria de la computadora: cuando un usuario, inocente de las consecuencias, ejecuta en su computadora un programa con virus, éste se instala en la memoria RAM, con objeto de apropiarse de la computadora, y por así decirlo, tomar el mando.

Se ejecutan involuntariamente: un virus sin ejecutar es imposible que dañe una computadora. En ese momento está en reposo, en modo de espera, necesitando de alguien que ejecute el programa "portador".

Funciona igual que cualquier programa: un virus, al ser un programa de computadora, se comporta como tal, en ese sentido necesita de alguien que lo ponga en funcionamiento.

Es perjudicial para la computadora: esto depende del virus con el que tratemos. Podemos encontrarnos con programas que destruyen parcial o totalmente la información, o bien programas que tan solo presentan un mensaje continuo en pantalla, el cual aunque no hace daño al final es muy molesto.

Se ocultan al usuario: claramente, el programador del virus desea que el usuario no lo advierta. Conforme pasa el tiempo, los virus van generando más y mejores técnicas de ocultamiento, pero también se van desarrollando los programas antivirus y de localización.

Los últimos virus que se han visto, son más difíciles de encontrar porque tardan más en realizar daños, es decir lo hacen poco a poco con el fin de que el usuario no se de cuenta y se siga propagando a otras computadoras. Por ello, algunos programas de virus se modifican a sí mismos para no ser detectados.

Los virus son creados por un programador y colocados en programas ejecutables, de esta forma el contagio se inicia por uso de estos programas infectados.

2.5.1. Clasificación del software maligno por su manera de infectar

Bug-ware

Son programas legales que realizan una serie de tareas concretas, por ejemplo, probadores de hardware o incluso antivirus. Si no se conoce bien su manejo, o tienen una programación complicada, pueden producir daños al hardware de la computadora o al software. Este se debe al mal uso de los usuarios, por eso no se considera virus.

Troyanos

Hace alusión a la obra épica griega de Homero. Un troyano parece ser una aplicación inocente y de utilidad que luego se revela como maligna. Es un programa que se oculta en otro programa legítimo, y que produce sus efectos perniciosos cuando éste se ejecuta. Salvo en casos mixtos un troyano no se puede reproducir, aunque es suficiente ya que en la mayoría de las ocasiones causa su efecto destructivo; su reproducción es la propia copia del programa por parte del usuario.

Camaleón

Es un pariente muy cercano del Troyano. Actúa como un programa parecido a otro de confianza (uno ya conocido por el usuario), pero produciendo daños. La diferencia es en que el programa no se basa en uno ya existente, sino que diseña otro completamente nuevo. Debe quedar claro que no se trata de la aplicación real, sino de un programa que simula el comportamiento de dicha aplicación. Así, un camaleón podría llegar a un sistema informático bajo la apariencia del Winzip, por ejemplo. Al ejecutarlo todo es igual que en el programa original, sin embargo puede estar borrando todos los datos del ordenador sin que nos demos cuenta. Esta técnica se utiliza, no en programas comerciales, sino en aplicaciones concretas. Bien programados son difíciles de eliminar pues reproducen fielmente al programa que imitan.

Bombas lógicas

Actúa a un determinado tipo de condiciones técnicas. Sólo espera a que sucedan las condiciones para actuar. Por ejemplo, un virus que se haga presente cuando haya un determinado número de megas ocupados en el disco duro. No suelen ser auto-reproductores, ni se propagan de una computadora a otra. Es interesante observar la filosofía con la que están diseñados, en la cual existe un segmento de código maligno dentro de un programa aparentemente normal, que se mantiene latente sin ser detectado durante un tiempo determinado.

Bomba de tiempo

Parecido al anterior, el cual puede ser considerado una variante del anterior. Se conocen dos versiones: la que actúa en determinadas fechas, como un Viernes 13, o la que se activa tras una serie determinada de ejecuciones. Un ejemplo de esto sería también el virus del moroso, si una empresa no paga un programa legal, se activa el virus.

Joke-program

Ahora ya no se les ve mucho. Eran virus (se reproducían e infectaban) pero no producían realmente daños a la computadora, simplemente eran molestos.

Conejo

También conocidos como “Peste”. En una red se puede dar un tipo determinado de trabajo que denominamos “multitarea”, consiste en que las distintas órdenes (correo, impresiones, compilaciones...) siguen un orden determinado formando lo que conocemos como una “cola”. De esa forma se ejecuta primero una, luego otra, y así sucesivamente mientras las que no se están ejecutando permanecen en la “cola” en una especie de lista de espera. Dentro de una red se pueden especificar preferencias para determinados usuarios que se saltan la “cola” por encima de otros. La mayoría se autodestruyen una vez que han actuado.

Gusanos

No son exactamente virus informáticos, pero se les confunde frecuentemente con ellos, incluso en algunos casos se ha llegado a utilizar esta denominación como sinónimo de virus. Se dan en redes, de tal forma que se trasladan de una a otra terminal, se reproducen automáticamente. Viajan a través de una red reuniendo información (contraseñas, direcciones, documentos...). Generalmente, el objetivo final de un gusano es colapsar el funcionamiento de las redes por sobrecarga de sus

recursos, como lo son el consumir memoria o ancho de banda de la red. No es raro que borren toda clase de vestigio de su paso por la red para no ser detectados por los operadores de sistema.

Leapfrog o "rana"

Es un programa parecido al gusano que a partir de una serie de datos conocidos, como la clave de acceso a una cuenta y el nombre de usuario, se dedica a recopilar información reservada.

Máscara

Este programa asume la identidad de un usuario autorizado y realiza así las mismas labores del anterior considerándose una variante.

Mockinbird

Espera en un sistema de forma latente, interceptando las comunicaciones en el proceso de login o entrada. En ese momento se introduce en la cuenta y empieza a actuar sin interferir en las operaciones lícitas que se estén realizando.

Spoofing

Una variación del anterior, observa lo que hace el usuario y lo repite de forma maliciosa buscando el bloqueo del sistema.

Macro-virus[4]

Son pequeños programas escritos en lenguaje propio (conocido como lenguaje script o macro-lenguaje) de un programa. Así se pueden encontrar con macro-virus para editores de texto, hojas de cálculo y utilidades especializadas en la manipulación de imágenes. Sus autores los escriben para que se extiendan dentro de los documentos que crea el programa infectado. De esta forma se puede propagar a otros ordenadores siempre que los usuarios intercambien documentos. Este tipo de virus altera de tal forma la información de los documentos infectados que su recuperación resulta imposible. Tan solo se ejecutan en aquellas plataformas que tengan la aplicación para la que fueron creados y que comprenda el lenguaje con el que fueron programados. Este método hace que no dependa de ningún sistema operativo. La figura 2.2 muestra cómo se puede expandir este tipo de virus de un sistema operativo a otro.

[4] Lars Klander., A prueba de Hackers., Anaya Multimedia., USA., 1998.

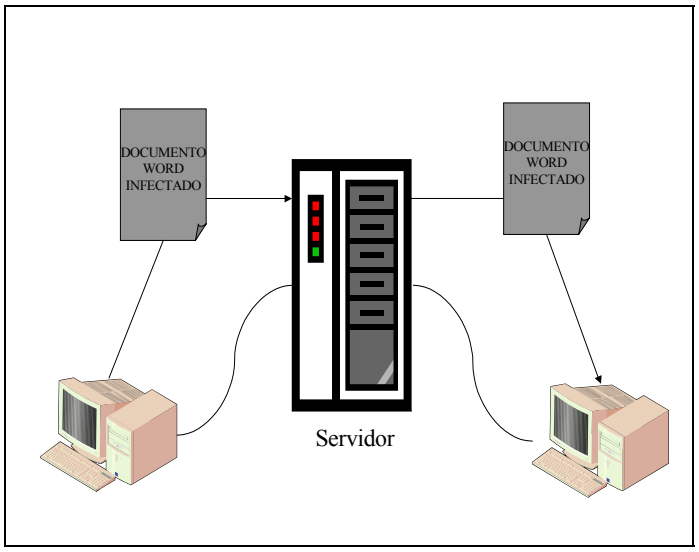

Figura 2. 2.- El macrovirus se puede propagar desde un sistema operativo a otro.

2.5.2. Clasificación de los virus por las zonas que afectan:[5]

BSI (Boot Sector Infector)

Contaminador del sector de arranque. Son los más comunes entre los virus PC, los más peligrosos y por regla general los que más fácilmente se destruyen una vez detectados. Virus que altera o infecta de algún modo el sector de arranque.

CPI (C.P u´s Infector)

Contaminador del proceso de órdenes. Así todo virus que infecte archivos de órdenes centrales como el COMMAND.COM se denomina CPI's. No es raro que esta clase de virus se extienda con una enorme rapidez por el disco duro.

GPI (General Purpose Infector).

Contaminador de Propósito General. No están diseñados precisamente para infectar un determinado tipo de archivo de sistema. Son rápidos en la propagación.

MPL (Multi Purpose Infector).

Contaminador Multipropósito. Estos virus integran todas las características de los tres anteriores, resultando muy peligrosos. Infectan en primer lugar los sectores de arranque y procesadores de órdenes, extendiéndose luego a archivos ejecutables, aprovechando en principio los ubicados en la memoria RAM (por haber sido cargados en el AUTOEXEC.BAT o en CONFIG.SYS). Al tener varias propiedades aumenta su vida operativa.

FSI (File Specific Infector)

[5] Arturo Hernández Hernández. Virus Informático. DGSCA. UNAM

Contaminador de Archivo Específico. De forma similar que los CPI restringen las infecciones a archivos determinados. Podríamos distinguir dos tipos: los producidos por venganza (el típico empleado despedido que deja uno de éstos para fastidiar a la compañía), o bien alguien con una fijación por un lenguaje de programación (caso del virus Dbase, Pascal...). Se suele producir un pequeño retraso cuando el virus busca a su víctima pero nadie suele darse cuenta, una vez localizada ésta, la borran o le destrozan el formato.

MRI (Memory Resident Infector)

Contaminador Residente en Memoria. Los BSI y CPI se pueden englobar como MRI, puesto que ambos permanecen activos en la memoria mientras se ejecutan. Pueden disfrutar de algunas de las ventajas de los CPI y BSI, ya que siempre están cargados y activos interfiriendo en todas las operaciones informáticas. Las salidas de pantalla e impresión pueden ser interceptadas, así como los archivos de datos, que resultan corrompidos.

2.6. Combinación de problemas

Como se ha estudiado, actualmente existen problemas mezclados. Programas con apariencia de aplicaciones con virus introducido a la red por intrusos y/o personas conocidas, además estos programas se propagan utilizando gran ancho de banda como gusanos, y/o dejando puertas traseras. Si los virus junto con otro software maligno están combinados, también hay que combinar soluciones, por lo que además del antivirus se debe pensar en integrar otras herramientas, como lo son el antispyware, firewalls personales entre otros. En la figura 2.3 se muestra cómo se mezclan los problemas.

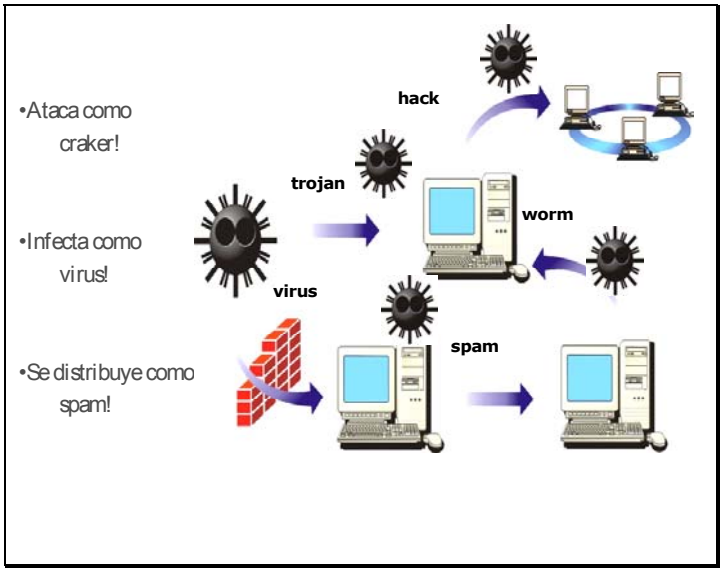

Figura 2. 3.- Imagen de problemas mezclados[6]

[6] Imagen tomada de una presentación de Trend Micro.

En la figura 2.4 representa una combinación de malware.

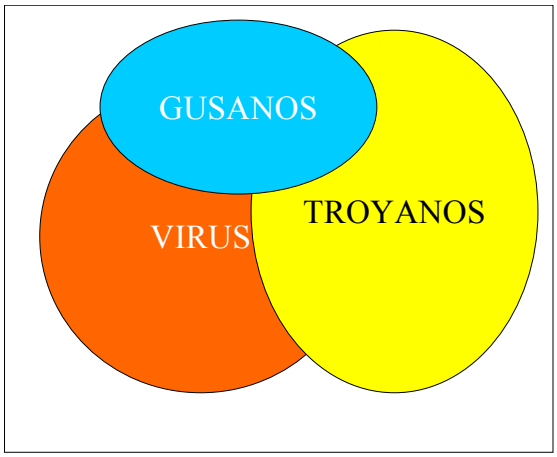

Figura 2. 4.- Combinación de malware.

En la figura 2.5 se representa una integración de soluciones.

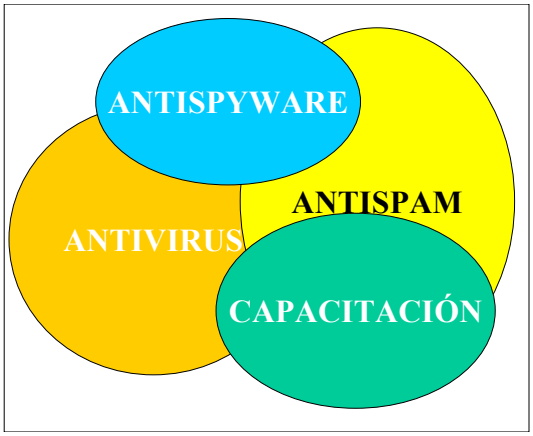

Figura 2. 5.- Combinación de soluciones.

2.7. ¿Cómo llegan a las empresas?

Los virus y otras formas de software maligno se propagan de máquina a máquina

Anteriormente los virus se propagaban a través de discos flexibles y solo infectaban programas y sectores de booteo. Hoy en día, cualquier documento digital es vulnerable a un virus. Los programas malignos son ahora capaces de propagarse sobre redes y por Internet. Internet tiene nuevos medios de distribución los cuales no estaban antes disponibles.

Con el incremento del correo electrónico como una herramienta importante pone la comunicación e intercambio de información en las organizaciones, por lo que los virus

y otras formas de software maligno son distribuidos cada vez más rápido. En la figura 2.6 se tienen estadísticas de los cambios de las fuentes de infección en los últimos 9 años.

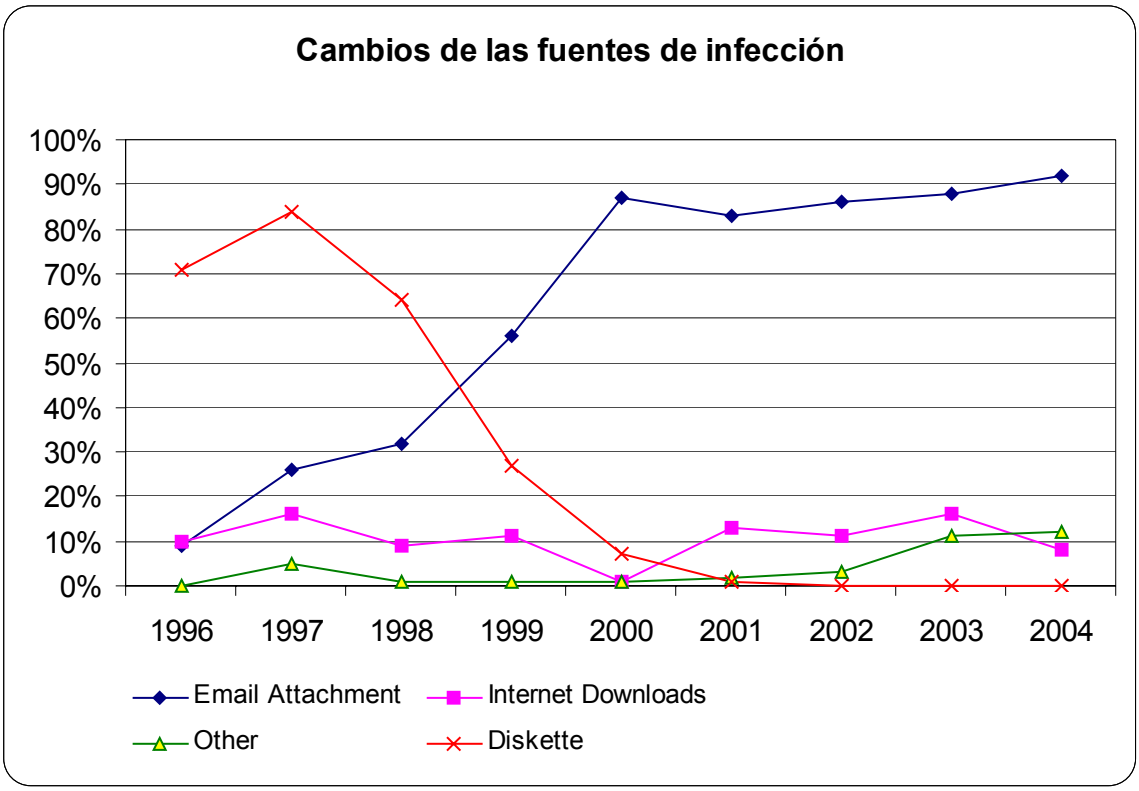

Figura 2. 6.- Imagen de los cambios de las fuentes de infección[7].

2.8. Indicios de aviso de software maligno[8]

La siguiente es una lista de indicios comunes de avisos de software maligno:

- Las operaciones informáticas parecen lentas.
- Los programas tardan más de lo normal en cargarse.
- Los programas acceden a múltiples unidades de discos cuando antes no lo hacían.
- Los programas dirigen los accesos a los discos en tiempos inusuales.

[7] Imagen obtenida de ICSA Labs Virus Survey, 2004.
[8] Virus Informático., Arturo Hernández Hernández., DGSCA., UNAM.

- El número de sectores dañados de disco aumenta constantemente.
- Programas que normalmente se comportan bien, funcionan de modo anormal o se cierran sin motivo.
- Los programas encuentran errores donde antes no los encontraban.
- Programas aparentemente benignos, de “travesuras” divertidas se materializan misteriosamente y nadie reconoce haberlos instalado. Por ejemplo, agujeros negros, pelotas que rebotan, caras sonrientes o caracteres alfabéticos “lluviosos” empiezan a aparecen en la pantalla.
- Desaparecen o aparecen archivos misteriosamente.
- Los archivos son sustituidos por objetos de origen desconocido o por datos falseados.
- Nombres, extensiones, fechas, atributos o datos cambian en archivos o directorios que no han sido modificados por los usuarios.
- Aparecen archivos de datos o directorios de origen desconocido.
- CHECKUP (u otro sistema de detección de virus) detecta cambios en objetos estáticos (archivos). Los cambios detectados en objetos dinámicos (archivos que se espera que cambien periódicamente, como archivos de datos de documento y de hojas de cálculo) no son necesariamente indicios de actividades víricas.
- Cambios en las características de los archivos ejecutables. Casi todos los virus de archivo, aumentan el tamaño de un archivo ejecutable cuando lo infectan. También puede pasar, si el virus no ha sido programado por un experto, que cambien la fecha del archivo a la fecha de infección.
- Aparición de anomalías en el teclado. Existen algunos virus que definen ciertas teclas, las cuales al ser pulsadas, realizan acciones perniciosas en la computadora. También suele ser común el cambio de la configuración de las teclas, por la del país donde se programó el virus.
- Aparición de anomalías en el video. Muchos de los virus eligen el sistema de video para notificar al usuario su presencia en la computadora. Cualquier desajuste de la pantalla o de los caracteres de ésta, nos puede notificar la presencia de un virus.
- Se modifican el Autoexec.bat y el Config.sys. En ciertas ocasiones, los virus modifican dichos archivos para adaptarlos a su presencia, al igual que las aplicaciones de software.

- Reducción del tamaño de la memoria RAM. Un virus, cuando entra en una computadora, debe situarse obligatoriamente en la memoria RAM, y por ello ocupa una porción de ella. Por tanto, el tamaño útil operativo de la memoria se reduce en la misma cuantía que tiene el código del virus.

- Desaparición de datos. Esto es consecuencia de la acción destructiva para la que son creados casi todos los virus. Depende de la maldad del virus si se borran con la orden DEL, o mediante el uso de caracteres basura, lo que hace imposible su recuperación.

- El disco duro aparece con sectores en mal estado. Algunos virus usan sectores del disco para camuflarse, lo que hace que aparezcan como dañados o inoperativos.

- Aparición de mensajes de error inesperados. Lo más normal, es que en ciertos virus, el sistema operativo produzca errores inusuales, cosa que debe alertar al usuario.

- Reducción del espacio disponible del disco. Ya que los virus se van duplicando de manera continua, es normal pensar que esta acción se lleve a cabo sobre archivos del disco, lo que lleva a una disminución del espacio por el usuario.

2.9. Virus reportados

En las noticias ya no se mencionan los virus. ¿Acaso hubo virus más fuertes antes? La respuesta es que sigue habiendo virus cada vez más fuertes, pero ahora el suceso se ha vuelto cotidiano, además estos virus ocupan vulnerabilidades que dejaron otros virus. Como ejemplo se tiene Nimda que es un virus del año 2001 y sigue afectando, además se apoya de la vulnerabilidad que dejó Código Rojo (Code Red).

En la gráfica del número de incidentes reportados al CERT veremos que de dos años (2000-2002) la cantidad de incidentes reportados por virus se ha cuadruplicado (Vea la figura 2.7). Faltaría saber la cantidad de incidentes que no son reportados.

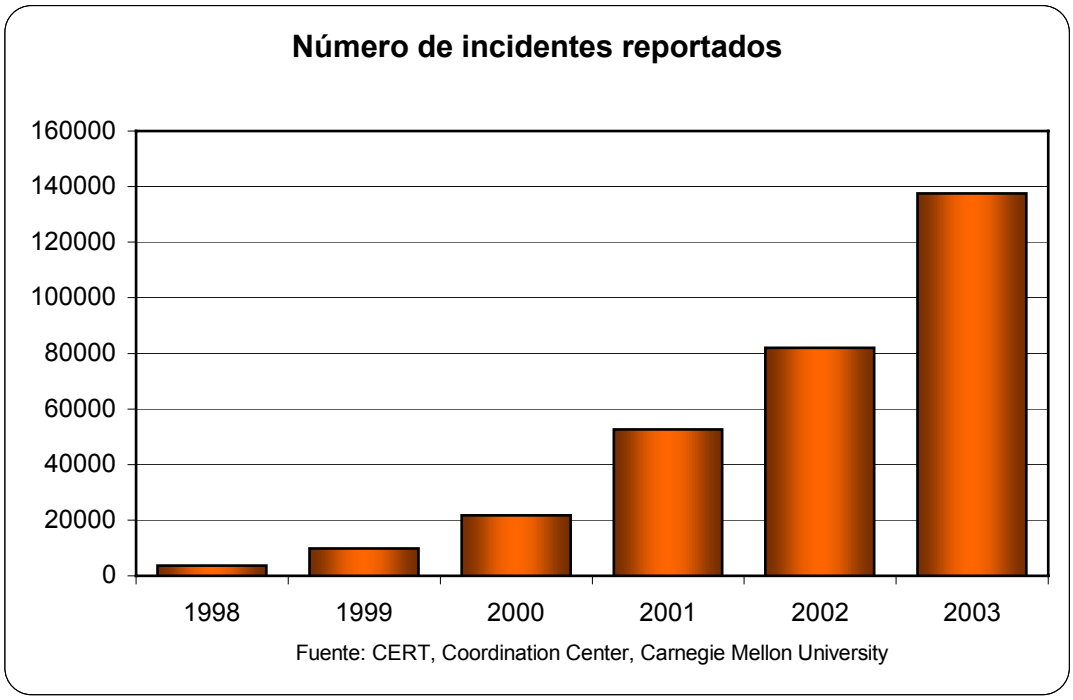

Figura 2. 7.- Imagen de número de incidentes reportados. [9]

El mayor de los efectos de los virus en las corporaciones son el dejar las PC's no disponibles a los usuarios. A esto le sigue la pérdida de productividad. En la empresa eléctrica el dejar una máquina en tiempo real no disponible para el operador de la red eléctrica puede ser el perder el conocimiento de la medición de puntos del sistema eléctrico, con lo que en su momento perdería la supervisión y por lo tanto el control de la red de distribución eléctrica.

En la figura 2.8 hay una gráfica que muestra el porcentaje de los efectos de los virus reportados en 962,278 equipos reportados a un prestigiado sitio de seguridad informática:

[9] Datos tomados de http://www.cert.org/stats.

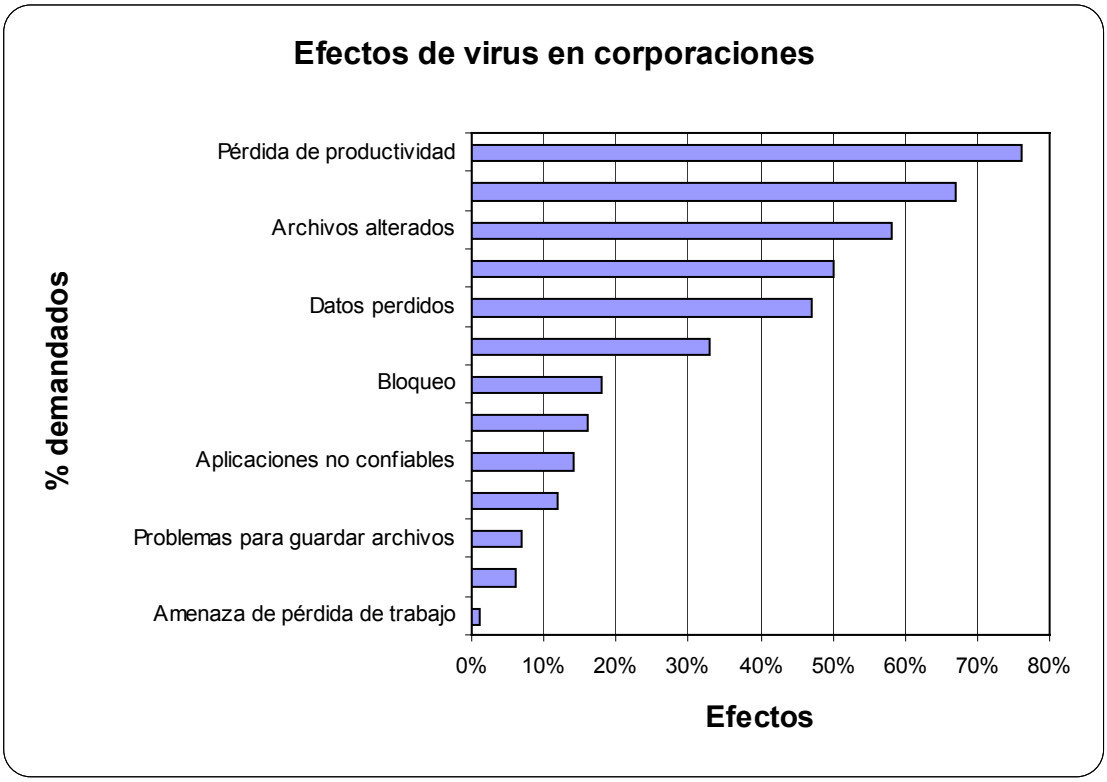

Figura 2. 8.- Imagen de efectos de virus en corporaciones[10]

2.10. Peligros existentes en los Servicios de Internet

Una razón para conectarse a Internet es para usar sus servicios, de no ser así no tiene caso esta conexión. Sabemos de las ventajas que brinda esta gran red, por ello el sitio debe proteger los servicios que utilizará o proporcionará por Internet.

En esta sección se describirán algunos de los servicios más usuales, en la que se verá que ninguno de estos servicios es seguro. Antes de que decida qué servicios va usar en un sitio, se debe evaluar qué tan importante son estos para los usuarios de la corporación y si se podrá proteger los servicios de sus peligros.

Correo electrónico

Este servicio está diseñado para facilitar comunicaciones asíncronas. Funciona aun si los participantes no están en sesión en ese momento: la siguiente vez que inicien una sesión, los mensajes de correo electrónico estarán esperándolos.

Protocolo: SMTP (Simple Mail Transfer Protocol). Es el protocolo estándar de Internet para enviar y recibir correo electrónico. El servidor SMTP más común en UNIX es Sendmail.

[10] Imagen tomada de ICSA Labs Virus Prevalence Survey, 2004.

Peligro: Se puede falsificar el correo electrónico, se expone a ataques de negación de servicio y sin la suficiente supervisión se pueden recibir Troyanos.

Transferencia de archivos

Protocolo: FTP (File Transfer Protocol). Es el protocolo estándar de Internet para transferir archivos.

Peligro: Las personas realizan más transferencias de archivos cuando FTP está disponible que con el correo electrónico. Es más probable que obtengan programas y datos indeseables. Se pueden obtener Troyanos, juegos de computadoras, software pirata e imágenes pornográficas, que tienden a ocupar una gran cantidad de tiempo y espacio en el disco.

Protocolo: TFTP (Trivial File Transfer Protocol). Es un protocolo FTP simplificado que las máquinas sin disco duro utilizan para transferir información.

Peligro: Es sencillo integrarlo al hardware y, por lo tanto, no soporta ninguna autentificación. No hay razón para proporcionar acceso TFTP fuera de su red; los usuarios comunes no transfieren archivos con ese protocolo.

Protocolo: FSP (File Service Protocol). Es un protocolo para transferir archivos desarrollado para circundar las restricciones de FTP. Las transferencias FSP pasan cuando las transferencias FTP han sido bloqueadas.

Peligro: Es susceptible a los mismos tipos de problemas que FTP, y se han hecho menos intentos para evitarlos o corregirlos.

rcp: Es un programa para transferir archivos que se comporta como una versión extendida del comando cp de UNIX.

Peligro: Emplea un modelo de autentificación basado en el host. En lugar de requerir autentificación del usuario en la máquina remota, ve la dirección IP del host de quien viene la solicitud. Desafortunadamente no puede saber cuáles paquetes en realidad vienen de ese anfitrión (host).

Acceso de terminal remota y ejecución de comandos

Telnet: Es el estándar para acceso de terminal remota en Internet. Imita una terminal, no una estación de trabajo gráfica; proporciona acceso sólo a aplicaciones basadas en caracteres. También brinda acceso remoto a sus usuarios desde cualquier sitio conectado a Internet sin hacer arreglos especiales.

Peligro: Telnet envía toda su información sin codificar, lo que lo hace muy vulnerable a ataques de espionaje (utilizando analizadores de protocolo) y robo. Telnet es seguro sólo si la máquina remota y todas las redes entre ella y la máquina local son

seguras, lo cual significa que no es seguro a través de Internet, donde no puede identificar con certeza las redes que intervienen, mucho menos confiar en ellas.

rlogin, rsh y on: Programas que pueden usarse como terminal remota y ejecución remota de programas.

Peligro: Estos programas se utilizan en un ambiente confiable para permitir que los usuarios tengan acceso remoto sin que deban autentificarse nuevamente. El anfitrión al que se conectan confía en que el sistema solicitante ha dado autentificación al usuario en forma correcta. El modelo de autentificación basado en el anfitrión es, inapropiado para utilizarse a través de Internet, en general, no puede confiar en los anfitriones fuera de la red. Ni siquiera se puede estar seguro de que los paquetes sean del anfitrión que dicen ser.

Noticias de Usenet

Los grupos de noticias (newsgroups). Están diseñados para la comunicación de muchos a muchos. De igual forma que el correo electrónico este servicio está diseñado para facilitar comunicaciones asíncronas.

Peligro: Los riesgos de las noticias son muy similares a los del correo electrónico: sus usuarios pueden confiar ciegamente en la información recibida; pueden divulgar información confidencial. Las noticias asemejan una inundación cuando funcionan de forma normal, así que debe asegurarse de configurarlas para que las inundaciones no afecten otros servicios.

Protocolo: NNTP(Protocolo de Transferencia de Noticias en Red o Network News Transfer Protocol). Se utiliza para transferir noticias a través de Internet. Para instalar el servidor de noticias en su sitio debe determinar la forma más segura de que fluyan las noticias a sus sistemas internos para que NNTP no pueda ser utilizado para penetrar su sistema principal. Algunos sitios ponen el servidor de noticias en el anfitrión bastión (el más confiable), otros en un sistema interno. Las transferencias externas de NNTP son con máquinas específicas.

Peligro: Muchos sitios crean grupos locales privados para facilitar las discusiones entre sus usuarios; estos grupos con frecuencia contienen información delicada, confidencial o propietaria. Alguien con acceso a su servidor NNTP puede, en potencia, acceder a estos grupos de noticias privados, lo que deviene en divulgación de esta información.

Word Wide Web (WWW)

El WWW es el conjunto de servidores de HTTP en Internet. El Web utiliza tecnología de hipertexto para enlazar una gran cantidad de documentos que pueden incluir texto, imágenes, sonido, video y otros formatos (el más común es HTML). El hipertexto proporciona la posibilidad de navegar de un documento a otro en Internet, con solo hacer clic en una palabra o imagen para la cual ha sido definido un enlace (o link) HTTP.

Un concepto que acompaña al WWW es el navegador. El navegador proporciona una interfaz gráfica rica en un gran número de servicios de Internet.

Protocolo: HTTP (Protocolo de transferencia de hipertexto o HyperText Transfer Protocol). Es el principal protocolo de aplicación que utiliza el WWW.

Peligro: La utilidad del Web se basa, en gran medida, en su flexibilidad, pero ésta dificulta su control. Así como es más fácil transferir y ejecutar el programa correcto utilizando un navegador Web que por medio de FTP, es más fácil transferir y ejecutar uno peligroso.

Información sobre personas

Servicio finger: Busca información sobre un usuario que tiene cuenta en la máquina que está consultando, sin importar si el cliente inició o no una sesión en ese momento en esa máquina. Esta información puede incluir el nombre real de la persona, su clave de acceso, número de teléfono, ubicación de su oficina, información sobre cuándo y dónde inició una sesión recientemente y un mensaje breve escrito por el usuario mismo.

Peligro: No necesita conocer el nombre del usuario para poder utilizar finger; por lo general este servicio da información sobre cualquier persona cuyo nombre de usuario o nombre real contenga la cadena de texto que usted especifique. Si no especifica cadena alguna, le dará información sobre todas las personas que tengan una sesión en ese momento en la máquina que está consultando. Finger puede proporcionar información valiosa a intrusos, por ejemplo, al identificar usuarios que rara vez se dan de alta. Finger es utilizado en forma legítima por muchas personas que sólo intentan saber a qué nombre de usuario enviar correo, pero ellas no necesitan toda la información que habitualmente les da finger. Dependiendo del cliente finger y de la terminal, o del emulador de terminal, en que está ejecutándose, los caracteres de control pueden producir efectos que van desde lo molesto hasta lo desastroso (como el descargar macros y presionar cualquier tecla para ejecutarlos pudiendo borrar todos sus archivos).

Servicio whois: Es similar al servicio finger, pero obtiene información disponible al público sobre anfitriones, redes, dominios y sus administradores.

Peligro: Whois puede proporcionar información valiosa a los intrusos.

Servicios de conferencias en tiempo real

Proporcionan un método para que las personas interactúen con otras personas, a diferencia de las bases de datos o archivos de información. Los servicios de conferencias en tiempo real están diseñados para que los participantes los empleen de modo interactivo.

Servicio talk: Está disponible en la mayoría de las máquinas Unix y permite que dos personas mantengan una conversación.

Peligro: Puede ser muy engañoso para permitirlo a través de un firewall sin abrir involuntariamente otros agujeros de seguridad.

Servicio IRC: Permite que muchas personas conversen entre sí en forma simultánea.

Peligro: El problema de seguridad se relaciona con los clientes y con quien utiliza IRC y cómo lo hace. Muchos de los usuarios de IRC son vándalos y atacantes que utilizan el servicio para intercambiar información técnica y para intentar engañar a otros usuarios de IRC haciendo que sigan instrucciones para dañar el sistema.

Multicast Backbone (MBONE): Es la fuente de un conjunto de servicios en Internet, enfocado a extender los servicio para conferencias en tiempo real más allá de servicios basados en texto, como talk e IRC, para incluir audio, video y pizarrones electrónicos. MBONE se utiliza para enviar videos en tiempo real de muchas conferencias y programas técnicos a través de Internet.

Peligro: La negación del servicio sin intención puede ser una verdadera preocupación con MBONE debido a que audio y video utilizan mucha memoria.

Servicio de nombres

El servicio de nombres se encarga de traducir los nombres de host que utilizan las personas a las direcciones IP numéricas que utilizan las máquinas.

El Servicio de Nombres de Dominio (DNS o Domain Name Service): permite que cada sitio tenga información sobre sus propios hosts y pueda encontrar la información para otros sitios. DNS no es un servicio a nivel usuario en sí mismo, pero soporta SMTP, FTP, Telnet y casi cualquier otro servicio que necesiten los usuarios. Además muchos servidores de FTP anónimo no permiten conexiones de clientes a no ser que puedan utilizar un DNS para buscar el nombre de anfitrión del cliente a fin de iniciar la sesión.

Peligro: DNS le permite incluir información sobre qué hardware y software está ejecutando, lo cual no conviene que sepa el atacante.

Servicio de Información de Red de Sun antes conocido como Yellow Pages (NIS/YP): Está diseñado para administrar un solo sitio, no para intercambiar información entre sitios.

Peligro: No sería posible proporcionar información desde su host a sitios externos por medio de NIS/YP sin también proporcionar su archivo de contraseña, si ambos están disponibles internamente.

Servicios para administración de redes

Son servicios para administrar y mantener las redes.

El ping y el traceroute son las dos herramientas para administración de redes más comunes. Ocupan el Protocolo de Control de Mensajes de Internet (ICMP o Internet Control Message Protocol). ICMP se implementa a bajo nivel como parte indispensable de los protocolos TCP/IP que usan todos los anfitriones en Internet.

Ping: Dice si puede o no hacer llegar un paquete a y de un anfitrión determinado y, con frecuencia, información adicional, como cuánto tarda en hacer el viaje de ida y vuelta.

Traceroute: Notifica no sólo si puede llegar a un anfitrión específico y si puede responder, sino además la ruta que siguen sus paquetes para llegar a él, lo cual es muy útil para analizar problemas de la red en alguna parte entre usted y algún destino.

Peligro: Tanto ping como traceroute pueden utilizarse para ataques de negación del servicio, pero no más que otros protocolos. Más amenazante, pueden emplearse para determinar qué anfitriones existen en su sitio como paso preliminar para atacarlos.

Protocolo Simple de Administración de Redes (SNMP o simple Network Management Protocol): Es un protocolo diseñado para facilitar la administración central de equipo de red. Las estaciones de administración SNMP pueden solicitar información (si una interfaz tiene enlace o no, cuántos bytes se han transferido a través de esa interfaz, cuántos errores han habido en ella, etc.) del equipo de red (configurando parámetros). El equipo de red también puede reportar información urgente (por ejemplo, que una línea esté descompuesta o que hay un número importante de errores en una línea específica) a tales estaciones por medio de SNMP.

Peligro: Alguna otra persona puede asumir el control de su equipo de red y reconfigurarlo para sus propios propósitos (desactivar el filtrado de paquetes, cambiar el enrutamiento o, simplemente, destruir su configuración).

Servicio de hora

El protocolo de Hora de red (NTP o Network Time Protocol) es un servicio de Internet que pone a tiempo los relojes de un sistema con gran precisión.

Desde el punto de vista de la seguridad, examinar las horas precisas anotadas en los archivos de registro de diferentes máquinas puede ayudar a analizar patrones de entradas indeseadas.

Tener relojes sincronizados también es un requisito para evitar que los atacantes graben una interacción y luego la repitan; si los registros de horas están codificados en la interacción, serán incorrectos la segunda vez que la transacción se repita.

No se tiene que utilizar NTP a través de Internet; se deben sincronizar los relojes entres sí dentro del sitio de la empresa.

Peligro: Si se usa un servicio externo puede hacerse vulnerable a falsificaciones. Sin un servicio de hora externo, todos sus equipos pueden tener la misma hora equivocada.

Sistemas de ventanas

La mayoría de las máquinas UNIX proporciona en la actualidad sistemas de ventanas basadas en X11 que le proporciona gráficas remotas. Por desgracia, lo hace proporcionando acceso total a todas las capacidades que le da cuando está sentado frente a la máquina.

Peligro: Un intruso con acceso a un servidor X11 puede hacer cualquiera de los siguientes tipos de daño:

- Obtener descarga de pantallas.- Copias de cualquier cosa que se muestre en las pantallas del usuario.
- Leer las teclas que oprime el usuario.- Puede incluir contraseñas del usuario.
- Inyectar pulsaciones de teclas.- Se verán como si las hubiera oprimido el usuario.

De modo predeterminado, los servidores X11 utilizan autentificación basada en direcciones, si es que emplean alguna; muchos usuarios desactivan esta característica en aras de la conveniencia. Por lo tanto, X11 no es seguro para usarse a través de Internet. El servidor sí proporciona la opción de utilizar una autentificación más estricta, pero la mayoría de los clientes no son capaces de utilizarla y rara vez está encendida.

Sistemas de impresión

Tanto lp, el sistema de impresión de System V, como lpr, el sistema de impresión de BSD proporcionan opciones para impresión remota. Estos sistemas permiten que una computadora imprima en una impresora físicamente conectada a otra computadora.

Peligro: Las opciones para impresión remota son formas inseguras e ineficientes de transferir datos a través de Internet. No hay razón para permitirlo.

2.11. Mal uso de los servicios de Internet.

Dentro de la red interna se debe tomar en cuenta el mal manejo de los usuarios a los sistemas, dando como resultado la inconsistencia de la red.

Éstas son sólo algunas de las consecuencias de los abusos en Internet ocasionadas por los empleados:

- **Improductividad:** Los empleados que dedican tiempo de la compañía, incluso una hora diaria, para acceder a los sitios de Internet para uso personal, le cuestan al empleador miles de dólares al año de improductividad.

- **Responsabilidad corporativa:** Si un empleado utiliza el acceso a Internet de la compañía para visitar material inadecuado -como material pornográfico- puede exponer a la organización a acusaciones por crear un ambiente laboral hostil.

- **Consumo del ancho de banda:** Los empleados que escuchan radio por Internet o descargan música en el trabajo, consumen ancho de banda valioso. El uso del ancho de banda no autorizado -ancho de banda que transporta tráfico sin beneficio para la organización- puede ocasionar cuellos de botella que demoran el tráfico y actividades en la red legítimas.

2.12. Conclusiones

Al cubrir necesidades con el uso del Internet, también se expone la información a un mayor alcance de personas ajenas a ésta. Los intrusos de los que se ha hecho mayor énfasis son los que están fuera de la empresa, sin embargo también los hay dentro.

Para anticiparnos a los incidentes se han conocido las técnicas más frecuentes de ataque y se han mencionado herramientas utilizadas en éstos, así como se ha seguido el patrón de comportamiento de los intrusos. De esto se puede concluir que no se debe dejar información sobre los sistemas informáticos al alcance de cualquier persona ajena a éstos. Por ello se deben minimizar las vulnerabilidades y reforzar los puntos de acceso. Así como minimizar cuentas y privilegios de los usuarios, hacia los sistemas de información.

En éste capítulo también se definieron algunos de los tipos mas comunes de atacantes informáticos, lo cual confirma la facilidad de acceso a software de intrusión no importando en muchos casos el conocimiento y habilidad informática para ser un atacante. Es aquí donde también se confirma que el 80% de incidentes es provocado dentro de las mismas expresas, esto nos sirve para considerar medidas de seguridad contra intrusos dentro de la empresa eléctrica.

Otro punto de gran importancia es el problema que se ha visto en el software maligno por lo que se explicaron sus principales características. Con el conocimiento de estas características se puede detectar a tiempo y evitar el mal comportamiento de los sistemas de información, así como evitar su propagación con antivirus que anticipen la llegada de éstos a la empresa eléctrica, así como otras formas de evitarlos. Por ello, se debe tomar en cuenta distintas estrategias para evitar la propagación del software maligno.

Al final de la sección se concluye que todo servicio tiene sus propios riesgos, unos en mayor medida que otros por lo que se debe de elegir los servicios que realmente son necesarios y generan valor para la empresa se dan a conocer las

características incluyendo los peligros de tales servicios. Hay varias formas de protegerlos, por ejemplo, ejecutar los servicios sólo en máquinas protegidas, empleando variaciones especialmente seguras de los servicios estándar; o bloquear los servicios por completo desde o hacia algunos o todos los sistemas externos en caso de no ser necesarios.

Capítulo 3
Conceptos de seguridad

Cada día las redes se vuelven más abiertas y accesibles para los empleados, socios y clientes por lo que los recursos de información en línea se vuelven cada vez más expuestos a los diferentes tipos de amenazas. Por lo que la conexión de redes corporativas requiere contemplar los diferentes aspectos referentes a la seguridad.

3.1. Bases de la seguridad

Las bases de la seguridad son las distintas categorías que se pueden usar para implantar diferentes servicios de seguridad.

Las categorías de protección que se deben tomar en cuenta son las siguientes:

- Integridad de datos.- La información no debe ser borrada ni modificada por alguien que carezca de autorización para hacerlo. Así también, que el mensaje que leemos es el mismo que nos envían.

- Confidencialidad.- La información debe ser leída por su propietario o por alguien explícitamente autorizado para hacerlo.

- Disponibilidad.- La información debe estar siempre disponible en el lugar y cantidad de tiempo requeridos.

- Autorización.- Es el permitir el acceso lícito a determinados usuarios, de acuerdo a las políticas de la organización. Así, la autorización es la responsabilidad de cada elemento de información y a la delegación de la responsabilidad a otros.

- No repudio.- El emisor no puede negar el haber enviado el mensaje.

- Consistencia.- El sistema, al igual que los datos, debe comportarse como el usuario autorizado espera que lo haga. Este tipo de seguridad también puede considerarse como asegurar que los datos y programas que se usan sean correctos.

3.2. Mecanismos de seguridad

Normalmente, una correcta configuración de los servidores y una actualización constante mediante los últimos parches de seguridad es suficiente para protegerse frente a atacantes informáticos.

Sin embargo, el verdadero experto en redes, protocolos y sistemas operativos es mucho más difícil de detener. Firewalls, sistemas de detección de intrusos, señuelos, contraseñas fuertes, y un sinfín de medidas de seguridad son necesarias para estar a salvo. Atacar un ordenador tiene su arte. Defenderse, también.

Para implantar diferentes servicios de seguridad, se usan los distintos mecanismos de seguridad. Entre los que están: El control de acceso, la auditoría, autenticación, autorización y criptografía.

- Control de acceso.- Reglamentar el acceso al sistema. Debe conocerse en todo momento quién entra al sistema y de dónde procede.

- Auditoría.- Así como tan preocupante es que los individuos sin autorización entren, es preocupante como los usuarios autorizados algunas veces cometen errores o actos maliciosos. Para cada caso deben conocerse en todo momento las actividades de los usuarios dentro del sistema. ¿Qué fue hecho? ¿Por quién? ¿Qué fue afectado?

- Autentificación.- Es garantizar que la persona que usa el sistema sea quien dice ser, de esta forma, únicamente deben de acceder al sistema personas autorizadas, siempre y cuando comprueben que son usuarios legítimos. En resumen, una autentificación es una identificación comprobada.

- Autorización.- Son los permisos lícitos dentro del sistema.

- Criptografía.- Es el arte de esconder los mensajes para que usuarios no autorizados no puedan leerlos.

3.2.1. Control de accesos.

Una razón para conectar la red corporativa a redes externas (Internet) es para usar sus servicios, de no ser así no tiene caso esta conexión. Sabemos de las ventajas que brinda esta gran red, por ello el sitio debe proteger los servicios que utilizará o proporcionará por Internet.

Antes de que se decida qué servicios se van a usar en la organización, se debe determinar qué servicios serán permitidos y cuáles no, quienes podrán acceder a determinados servicios, bloquear los servicios por completo desde o hacia algunos o todos los sistemas externos, etc.

El control de acceso permite administrar el acceso a la información o a los diferentes recursos de la organización basándose en los requerimientos de seguridad y del negocio.

El control de acceso puede aplicarse a entornos físicos (por ejemplo, llaves de oficinas, tarjetas magnéticas de acceso), a documentación en papel (contratos, manuales) o a los sistemas informáticos y datos.

Dado el alcance de este proyecto, esta sección se refiere y enfoca al control de acceso a los sistemas informáticos y de datos.

Para el control de accesos existen mecanismos de autentificación, los tradicionales permisos de acceso a recursos, los firewalls, rutas y listas de control de accesos (ACLs) definidas en los ruteadores.

ACL (Access Control Lists)

Las listas de control de Acceso, son reglas para gestionar los permisos de acceso a un archivo dando o negando el acceso a usuarios y grupos específicos en vez de servirnos del genérico sistema UGO (user, group, others) de Unix. Este mecanismo está disponible en la mayoría de las versiones de Unix. En Linux no se proporciona pero puede instalarse como software adicional. Finalmente podemos decir, que una ACL es una lista en la que el sistema comprueba si el usuario tiene acceso al objeto. La mayoría de los derechos incluyen la autorización a los archivos de lectura, escritura, ejecución o negación de todos los derechos. Así como existen sistemas operativos que usan listas de control de accesos, también las usan bases de datos, firewalls, ruteadores y otras plataformas.

ARM (Account Resource Management)

ARM provee protección a las cuentas y características de restricción de acceso, incrementa la seguridad de sistemas UNIX. ARM incluye características tales como expiración de cuentas (es el definir tiempos de acceso a las cuentas), auto-logout (si está sin actividad esa cuenta, se desactiva), auto-lockscreen (se cierra la ventana de acceso para evitar accesos), deshabilitar login (se desactiva la cuenta después de un número de intentos para entrar), etc.

Firewall

Un firewall es un componente o conjunto de componentes (hardware y/o software) que está diseñado para evitar que el tráfico no deseado y sin autorización de una red no protegida como Internet esté dentro de una red privada. Así el objeto principal de una firewall es proteger a una red de otra.

Un firewall se coloca entre la red interna confiable y la red externa no confiable. El firewall actúa como un punto de cierre que examina y rechaza el tráfico de red a nivel de red, a nivel de aplicación o ambos (vea la figura 3.1).

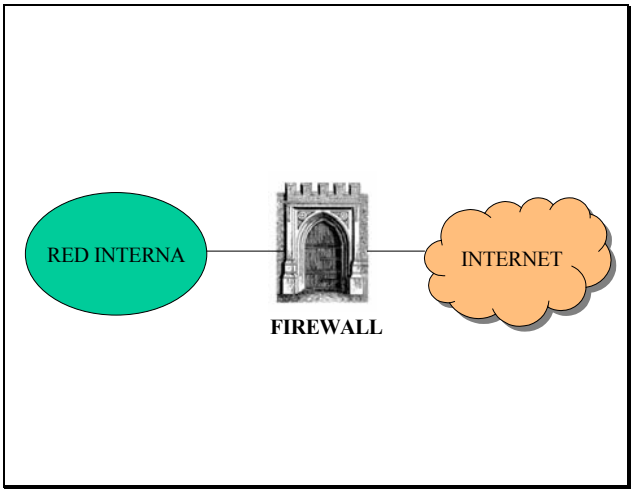

Figura 3. 1.- Colocación del firewall.

Los firewalls trabajan en las capas superiores del modelo OSI (**O**pen **S**ystem **I**nterconnection), tienen información íntegra de las funciones de la aplicación en la que basan sus decisiones. Los firewalls también trabajan en las capas de red y transporte, en cuyo caso examinan los encabezados de IP y de TCP de paquetes que entran y salen, aceptan o rechazan paquetes con base en las reglas de filtración de paquetes programados.

Para la implantación de la políticas de seguridad el principal instrumento es el firewall.

Un firewall por sí solo no asegurará la red, sólo es parte de la protección del sitio. Un firewall refuerza en gran medida la seguridad de red y reduce los riesgos para los servidores al permitir que sólo pasen los servicios aprobados y aquellos que cumplen con las reglas establecidas para ello, esto es, no dejar pasar servicios inseguros. Como resultado, el entorno de red está expuesto a menos riesgos debido a que sólo los protocolos seleccionados son capaces de pasar a través de un firewall.

Los firewalls pueden ofrecer control de acceso a los sistemas de un sitio. Por ejemplo, algunos servidores pueden ponerse al alcance de redes externas, mientras que otros pueden cerrarse al acceso no deseado. Un firewall puede mantener separada una sección de la red de otra sección. Esto, evita que los problemas que impactan una sección se extiendan a través de toda la red.

Un firewall además de ser más fácil de configurar que otras técnicas, también puede bloquear accesos a servicios como es el DNS. Otra ventaja de usar el firewall es que se puede llevar una bitácora de los accesos que pasan hacia y desde Internet al firewall y proporcionar estadísticas valiosas sobre el uso de la red. En la bitácora se pueden detectar los ataques de quienes tratan de adivinar las contraseñas.

Políticas que no pueden ser implantadas por algún firewall

Las políticas de seguridad son los procedimientos y planes documentados para proteger los recursos de la red contra pérdida y daño. Es un documento que debe acatar la gente que tiene acceso a la tecnología e información de la organización. Para esto existe todo un capítulo de políticas de seguridad donde se amplía este concepto. Lo que sí se puede adelantar aquí, es que para la implantación de las políticas de seguridad el principal instrumento es el firewall.

No toda la seguridad la proporciona un firewall. Por ello se deben encontrar otras formas de seguridad. Como lo son la seguridad física, la seguridad para anfitrión y capacitación para el usuario en el plan de seguridad.

Un firewall no puede proporcionar toda la protección para la intrusión interna, recuerde los enemigos no siempre están fuera del sitio. Un usuario interno puede copiar discos, cintas, imprimir la información y salir como si nada. Los usuarios internos pueden dañar la red, robar o modificar datos. Así también existen desastres por accidentes o sin intención de los usuarios. Para ello debe pensar también en sus soluciones, como lo son el plantear e implementar seguridad interna (el planteamiento de la seguridad interna de la empresa eléctrica se incluye en el capítulo 6) y brindar capacitación para los usuarios.

Un firewall no protege por sí solo contra nuevas amenazas, un firewall debe tener un mantenimiento continuo porque no va a proteger lo que no tiene a su alcance. Cabe recordar que siempre hay personas que encuentran nuevas formas de atacar y también encuentran otros accesos a los sistemas. Es decir, un firewall no puede proteger contra conexiones que no pasan por él.

Un firewall no protege como un antivirus, aunque se pueden detectar algunos virus, no lo va hacer con la mayoría de ellos.

3.2.2. Auditoría

Es el mecanismo que automáticamente genera registros de seguridad relacionando usuarios y actividades en un sistema informático. La auditoría requiere de autentificación adicional para estar seguros de que la persona que ejecuta el comando realmente es quien dice ser. La desventaja de la auditoría es que requiere recursos adicionales del procesador y del subsistema de disco.

En UNIX se tienen los archivos "log" que se muestran en texto, son fáciles de leer, el problema es cuado son muchos sistemas y se tiene que revisar el archivo. Estos archivos no se deben mostrar a nadie, puesto que ahí se ve la seguridad de su sistema.

3.2.3. Autentificación

La autentificación se puede clasificar en: a) autentificación biométrica, b) algo que el usuario sabe y c) algo que el usuario posee.

Autentificación biométrica

La tecnología informática hoy en día permite el uso de características del cuerpo de una persona para autenticarla. Se usan características que no se alteren fácilmente y que sean distintas de una persona a otra. Deben ser expresables matemáticamente en forma sintética. Además su visibilidad debe ser compatible con el atuendo normal de las personas. La biometría es el uso automatizado de características fisiológicas. Las características se depositan en el momento del registro y su descripción matemática se guarda en la lista de usuarios.

Al solicitar acceso el usuario exhibe la característica que haya registrado y el sistema recalcula la descripción matemática.

La biometría existe biológica y conductual. La biometría biológica es como la del reconocimiento del iris y huellas dactilares. La biometría conductual es la verificación de firmas, posición del estilete en función del tiempo, las formas y el momento que separamos el estilete del papel. Se ha estudiado y esto es característico de cada persona; es decir, nadie escribe de la misma forma que otra persona con el mismo tiempo y la misma separación del estilete.

Algo que el usuario sabe

Esto es cuando se escriben contraseñas en forma tradicional. La seguridad está en que sólo una persona conoce el password y las otras no.

Algo que el usuario posee

El reconocimiento por un objeto se da cuando lo porta siempre la misma persona, como lo son las tarjetas de identificación.

3.2.3.1. Mecanismos de autentificación

El mecanismo de autentificación ha de poseer algunas características para ser viable; ha de ser fiable con una probabilidad muy elevada, económicamente factible para la organización y ha de soportar con éxito cierto tipo de ataques. Además debe ser aceptable por los usuarios. De esta forma es mucho mejor combinar los mecanismos de autentificación. Algunos sistemas son combinación de los anteriores.

Para usar cualquiera de los mecanismos de autentificación antes descritos, se necesita hardware y/o software para implantarlos.

Algunos ejemplos de mecanismos de autentificación son:

Autentificación de mensajes por clave pública.- La autentificación de mensajes es un método que puede ser utilizado por los destinatarios de los mensajes para comprobar la validez y el origen de un mensaje. El remitente debe utilizar su clave privada para codificar el mensaje, es así como lo firma. La clave privada crea una firma digital en el mensaje que puede comprobar el destinatario o cualquier otra persona, por lo que sólo debe utilizar para firmar mensajes. El destinatario comprueba la clave pública del remitente para decodificar la firma digital. Con la firma digital el destinatario del mensaje puede comprobar que el remitente es realmente el origen real del mensaje. Sólo el poseedor de una clave privada puede crear una firma digital, ésta garantiza la identidad

del remitente. Así la firma digital procesa el archivo y crea un número único que representa el contenido, la fecha, la hora (ver la figura 3.2).

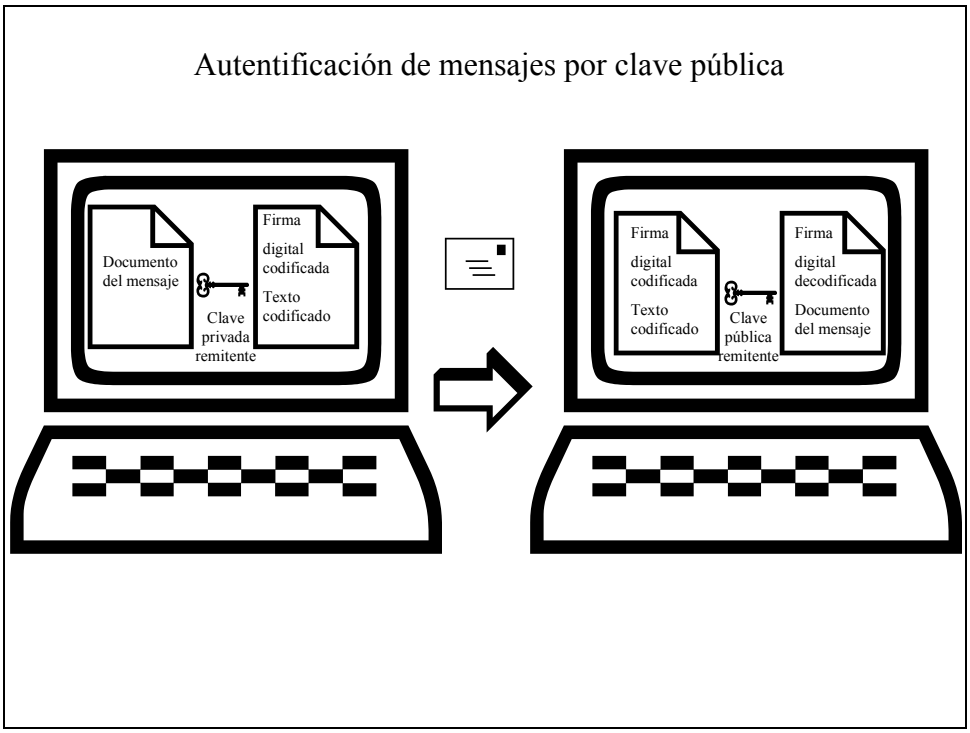

Figura 3. 2.- Autentificación de mensajes por clave pública.

Contraseñas tradicionales.- Es un conjunto de caracteres, el cual se debe mantener en secreto. Para que sea práctico y eficaz deben ser palabras que no se encuentren en ningún diccionario. Estas contraseñas no son seguras para pasarlas a través de Internet.

Para pasar una contraseña tradicional por Internet hay que asegurarse que no sea reutilizable.

Contraseñas de una sola vez (One-Time Passwords).- Dos de las formas más comunes de ataques contra sistemas informáticos conectados a Internet (y otros que no lo están) se basan en el robo del archivo de contraseñas del sistema y en la escucha furtiva de conexiones de red para obtener identificaciones y contraseñas de usuarios autorizados. La identificación y contraseña capturadas se utilizan para tener acceso al sistema; o en el caso del archivo adecuado de contraseñas, las contraseñas encriptadas se convierten a texto en claro mediante un descifrador de contraseñas. Ver figura de autentificación típica en un sistema en la figura 3.3.

El sistema de contraseña usada una sola vez está diseñado para hacer frente a este tipo de ataques y obligar al usuario a usar una contraseña diferente cada vez que se registra. Esto se realiza proporcionándole al usuario una contraseña diferente en cada conexión, ya sea que el intento de conexión tenga o no éxito. Como consecuencia,

no es posible volver a usar las contraseñas en un ataque. En la figura 3.4 se da un ejemplo del uso de passwords de una sola vez.

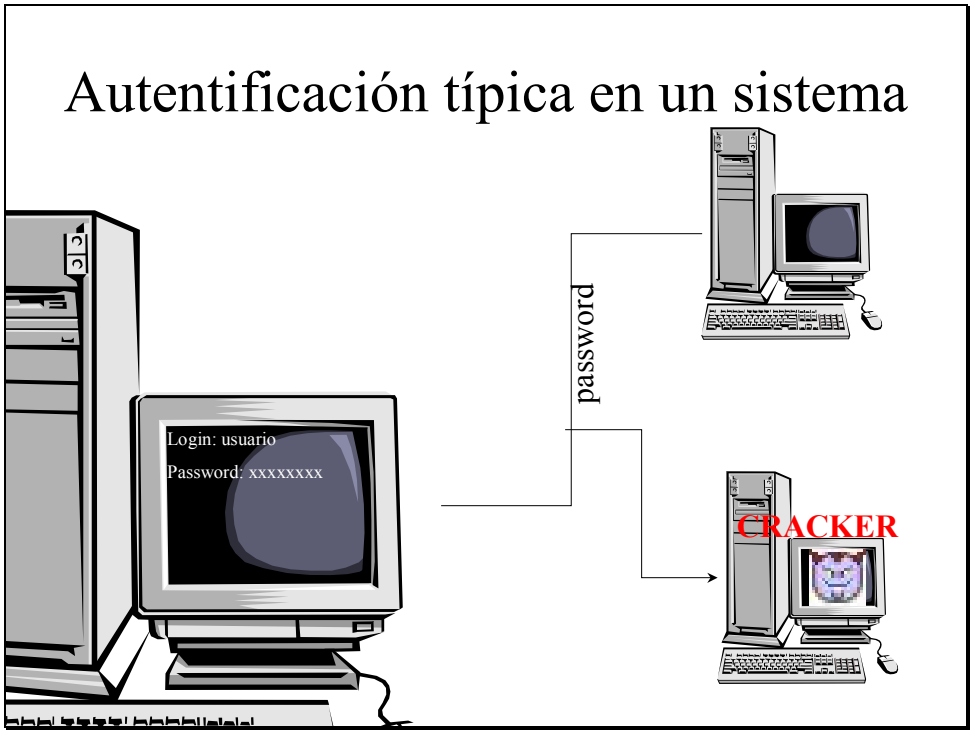

Figura 3. 3.- Autentificación típica en un sistema

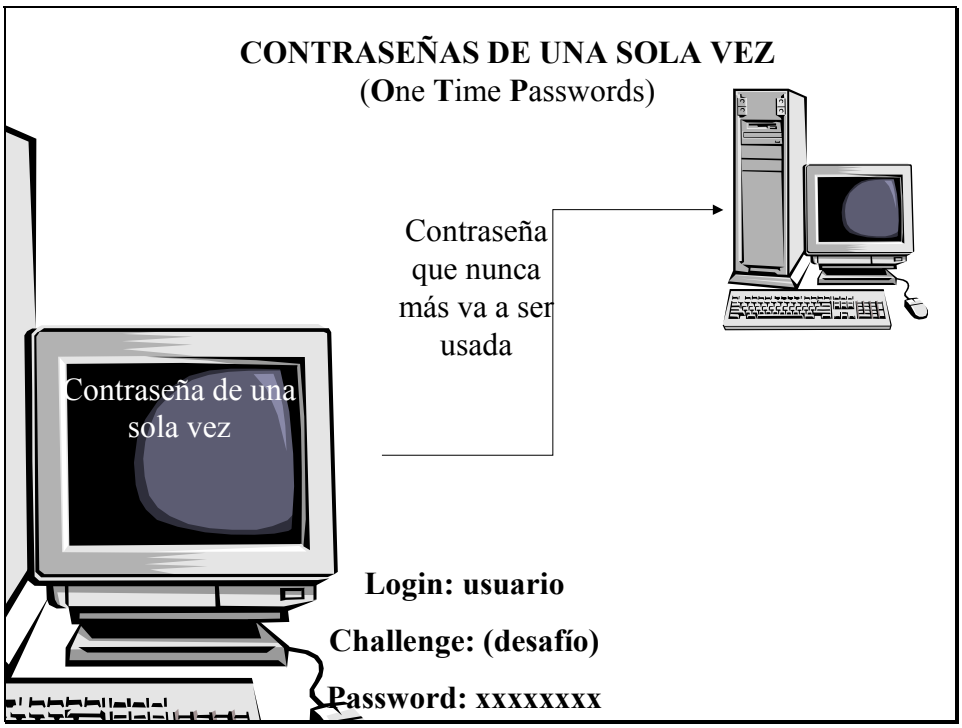

Figura 3. 4.- Contraseñas de una sola vez.

Cuando se usan passwords de una sola vez, al usuario se le presenta una pregunta cuya respuesta sólo él puede conocer.

Existen diferentes mecanismos de passwords de una sola vez. Los hay desde imprimir en papel hasta el uso de pequeños dispositivos para que el usuario lleve consigo como lo son las tarjetas inteligentes (smart cards).

Existen mecanismos que consisten en imprimir una lista de passwords y cada vez que se usa un password se va tachando, la siguiente vez que se introduzca un password se usará el siguiente al que se tachó; la lista se realiza por un algoritmo que no repetirá, cuando se termina la lista, el administrador del sistema o el usuario genera otra lista.

Otro mecanismo es una pequeña tarjeta; la tarjeta tiene un procesador incorporado con capacidad de ser programable y la capacidad de almacenar datos como lo son las claves secretas. La tarjeta desplegará un número que cambia cada minuto aproximadamente, este será la contraseña. La mejora de esta tarjeta es la de basar sus cálculos en el tiempo y en la función secreta de la serie de números.

Otro mecanismo es una calculadora especial que también se puede portar como la tarjeta; cuando la computadora acepta el login, desplegará un número, ese número se escribe en la calculadora, entonces la calculadora devuelve un número que es la desencriptación del reto, finalmente este número se introduce a la computadora la cual lo encriptará con la misma clave programada en la calculadora, para activar las

calculadoras se tiene que introducir un número de identificación personal (así que lo único monitoreable es el reto al azar y el resultado codificado, no el PIN ni la clave programada en la calculadora), finalmente el sistema hace la comparación de que el usuario es en realidad quien dice ser y lo deja entrar; la diferencia de este mecanismo basado en un reto al de la tarjeta inteligente es que no se basa en el tiempo. En la figura 3.5 se muestran ejemplos de los mecanismos antes mencionados también conocidos como tarjetas de seguridad dinámica. Otros mecanismos están basados en la criptografía y requieren que el usuario corra un programa especial.

Figura 3. 5.- Tarjetas de seguridad dinámica.[15]

Sistemas de autentificación completa.- Kerberos y el módulo del servidor de autentificación de TIS FWTK son dos sistemas que le permiten evitar enviar contraseñas reutilizables a través de Internet. Estos sistemas están ampliamente disponibles.

Kerberos.- Está diseñado para proporcionar servicios de autentificación estricta y encriptación a través de versiones modificadas de clientes y servidores estándar, por ejemplo clientes y servidores Telnet.

Kerberos fue desarrollado por el MIT (Massachusetts Institute of Technology) y tiene varias implementaciones disponibles para muchas versiones de UNIX; y el código está disponible si quiere llevarlo a un sistema operativo que aún no tiene una implementación.

Kerberos se basa en conservar la seguridad en un ordenador, en lugar de mantener la seguridad de todos los ordenadores de una red. Utiliza un único ordenador (conocido como servidor fiable) como centro de seguridad, que se puede encontrar bien asegurado físicamente y en el que se guardan las contraseñas e información de acceso de todos los usuarios, sólo en este servidor fiable va a confiar Kerberos, y en ningún otro de la red.

Un usuario que mantiene una de las máquinas de una red que trabaja con Kerberos si quiere acceder a otro de los servidores de la red, tendrá que obtener el permiso correspondiente del servidor fiable.

[15] Imagen obtenida de http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/network/authen.asp

Esto es como sigue:

El usuario de un equipo (cliente) que quiere acceder a un servidor no fiable hace la petición al servidor fiable. Para hacer esta petición firma digitalmente el mensaje, para ello ocupa la llave privada para la encriptación y la llave pública del servidor fiable, para que este servidor pueda desencriptar.

El cliente se encarga de enviar el mensaje encriptado al servidor fiable.

El servidor fiable analiza el mensaje, así comprueba la identidad del usuario, consulta la lista de permiso de acceso del archivo solicitado (si es que se solicitó alguno). Si el cliente carece de permisos de acceso al archivo solicitado, Kerberos deniega la petición al cliente. Si el cliente tiene permiso de acceso al archivo solicitado, el servidor fiable le pondrá en contacto con el servidor no fiable y le informará que desea un archivo; para ello, el servidor fiable le envía al cliente una llave única que se conoce como ticket. El servidor fiable ocupa la llave pública del cliente para encriptar el ticket y así evitar interceptaciones. El ticket contiene información de acceso y la llave de la sesión. La llave de sesión es una clave temporal que se usará durante la conexión del servidor. El servidor fiable también envía una copia del ticket al servidor en el que se encuentra el archivo solicitado; esta copia está encriptada por la llave pública del servidor solicitado.

Finalmente, el cliente y el servidor que tiene el archivo solicitado, se ponen en contacto y comparan sus copias del ticket para identificarse mutuamente. Para ello, el cliente encripta la copia del ticket con la llave pública del servidor que contiene el archivo y se lo envía. El servidor usa su llave privada para desencriptar el ticket recibido. Si coincide con la copia que ha recibido del servidor fiable, le permitirá establecer conexión. En otro caso, le denegará la comunicación.

Una vez puestos en comunicación (cuando los tickets coinciden) el cliente y el servidor con el archivo solicitado, este servidor le enviará el archivo encriptado con llave pública del cliente (esta llave se encuentra en el servidor fiable) o como texto plano (de acuerdo a la configuración del sistema). Cuando el servidor completa la transmisión del archivo le envía un mensaje al servidor fiable para comunicarle que ha completado la transmisión. De esta manera el servidor fiable descarta el ticket utilizado en la transmisión. Si el cliente tratase de acceder nuevamente al servidor con el mismo ticket, el servidor fiable le negaría el acceso (vea la figura 3.6).

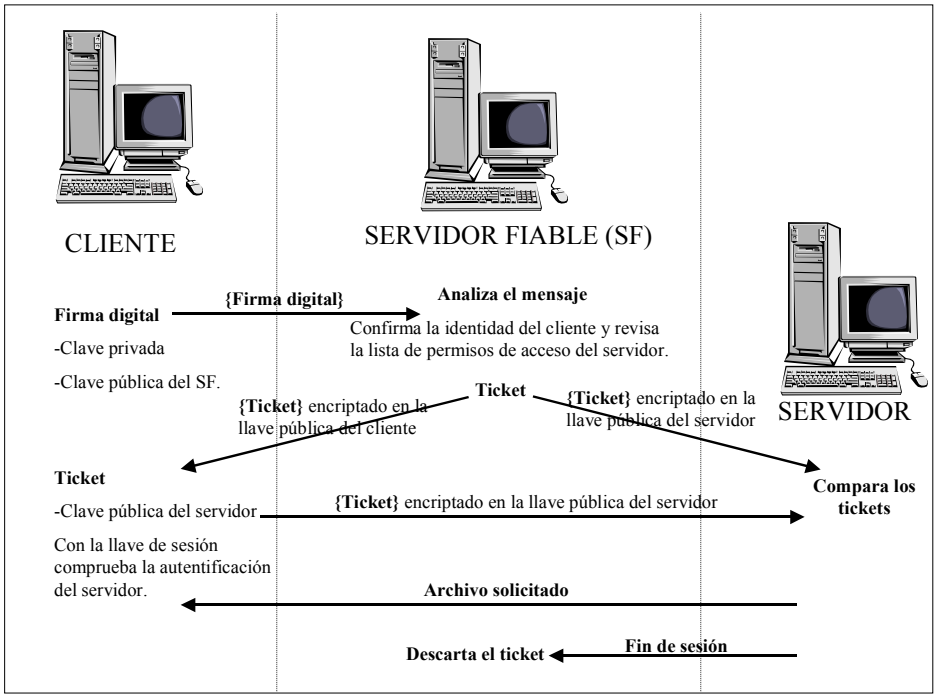

Figura 3. 6.- Autentificación con Kerberos.

Otro método de Kerberos es el que sigue:

El cliente envía una petición en texto plano para que se le envíe un ticket que garantice un ticket de transmisión al servidor fiable. Este verifica la identidad del cliente a través de una llave secreta compartida y le envía el ticket de garantía al cliente. Ahora el cliente ya puede utilizar este ticket de garantía para obtener el ticket definitivo del servidor fiable para cada destino al que desee acceder una vez que establezca la conexión. Cuando el servidor fiable recibe la petición del cliente, encripta el ticket de acceso junto a la llave maestra de la sesión y lo introduce todo en el ticket de garantía, en este ticket también van los derechos de acceso. Finalmente el servidor se lo envía al cliente. (Ver figura 3.7)

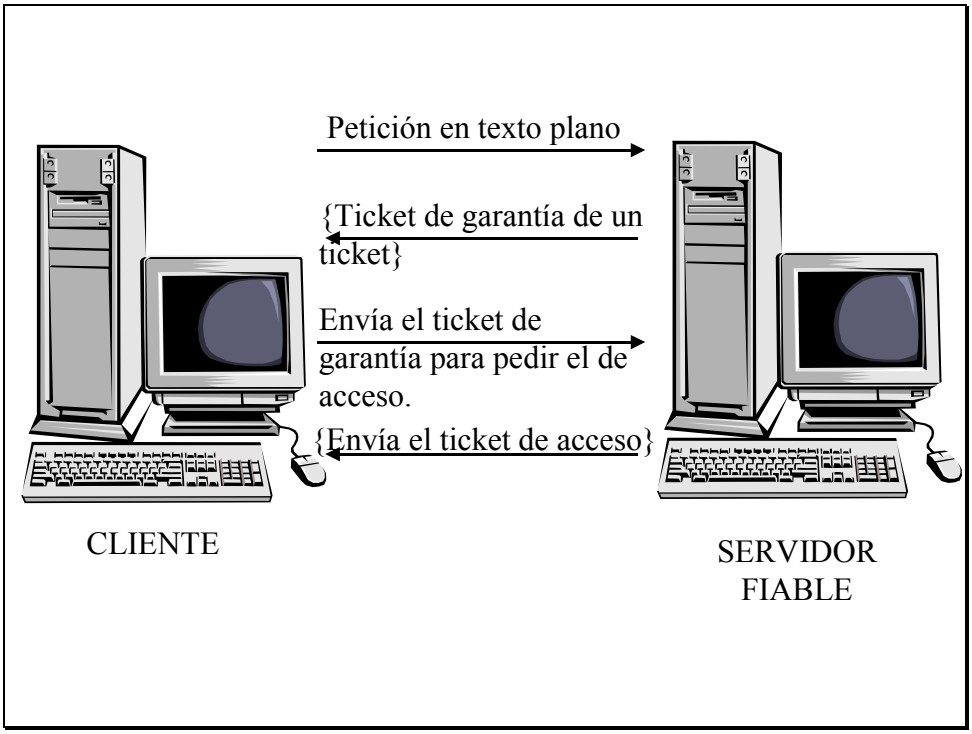

Figura 3. 7.- Kerberos sin usar llave pública.

Todo lo anterior es transparente al usuario. El sólo verá desplegar en la pantalla del monitor la petición de login y password.

Sin embargo esta solución, Kerberos, tiene grandes problemas: Kerberos tiende a ser difícil de configurar y manejar.

Kerberos no se puede escalar bien para más de un solo dominio administrativo. Cada dominio de Kerberos es independiente. Para hacer autentificación entre dominios, es esencial que los servidores en los dos dominios confíen uno en el otro, y deben compartir una clave conocida sólo por ambos. Se necesita una clave independiente para cada par de dominios que van a autenticarse entre sí; conforme aumenta el número de dominio implicados, aumenta en forma geométrica el número de claves requeridas, hasta que rápidamente se convierte en algo imposible de manejar. La mayoría de los sitios no tienen clientes Kerberos disponibles, así que aunque instale en sus servidores de Kerberos, los usuarios no podrán acceder desde otros sitios arbitrarios, porque se necesita software modificado en ambos extremos.

El módulo servidor de autentificación TIS FWTK.- El servidor implementa diversos mecanismos de autentificación, como contraseñas estándar reutilizables, S/Key, tarjetas SecurID de Security Dynamics y tarjetas SNK-004 de Digital Pathways, (mecanismos que usan contraseñas de una sola vez). Está diseñado de modo que puedan integrarse con facilidad nuevos mecanismos de autentificación. Un solo servidor de autentificación puede manejar cualquier número de máquinas y programas cliente y cualquier cantidad de métodos de autentificación distinto.

Cuando un programa cliente desea autenticar a alguien usando el servidor de autentificación de TIS FWTK, sigue estos pasos:

1. Pide al usuario una clave de acceso.
2. Se comunica con el servidor de autentificación y le dice que intenta entrar.
3. Recibe una respuesta del servidor de autentificación que le dice qué pedirle al usuario (que va de acuerdo al mecanismo).
4. Muestra en pantalla el indicador especificado por el servidor de autentificación.
5. Recibe la respuesta del usuario y la envía al servidor de autentificación.
6. Recibe un mensaje de aceptación o de error del servidor de autentificación.
7. Permite el acceso al usuario en caso de aceptación o muestra la pantalla de error.

3.2.4. Autorización

Se implementa con el uso de tablas de control de accesos para usar autentificación y definición de roles. Un rol representa un conjunto de acciones que un usuario puede ejecutar, si la autentificación es exitosa. Asumiendo que el rol involucra la identificación y la autentificación para asumir dicho rol.

3.2.5. Criptografía

Las raíces etimológicas de la palabra criptografía son kriptos y graphos, que se traduce como escribir. Concluyendo que criptografía significa: arte de escribir mensajes en claves o enigmáticamente. El criptoanálisis es el que trata de descifrar los mensajes en clave.

3.2.5.1. Variantes de cifrado

La palabra criptología se deriva del griego *kryptós*, oculto, y *logós*, palabra. En consecuencia, la criptología se puede definir como la ciencia de las palabras ocultas. El criptoanálisis es el descifrar los mensajes en clave. La criptología se divide en criptografía y criptoanálisis.

El objetivo original de la criptografía era mantener en secreto un mensaje, en la actualidad no se persigue únicamente la privacidad o confidencialidad de los datos, sino que se busca además garantizar la autentificación de los mismos, su integridad y su no repudio.

Así la encriptación es un proceso por el cual un mensaje (llamado texto plano, texto en claro o texto llano) es transformado en otro mensaje (llamado texto cifrado) usando alguna función matemática y un password de encriptamiento (conocido como llave).

El descifrado o desencriptación es el proceso invertido: el texto cifrado regresa al texto plano usando una función matemática y una llave.

> "Entonces se detenían las caras y papeles dirigidos a ellas y los entregaban a artistas muy hábiles, capaces de encontrar el sentido oculto de palabras, sílabas y letras."[16]
>
> Viajes de Gulliver
> Jonathan Swift

3.2.5.2. Criptosistemas[17]

Para conocer el funcionamiento, es necesario saber la estructura del criptosistema (vea la figura 3.8).

Matemáticamente se puede definir un criptosistema como una cuaterna de elementos $\{A, K, E, D\}$, formada por:

Un conjunto finito llamado alfabeto, A, a partir del cual, y utilizando ciertas normas sintácticas y semánticas, se puede emitir un mensaje en claro u obtener el texto en claro (o texto plano) correspondiente a un mensaje cifrado.

Otro conjunto finito denominado espacio de claves K, formado por todas las posibles claves, tanto de cifrado como de descifrado, del criptosistema.

Una familia de aplicaciones del alfabeto en sí mismo, E: $A \to A$, llamadas transformaciones de cifrado. El proceso de cifrado se suele representar como

$$E(\kappa, a) = c, \qquad \text{donde } \kappa \in K, \ a \in A \text{ y } c \in A.$$

Otra familia de aplicaciones del alfabeto en sí mismo, D: $A \to A$, llamadas transformaciones de descifrado. Análogamente al proceso de cifrado, el de descifrado se representa como:

$$D(\kappa', c) = m, \qquad \text{donde } \kappa' \in K, \ c \in A \text{ y } m \in A.$$

[16] Podemos ver que la criptografía no es una ciencia nueva.
[17] Seguridad en Unix y Redes, Antonio Villalón Huerta, V.1.2, octubre 2000.

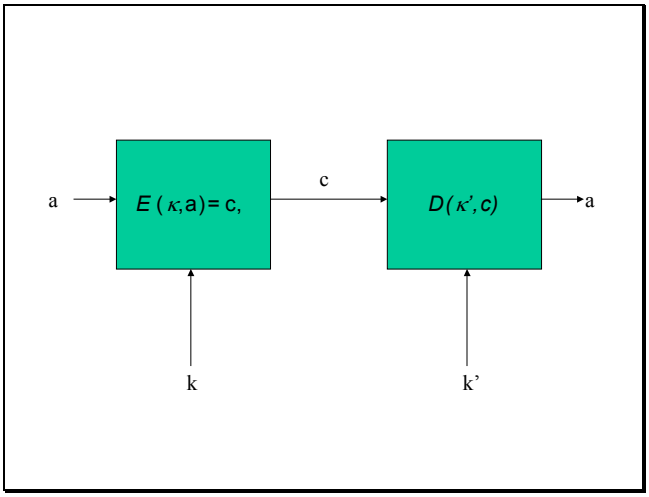

Figura 3. 8.- Estructura de un criptosistema.

El emisor emite un texto en claro, que es tratado por un cifrador con la ayuda de cierta clave, κ, creando un texto cifrado (criptograma). Este criptograma llega al descifrador a través de un canal de comunicaciones. El descifrador convierte el criptograma de nuevo en texto claro, apoyándose ahora en otra clave, κ', y este texto claro ha de coincidir con el emitido inicialmente.

Después de lo expuesto, es evidente que el elemento más importante del criptosistema es el cifrador, que ha de utilizar el algoritmo de cifrado para convertir el texto claro en un criptograma. Para hacer esto, el cifrador depende de un parámetro exterior, llamado clave de cifrado (o descifrado, para el descifrador) que es aplicado a una función matemática irreversible (al menos computacionalmente); no es posible invertir la función a no ser que se disponga de la clave de descifrado.

La clasificación de criptosistemas se hace en función de la disponibilidad de la clave de cifrado/descifrado. Existen, por lo tanto, dos grandes grupos de criptosistemas: criptosistemas de clave privada y criptosistemas de clave pública.

Criptosistemas de clave privada

Se denominan criptosistemas de clave privada (de clave secreta, de clave única o simétrico) aquel criptosistema en el que la clave de cifrado, K, puede ser calculada a partir de la de descifrado, K', y viceversa. En la mayoría de estos sistemas, ambas claves coinciden, y por supuesto han de mantenerse como un secreto entre emisor y receptor: si un atacante descubre la clave utilizada en la comunicación, ha roto el criptosistema. De todos los sistemas de clave privada, el más usado en la actualidad es DES (Data Encryption Standard). Los sistemas de cifrado de clave privada se dividen en dos grandes grupos de criptoanálisis: por un lado están los cifradores de flujo, que son aquellos que pueden cifrar un sólo bit de texto claro al mismo tiempo, y por tanto su cifrado se produce bit a bit, y por otro lado tenemos los cifradores de bloque, que cifran un bloque de bits como una única unidad.

Criptosistemas de clave pública

El cual usa una llave que se puede hacer pública a las partes interesadas, esta llave se llama pública y es para encriptar el mensaje y una llave privada para desencriptarlo, la llave privada sólo la ha de conocer la persona que debe desencriptar el mensaje.

Cuando un receptor desea recibir una información cifrada, ha de hacer llegar a todos los emisores su clave pública, para que estos cifren los mensajes con dicha clave. De este modo, el único que podrá descifrar el mensaje será el legítimo receptor, mediante su clave privada.

Matemáticamente, si *E* es el algoritmo cifrador y *D* el descifrador, se ha de cumplir que

$$D(\kappa, E(\kappa', M)) = M,$$

representando M un mensaje, y siendo κ y κ' las claves de descifrado y cifrado, respectivamente. Este criptosistema también es llamado como llave asimétrica por el hecho de que las claves son diferentes.

Criptosistemas híbridos público/privado

En estos sistemas son usados para cambiar una llave de sesión aleatoria, la cual es empleada como la base de un algoritmo de llave privada. (Una llave de sesión es usada solo una vez por una sesión de encriptación y es descartada). La criptografía actual de llaves públicas en su mayoría son sistemas híbridos.

Resumen de los sistemas de clave privada que se usan en la actualidad[18]

ROT13

Un algoritmo simple de cifrado que se usa, generalmente, para oscurecer el contenido de chistes escabrosos en varios grupos de usuarios de Usenet. El algoritmo de cifrado ROT13 no tiene clave y no es seguro.

cryp

Crypt usa una clave de longitud variable. Algunos programas pueden descifrar automáticamente archivos cifrados con crypt sin tener conocimiento previo de la clave o del texto en claro. Crypt no es seguro. (Este programa no debe confundirse con el programa crypt() de un solo sentido que es seguro y que UNIX utiliza para cifrar contraseñas).

DES

El Estándar de Cifrado de Datos, es un algoritmo de cifrado desarrollado en los años 70 por la National Bureau of Standards and Technology (nombrado desde

[18] Practical UNIX & Internet Security, Simson Garfinkel and Gene Spafford.

entonces el National Institute of Standars and Techonology o NIST) e IBM. DES utiliza una clave de 56 bits. A DES también se le conoce como DEA.

RC2

Un cifrador de bloque originalmente desarrollado por Ronald Rivest y mantenido como una patente secreta por la RSA Data Security. Este algoritmo fue revelado por un usuario anónimo de la Red quien lo publicó en 1996 y parece ser razonablemente sólido (aunque hay algunas claves en particular que son débiles). RC2 se vende con una implementación que permite claves de 1 a 2048 bits de longitud. La longitud de clave de correo RC2 a menudo se limita a 40 bits en el software que se exporta. Sin embargo, una clave de 40 bits de longitud es vulnerable a un ataque con fuerza bruta.

RC4

Un cifrador de cadena originalmente desarrollado por Ronald Rivest y mantenido como una patente secreta por la RSA Data Security. Este algoritmo también fue revelado por un usuario anónimo de la Red quien lo publicó en 1994 y parece ser razonablemente sólido (aunque hay algunas claves en particular que son débiles). RC4 se vende con una implementación que permite claves de 1 a 2048 bits de longitud. La longitud de clave en RC4 a menudo se limita a 40 bits en el software que se exporta.

RC5

Un cifrador de bloque desarrollado por Ronald Rivest y publicado en 1994. RC5 permite al usuario definir la longitud de la clave, el tamaño del bloque de datos y el número de rondas del cifrado.

IDEA

El Algoritmo Internacional de Cifrado de Datos, desarrollado en Zurich, Suiza por James L. Massey y Xuejia Lai y publicado en 1990. IDEA usa una clave de 128 bits y se cree que es bastante sólido. IDEA es usado por el popular programa PGP para cifrar archivos y correo electrónico. Desafortunadamente, el uso de IDEA puede verse limitado por una serie de patentes dentro del algoritmo, que pertenecen actualmente a Ascom-Tech AG, en Solothurn, Suiza. Supuestamente Ascom-Tech permitirá el libre uso de IDEA en implementaciones de PGP fuera de Estados Unidos, pero los usuarios interesados deben verificar los términos con Ascom-Tech o con sus agentes autorizados directamente.

Skipjack

Un algoritmo clasificado (secreto) desarrollado por la Agencia Nacional de Seguridad (NSA) de Estados Unidos. Se dice que se necesita un pase de seguridad a información altamente secreta para ver el código fuente y las especificaciones de diseño de este algoritmo. Skipjack es el algoritmo usado por el circuito integrado de cifrado llamado Clipper. Utiliza una clave de 80 bits. Este algoritmo se dejó de usar porque era seguro ante terceros y transparente ante el gobierno de los Estados Unidos.

Resumen de los sistemas de clave pública que se usan en la actualidad[19]

Diffie-Hellman

Un sistema para el intercambio de claves criptográficas entre partes activas. Diffie-Hellman no es realmente un método de cifrado o descifrado, sino un método para desarrollar e intercambiar una clave privada compartida y usada a través de un canal de comunicaciones público. En efecto, las dos partes acuerdan el uso de algunos valores numéricos comunes y después cada parte crea una clave. Las transformaciones matemáticas de la clave son intercambiadas. Cada parte puede entonces calcular una clave para una tercera sesión que no pueda ser fácilmente derivada por un agresor que conozca ambos valores intercambiados. Existen varias versiones de este producto, las cuales involucran un número de partes y transformaciones diferentes. Se debe tener particular cuidado en la selección de algunos de los números y cálculos que se utilizan para no comprometer el intercambio. El algoritmo Diffie-Hellman se usa frecuentemente como la base para el intercambio de claves criptográficas para cifrado en una línea de comunicaciones. La clave puede ser de cualquier longitud, dependiendo de la implementación de la que se trate. Entre más largas sean las claves generalmente son más seguras.

RSA

El reconocido sistema de cifrado público desarrollado por Ronald Rivest y Adi Shamir, y por el profesor Leonard Adleman de la USC. RSA puede usarse tanto para cifrar información como para ser la base de un sistema digital de firmas. Las firmas digitales pueden usarse para verificar la autenticidad de la información digital. La clave puede ser de cualquier longitud, dependiendo de la implementación de que se trate. Las claves más largas generalmente son consideradas más seguras.

ElGamal

Otro algoritmo basado en aritmética exponencial y modular. ElGamal puede usarse para cifrado y para firmas digitales de manera similar que el algoritmo RSA. Las claves más largas generalmente son consideradas más seguras.

DSA

El algoritmo de firmas digitales, desarrollado por la NSA y adoptado como el Estándar Federal de Procesamiento de Información (FIPS) por NIST. A pesar de que la clave en DSA puede ser de cualquier longitud, solamente se permiten claves de entre 512 y 1024 bits bajo FIPS. Como se especificó DSA se utiliza solamente para firmas digitales, aunque es posible usar las implementaciones de DSA también para cifrado. En ocasiones a DSA se le conoce como DSS.

3.2.6. Antivirus

Los antivirus son aplicaciones para la detección, eliminación de virus informáticos y protección de sistemas informáticos. El antivirus debe poder reconocer los distintos virus u otros programas malignos y debe conocer de alguna manera su

[19] Practical UNIX & Internet Security, Simson Garfinkel and Gene Spafford.

comportamiento para actuar en consecuencia o recomendar al usuario de las medidas a tomar.

Para la instalación de un antivirus se debe tomar en cuenta cada lugar en el que se puede infectar una computadora. Un ejemplo es que si se pueden infectar las computadoras por un correo electrónico, entonces pensamos que el correo electrónico se puede obtener por SMTP, HTTP, en notebooks, en redes VPN, entre otros.

3.2.61. Forma de contraatacar al software maligno

Diariamente se registran aproximadamente 30 nuevos virus al día. La mejor forma de atacarlos es con un antivirus que se esté actualizando frecuente y permanentemente. A esta solución se debe agregar antispyware y firewalls que filtren las conexiones.

Bug-ware

Como se mencionó, este no es un virus, pero la forma de evitarlo es leyendo los manuales o dando una capacitación a los usuarios finales sobre el software, para un uso correcto.

Troyano

Aunque este no se reproduce mas que una vez y ésta es cuando el usuario lo ejecuta, sí perjudica. Una forma de atacarlo es ser legal y no piratear. Otra forma de evitarlos es no abrir archivos ejecutables que no se sabe qué son o quién los envía.

La característica más importante y común de los Troyanos en sistemas Windows es su doble extensión, por ejemplo: un archivo nombrado como ele.gif.exe. el archivo aparecerá en el explorador como ele.gif sin la doble extensión .exe, de ahí que sea imprescindible configurar el sistema para que muestre todas las extensiones de los archivos. Tenga un antitroyano que rechace las dobles extensiones.[20]

Bombas lógicas y bombas de tiempo

Lo mejor para evitar algunos de estos virus es sólo usar las licencias permitidas. Pagar a tiempo los programas.

Conejo

La mejor forma de evitarlo es por la observación de quién tiene siempre su impresora, haga caso de los reportes de los usuarios.

Gusanos y ranas (worms)

La cura es simple: Tener el sistema al día. Los gusanos no son inteligentes, saben atacar únicamente a una versión de un demonio. Actualizar la versión vulnerable por una más nueva. Algunos antivirus pueden ayudar enviándolos a cuarentena.

[20] Enter@te. UNAM., 29 de agosto del 2002., No. 11. Suplemento mensual.

Camaleón

Un programa camaleón puede utilizarse, por ejemplo, para desviar los céntimos de las transacciones bancarias a una cuenta determinada; en este caso, lo mejor que puede hacer ante este tipo de técnica es... llamar a la policía.[21]

Spoofing[22]

Con el uso de las tecnologías IP resulta imposible eliminar todos los paquetes de direcciones falsas (spoofing IP). Sin embargo, es posible reducir el número de estos si se siguen un grupo de pasos para restringir el flujo de entrada y salida de la red.

Actualmente, el mejor de los métodos consiste en instalar un ruteador, con capacidad de filtrado, en el borde de la red. El ruteador puede formar parte de un firewall o constituir él mismo uno, formando una arquitectura denominada "screening router" (ruteador apantallado que consiste en el filtrado de paquetes en el ruteador). Este equipo debe restringir el tráfico de entrada en la interfaz externa, con el conocido filtro de entrada. Por otra parte, debe establecerse un filtro de salida en la interfaz con la red interna. En el filtro de entrada se recomienda bloquear el siguiente grupo de direcciones:

- Las direcciones de difusión, que son aquellas empleadas por los atacantes que usan smurf y otros ataques.
- Los paquetes de entrada con dirección fuente correspondiente a las direcciones internas. Evidente prueba de spoofing que puede ser utilizada en los ataques DoS, spoofing SMTP o para la obtención de algún otro servicio.
- Los paquetes con direcciones privadas referenciadas en RFC 1918. Estas direcciones no pueden ser utilizadas por ninguna red para acceder a Internet.

10.0.0.0	-	10.255.255.255 (prefijo 10/8)
172.16.0.0	-	172.31.255.255 (prefijo 172.16/12)
192.168.0.0	-	192.168.255.255 (prefijo 192.168/16)

- Paquetes con direcciones fuente 127.0.0.1. Estos son paquetes utilizados normalmente para enrutamiento interno de la computadora.
- Las direcciones que contienen .0 en uno de sus campos u octetos. Esto tiene la dificultad de que muchos ruteadores no son buenos bloqueando este tipo de paquetes.

En cuanto al filtro de salida deben ser bloqueados:

- Paquetes de salida con dirección fuente correspondiente a direcciones externas a la red. Evidencia el trabajo de un usuario mal intencionado.

En este último filtro, además, pueden bloquearse casi todas las variantes recomendadas para el filtro de entrada y evitar en mayor medida ser la fuente de ataques.

[21] Virus Informático., Arturo Hernández Hernández., DGSCA., UNAM.
[22] Los ataques spoofing. Estrategia general para combatirlos., Walter Baluja García, Depto. Telemática, ISPJAE, Cuba. http://www.criptored.upm.es/guiateoria/gt_m189a.htm

Las medidas de filtrado expuestas son válidas para todos los niveles del árbol de conexiones de Internet. Son reglas aplicables en todos los nodos, incluidos ISP's (Internet Service Providers - empresas dedicadas a ofrecer acceso a Internet como a otros servicios de red), y hasta en los usuarios finales. En el caso de entidades que de alguna forma proveen servicios, deben tener en cuenta las direcciones de los clientes para elaborar las reglas de filtrado.

Autenticación (engaño de e-mail)

La única forma de estar seguro de que un mensaje del correo electrónico es de quien dice ser es mediante una verificación de la firma digital. Una firma digital es un valor único creado por un programa aplicando una función matemática y una clave de codificación a un mensaje o archivo. Una firma digital es un valor único que corrobora tanto la identidad del autor del archivo como que nadie lo ha modificado durante la transmisión del remitente al receptor. Si por cualquier razón, recibe una gran cantidad de mensajes falsos, podrá ser capaz de seguirle la pista al falsificador gracias a la información de la cabecera del mensaje, que normalmente incluirá la información del servidor originario de su mensajero hostil. Dotado con esa información, se puede hablar con el administrador de ese sistema y ver si hay algún medio de impedir a ese mensajero futuras acciones de engaño, por lo menos contra quien reporta.

3.2.6.2. Forma de anticipar a los virus

Además de estar poniendo al día el antivirus, sí existe la forma de anticipar a los virus. Existen compañías de antivirus que ahora son capaces de detectar los virus cuando inician a infectar, estas compañías en primera instancia pueden mandar por Internet un filtro del contenido a los sistemas de las organizaciones con las características de los virus que inician su propagación aún sin saber el nombre de éstos. Una vez prevenido el ataque, se reporta si intentó ingresar. Si es así se pueden deshacer las últimas acciones que caracterizan al nuevo virus. Posteriormente encuentran el antivirus para distribuirlo por vía de redes internas, locales e Internet a los usuarios finales.

Para elegir una compañía antivirus debe considerar la velocidad con la que elaboran la vacuna o en su caso la plantilla para el filtrado del contenido.

3.2.6.3. Recomendaciones generales

En primer lugar debemos utilizar un antivirus para revisar todo el software que nos llegue, a través de disquetes, archivos, ejecutables y correo electrónico.

Si se recibe un correo no se debe abrir cuando se desconoce al emisor o no se está seguro del mismo, así cuando se espera un correo con adjuntos hay que revisarlos por un antivirus. Muchos de los virus se envían por tarjetas de felicitación y programas que se hacen curiosos a los usuarios.

El antivirus caduca en cuanto existe un virus que no puede detectar o limpiar por lo tanto debe renovar el antivirus para atacar también a los nuevos virus que van surgiendo.

Una forma práctica de actualizar y hacer funcionar un antivirus es programar la computadora para que realice una renovación y revisión a una hora en que no se labora con ese equipo.

3.2.7. Antispam

Una forma de evitar el spam es no reenviar mensajes masivos o en cadena para otros usuarios, por más que el objetivo parezca noble. Compañías y organizaciones serias no utilizan este tipo de estrategia y no piden que un miembro de la compañía envíe tales mensajes, puesto esto solo congestiona la red. Pero si su voluntad fuera irresistible, por lo menos coloque las direcciones de sus amigos en el campo CCO (o BCC), con copia oculta, pues esto esconde la información del destinatario. Sin embargo sus propios datos aún estarán visibles, aunque por lo menos estará preservando la privacidad de las otra personas.[23]

También existen mecanismos antispam que detienen los correos electrónicos para que no lleguen a las máquinas de usuarios finales. Estos se basan en el filtrado de texto, en algoritmos para realizar un análisis de contenido de correos, en la repetición de los textos así como en bases de datos con el nombre del asunto y dominios conocidos por el envío de estos correos molestos.

3.2.8. Filtrado de contenido

A medida que Internet y sus contenidos son más sofisticados y accesibles, también son más variadas y frecuentes las amenazas a la seguridad de la red, a la productividad de los empleados, a la responsabilidad corporativa y al consumo del ancho de banda.

Las empresas al reconocer el perjuicio que ocasionan estas amenazas complejas y las múltiples formas de propagación, deben expandir su caracterización de seguridad de la red para incluir la protección con el filtrado de contenido en los gateways de protocolo HTTP y FTP.

Con el filtrado de contenido se puede:

- Ver y ajustar los valores de restricciones para que reflejen lo que la corporación considera que es el contenido adecuado en cada una de las siguientes áreas: lenguaje obsceno, desnudos, sexo y violencia.
- Ajustar los tipos de contenido que otras personas pueden ver con o sin autorización.

[23] http://www.vsantivirus.com/hoax-carlson.htm

- Configurar una lista de los sitios Web que no podrán ver los usuarios, con independencia de las posibles restricciones que tengan.
- Configurar una lista de los sitios Web que podrán ver siempre otras personas, con independencia de las posibles restricciones que tengan.

3.2.9. Detección y prevención de intrusos

En la actualidad las redes son rastreadas en búsqueda de nuevas vulnerabilidades, esto puede ocurrir sólo una vez al mes o dos veces al día, de una u otra forma hay gente no autorizada tratando de buscar nuevas vulnerabilidades a las redes.

El problema crece cuando distintos intrusos intentan penetrar la organización usando herramientas simples y fáciles de obtener.

Una de las técnicas más usadas hoy en día para tratar de introducirse a sistemas es la de los rastreadores de puertos, los cuales hacen una búsqueda puerto por puerto en cada máquina en busca de puertas abiertas del sistema que combinada con distintas vulnerabilidades en los servicios, son un blanco más fácil.

Dichos rastreadores pueden ser dirigidos a redes en general o a una parte de la red en específico, incluyendo una sola máquina. Los intrusos pueden usar números de redes aleatorias para poder penetrar a los sistemas. Con lo cual los intrusos reciben información de servicios y puertos que proporcionan los objetivos.

Existen diversos métodos para detectar los rastreos que realizan los intrusos a las redes, al igual forma que existen diversos rastreadores conocidos como scanners para poder buscar vulnerabilidades.

La mayoría de las veces cuando los intrusos rastrean nuestra red, intentarán posteriormente atacar las máquinas más vulnerables para posteriormente acercarse al objetivo.

Agreguemos que por no parchar los sistemas operativos o no tener una buena administración de ellos los problemas de seguridad en los sistemas operativos se siguen repitiendo.

Para saber si existe algún intruso, se debe conocer cuántas puertas se tienen abiertas y tener el control de lo que se hace en los sistemas, así como llevar un control de todos los accesos puerto por puerto. En este control se debe conocer a los usuarios, saber dónde tienen accesos y para qué.

Para hacer una intrusión por scanning (barrido) de puertos un intruso lleva los siguientes pasos:

- Conforma una base de datos de direcciones lógicas (IP) como posibles blancos. Generalmente este barrido es aleatorio.

- Rastrea los puertos de una o varias máquinas, o un segmento completo de ellas, en busca de datos tales como:
  - Dirección IP de la máquina.
  - Sistema operativo y versión.
  - Puertos abiertos.
  - Servicios de red activos.
  - Vulnerabilidades asociadas.
  - Nivel de dificultad para ser atacada.
- Intenta entrar a los sistemas escaneados aprovechando sus vulnerabilidades.
- Busca privilegios de root haciendo uso de un exploit.
- Trabaja en el sistema.
- Asegura el regreso con el uso de rootkit's.
- Borra huellas
- Sale del sistema y puede regresar posteriormente.

Cuando un intruso realmente desea penetrar un sitio no escatima en recursos y tiempo invertido, para obtener la forma de atacarlo. Sin embargo, buscará la forma más rápida y confiable para él. Entonces el intruso usará rastreadores para buscar vulnerabilidades, por lo que los administradores o responsables de la seguridad de los sistemas deben conocer la forma de trabajar de los rastreadores y conocer las debilidades en los sistemas críticos, para estar mejor preparados ante ésta búsqueda de información en los equipos y las redes de la organización.

Existen en general distintos tipos de rastreadores de puertos que lo que hacen es un barrido de puertos para saber cuáles están abiertos, que servicios prestan y si son vulnerables, e incluso algunos evalúan el grado de complejidad para accesar al sistema. Existen de diversos tipos, para distintas plataformas, Windows y Unix generalmente. Entre los más conocidos se tienen: Queso, nessus, nmap, mscan y sscan.

Un rastreador es un programa especializado que es usado para determinar qué puertos TCP de un servidor se encuentran esperando conexión para poderla llevar a cabo.

El uso de estas herramientas hacen la diferencia de buscar vulnerabilidades para asegurar las redes de la empresa o para ser atacadas por los intrusos.

Así los detectores de intrusos son sistemas que conglomeran un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

3.2.9.1. Pasos a seguir para detectar un intruso:

Si se han sido configurado correctamente los servidores de la empresa y se está al día en la materia de seguridad, así como de fallos (bugs) que van surgiendo, el problema de que un intruso entre a los sistemas críticos será más fácil de detectar y no será gran problema.

En ocasiones es posible que se piense que alguien no autorizado entró al sistema crítico, pero en muchas ocasiones esto no es cierto. Así como en otras ocasiones se puede pensar que están atacando un sistema y el administrador se alarma por ello cuando en realidad sólo es señuelo para poder atacar otro sin que el administrador del sistema lo identifique. Aún así se debe mantener la calma.

Hay que remarcar que toda acción tomada durante el curso de la investigación deberá estar de acuerdo con las políticas y procedimientos de la organización.

Si algún intruso entra al sistema y sólo entra como usuario normal, intentará explotar algún fallo del sistema para obtener ID 0 o lo que es lo mismo privilegios de superusuarios.

Ahora si el intruso logra accesar como superusuario intentará controlar el sistema, dejando mecanismos para volver cuando así lo desee, por ejemplo: copiará el archivo /etc/passwd y el /etc/shadow (en caso de que utilice shadow), también puede instalar un sniffer, troyanos, leer correos ajenos, etc. Si el intruso es malicioso, modificaría páginas web, borraría archivos o los robaría, produciría un DoS, cambiaría passwords, entre otras cosas.

Lo primero es revisar la bitácoras del sistema, por si no se tiene instalada ninguna herramienta de detección de intrusos. Para ello primero se debe definir lo que se quiere conocer y determinar qué información se necesita de las bitácoras. El segundo paso es identificar qué bitácoras tienen esa información.

Por ejemplo en la bitácora /var/log/messages o /var/adm/messages puede ser detectado un ataque bufferoverflow, en esta bitácora se vería caracteres repetitivos y sin sentido alguno, muchas veces se le conoce como basura. Si aparece algo similar significará que alguien ha intentado explotar una vulnerabilidad del automount del sistema. Es difícil determinar si fue exitosos o no. Para saber si fue exitoso o no, hay que revisar si hay conexiones de lugares remotos hacia el sistema. Otra forma de ver si el intruso tuvo éxito es buscando cuentas con nombre atacante como pueden ser “crack0”, “w0rm” u algunas otras, que se hayan agregado recientemente al sistema, específicamente a la tabla /etc/passwd.

Una vez que el intruso está adentro, lo más común es que limpien las bitácoras e instalen troyanos para las bitácoras. De aquí en adelante ya no se recibirán bitácoras provenientes del sistema.

En la bitácora de messages también se puede ver si se ha sido rastreado recientemente y nos podemos dar cuenta si se encuentran los procesos ejecutados por servicios FTP (en caso de que tenga este servicio).

Se deben examinar archivos log a conexiones de lugares inusuales u otra actividad inusual. Por ejemplo, se debe buscar el último acceso al sistema, conteo de procesos, o todos los accesos generados por syslog y otros accesos de seguridad. Si el firewall o el ruteador escribe accesos a una localidad diferente que la del sistema comprometido, se deben revisar también tales accesos. Se debe notar lo importante que

es conocer los mensajes de las bitácoras. Muchos intrusos editan archivos log en un esfuerzo por esconder su actividad.

Se deben buscar archivos ocultos. Muchos de ellos empiezan con un '.' (signo de puntuación). Se deben revisar exhaustivamente todos los archivos ocultos, estos no son mostradors con un simple ls (se recomienda un ls -a), estos se utilizan para esconder herramientas para romper la seguridad del sistema, por ejemplo un programa crack o también contener el /etc/passwd del sistema o de otros sistemas a los que ha entrado el intruso.

Otros archivos que se deben buscar son los SETUID o SETGID (especialmente los que pertenecen a root). Para eso se puede utilizar el comando find.

Se deben buscar archivos troyanos en los archivos binarios. Ésta es una de las tareas principales de un intruso cuando ha comprometido la seguridad de un servidor. Para ello se pueden comparar los archivos del sistema con archivos de instalación original o respaldos. Si se compara con los respaldos se ha de ser cuidadoso, puesto que pueden contener también troyanos.

Los programas troyanos pueden producir el mismo checksum y timestamp estándar como la versión legítima. Debido a esto, el comando estándar sum de UNIX y los timestamps asociados con los programas no son suficientes para determinar si los programas han sido reemplazados. El uso de herramientas checksum como cmp, MD5, tripwire y otras herramientas checksum criptográficas son suficientes para detectar estos programas troyanos, provistas las herramientas checksum ellas mismas son mantenidas seguras y no están disponibles para modificación por el intruso.

Se tienen que buscar sniffers, ya que ésta es una de las opciones favoritas y más utilizadas por los intrusos, ya que los usan para capturar todo el tráfico de la red atacada, incluyendo sesiones de ftp y telnet a otros sistemas. De este modo el intruso puede obtener cuentas de usuarios (logins) y passwords.

Examinar todos los archivos que estén corriendo como los archivos "cron" y "at". Se ha visto que los intrusos dejan backdoors en archivos corriendo como "cron" o enviados como "at". Además se debe verificar que todos los archivos/programas relacionados (directa/indirectamente) por tareas del 'cron' y 'at', y las tareas que se archiven por si mismas no sean escribibles.

Se debe examinar el archivo /etc/inetd.conf, hay que buscar en especial entradas que ejecuten un shell (por ejemplo: /bin/sh o /bin/csh) y comprobar que todos los programas son legítimos y no troyanos.

Se deben buscar las alteraciones en el sistema y en los archivos, buscando los de atributo de escritura en donde no debería ser así.

Se deben examinar los equipos de la red local. Hay que buscar indicios de que la red ha sido comprometida. En particular aquellos equipos que compartan NIS+ o NFS o

aquellos sistemas listados en el /etc/hosts.equiv. También hay que revisar los sistemas que los usuarios comparten mediante el acceso del .rhost.

Examinar el archivo /etc/passwd en el sistema y checar las modificaciones a ese archivo. En particular busca la creación no autorizada de nuevas cuentas, cuentas sin password o cambios de UID (específicamente UID 0) a cuentas existentes. Otra cosa que hará el intruso es obtener la tabla de passwords, al cual le correrá un programa para buscar passwords débiles y así obtener mas cuentas para entrar al sistema.

3.2.9.2. Tips para detectar intrusos

Si la respuesta a las siguientes preguntas son afirmativas, existe la posibilidad de encontrar algún intruso dentro de la red.

- ¿Algunos comandos hacen cosas raras o no hacen nada?
- ¿El espacio en disco duro es muy poco?
- ¿La máquina está muy lenta?
- ¿La red está muy lenta?
- ¿Se encuentran en ejecución procesos desconocidos o sospechosos?
- ¿Existen conexiones desde máquinas desconocidas?
- ¿Las bitácoras muestran repetidos intentos de conexión?
- ¿Existen conexiones en días u hora inusuales?
- ¿Existen cuentas nuevas?
- ¿Existen archivos nuevos o modificados?

3.2.9.3. Herramientas a utilizar

Algunas herramientas que se pueden usar para ayudar a detectar intrusos son las siguientes:

- Para detectar sniffers: nestat, primisc.c, cpm, ifstatus, nePED.
- Para detectar Troyanos: sum, cmp, md5, PGP, COPS (módulo crc.chk), tripwire.
- Para detectar programas de borrado de rastros: antizap.c, antizap2.c.
- Para análisis de red: SATAN, TCP-Wrappers, Netcat, AAFID, ISS, Nessus, Isoft.

Otras herramientas son los productos comerciales dedicados a la detección de intrusos. Tales productos monitorean la red y siguen el comportamiento de los intrusos, teniendo ya las técnicas comunes. Si detecta un seguimiento común de los hackers dará aviso por medio de mensajes o alarmas a los administradores. Claro que no todas las alarmas son intrusiones de hackers, en ocasiones pueden ser tareas de la misma empresa, por ello se debe hacer un seguimiento de estas labores. Estos sistemas de detección de intrusos se deben ir actualizando porque los hackers también inventan o descubren nuevas técnicas de intrusión. Si existe una técnica nueva que empleen en contra de los sistemas, tal vez el IDS (Intrusion Detection System) no la detecte.

Además del IDS también está el IPS(Intrusión Prevention System) que tiene las características del IDS y además puede detener las intrusiones.

3.2.10. Infraestructura de clave pública (PKI)

Un sueño para muchos es el poder autentificar a las personas en cualquier lugar del mundo, para cualquier organización. El PKI es una solución que se está desarrollando para cumplir con ello. El PKI es para transferir información privada. Todos los datos que se necesiten son encontrados en el PKI.

Para que funcione el PKI debe haber:

- Una legislación mundial para que sea reconocido entre países.
- Se debe estandarizar la firma.
- Debe haber reglamentaciones sobre la privacidad.
- Debe haber crecimiento de modelos de comercio.

El problema del PKI es que sea reconocido por todos, es decir depende de la validez que se le quiera dar por los usuarios.

La ITU (International Telecommunications Union) piensa que PKI sólo será funcional cuando sea adoptado por la mayoría en forma estándar.

3.3. Recomendaciones ISO sobre seguridad[24]

El organismo internacional de normalización (ISO) recomienda que el cifrado se realice en el nivel de presentación del modelo OSI. ISO explica las razones de esta recomendación:

- Hay un consenso general en que los dispositivos de cifrado deben estar en un nivel superior del modelo de red, para facilitar las operaciones de cifrado entre extremos. El nivel de transporte es el nivel inferior en el que se pueden proporcionar servicios entre extremos; por lo tanto, el cifrado se deberá realizar a partir del cuarto nivel.

- Pero los servicios de cifrado deben estar en un nivel superior al de transporte, de forma que se minimice la cantidad de programas a los que ha de confiarse el texto legible. Es decir, cuanto menos software opere contexto delicado, mejor. Es sensato, por tanto, desplazar los procesos de cifrado hacia un nivel superior al de transporte.

- El cifrado se debe realizar por debajo del nivel de aplicación, debido a que sería muy complicado realizar transformaciones sintácticas en el texto

[24] Redes de computadores., Protocolos, normas e interfaces. Uyless Black.

cifrado. Además, si las transformaciones sintácticas se realizan en el nivel de presentación, deben realizarse antes del proceso de cifrado.

- Como es deseable una protección de tipo selectivo (no hay por qué proteger todos los campos o registros), ISO piensa que lo mejor es realizar la selección en el nivel de presentación o un superior, ya que la información de los campos en los que se divide una cadena de datos de usuario es transparente por debajo del nivel de presentación.

- Aunque el cifrado se puede realizar en cualquier nivel, la protección adicional que obtienen los datos de usuario puede no compensar la sobrecarga de trabajo que supone el cifrado.

3.4. Conclusiones

En este capítulo se vieron los conceptos básicos en seguridad, los cuales son el principio para la comprensión del desarrollo de cualquier sistema de seguridad. Cada uno de los conceptos vistos se consideran antes de la implantación del diseño, pudiendo con ellos realizar una buena elección de los componentes del sistema de seguridad y de acuerdo a las necesidades de la empresa.

Existen varios componentes para evitar incidentes en la red. De los cuales el que evita que el tráfico no deseado entre a la red de nuestro interés es el firewall. De esta forma también se puede seccionar la red para dar un protección contra usuarios internos a los sistemas de información de los cuales se consideran críticos.

Para realizar este trabajo no sólo se instalan el firewall y otros dispositivos, sino que antes se estudia el problema y se elaboran los planes y procedimientos para salvar los recursos e información de la red contra pérdida y daño.

Por otro lado, dentro de la implantación de políticas también se deben considerar las que no pueden ser implantadas por un firewall, buscando solución a éstos con los mecanismos de seguridad para lograr la integridad de datos, la disponibilidad de la información, la consistencia en los sistemas, el control de los recursos de red, registros de lo sucedido, el tener seguro quien nos envía la información y la autorización de acuerdo a las políticas.

Dentro de los mecanismos de seguridad se eligen los que cubren las necesidades de la empresa eléctrica y también de acuerdo a sus facilidades.

En el capítulo 3 además de conocer los conceptos básicos también se dieron algunas formas de detectar intrusos, en las cuales siempre está el conocer bien los sistemas informáticos que se administran.

Capítulo 4
Políticas de seguridad

Una política de seguridad es una serie de procedimientos y planes documentados que regulan el cómo una organización maneja, protege y distribuye sus recursos de información, con el fin de resguardar los recursos de la red contra pérdida y daño. De acuerdo al RFC 2196 una política de seguridad es un documento que debe acatar la gente que tiene acceso a la tecnología y a la información de la organización[21].

Para realizar las políticas de seguridad se puede tomar cualquiera de los siguientes dos enfoques:

- Lo que no se permite debe quedar expresamente prohibido.
  En esta política se debe escribir todo lo que se quiere prohibir, todo lo demás está permitido.

- Lo que no se permite expresamente está prohibido.
  En esta política se debe escribir todo lo que se permite, todo lo demás está prohibido.

4.1. Planeación de seguridad en redes

La política debe considerar qué acciones se toleran y cuales no. Por lo que, se debe tener una política de seguridad de red efectiva la cual pueda proteger la inversión y los recursos de información de la compañía. La mayoría de las compañías tienen información crítica y confidente (secretos importantes) que debe ser protegida del vandalismo.

Lo ideal es implantar soluciones de firewall antes de que se haya identificado algún problema de seguridad, porque bien dice el refrán “después de niño ahogado tapar el pozo”. La implantación se hace antes planteando preguntas acerca de los servicios de interredes y recursos cuyo acceso se permitirá a los usuarios y de ahí señalar cuáles tendrán que restringirse debido a los riesgos de seguridad.

Cuando sus usuarios tienen acceso irrestringido en la red, implantar las políticas de seguridad va a ser más difícil. La política de seguridad debe dar flexibilidad en cuanto los usuarios puedan cumplir con sus tareas, esto es, no debe disminuir la capacidad de producción dentro de la organización. Si no se elabora bien este punto, las políticas de seguridad pueden traer resultados indeseables; los usuarios de la red pueden encontrar la forma de eludir la política de seguridad, lo que la haría inefectiva.

[21] Existen documentos con reconocimiento internacional como el BS7799 o el ISO 17799 que ya definen buenas prácticas de seguridad de la información, se puede hacer uso de ellos como herramienta para la elaboración de políticas de seguridad.

Una política de seguridad efectiva es aquella que todos los usuarios y administradores de redes pueden aceptar y están dispuestos a aplicar.

4.2. Política de seguridad del sitio

Un sitio es cualquier parte de la organización que posee computadoras y recursos relacionados con redes. Algunos recursos son: estaciones de trabajo, computadoras hosts y servidores, dispositivos de interconexión: gateways, ruteadores, bridges, repetidores, servidores de terminal, software para la conexión de red y de aplicaciones, cables de red, la información de archivos y bases de datos.

Se puede pensar en una organización que tenga varios sitios y cada uno contar con sus propias redes. De ser así cada sitio puede tener sus propias políticas de seguridad dado que los intereses y administración de los sitios no son los mismos. Si los sitios están interconectados por una red interna entonces la política de seguridad debe abarcar todos los sitios interconectados. En esta tesis se trabajó bajo el primer esquema.

Por lo que, se debe considerar la centralización o descentralización de la empresa. Si es descentralizada se debe hacer cargo de su propia seguridad cada departamento, esto hace difícil el realizar la política de seguridad porque se deben hacer lineamientos globales acerca del servicio que debe tener cada usuario. En una empresa centralizada es más fácil mantener la seguridad pero puede crear el conflicto de que algunos departamentos quieran más privilegios para algunos de sus usuarios para que puedan realizar su trabajo. Como conclusión se tiene qué conceder sólo los privilegios suficientes para cumplir con las tareas necesarias.

En una política de seguridad de red es importante asegurar que todos conozcan su propia responsabilidad para mantener la seguridad. Es difícil que una política de seguridad anticipe a todas las amenazas posibles. Sin embargo, las políticas sí pueden asegurar que para cada tipo de problemas haya alguien que lo pueda manejar de forma responsable.

Norma BS7799/ISO17799

La norma BS7799 es un conjunto de controles basados en las mejores prácticas de la seguridad de sistemas de información. Éste estándar cubre cada aspecto de la seguridad de sistemas de información:

- Equipamiento;
- Políticas de Administración;
- Recursos Humanos;
- Aspectos legales.

El ISO17799 es un estándar basado en la norma BS7799.

RFC 2196

La RFC 2196 es una guía para desarrollar políticas de seguridad en cómputo y procedimientos para sitios que tienen sistemas en Internet. El propósito de este RFC es

proveer una guía práctica para administradores que quieren asegurar su información y servicios. Los temas cubiertos incluyen políticas de contenido e información, un amplio rango de temas técnicos de sistemas y seguridad, así como respuesta a incidentes.

4.3. Identificación de activos

Una de las principales fases para poder establecer una Política de Seguridad es identificar y clasificar cada uno de los activos comprendidos en el alcance de la misma.

Los activos pueden ser:

1. Hardware: CPU's, tarjetas, teclados, terminales, estaciones de trabajo, computadoras personales, impresoras, unidades de disco, líneas de comunicación, servidores terminales, ruteadores.

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

3. Datos digitales: durante la ejecución, almacenados en línea, archivados fuera de línea, respaldos, registros de auditoría, bases de datos, en tránsito a través de medios de comunicación.

4. Personas: usuarios, administradores, personas necesarias para el mantenimiento físico.

5. Documentación en papel: manuales de programas, hardware, sistemas, contratos, procedimientos administrativos locales.

6. Suministros: papel, formularios, cintas, medios magnéticos, sistemas de almacenamiento secundario.

7. Servicios: de computación y comunicación, técnicos (iluminación, energía eléctrica)

8. Reputación de la organización.

Después de la identificación de los activos, sigue identificar las amenazas a las que están expuestos los recursos.

4.4. Posibles amenazas

- Acceso no autorizado.- Es el uso de la red sin una autorización previa.
- Riesgo de revelación de información.- Es cuando se pierde la confidencialidad de la información, este riesgo puede ser voluntario o involuntario.

- Negación del servicio.- La productividad depende del servicio, una negación puede darse por software maligno (malware) al volver inservible el equipo.
- La red puede volverse inservible por un paquete extraviado.
- La red puede volverse inservible por inundación de tráfico.
- La red puede ser fraccionada al desactivar un componente importante (como el ruteador que enlaza los segmentos de red)
- Un virus puede alentar o invalidar un sistema de cómputo al consumir los recurso del sistema.
- Los dispositivos reales que protegen a la red podrían derribarse.

Se debe determinar qué servicios son necesarios y contemplar cuál es el efecto de su pérdida.

Se habló antes de las responsabilidades sobre la red, ahora es importante identificar quienes están autorizados y qué uso se va a dar o va a ser dado por administradores y usuarios. Para ello es necesario hacer una lista de usuarios que necesitan acceso a la red. Para hacer fácil el listado se puede hacer por grupos. Entre los usuarios se deben considerar los usuarios externos y también los usuarios de la red que necesitan acceso desde otro lado.

Ya que están determinados los usuarios autorizados se deben establecer los lineamientos del uso aceptable de los recursos de red. Estos lineamientos dependen del tipo de usuario.

La política debe establecer la manera de usar un recurso y de cuando esta es aceptable y cuando es inaceptable, así como cuando este tipo de uso está restringido. Si el acceso a un recurso de la red está restringido, debe considerar el nivel de acceso que tendrá cada clase de usuario. Esta política es llamada por algunos sitios “política de uso aceptable” o “política apropiada del uso (AUP, Aceptable Use Policy) de la red. Esta política debe aclarar que cada usuario es responsable de sus acciones. Tanta tecnología no tiene caso si algún usuario pone a disposición del intruso la información confidencial. Además si la AUP no establece claramente lo que está prohibido, será difícil demostrar que un usuario ha violado una política.

Al desarrollar la AUP se debe establecer claramente lo que no está permitido aunque parezca obvio, de esta forma se evitan las ambigüedades y los malentendidos. Esto es para evitar que los usuarios digan posteriormente que no se les informó o no tuvieron la capacitación necesaria.

Los lineamientos que no deben pasarse por alto son los siguientes:

- No se permite introducirse en las cuentas no autorizadas.
- No se permite descifrar las contraseñas.
- No se permite interrumpir servicios.
- Los usuarios deben suponer que, si un archivo tiene permiso general de lectura, eso no los autoriza a leerlo.

- No debe permitirse que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura.
- Los usuarios no deben compartir cuentas.

Estos lineamientos se tienen en la mayoría de las grandes organizaciones, se pueden cambiar estos lineamientos a menos que los requerimientos sean otros, aún estos deben de ser claramente especificados por niveles de usuarios.

Es recomendable incluir en la AUP una declaración sobre el uso de software registrado y patentado para que no se baje software no autorizado ya que en México así como en la mayoría de los países occidentales copiar software de manera ilegal está penado por la ley.

Si se incluye información con respecto al software con derechos de autor, algunos puntos que se necesitan abordar son:

- No se puede reproducir el software con derechos de autor y con licencia a menos que se exprese en forma explícita.
- Indicar métodos de transmitir información acerca de la situación del software con derechos de autor y con licencia.
- Conceder el beneficio de la duda a la precaución. Si se tiene dudas, no hay que copiar.

Las personas responsables de realizar sondeo de las debilidades de la seguridad están exentas de las políticas de seguridad, pues su trabajo está justificado y es encontrar inseguridades. Entonces la política debe tener margen para estas situaciones.

4.5. Análisis de riesgo

Al crear una política de seguridad hay que comprender la razón por la cual se está creando. Esto es, no hay que “dar palos de ciego”. Hay que conocer cuáles activos hay que proteger, cuáles son los que valen la pena proteger y cuáles son más importantes que otros. También se deben identificar las amenazas, protegiendo los recursos de la red. Así el análisis de riesgo implica el determinar lo que se necesita proteger, qué necesita para protegerlo y cómo protegerlo. Se debe tomar en cuenta que a pesar de los intrusos que irrumpen la red, la mayor pérdida se da por usuarios internos.

Los riesgos deben clasificarse por nivel de importancia del activo y gravedad de la pérdida de éste. No se debe terminar en una situación en la que se gaste más en proteger algo que es de menos valor para la empresa.

El análisis de riesgo se debe realizar periódicamente como esté indicado en las políticas de seguridad.

En el anexo A se encuentra una hoja de trabajo que es de gran ayuda para desarrollar un planteamiento de seguridad.[22]

[22] Del libro Firewalls y la Seguridad en Internet de Karnjit Siyan y Chris Hare.

Para realizar el análisis de riesgo se determina lo siguiente:

- Qué se necesita proteger.
- De qué o de quién se necesita protegerlo
- Cómo protegerlo.

Los dos factores que hay que determinar son:

1) Estimación del riesgo de perder el activo (Ri)

2) Estimación de la importancia del activo (Wi).

En estos dos factores se asigna un valor numérico dentro de una escala para poder cuantificar el riesgo de perder un activo. La escala puede ser dada de 0 a 10 (una escala pequeña facilita los cálculos), dentro de la escala el número menor es el mínimo riesgo de perder algo, es decir un cero es no tener riesgo de perderlo. El número más alto de la escala representa el tener el máximo riesgo.

$$Ri \in [\text{ningún riesgo, más alto riesgo}].$$

De la misma forma se cuantifica la importancia de un activo.

$$Wi \in [\text{sin importancia, la más importante}].$$

El riesgo evaluado en un activo se puede cuantificar entonces como el producto del riesgo de perder el recurso por un peso que es la importancia del recurso. Teniéndose:

$$Wri=Ri*Wi$$

En el anexo A se encuentran unas tablas que pueden ayudar a la administración en cuanto a la evaluación de riesgos de seguridad de la red.[23]

4.6. Sondeo de seguridad

La AUP (Appropriate Use Policy) debe responder las siguientes preguntas en cuanto a sondeo de seguridad:

- ¿Está permitido el vandalismo a nivel de usuarios dentro de la empresa?
- ¿Qué actividades de sondeos de seguridad se permiten dentro la empresa?
- ¿Qué medidas deben implantarse para asegurar que los sondeos no se salgan de control?
- ¿Qué medidas deben implantarse para proteger a los usuarios de la red para que no se expongan a graves riesgos por las actividades de sondeos de seguridad?

[23] Del libro Firewalls y la Seguridad en Internet de Karnjit Siyan y Chris Hare.

- ¿Quién debe tener permiso de realizar sondeos de seguridad?
- ¿Cuál es el procedimiento para la obtención del permiso para realizar las pruebas de seguridad ?

Para permitir sondeos de seguridad legítimos, se deben tener hosts y segmentos separados de red para esas pruebas. Es muy peligroso probar virus y otros tipos de software maligno (malware) dentro de redes en producción. Si se tienen que realizar las pruebas con software maligno, no se debe hacer en una red activa. Se debe separar físicamente a los hosts y a los segmentos de red que se utilicen para la prueba y después de cada prueba volver a cargar, por completo y con cuidado todo el software.

Evaluar las vulnerabilidades de la seguridad y tomar las medidas adecuadas puede ser eficaz para evadir ataques de hackers. Existen asesores externos a los que se puede acudir para que evalúen la seguridad de los servicios. Estas organizaciones actúan con herramientas de vandalismo para realizar la evaluación, la política debe incluir esta situación.

4.7. Componentes de la política de seguridad.

A continuación se describirán los principales componentes y documentos que se sugieren implementar para crear una política de seguridad acorde a las necesidades de la organización y de acuerdo al alcance de este proyecto.

En esta sección se brindarán los principales puntos a considerar en el desarrollo de cada uno de dichos procedimientos.

4.7.1. Definición de roles

A continuación se establecerán algunas pautas para definir las responsabilidades el rol “Administrador de red”. Como buena práctica de seguridad de red, se recomienda identificar todos los roles de la organización y definir cada uno de ellos acordemente.

Administradores de la red

El término "administrador" se utiliza para cubrir a toda esa gente que sea responsable de la operación cotidiana de los recursos del sistema y de la red. Esto puede ser un número de individuos o una organización. El término "administrador de la seguridad" se utiliza para cubrir a toda esa gente que sea responsable de la seguridad de la información y de la tecnología de información. En algunos sitios esta función se puede combinar con el término administrador; en otros, esto será una posición separada. En el congreso de Seguridad en Cómputo 2001 impartido por la UNAM se recomendó el realizar actividades específicas, puesto que en México se acostumbra tener todólogos y se llega a poner menos atención en algunas actividades, esto hace que crezcan las vulnerabilidades además de tener un menor rendimiento en cuestiones laborales. El término "fabricante de decisión" refiere a esa gente en un sitio que fije o apruebe la política. Éstas son a menudo (pero no siempre) la gente que posee los activos.

En la política de seguridad de red se debe especificar quién está autorizado para permitir acceso a los servicios de red.

Identificando a las personas encargadas de permitir acceso a la red, se puede dar seguimiento a qué tipo de acceso o control se ha otorgado, tanto a los administradores de la red como a los usuarios finales. Esto es útil para reconocer el origen de las fallas de seguridad como consecuencia de que se hayan concedido privilegios excesivos a ciertos usuarios.

Se debe dar la capacitación necesaria a los administradores, porque se les puede hacer fácil el asignar más atributos de los que se deben para que el usuario no esté molestando y así se olvida de la finalidad del asignar atributos que es la seguridad.

Una característica de las personas que tengan privilegios es que deben ser responsables y deben rendir cuentas ante alguna autoridad identificada en la política de seguridad. Si no se tiene esta característica, el sistema va a ser difícil de administrar puesto que se corre el riesgo de crear fallas y de estar asignando privilegios arbitrariamente. Para que los usuarios con privilegios no abusen de la confianza se pueden tener mecanismos de auditorías personalizadas en algunos sistemas.

El número de administradores de red y de sistemas debe estar determinado. Si son muchos los administradores se puede perder la cuenta de los permisos que se han concedido.

4.7.2. Identificación y definición de responsables (No pierda tiempo)

Cada segundo que pasa durante un incidente vale oro, ya que de ello depende la productividad de la organización. Esta sección se llamó originalmente “No pierda tiempo” debido a que cuando existe el incidente se debe actuar conforme a los lineamientos teniendo contactos con personas que pueden ayudar a resolver el incidente de forma organizada.

Se ha de realizar una lista con el nombre de las personas con las que se puede tratar en caso de que exista un incidente, como lo son las personas afectadas de otros sitios, el equipo de respuesta a emergencias de cómputo (CERT), en México existe el CERT UNAM. Esta lista debe tener la forma de comunicarse con ellos como puede ser su número telefónico. Debe identificar a más de dos responsables por área para casos en que no se encuentre la persona designada. Esta lista debe encabezar el documento de políticas de seguridad porque es la primera que se consulta. Así que no se deberá perder el tiempo realizando una lista de las personas que pueden ayudar precisamente cuando se presenta el incidente, con la lista previamente realizada podrían ya estar ayudando.

Es importante ponerse en contacto con autoridades legales para ayudar a realizar investigaciones de cómputo, en México como en muchos países aún no se tienen lineamientos legales específicos para cómputo en Internet, pero aún así se debe buscar asesoría legal para recibir apoyo.

4.7.3. Definición de procedimientos

La política de seguridad también incluye los procedimientos que definen cómo se deben realizar determinadas tareas. A continuación se enumeran los principales procedimientos.

Procedimiento de asignación de permisos.

Puede realizarse de una manera formal solicitudes de otorgamiento. Cuando el usuario hace la solicitud, el supervisor del usuario es quien da la autorización, el administrador del sistema debe documentar las restricciones de seguridad o de acceso a las que esté sujeto el usuario.

En el anexo A se incluye una hoja de trabajo para dar un seguimiento formal a la asignación de permisos.[24]

Procedimiento de ABM de usuarios (Altas, Bajas y Modificación de Usuarios)

Se debe analizar el método que se seguirá para asignar cuentas nuevas y permisos. Este procedimiento debe estar bien documentado.

El procedimiento de creación de cuentas de usuarios debe ser de lo más sencillo y fácil de entender, puesto que así se puede entrenar a nuevos administradores y esto asegura que se cometerán menos errores.

Procedimiento de administración de claves de acceso

Se debe tener una política para seleccionar la contraseña inicial. La contraseña no debe ser obvia porque es muy vulnerable a la cuenta del usuario. Se consideran obvios los nombres que se encuentren en diccionarios (pensando en diccionarios de todos los idiomas) así como la generación de nombres por algoritmos sencillos.

Cuando se da una contraseña inicial esta debe ser cambiada inmediatamente por el usuario. Suele haber usuarios que usan su cuenta mucho tiempo después de haber sido creada, esto hace que duren en el mismo tiempo sin acceder a la cuenta con una contraseña inicial, para ello debe haber una política en la que se desactive una cuenta después de no haber sido accedida durante un cierto periodo. El usuario se ve obligado a pedir que se le active nuevamente la cuenta. También si el sistema lo permite, se puede obligar al usuario que cambie su contraseña la primera vez que se registre.

[24] Del libro Firewalls y la Seguridad en Internet de Karnjit Siyan y Chris Hare.

4.7.4. Privacidad de usuarios

Respecto a la privacidad de los usuarios, la Asociación de Correo Electrónico (EMA, Electronic Mail Association) sugiere que todo sitio tenga una política acerca de la protección de la privacidad de los empleados.

El usuario tiene derecho a conservar su privacidad, pero en caso de amenaza de seguridad se le da prioridad al administrador de revisar los archivos y directorio base de los usuarios, esto tiene que ser especificado en la política junto con el grado en que se puede dar esta situación.

4.7.5. Identificación y clasificación de información delicada

Se debe determinar qué tipo de datos delicados pueden almacenarse en un sistema específico. La información muy delicada se debe tener en unos cuantos hosts. Se debe tener en cuenta qué información y servicios se tiene en un host para cuando un usuario solicite el acceso se le pueda conceder o denegar éste. Si un usuario no tiene la necesidad de manejar información delicada, no se le da una cuenta en un sistema que contenga esta información.

Así mismo se debe especificar a los usuarios qué sistemas pueden contener información delicada para cuando necesiten guardar información de este tipo. Este servicio es justificable porque no se desea que la información delicada se guarde en un sistema al que no se le provee la seguridad suficiente por causas de rentabilidad.

4.8. Publicación de la política de seguridad.

Antes de publicar la política de seguridad se comisiona un grupo de personas que deben interpretar; revisar y repasar el documento.

Después de haber redactado la política de seguridad y sólo después de que se haya alcanzado un consentimiento unánime en sus puntos, el sitio debe asegurarse de divulgarla y de que se discuta ampliamente. Para reforzar la política se debe capacitar con ella a todos los usuarios mediante talleres, pláticas, reuniones o atenciones personales con los administradores, a éstas deben asistir los miembros de alto nivel de la administración para tomar decisiones en cuanto a preguntas importantes. Se debe permitir que los usuarios hagan comentarios sobre la política para aclararla, mejorarla y evitar así ambigüedades. Para que ésta sea efectiva debe haber un equilibrio entre productividad y seguridad.

A los usuarios se les debe recordar periódicamente la política de seguridad para que no la olviden con el paso del tiempo. Se debe incluir en los paquetes de información la política a usuarios nuevos. Esta política de seguridad deberá adquirir al final la aceptación de los usuarios. Esta aceptación es que ha quedado claramente comprendida y aceptada por cada usuario. La política puede ser firmada para tener la “seguridad” de que el usuario aceptará la responsabilidad del uso de la red.

4.9. Lo que no incluye la política de seguridad

La política de seguridad define lo que necesita protegerse y por qué, pero no señala detalles como el cómo. Esto es porque es mucho más útil un documento que todos entiendan y no sólo los administradores de la red. La parte técnica debe ser referenciada en otros documentos.

Las políticas de seguridad son acciones preventivas, sin embargo no pueden abarcar todo el universo de problemas, pero sí la mayoría. De todas formas debe tomar en cuenta las acciones correctivas; para ello, la siguiente sección trata sobre la acción cuando se viola la política de seguridad.

4.10. Acciones contra las violaciones de la red y la política de seguridad

Si existe alguna violación al sistema de seguridad, entonces las políticas deben ser cambiadas, con el fin de eliminar los elementos que no sean seguros y mejorar el sistema.

Cuando se viola el sistema de seguridad, éste está sujeto a amenazas. Por lo tanto se deben tomar las medidas de acción para después de que se viole una red.

Las circunstancias pueden ser las siguientes:

- Negligencia por un individuo.
- Accidente.
- Por ignorancia de la política.
- Por pasar por alto la política.

En cada caso se sanciona de acuerdo al nivel de gravedad, así se necesita definir claramente la acción según el tipo de violación. Se debe investigar las circunstancias en torno a la violación de seguridad, y cómo y por qué ocurrió.

Debe llevarse un registro completo de las violaciones y monitorear periódicamente las tendencias de violación, para poder modificar las políticas de seguridad.

Las respuestas de estrategias que se pueden tomar ante un incidente de seguridad son dos:

- **Proteger y continuar**

  Esta estrategia trata de que al detectar al intruso, se apaguen los sistemas o se aíslen segmentos de la red y continuar restableciendo el sistema, con el fin de proteger la red y restablecer de inmediato. Una desventaja de esta estrategia es que el intruso se da cuenta de que ha sido detectado y puede continuar su intrusión de otra forma o por lo menos en otro sitio. Por lo regular se toma esta estrategia cuando el sistema es muy vulnerable, ya que no existen los elementos para entrar en cuestiones legales.

- **Perseguir y demandar**

  Esta estrategia al contrario de la anterior, se usa cuando existen los elementos suficientes para demandar de forma legal al intruso. Lo que se hace es dejar dentro al intruso registrando cada actividad que realice para poder demandarlo o sancionarlo según los lineamientos que se tomen por el tipo de usuario. Una desventaja es que el sistema puede seguirse dañando si no se toman las medidas pertinentes como podría ser el simular el ambiente del sistema para engañar al intruso y seguir vigilándolo para posteriormente demandarlo legalmente.

La lista que se muestra a continuación ayudará a determinar la estrategia a seguir. Por lo que si coincide a alguno de los siguientes enunciados, se deberá utilizar la estrategia de “proteger y continuar”:

1. La red no protege demasiado bien los datos que contiene.
2. Una penetración continuada puede terminar convirtiéndose en un riesgo.
3. No hay posibilidad de perseguir al intruso.
4. Se desconoce al usuario de la red, es decir, que no se puede identificar al intruso.
5. Los usuarios carecen de cierto nivel de sofisticación, por lo que su trabajo es vulnerable.
6. La red es vulnerable ante los juicios que pudiesen poner los usuarios.
7. El personal de soporte carece de los conocimientos necesarios sobre el sistema operativo, las utilidades y los sistemas, como para que merezca la pena involucrarse en una persecución.

La estrategia de “perseguir y demandar” se utilizará si ha contestado negativamente a la mayoría de los enunciados anteriores. Únicamente se seguirá esta estrategia si son afirmativas todas las oraciones que siguen.

1. La protección de los bienes de la red está asegurada.
2. Se tiene copia de seguridad de todo.
3. El riesgo de que alguien irrumpa en el sistema y dañe la red es mínimo.
4. Los ataques suelen ser concentrados y repetitivos.
5. El sitio tiene una atracción natural ante los hackers.
6. El administrador del sistema está deseando comprometer la información económica de la empresa al permitir que una penetración siga activa.

7. Se tiene una gran probabilidad de controlar el acceso de los intrusos.

8. Se tiene las suficientes herramientas de registro para la red que le merece la pena involucrarse en una persecución. Es decir, que la posibilidad de agarrar al intruso es bastante alta.

9. La administración está deseando tener pleitos en el momento que capturen al intruso.

10. El administrador del sistema conoce el tipo de evidencias que suelen utilizar en las persecuciones y guarda copia de toda la documentación y de los registros del sistema.

11. Se pone en contacto con las fuerzas de la ley y el orden.

12. Se tiene todo preparado por si hay que tomar medidas legales contra sus propios usuarios si sus datos o los del sistema le comprometen durante un persecución.

4.11. Implantación de políticas de seguridad de la red

Después de hacer las políticas y una revisión completa con los administradores de sistemas, hay que llevarlas a cabo. En esta parte se tiene que ver la disponibilidad que se tiene con las políticas, es decir que todos puedan hacer su trabajo con ellas. También se debe dar la capacitación necesaria a los usuarios para llevar a cabo las políticas de seguridad. Puede replantear algunas políticas para que se pueda llevar un buen trabajo y una buena seguridad. Así también, las políticas se deben ir actualizando periódicamente y conforme sea necesario. Por lo que existe una sección completa de las políticas que se implantan.

4.12. Recomendación

En el monitoreo es importante que se vea si existen tendencias de violación, para vigilar de cerca el problema previniéndola.

Si se quiere vigilar de cerca al intruso, se llama a un buen programador para que simule el ambiente del sistema.

Para la estrategia de perseguir y demandar, se debe tener cuidado en cuanto a la publicación de información cuando sucede un incidente, puesto que la prensa puede desprestigiar la empresa así como puede publicar información delicada y confidencial. Lo más importante es tener una buena asistencia legal, se debe consultar ampliamente esta sección con la empresa.

4.13. Conclusiones

Las herramientas más fuertes para realizar una buena implementación del firewall son las políticas.

En este capítulo se hace notar la importancia que tiene el que queden claras las políticas de seguridad. Con estas políticas quedan las responsabilidades de los usuarios finales y administradores sobre los recursos y la información de la red.

En ellas se declaran los servicios que podrán ser usados y la forma en que se permitirá o negará el uso de éstos.

Para crear las políticas se realiza un análisis de riesgo en el que se cuantifica la importancia de los sistemas de información y los riesgos que éstos corren. En las políticas se considera la autorización a los recursos e información tanto de los usuarios internos como de los externos.

Estas políticas también conocidas como “políticas de uso aceptable” deben ser redactadas explícitamente de la forma más clara posible, evitando que haya lugar a ambigüedades.

La AUP se ajusta al sondeo de seguridad y a otras necesidades de la empresa.

La AUP debe ser aceptada por todos los usuarios de la red con el fin de que no se salten las políticas.

En la AUP es donde queda redactada cada una de las actividades que se pueden o no realizar en los sistemas de información de la red. La política también contiene la información necesaria para ponerse en contacto con los responsables de los distintos departamentos de la compañía en caso de que suceda un incidente.

Capítulo 5
Estado de la seguridad al momento del levantamiento inicial de información de la organización

Antes de escribir e implantar las políticas de seguridad se realiza un estudio del nivel de seguridad con el cual cuenta el centro de control de la empresa eléctrica, con el fin de conocer las medidas preventivas y correctivas de seguridad que se llevan a cabo, con el propósito de fortalecerlas y en caso de que no hayan medidas básicas de seguridad introducirlas en las políticas. Con el fin de aplicar este cuestionario a la empresa eléctrica en el mantenimiento del sistema de seguridad se agrega el cuestionario (sin respuestas) de este capítulo en el anexo B. Esas preguntas pueden ser utilizadas para cualquier otra empresa.

5.1. Encuesta del nivel de seguridad para iniciar la implantación de políticas

1.- ¿Hay alguien responsable de la seguridad informática?

No. No hay nadie responsable en el centro de control de energía de la empresa eléctrica.

2.- ¿Se tiene alguna política de seguridad?

No, salvo las implementadas por los propios sistemas y bases de datos por vía passwords.

3.- ¿Los servicios y accesos a la red se restringen de alguna forma a los usuarios?

No. Todos los servicios están abiertos a todos los usuarios.

4.- ¿Existen antecedentes de intrusión a los sistemas?

Sí, en una base de datos del sistema de administración eléctrica. Fue un ataque interno que fue detectado semanas posteriores por los administradores de sistemas.

5.- ¿El centro de control de energía tiene muchos sitios?

Sí.

5.1.- En caso de ser afirmativo ¿cada uno cuenta con sus propias redes? De ser afirmativa la respuesta, ¿cada sitio maneja su seguridad o la seguridad es centralizada?

Sí cuentan con sus propias redes.

Con relación a Internet la única seguridad proporcionada a cada sitio es de la gerencia de telecomunicaciones la cual tiene un servidor con la aplicación de antivirus. Todo el tráfico de las áreas remotas primero pasa por la gerencia de telecomunicaciones para ser revisado por el antivirus el cual sólo permite cierta

cantidad de tráfico. Si se excede el tráfico a lo permitido por la gerencia de telecomunicaciones es probable que exista un virus en el sitio del cual se envía éste. Al detectar la gerencia de telecomunicaciones el crecimiento de tráfico no permite el paso del mismo. En conclusión, el problema lo tiene que solucionar el sitio al cual se le rechaza el tráfico de la red. Y por lo que cada sitio se hace responsable de su propia seguridad.

6.- ¿Qué recursos están protegidos?

En la Intranet ninguno como se comentó anteriormente.

7.- ¿Qué recursos se quieren proteger?

Se quieren proteger el sistema de administración de datos en tiempo real, el sistema de administración eléctrica, el sistema de gestión de flujo de trabajo, el sistema SM y el sistema SMAR, así como los equipos que conforman cada uno de los sistemas y la red que enlaza los mismos.

8.- ¿Ha protegido estos recursos anteriormente?

No. No han sido protegidos

9.- ¿Actualmente, de quienes se protegen los recursos?

De nadie.

10.- ¿Qué tan posibles son las amenazas?

La posibilidad de amenazas a los sistemas de la red de cómputo es alta puesto que se tienen antecedentes de intrusión a los sistemas y robo del contenido de las bases de datos. Específicamente se detectó la intrusión del sistema de administración eléctrica por el robo de la base de datos de este.

En una escala de 0 a 10 la posibilidad de amenaza al sistema de administración eléctrica es 10, puesto que sí ha tenido intrusión.

Ver hoja de trabajo en el anexo A para desarrollar un planteamiento de seguridad.

11.- ¿Qué tan importantes son los recursos de la red?

La importancia de los recursos en conjunto es alta puesto que con cada uno de ellos se trabaja para tener la operación de la red del sistema eléctrico. Sin embargo, los sistemas que tienen información crítica para la empresa eléctrica son el sistema de administración de datos en tiempo real y el sistema de administración de energía incluyendo el equipamiento de cada uno de ellos. En una escala de 0 a 10 el valor más alto en importancia la tiene el sistema de administración de datos en tiempo real y posteriormente el sistema de administración eléctrica, con los valores 10 y 9.5 respectivamente.

Ver hoja de trabajo para desarrollar un planteamiento de seguridad en el anexo A.

12.- ¿Qué medidas lleva a cabo para proteger sus bienes de forma económica y oportuna?

Se tiene el sistema de seguridad física por medio de tarjetas magnéticas para el acceso a los departamentos de informática.

13.- ¿Qué recursos informáticos se identificaron?

Este inventario existe en el departamento de mantenimiento.

14.- ¿Qué amenazas y vulnerabilidades se identificaron?

- No se tienen políticas de seguridad.
- Uso indebido de los recursos de los sistemas de información. Como el envío de cadenas y SPAM.
- Envío y recepción de información no revisada por un antivirus a través del correo electrónico.
- Intercambio de cuentas de acceso a los sistemas entre usuarios.
- Vulnerabilidad en los sistemas operativos.
- Accesos físicos no autorizados a los servidores de los sistemas de información del centro de control.
- Envío y recepción de troyanos.
- Accesos no autorizados a los sistemas de información del centro de control de la empresa eléctrica.
- Las bases de datos están abiertas.
- No se usan passwords. Y donde se usan los passwords no se lleva el control de estos.
- No existe la capacitación en materia de seguridad informática para los usuarios.
- Por ser dependencia gubernamental llama más la atención de los hackers.
- Ya existen antecedentes de intrusión.
- Existen cuentas que no son activas (cuentas olvidadas).
- No hay control del tráfico en las redes.
- Existen puertos abiertos sin saber si se ocupan.
- Los antivirus no son actualizados.
- No se revisan las páginas de los proveedores de los sistemas operativos para realizar mejoras en los mismos y conocer las vulnerabilidades de estos.
- No se consultan los sitios de noticias para la seguridad de los sistemas operativos.

15.- ¿Quién está autorizado para usar los recursos?

Cualquiera, porque no hay control sobre el uso de recursos.

16.- ¿Se tiene algún documento para saber cuál es el uso adecuado de los recursos?

No existe.

17.- ¿Quién está autorizado para conceder acceso y aprobar el uso de los servicios de la red?

El jefe del Departamento de Redes de Datos.

18.- ¿Quién puede tener privilegios de administración del sistema?

Sólo los administradores de cada sistema (Sistema de administración de datos en tiempo real, sistema de administración eléctrica, sistema de gestión de flujo de trabajo, SM y SMAR).

19.- ¿Cuáles son los derechos y responsabilidades de los usuarios?

No existe un documento sobre los derechos y responsabilidades de los usuarios. Los usuarios realizan su trabajo y no se les limitan los recursos de la red para otras actividades.

20.- ¿Cuáles son los derechos y las responsabilidades del administrador del sistema, en comparación con los de los usuarios?

Los derechos y las responsabilidades del administrador del sistema (en comparación con los de los usuarios) son: poder modificar sus sistemas o bases de datos, y tener siempre disponible la información de sus sistemas para consultas de usuarios del sistema eléctrico. Para ello requiere depurar, revisar y dar mantenimiento a sus bases de datos.

20.1.-¿El administrador de sistema es responsable de la seguridad? No realmente, él sólo se encarga de que exista la comunicación requerida.

21.- ¿Qué hacen los administradores y los usuarios con la información delicada?

Sólo se respalda la información del sistema de administración de datos en tiempo real.

22.- ¿Quién puede instalar módems para entrar a la red?

Los permitidos por la central de telecomunicaciones.

23.- ¿Hay algo especial acerca de las líneas PPP (point to point protocol), SLIP (serial line Internet protocol) o ISDN (Integrated Services Digital Network)?

No se manejan esas líneas.

24.- ¿Se permite introducirse a las cuentas de otros usuarios?

Sí, mientras el propietario de la cuenta o el administrador lo permitan.

25.- ¿Se permite descifrar las contraseñas?

No existe un documento que prohíba el descifrar contraseñas. Si el usuario tiene los conocimientos para descifrarlas, no se le puede sancionar si lo practica.

26.- ¿Se permite interrumpir servicios?

La interrupción de servicios es permitida cuando la base de datos requiera mantenimiento. Pero se realiza en días y horarios que no afecten la productividad del sistema eléctrico.

Por otro lado, si el administrador de un sistema se da cuenta que alguien quiere realizar un proceso no permitido, el administrador del sistema puede deshabilitar la conexión.

27.-¿Los usuarios suponen que, si un archivo tiene permiso general de lectura, eso los autoriza a leerlo?

Hasta el momento sí.

28.- ¿Se permite que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura?

Sólo cuando hay cuentas en común. Los usuarios tienen cuentas con permisos a sus propios archivos.

29.-¿Los usuarios comparten cuentas?

Sí. Debido a que el sitio no cuenta con un documento que indique que no se puede hacer, aunado a que no se cuenta con una conciencia de seguridad informática.

30.- ¿Qué hay de los proyectos en común, es necesario compartir cuentas?

No es necesario compartir cuentas, pero si los usuarios así lo quieren no hay nada que se los impida.

31.- ¿Se permiten cuentas para compartir con los miembros de la familia?

No se sabe si alguien comparte su cuenta con personas ajenas a la organización.

32.- ¿Se comparte una cuenta si permite que alguien tome prestada por un momento una ventana en su máquina?

Sí, mientras el usuario de esa sesión lo permita.

33.- ¿Cómo se maneja la legalidad de software?

Todo software se maneja bajo licencia. Por lo que no está permitido bajar o traer software sin licencia, pero aun cuando el usuario lo haga sin autorización y en caso de auditoría el único responsable será el usuario de la PC.

34.- ¿Quién es la autoridad a la cual le rinden cuentas las personas que tienen privilegios?

A su jefe de departamento.

35.- ¿Qué debe hacer la gente antes de conectar una computadora a la red principal?

Solicitar su conectividad al Departamento de Redes de Datos. Siempre y cuando hayan IPs disponibles.

36.- ¿Qué tan seguras son las computadoras para conectarse a una red sin protección con acceso a Internet?

No lo suficiente, pues sólo tienen instalado un antivirus.

37.- ¿Cómo se protege la información financiera?

Por el acceso físico restringido.

38.- ¿Cuándo pierde la gente el derecho de tener una cuenta y qué se hace al respecto?

El administrador de cada sistema toma la decisión.

39.- ¿Qué pasa si la gente se va o se le niega el acceso a las instalaciones de la organización?

Si se va, el administrador borra la cuenta. Si se le niega el acceso, el departamento responsable da un aviso, siendo éste el caso, también se borra.

40.- Si tiene sitios remotos ¿Cómo se restringe el acceso hacia su red principal?
No se restringe el acceso.

41.- ¿Existen conexiones a equipos remotos?
Sí.
41.1.-¿Cómo se aseguran estas conexiones?
No se aseguran estos equipos ni sus conexiones .

42.- ¿Se tiene acceso seguro a su red?
No. Sólo se cuenta con un firewall el cual sólo filtra algunas conexiones para los diferentes sitios de la misma compañía.

43.- ¿Cómo tiene acceso a la red la gente que viaja?
No hay accesos, a menos que sea de un área perteneciente a la empresa eléctrica.

44.- ¿Qué información de la compañía se considera confidencial?
La del sistema de administración eléctrica.
44.1.-¿Cómo es protegida?
Por el sistema operativo.
44.2.-¿Puede enviarse fuera del sitio por medio del correo electrónico?
Sí, pues no existe control del envío del correo electrónico.

45.- ¿Qué precauciones toma contra los virus de las computadoras personales?
Se cuenta con personal que instala los antivirus y los configuran para que corran periódicamente en las PC's.

46.- ¿Qué se hace para la seguridad física de las redes de computadoras?
Para los equipos que controlan la red así como los servidores de los sistemas se tienen accesos físicos restringidos en las áreas y sólo ingresa el personal autorizado.

47.- ¿Quién se puede conectar a su sitio con redes externas y qué es una red externa?
Se hace mediante un acuerdo con la empresa que se quiere accesar. De otra forma no se puede conectar. Una red externa es aquella que está fuera del dominio de la empresa eléctrica y que no se encuentra en el documento de control de asignación de redes (este documento lo proporciona la gerencia de telecomunicaciones). Es decir direcciones IP's que no fueron asignadas a la empresa eléctrica.

48.- ¿Es correcto que un administrador de proyecto conecte su sitio a otro sitio específico?
No es correcto.

49.- ¿Qué pasa si establecen una segunda conexión a Internet?
La única puerta de acceso a Internet es la gerencia de telecomunicaciones y no debe de haber una segunda conexión en virtud de las políticas de la empresa.

50.- ¿Cómo se protege la información confidencial (datos personales) de la gente de la empresa?

La persona que tiene acceso a esa información no le está permitido revelarla. Pero en esta Intranet (área de control de la empresa eléctrica) no se maneja esa información.

51.- ¿Qué métodos se usan para crear cuentas y finalizar accesos?

Los métodos que proporcionan los sistemas operativos.

52.- ¿Hay alguna política que descarte donde la contraseña inicial sea igual al nombre del usuario, o que se quede en blanco?

No, no existe tal política.

53.- ¿Cuál es el periodo que se da para acceder a una cuenta sin que se inhabilite?

No existe, a menos que se reporte que el usuario ya no está laborando en el área.

54.- ¿Qué se tiene para los lineamientos acerca del uso de los recursos de red?

Nada. Aún no se cuenta con ningún lineamiento.

55.- ¿Qué constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red?

Archivos de video y música. Pero no está estipulado en ningún documento.

56.- ¿Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas?

Sí, dado que no se tiene un control sobre las contraseñas.

57.- Política de contraseña de usuario: ¿Con qué frecuencia cambian de contraseña los usuarios y qué otras restricciones o requerimientos hay al respecto?

No existe tal frecuencia y no existe ninguna restricción o requerimiento alguno.

58.- ¿Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema?

Los usuarios son los responsables de hacer los respaldos de su información en las unidades de almacenamiento que se destinen para ello.

59.- Consecuencias para los usuarios que divulguen información que pueda estar patentada, ¿Qué acciones legales u otros castigos se llevan a cabo?

Esta información no se considera en ningún documento.

60.- ¿Existe una declaración sobre la privacidad del correo electrónico?

No, no existe tal declaración.

61.- ¿Existe una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión?

No, no existe.

62.- ¿Existe una política sobre comunicaciones electrónicas, tales como falsificación de correo?

No, no existe tal.

63.- ¿Qué hacen los usuarios para protegerse a sí mismos y al sitio?

La acción que llevan a cabo, es la de no compartir su PC en red.

64.- ¿Qué puede hacer la gente en Internet?

De todo, porque no existen restricciones al respecto.

65.-¿Pueden transferir archivos ejecutables al azar y ejecutarlos?

Sí porque no hay una cultura sobre la seguridad informática.

66.- ¿Puede el administrador revisar o leer los archivos de un usuario por alguna razón?

66.1.-De ser afirmativa la pregunta anterior, ¿en qué grado tiene esa prioridad?

Hasta el momento se deja a la ética del administrador.

67.- ¿Los administradores de la red tienen el derecho de examinar el tráfico de la red o del host?

Sí para optimizar el rendimiento de la red.

68.- ¿Cuáles son las responsabilidades legales de los usuarios, los administradores del sistema y de la organización por tener acceso no autorizado a los datos privados de otras personas?

No existen

69.- ¿Existe algún control de seguridad o políticas para los visitantes?

Sólo el acceso físico restringido a áreas determinadas.

70.- ¿Ya se tomó en cuenta el monitorear las tendencias de violación?

Sí. A partir del incidente.

71.- ¿Qué tipo de estrategia de respuesta aplica a cada tendencia de violación?

Se está iniciando el proceso de implantación de sistemas de seguridad.

72.- ¿Existe entre sus contactos organizaciones externas como el CERT de la UNAM y/u otras organizaciones?

No.

CERT.- Equipo de respuesta a Emergencias de Cómputo. El objetivo de este equipo es abordar preocupaciones acerca de seguridad de cómputo de los investigadores en Internet. Este equipo puede comunicarse inmediatamente con expertos para diagnosticar y resolver problemas de seguridad. También pueden ayudar a establecer y mantener la comunicación entre un sitio y las autoridades del gobierno. Cuando no está dedicado a atender emergencias, el CERT sirve de centro de intercambio para identificar y reparar puntos vulnerables en los principales sistemas operativos. También puede proporcionar evaluaciones informales de sistemas existentes y orientar para mejorar la capacidad de respuesta a emergencias. Puede ayudar indirectamente a formular una política eficaz de seguridad de redes. También se sabe que este equipo ha trabajado

con proveedores de sistemas de software para coordinar las soluciones a los problemas de seguridad.

73.- ¿Se pone en contacto con dependencias judiciales locales y federales, así como con las dependencias investigadoras (esta pregunta es para saber qué hacen en caso de un incidente)?

No, no se ponen en contacto en el caso de informática.

74.- ¿Qué tipo de información puede ser divulgada a la dependencia investigadora y a la prensa cuando existe algún incidente?

No existen esas políticas en informática.

75.- ¿Existe algún plan de contingencia en caso de algún incidente?

No. No existe tal plan

5.2 Conclusiones

Las políticas de seguridad son la herramienta más fuerte para realizar un sistema de seguridad. Éstas políticas son cubiertas en su mayoría por un firewall. Así la herramienta más fuerte para un firewall son las políticas. Para la realización de las políticas se llevó a cabo un estudio de la situación de la empresa en cuanto a la seguridad mediante una encuesta.

En la encuesta realizada se midió el nivel de seguridad que tenía la empresa en la que se deduce que la seguridad en ese entonces era nula. Es decir la información de los sistemas estaba al alcance de cualquier usuario. No es difícil de suponer y probar que siendo una empresa de interés, esta fuera el blanco de intrusión como se encontró en la encuesta.

En esta misma encuesta se obtiene la evaluación de los recursos de la empresa, y con ellos se determinó que recursos son los que se protegerían con el nivel de importancia y amenaza.

Aunque hay situaciones que aparentan tener un control, lo cierto es que no había nada documentado y por lo tanto no hay responsables definidos. Es decir, había quien llevar las medidas y había quien no las cumplía sin ningún problema administrativo.

En este capítulo se hace evidente la falta de medidas preventivas de seguridad informática así como la falta de los planes de contingencia con respecto a lo mismo.

Capítulo 6
Propuesta de las políticas de seguridad

Actualmente muchas de las compañías incrementan la vulnerabilidad en su red de cómputo, a cambio de percibir mejoras en la productividad mediante el uso de distintos servicios de red tales como:

Acceso remoto para correo electrónico, el cual puede generar riesgos si no se tiene un proceso de autentificación y acceso adecuado.

Un sitio de Word Wide Web (WWW) y servidor FTP mediante el cual los clientes, instantáneamente, puedan obtener información de productos y software desde cualquier parte del mundo a cualquier hora del día. Un problema común es que las compañías no se percatan de que pueden estar generándose túneles electrónicos hacia lugares internos de la red los cuales no deben ser públicos.

Servicios EDI (Electronic Data Interchange) para órdenes de ventas y sistema de pagos. Las compañías sin su consentimiento podrían estar permitiendo el acceso indebido a los inventarios o cuentas privadas.

Debido a los resultados de la investigación en cuanto a la importancia de los sistemas de información del centro de control de la empresa eléctrica y al nivel alto de inseguridad que se tiene actualmente se realiza la propuesta de las políticas de seguridad, con éstas se quiere evitar vulnerabilidades de la red y al mismo tiempo no alterar la productividad.

Las siguientes propuestas son un seguimiento para la implantación de las políticas de seguridad y así prevenir incidentes. Como primer paso se tiene que tener comunicación con las personas a las que hay que consultar en caso de que se presente un incidente. Para ello se encabeza un listado de las personas con las que se puede comunicar y auxiliar en caso de que ocurra un incidente.

6.1 Lista de contactos en caso de un incidente

Esta lista tiene los nombres de los responsables de las áreas con las que se tiene comunicación en caso de un incidente. Esta lista debe ser la portada de las políticas de seguridad.

Área	Nombre	No. De Ext.	Teléfono Directo
A	Miguel Cano Aguilar	5966	51-40-02-65
	José Luis Manzano	5732	
	Mario León Aponte	2959	
	Cómputo		51-40-01-06
	Telecomunicaciones		51-40-02-16
	Conmutador		56-29-71-00
B	Raúl Fernández	5240	
	Antonio Cordero	5249	
	Antonio Luna	5254	
	Javier Santos Lara	5250	
	Rosario Espinosa	5259	
	Comunicaciones	1214	
	Conmutador		01-22-40-32-00
C	Carlos Cárdenas	6467	
	Fernando Llamas	6471	
	Luis Aguirre Vázquez	6460	01-3-668-64-65
	Juan Velásquez	6472	
	Sala de Cómputo	6469	
	Comunicaciones	6472	
	Cómputo	6477	
	Conmutador		01-3-668-64-00
Generación			
G.S.I.A.E	Ing. Fernando Holguín R.	5698, 5699	5813
Subgerencia De Equipos Y Proceso Digital	Ing. José Martínez.	5964, 5537	5644
Subgerencia De Aplicaciones Informáticas	Ing. Pedro García	5733 y 5792	
SISTEMA DE ADMINISTRACIÓN ELÉCTRICA	Ing. Riki Román	5668 y 5866	
	Lic. Berta Rodríguez	5771	
	Eduardo Ortíz	5582	
	Roberto Ibarra	5668	
WEB	Ing. Rikica Román	5238	
	Ing. Fernando Barradas	5078	
	Ing. Felix Tovar	5072	

Área	Nombre	No. De Ext.	Teléfono Directo
SISTEMA DE GESTIÓN DE FLUJO DE TRABAJO	Ing. Rikica Román	5668	
	Ing. Fernando Paredes	5718	
	Ing. Ma. Eugenia Barrada	5579	
SMAR	Ing. Pedro Alatorre	5724	
	Susana Ayala	5118	
SM	Luis Manuel de la Torre		
SINAME	Shantal Covarrubias	5244	
SISTEMA DE ADMINISTRACIÓN DE DATOS EN TIEMPO REAL	Ing. Pablo A. García	5743	
	Ing. Antonio Chávez	5870	
	Francisco Martínez	5971	
	Antonio Abad	5935	
	Nancy Castañeda	5640	
PREDESPACHO	Ing. Mauricio Cuellar	5602	
	Edgar Benito		
	Jaime Díaz	5641	
ESTADISTICA	Ing. Alfredo García Mascorro	5539 ó 5662	
	Benjamín Carpio	5508	
	Miguel Bautista		
SARE	Ing. Gilberto Carreón	5779	
	Juan José Mendoza	5590	
Depto. de Redes de Datos	Ing. José Luis Pérez M.	5660	57-24-58-63
	Ing. Sergio Navarrete	5931	5943
	Ing. Rubén Solís	5530	5543
	Ernesto Valdés	5949	
Depto. de Redes de Voz	Ing. David Zacarias	5663 y 5845	
	Ing. Victor Lemoine G.	5964	
	Ing. Enrique Blancas	5987	
	Enrique Flores López	5694 y 5912	
CÓMPUTO	Lic. Jesús Cerda	5981	
	Ing. Jesús Ochoa	5909	
	Luis Herrera	5936	
SALA DE CÓMPUTO		5606 y 5686	
OPERADORES		5673, 5676	5772
Manto. de Equipo Auxiliar e Infraestructura	Ing. Miguel López	5920	

6.2 Implantación de una política de seguridad

Recomendación.- Estas preguntas se realizan para hacer un seguimiento en cuanto a la implantación de una política, puesto que éstas no abarcan toda clase de riesgos, pueden ir surgiendo más cuestiones al hacer la implantación y deben ser tomadas en cuenta para lograr una mejor política. Hay que recordar que se debe incluir específicamente todo en la política aunque parezca obvio. Las preguntas deben ser contestadas dando un por qué. En la política de seguridad es mejor incluir un por qué que es el que da sentido a la creación de las políticas de seguridad en lugar de sólo prohibir o permitir.

1.- Se propone un comité para la revisión de las políticas de seguridad. El comité puede estar formado por los administradores de los sistemas críticos, así como el gerente y los subgerentes.

2.- Puesto que no hay responsables de la seguridad informática, primero se nombra a las personas que serán los administradores de seguridad. Estas personas no deben ser muchas porque vuelven difícil la administración, además los usuarios no sabrían a quien dirigirse. Sin embargo, sí se recomienda que por lo menos sean dos personas para cuando una de ellas no esté por cualquier motivo oficial o personal.

La propuesta a este enunciado es el que se nombren dos personas para dar cumplimiento a lo anterior.

3.- La persona a la que se le asigne la responsabilidad de la seguridad informática debe sólo hacerse cargo de esta función. Dado que en México se acostumbra (por una mala administración o escasez de recursos) a que todos hacen de todo, el desgaste físico de las personas es mayor atendiendo lo urgente y no lo primordial. En este caso lo primero y lo más importante que deben atender los administradores de los sistemas de seguridad (sistema que aún no hay) son la seguridad de los sistemas informáticos y redes de computación del centro de control de la empresa eléctrica.

El responsable titular de la seguridad informática estará solamente dedicado al sistema de seguridad. Cabe señalar que la persona sustituta tendrá diversos trabajos pero en el caso de sustitución del titular solamente realizará esta tarea.

4.- ¿Qué tipo de enfoque se va a tomar en las políticas?

El administrador de seguridad toma el enfoque “lo que no está expresamente permitido, está prohibido. Este enfoque es documentar los servicios que están permitidos e implementarlo en los sistemas que los requieran, si no se encuentra en este se prohíbe el servicio. Para ello se deberán identificar cada uno de los servicios permitidos y avaladas por el comité de seguridad y documentar cada uno de ellos. Identificando los responsables de los mismos.

Se recomienda utilizar este enfoque porque se presta a menos confusión.

5.- ¿Cuáles son los tipos de servicios y recursos de la red interna cuyo acceso permitirá a los usuarios?

5.1. Identificación de servicios y recursos.

Se deberán identificar los servicios y recursos que podrán ser utilizados internamente en la red. Para cada uno de ellos se deberán identificar a los responsables de los mismos, y lo encargados de su mantenimiento.

5.2. Solicitud de acceso a servicios y recursos.

Se deberán definir procedimientos de cómo se llevará a cabo el proceso de "solicitud de acceso a sistemas de información".

Estos procedimientos serán usados internamente para solicitar a los correspondientes responsables el acceso a los sistemas de información, basados en una lista de autorización, proporcionada por los administradores de estos sistemas al administrador de seguridad. Estas listas deberán ser avaladas por los subgerentes de cada sistema, además del gerente de los Sistemas de Información y Administración de Energía.

6.- Dada la pregunta anterior, ¿debido a los riesgos cuáles tendrán que restringirse?

Se restringirá por IP del usuario con base a la lista arriba mencionada. Esta lista se llama "Registro de solicitud para accesos autorizados a usuarios a la Red del centro de control de la empresa eléctrica" (ver anexo A). Esta hoja es para llevar un control.

7.- ¿La organización tiene muchos sitios?

Sí. Estos sitios no están conectados a través de una red interna.

7.1.- En caso de ser afirmativo ¿cada uno cuenta con sus propias redes? De ser afirmativa la respuesta, ¿cada sitio maneja su seguridad o la seguridad es centralizada?

Sí cuentan con sus propias redes, todas las redes están interconectadas a través de equipos ruteadores.

Debido a la independencia de los sitios, se recomienda que cada sitio administre y defina su propia política de seguridad de acuerdo a los requerimientos específicos de cada uno.

Por lo cual, cada Intranet deberá ocuparse de su propia seguridad. Por lo que, el centro de control de la empresa eléctrica (y por ende este proyecto) sólo definirá la política de seguridad de su Intranet.

8.- ¿Qué recursos quiere proteger?

Para identificar y definir los activos que se desean proteger se recomienda utilizar la hoja de trabajo "Desarrollar un planteamiento de seguridad" que se adjunta en el anexo A.

Los activos definidos en el alcance de esta política de seguridad son: La información relacionada con el Sistema Eléctrico de esta área contenida en los sistemas críticos (sistema de administración de datos en tiempo real, el sistema de administración eléctrica, el sistema de gestión de flujo de trabajo, el SM y el SMAR), así como los elementos físicos que los conforman con el fin de que la información sólo pueda ser visualizada por personas autorizadas. Para definir qué recursos quiere proteger,

auxíliese de la hoja de trabajo para desarrollar un planteamiento de seguridad, en el anexo A.

9.- ¿De quienes necesita proteger los recursos?

Los activos identificados deben ser protegidos tanto de usuarios internos, como de usuarios externos que no estén vinculados directamente con la organización.

En particular, se recomienda proteger el activo de información digital que se tiene en los sistemas de información del centro de control de la empresa eléctrica referente al Sistema Eléctrico de una gran área.

Para realizar esta identificación en nuevos activos se recomienda utilizar la hoja de trabajo “Desarrollar un planteamiento de seguridad”, que se muestra en el anexo A.

10.- ¿Qué tan posibles son las amenazas?

Se identificaron y analizaron diversas amenazas eventuales a la organización. De todas ellas, cabe destacar que la posibilidad de amenazas como “acceso no autorizado” y ”falta de administración de seguridad” a los sistemas de la red de cómputo es alta. Dado que se tienen antecedentes de intrusión a los sistemas y robo del contenido de las bases de datos del sistema de administración eléctrica.

La escala que se usará es de 0 a 10, teniendo la amenaza más alta con el valor de 10, y 0 por si no existe la amenaza. La escala más alta, que es 10, es para sistema de administración eléctrica pues ya ha tenido intrusión porque se detectó el robo de la base de datos de este. Dada la importancia de la función y la información del sistema de administración de datos en tiempo real también se le asigna el mismo valor de sistema de administración eléctrica.

Las amenazas las evaluamos en una hoja de trabajo para desarrollar un planteamiento de seguridad. Para la hoja de trabajo, las amenazas se trabajan bajo la siguiente escala:

Escala	Tipo de amenaza
10	Falta de administración de seguridad (Intrusión como antecedente)
9	Posibilidad alta de intrusión
8	Posibilidad media de intrusión
7	Posibilidad baja de intrusión
6	Virus
5	El administrador (con todos los privilegios)
4	El administrador (con mayores privilegios)
3	El administrador
2	El usuario (con mayores privilegios)
1	El usuario
0	La amenaza es mínima

Nota: El sistema de administración de datos en tiempo real y el sistema de administración eléctrica se consideran que tienen posibilidad de amenaza con un valor de 10 por la importancia de la información que contienen.

11.- ¿Qué tan importante es el recurso?

La importancia de los recursos en conjunto es alta puesto que con cada uno de ellos se trabaja para tener la operación y la administración de corto, mediano y largo plazo de la red del Sistema Eléctrico a cargo. Sin embargo, los sistemas que tienen información crítica para la empresa eléctrica son el sistema de administración de datos en tiempo real y el sistema de administración eléctrica incluyendo el equipamiento de cada uno de ellos. En una escala de 0 a10 el valor más alto en importancia la tiene el sistema de administración de datos en tiempo real y posteriormente sistema de administración eléctrica, con los valores 10 y 9.5 respectivamente.

Ver hoja de trabajo para el análisis de riesgo de seguridad de la red, anexo A.

12.- ¿Qué medidas puede implementar para proteger sus bienes de forma económica y oportuna?

Tener un control de passwords.
No compartir las cuentas.
No prestar sesiones.
Dar capacitación de medidas básicas de seguridad.
No abrir archivos que sean desconocidos por los usuarios.

13.- Revisión y cumplimiento de la política de seguridad: El comité debe examinar periódicamente su política de seguridad de red para ver si han cambiado los objetivos y las circunstancias de la red. Para lo cual se debe establecer y documentar el periodo de verificación de la misma.

El periodo que se propone para la revisión de la política es cada 15 días durante el periodo de pruebas de las políticas y posteriormente se considerará un periodo de 6 meses. Se hace notar, que cualquier cambio en la red o en los servicios/activos identificados y documentados en la Política de Seguridad se deberán incorporar debidamente en forma inmediata en dicha política.

14.- ¿Qué activos físicos (levantamiento hardware) se identificaron? El inventario de los activos físicos que posee la organización se encuentra detallado en el documento DEPRYD325. Este inventario se encuentra en el documento DEPRYD325 del archivo de redes y datos.

15.- ¿Qué amenazas se identificaron? ¿Cómo pueden resolverse?
A continuación se describen las principales amenazas detectadas en la organización, y las cuales deben ser tratadas.

- Accesos físicos no autorizados a los sistemas de información del centro de control de la empresa eléctrica.

  Para poder disminuir o eliminar la posibilidad de ocurrencia de esta amenaza se propone llevar a cabo los siguientes puntos:
  En la seguridad física se debe restringir el acceso a los sistemas de información con el uso de tarjetas magnéticas en forma más estricta.

  Las personas autorizadas en las áreas informáticas deben portar su gafete.

Los visitantes deben ser acompañados por personal autorizado en la zona de equipos y sistemas. Además deberán completar sus datos en un libro de registros de acceso, con su nombre, empresa a la que pertenecen, motivo de entrada, persona de la organización que lo acompaña o autoriza su ingreso, hora de entrada, hora de salida y su firma.

- Acceso no autorizado a la información digital de los sistemas de información del centro de control de la empresa eléctrica.

  Para poder disminuir o eliminar la posibilidad de ocurrencia de esta amenaza se propone llevar a cabo los siguientes puntos:

  Los equipos de cómputo deben tener passwords controlados.

  Las sesiones no se deben prestar entre usuarios.

  Se recomienda encriptar a información confidencial.

- Uso indebido de los recursos de los sistemas de información.

  Se debe dar capacitación a los usuarios sobre el buen uso de los recursos de los sistemas de información. Así también se les debe capacitar en temas de seguridad informática.

  Se recomienda armar grupos de capacitación pequeños, de acuerdo a su nivel de responsabilidad dentro de la organización y manteniendo un nivel de conocimiento en seguridad homogéneo. Dichos cursos pueden ser impartidos por el mismo personal encargado de la seguridad informática dentro de la misma organización.

  De esta forma la información y los sistemas deben usarse sólo para propósitos que apoyen la misión del centro de control de la empresa eléctrica.

  De acuerdo al área o departamento al cual pertenezca el usuario se pueden prohibir/restringir para ciertas áreas el uso de determinados servicios fuera del horario laboral (uso de correo, navegación, etc.).

  Se pueden apagar equipos de forma remota, esto es para asegurar que en los horarios fuera de servicio no haya personas que hagan uso de los recursos de la red.

- Envío y recepción de información sin ser revisada por un programa antivirus a través del correo electrónico.

  Se debe tener un antivirus actualizado en red que revise el correo electrónico.

Mientras se instala el servidor del antivirus, los usuarios deben ser responsables de revisar su e-mail con el antivirus de su equipo. Este antivirus se debe estar actualizando por el departamento correspondiente al menos cada semana hasta que se implante el antivirus global en el sistema.

Los usuarios no deben abrir archivos adjuntos que no sepan de qué se trata.

No se debe ejecutar un archivo adjunto de un correo con doble click, aunque lo haya enviado el mejor de los amigos. Siempre es mejor guardar el adjunto, y ejecutar primero el programa que debería abrir ese adjunto y desde ese programa abrir el archivo.

- Envío y recepción de Troyanos.

  Los usuarios no deben abrir correos que no sepan de quienes son. Así tampoco archivos que no conozcan.

  Se deberá reportar los eventos no usuales que el usuario observe, ante las personas responsables de los sistemas o de la seguridad de la red.

  Informe cualquier cambio extraño encontrado en la información que usted tenga a cargo.

  Reportar cualquier archivo que resulte en su disco duro que usted no haya copiado o creado.

  Comunique inmediatamente a su jefe y a la oficina de sistemas cualquier pérdida de datos o programas (deje constancia escrita del caso).

- Intercambio de cuentas de acceso a los sistemas entre usuarios.

  Cada usuario deberá tener su propia cuenta, confidencial e intransferible, no debe existir el préstamo de la misma.

- Vulnerabilidad en los sistemas operativos.

  Se debe estar al tanto de las páginas de los sistemas operativos para las actualizaciones y parches así como de las páginas de noticias de seguridad.

  Al configurar los sistemas operativos se debe tener cuidado en las configuraciones que se tienen por default. La filosofía de los fabricantes es poner desde la instalación todas las características de sus productos, provocando muchos de los problemas de las vulnerabilidades de seguridad, debido a que los usuarios no dan mantenimiento a las aplicaciones y componentes del software necesarios que no usen.

- Administración de contraseñas

  Como primer paso será desarrollar el "Procedimiento de administración de claves" detallando las características y administración de las mismas.

  Luego se deberán detectar las cuentas que no tengan contraseña y a éstas asignarles una o eliminarlas del sistema por completo. De igual forma buscar contraseñas débiles y asignarles una fuerte, de acuerdo al "Procedimiento de de administración de claves" definido.

  El tercer paso será el validar a los usuarios cuando cambien su contraseña, evitando que usen siempre dos o mas como contraseñas reusables a través del uso de programas que permita validar passwords fuertes y no reusables en cierto periodo de tiempo (estos periodos de timpo deberán ser explicitados en el procedimiento).

  Los passwords deben ser usados y cambiados periódicamente.

  Otra manera de proteger los sistemas de usuarios sin contraseña o contraseñas débiles es el uso de formas alternativas de autenticación por token o seguridad biométrica.

- Accesos físicos no autorizados a los servidores de los sistemas de información del centro de control de la empresa eléctrica .

  Las áreas en que se encuentren los servidores de los sistemas de información del centro de control de la empresa eléctrica deben contar con accesos físicos restringidos.

- Administración de las cuentas de usuarios
  Se deberá definir el procedimiento de ABM (Alta, Baja y Modificación) de cuentas de usuarios, identificando el responsable de dicha tarea.

  De esta forma, cuando un usuario cambia de área, se podrá llevar a cabo el control de los permisos necesarios para desempeñar su nueva función. Así mismo, cuando un usuario es dado de baja, se deberá eliminar su cuenta de usuario al igual que el acceso a cualquier recurso interno de la organización.

- Desconocimiento de las políticas de seguridad.
  Se propone que una vez aprobadas las políticas de este documento por el comité se implanten capacitando a todo el personal sobre las políticas. Finalizando con un acuerdo firmado por cada usuario que tenga acceso a cualquier sistema de cómputo del centro de control de la empresa eléctrica.

♦ Otras medidas que se proponen para reducir el riesgo de pérdida, daño y fisgoneo de información.

Cada usuario debe :

- Proteger el equipo contra humedad, vandalismo y fuego.
- Asegurarse que nadie coma, beba o fume junto al computador.
- Infórmese dónde está el extinguidor más cercano, aprenda a utilizarlo y verifique que es adecuado para atender incendios en equipo electrónico.
- Mantenga a las personas no autorizadas y desconocidas lejos de su equipo.
- No compartir para la red directorios o archivos de manera innecesaria, especialmente aquellos que contienen información confidencial.
- No decir sus claves (passwords) a terceros y cámbielas a menudo.
- Nunca dejar su equipo desatendido con su clave activada.
- No utilizar software "pirata" (software sin licencia de uso).
- De forma regular y programada, hacer copias de la información importante a su cargo y guardarla bajo llave fuera de su área de trabajo. Coloque etiquetas que identifiquen correctamente el contenido de los medios de almacenamiento (CDs, diskettes, cintas, etc.) registrando su nombre, o el de la persona que hizo las copias, y la fecha en que se realizó la copia.
- Si debido a sus funciones o labores, el sistema a su cargo debe intercambiar software o archivos con otros -ya sea por la red, CDs, diskettes, etc.- utilice un antivirus actualizado (y debidamente licenciado).

16.- ¿Cuál será el uso adecuado de los recursos?

Utilizar la red así como los accesos autorizados a los diferentes servidores exclusivamente para su área de trabajo. Esto quiere decir que no estará permitido mandar mensajes de cadenas a través de correo electrónico, intercambiar videos MPEG, realizar impresión de documentos ajenos a sus labores, entrar al chat, visitar páginas XXX. Estas prohibiciones son para optimizar el desempeño de la red y prevenir el contagio de virus y otros softwares maliciosos.

17.- ¿Quién estará autorizado para usar los recursos?

Estas personas deben ser los administradores y los grupos de usuarios definidos en un documento (“Registro de solicitud para accesos autorizados a usuarios a la Red del centro de control de la empresa eléctrica”), con la previa autorización del subgerente y gerente, lo cual les permitirá acceder a través del firewall, y que además deberá estar validada la cuenta de usuario en el servidor por el administrador del sistema que se quiere acceder.

18.- ¿Se dan de alta cuentas de usuarios para visitantes externos a la organización? ¿cómo se controlan?

Sólo se dan de alta cuentas de usuarios para usuarios visitantes en los sistemas que no son críticos.

En primera medida se recomienda identificar, describir y documentar las aplicaciones que se consideran “no críticas” y sobre las cuáles ser posible dar de alta cuentas de usuarios para personal externo.

Luego se deberá documentar el procedimiento que se deberá llevar a cabo para realizar un ABM (Alta, baja o modificación) de una cuenta de usuario externo a la organización. Para ello se deberán considerar:

Motivo del requerimiento
Persona interna de la organización que autoriza dicho requerimiento (gerente o subgerente de área).
Tiempo por el cual permanecerá activa dicha cuenta.
Datos del personal externo: como nombre, empresa a la que pertenece, etc.

19.- ¿Quién estará autorizado para conceder acceso y aprobar el uso de los servicios de la red?

Debe ser el administrador de seguridad de la red basado en el documento de autorización que firma el subgerente es quien estará autorizado para conceder accesos y aprobar el uso de los servicios de la red.

El administrador de seguridad de la red consultará con los administradores de servidores que proveen los sistemas de información (sistema de administración eléctrica, sm, mercado, sistema de gestión de flujo de trabajo, sistema de administración de datos en tiempo real).

20.- ¿Quién podrá tener privilegios de administración del sistema?

Sólo los administradores de sistemas de información (sistema de administración eléctrica, sm, mercado, sistema de gestión de flujo de trabajo, sistema de administración de datos en tiempo real, seguridad) pueden tener privilegios de administración del sistema.

21.- ¿Cuáles serán los derechos y responsabilidades de los usuarios?

Los derechos de los usuarios los fijará el administrador de cada sistema con base al login y password. Puede ser desde lectura y permitirles hasta la escritura.

Las responsabilidades de los usuarios es el hacer el uso correcto de la información que se lee o la que se le permite accesar.

Cuando exista otro usuario con los mismos permisos que el administrador del sistema, que por administración de la aplicación sean requeridos, no estará facultado para modificar información del sistema (Sistema operativo, aplicaciones, base de datos, permisos de acceso a archivos, guardar información de uso personal, etc.), sin previa autorización por parte del administrador general. En caso que requiera realizar cambios o modificaciones lo solicitará por escrito y avalado por el subgerente y gerente de la Gerencia de Sistemas de información del centro de control de la empresa eléctrica al administrador general.

22.- ¿Cuáles serán los derechos y las responsabilidades del administrador del sistema de seguridad, en comparación con los de los usuarios y otros administradores?

Los derechos y las responsabilidades del administrador del sistema (en comparación con los de los usuarios) será poder modificar sus sistemas o bases de

datos, y tener siempre disponible la información de sus sistemas para consultas de usuarios del Sistema Eléctrico.

23.- ¿Qué se hará con la información crítica?

La organización deberá enumerar y documentar la información que considera crítica. Realizando la correspondiente clasificación de la misma.

Una vez identificada, se recomienda almacenar dicha información en sistemas de alta seguridad. Dichos sistemas deben contemplar características de tolerancia a fallas.

Se deberá además definir una política de respaldo acorde a la criticidad de la información. Se recomienda realizar un respaldo diario, uno semanal y uno mensual. Guardando históricos de dichos respaldos, en lugares físicos apartados al lugar donde se encuentra ubicado el sistema.

La información confidencial deberá ser encriptada.

La información delicada se controlará con un solo host y sólo se permitirán accesos de lectura. Se respaldará la información en cintas cada que se modifique la base de datos. En caso del relatorio no se respalda constantemente, sin embargo la aplicación estará en el cluster por lo que existirá una base de datos idéntica disponible para el caso en que falle la que está trabajando.

24.- ¿Quién podrá instalar módems para entrar a la red? ¿Es correcto que otras personas instalen módems par hacer llamadas externas?

En cuanto a la instalación de módems no existe la autorización para implantarlo dentro del centro de control de la empresa eléctrica. Sólo se accesa vía telefónica o módem por la gerencia de telecomunicaciones previo a requisitos de autentificación que proporciona la misma gerencia para accesar a la Intranet de la empresa eléctrica además que sea autorizado por el administrador del sistema de seguridad previo a documentos de solicitud de servicio entregado y firmado por el subgerente del sistema de información. Esto sólo se permite para administradores, subdirector, coordinador, gerentes y subgerentes de la STTyC (Subdirección de Transmisión, transformación y Control).

Por lo tanto sólo la gerencia de telecomunicaciones puede instalar módems.

Se recominda tratar de eliminar este tipo de acceso, salvo que existan razones realmente justificadas para ello. Dado que a través de este medio de acceso, las PCs se encuentran totalmente vulnerables a las amenazas existentes, al no existir un firewall, servidor de antivirus, IPS/IDS, etc. que la proteja.

De esta forma esa PC se encuentra expuesta a amenazas externas, como por ejemplo al robo de informacion que dicha PC contenga, a que sea infectada por un virus que luego, al ser conectada nuevamente a la red interna, infecte el resto de la red, etc.

25.- ¿Habrá algo especial acerca de las líneas PPP, SLIP o ISDN?

Las líneas PPP serán proporcionadas por la gerencia de telecomunicaciones.

26.- ¿Se permitirá introducirse a las cuentas?

Las cuentas multiusuario serán para uso de los invitados, con las cuales pueden consultar información o depositar información. Fuera de ello no está permitido ningún tipo de acceso con cuentas que permitan modificar las bases de datos a excepción de los administradores del equipo.

27.- ¿Se permitirá descifrar las contraseñas?

Estará prohibido el descifrar contraseñas.

28.- ¿Se permitirá interrumpir servicios?

La interrupción de servicios será permitida cuando la base de datos requiera mantenimiento. Pero se realizará en días que no afecten la productividad del Sistema Eléctrico a cargo.

29.-¿Los usuarios deberán suponer que, si un archivo tiene permiso general de lectura, eso los autorizará a leerlo?

Los usuarios sólo leerán los archivos que estén relacionados con su área de trabajo. El administrador de sistemas será el encargado de proporcionar el acceso a dicho directorio.

30.- ¿Debe permitirse que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura?

Cada usuario será propietario de su información. No se permite que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura.

31.-¿Los usuarios podrán compartir cuentas?

Cada usuario debe tener su propia cuenta y no debe compartirla. Si requiere acceder a la información deberá solicitar una cuenta con el administrador del sistema que se quiera accesar.

32.- ¿Qué pasa si una secretaria usa la cuenta de un ejecutivo para procesar el correo electrónico de esa persona?

Las cuentas de correo electrónico y passwords estarán ligadas al software de correo electrónico por lo que no será posible utilizar la cuenta de correo de un ejecutivo, al menos que el administrador configure la PC de la secretaria para que lo utilice, de este acto quedará el administrador como responsable.

33.- ¿Qué hay de los proyectos en común?

Para cada usuario se define una cuenta que les permita acceder a la información del proyecto aun cuando sea un proyecto en común.

34.- ¿Qué hay de los miembros de la familia?

Cada usuario será responsable de la información que guarda u almacena en el sistema. Además el permitirle el acceso a miembros de su familiar no está permitido por políticas de la empresa.

35.- ¿Se comparte una cuenta si permite que alguien tome prestada por un momento una ventana en su máquina?

No está permitido compartir una cuenta ni que alguien tome prestado por un momento una ventana en su máquina.

36.- ¿Cómo se manejará la legalidad de software?

Todo software se maneja bajo licencia. Por lo que no está permitido bajar o traer software sin licencia, pero aun cuando el usuario lo haga sin autorización y en caso de auditoría el único responsable será el usuario de la PC.

36.1.- En caso de ser afirmativo, revisar las cláusulas de la licencia de los productos.

36.2.- O se tienen acuerdo de licencia, sin embargo este software debe ser vigilado.

37.- ¿Va a evaluar algún asesor externo con respecto a la seguridad de los servicios de la red?

De acuerdo a esta propuesta, sí se va a evaluar con asesores externos los que deberán entregar un diagnóstico escrito de las debilidades y fortalezas de la administración de la red y sus servicios.

Independientemente de la evaluación externa. Como administrador de seguridad debe tener herramientas para realizar las auditorías en la red. Pero sólo el administrador puede usar estas herramientas.

38.- ¿Se otorgará el acceso a los servicios desde un punto central?

Todo el acceso a los servicios se da por centralización con previa autorización de los administradores de los sistemas.

39.- ¿Quién es la autoridad a la cual le rindan cuentas las personas que tengan privilegios?

Los administradores revisarán periódicamente las cuentas de usuario tanto en servidores como en los Firewall, para constatar que se esté haciendo buen uso de las mismas; esto permitirá que el administrador reporte al jefe de departamento y subgerente del estado que guardan los sistemas de información y de seguridad. El gerente de los sistemas de información es la autoridad que decidirá si se le niega el acceso a un usuario por hacer mal uso de sus privilegios.

40.- ¿Qué deberá hacer la gente antes de conectar una computadora a la red principal?

Solicitar la asignación de IP así como el servicio de la activación al departamento de redes de datos. Posteriormente se le instalará un antivirus, así como las aplicaciones necesarias para desempeñar su trabajo.

41.- ¿Qué tan seguras deberán ser las computadoras para conectarse a una red sin protección con acceso a Internet?

Todas las computadoras del centro de control de la empresa eléctrica deberán contar con un antivirus actualizado, así como con un firewall que checará las salidas y entradas a y desde Internet por lo que no existe una PC conectada a una Red sin protección.

42.- ¿Cómo se protegerá la información financiera?

Configurando una regla de seguridad en los firewalls que protegen a este servidor y es donde se especifica qué personas pueden acceder al mismo.

43.- ¿Cuándo perderá la gente el derecho de tener una cuenta y qué hacer al respecto?

Cuando por razones de trabajo se reubique en otra área, se notificará a los administradores de los sistemas. Otro caso es cuando deja de laborar en la empresa.

44.- ¿Qué pasa si la gente se va o se le niega el acceso?

Si la gente se va, perderá todos los derechos para acceder a las aplicaciones de los sistemas de información. Si se le niega el acceso es por hacer uso indebido de los privilegios que se le otorgaron y será acreedor a una sanción administrativa.

45.- Si tiene sitios remotos, ¿Cómo va a asegurarse el acceso hacia su red principal?

Con base a las políticas de seguridad implementadas en los Firewalls de cada sistema de seguridad del centro de control de la empresa eléctrica, en ellas se contempla el uso de métodos de autentificado, con los que cuenta el sistema de seguridad. (Client Authentication, User Authentication, Session Authentication), así también como el autentificado dinámico (Tokens).

46.- ¿Cómo van a asegurarse las computadoras caseras? ¿Cómo van a tener acceso seguro a su red?

Con el método del Client Authenticatication que requiere de un token. No todo usuario debe tener acceso desde su computadora casera o lap-top. Para esto se debe designar nombres de usuarios que sí tendrán acceso a la empresa desde sitios remotos.

47.- ¿Cómo va a tener acceso a la red la gente que viaja?

Conectándose con un IP que proporciona el área de control. Una vez proporcionado el IP accederá al servidor de correo electrónico o conectándose al MODEM que proporciona la gerencia de telecomunicaciones para acceso a la red de la empresa eléctrica.

48.- ¿Qué información de la compañía se considera confidencial? ¿Cómo será protegida? ¿Podrá enviarse fuera del sitio por medio del correo electrónico?

Se considera confidencial toda la información relacionada al Sistema Eléctrico a cargo. Esta se protegerá a través de firewalls. Además está prohibido mandar cualquier tipo de información que esté relacionado con los sistemas de información del centro de control de la empresa eléctrica y de la empresa eléctrica por correo electrónico, a menos que existan VPN's seguras con los sitios remotos y previa autorización de los subgerentes y gerentes de la gerencia de sistemas de información del centro de control de la empresa eléctrica.

49.- ¿Qué precauciones deberá tomar contra los virus de las computadoras personales?

Nunca abrir correos electrónicos cuyo remitente se desconozca.
Revisar siempre por un antivirus los discos que contienen archivos que se adjuntarán por correo electrónico.

Revisar por un antivirus las unidades de almacenamiento extraibles (Cd's, diskettes, cintas), antes de introducirlos a un equipo.

Tener siempre actualizado el antivirus. Se recomienda que eventualmente (6 meses) se esté cambiando el software por una versión más reciente. Esta medida de seguridad se llevará a cabo mediante el apoyo de un proveedor el cual informa sobre la liberación de una nueva versión.

Dar un mantenimiento automático de actualización de antivirus y revisión de software a las horas no laborales o al inicio o fin de las labores.

Archivo que se detecte con virus se debe mantener en cuarentena en caso de que sea necesario de no ser así eliminarlo.

50.- Para la seguridad física: Se recomienda que eventualmente (2 meses), el personal de equipos y mantenimiento realice una evaluación física de las computadoras personales para evaluar el estado en que se encuentren los equipos y también brindarles mantenimiento preventivo y en su caso el correctivo. Del mismo modo se recomienda usar equipo de seguridad física para saber qué máquinas se abren y porqué.

El sistema de aire acondicionado debe estar a una temperatura adecuada para el buen funcionamiento de los recursos.

Se requiere la evaluación del sistema eléctrico.
Se requiere la instalación de extinguidores
Se requiere de un sistema automatizado para el acceso al sitio.
Se requiere de UPS (uninterruptible power supply).

51.- ¿Quién podrá conectar su sitio con redes externas y qué es una red externa?

Nadie deberá conectarse a redes externas. Una red externa es aquella que está fuera del dominio de Comisión Federal de Electricidad y que no se encuentra en el documento de control de asignación de redes (este documento lo proporciona la gerencia de telecomunicaciones). Es decir direcciones IP's que no fueron asignadas a la empresa eléctrica.

52.- ¿Será correcto que un administrador de proyecto conecte su sitio a otro sitio específico?

Con base a los requerimientos de un proveedor y en común acuerdo con el centro de control de la empresa eléctrica para poder acceder remotamente a la base de datos del proveedor para su actualización y depuración del sistema hasta la entrega del proyecto.

53.- ¿Qué pasaría si establece una segunda conexión sin permiso a Internet?

Se aplicarían sanciones a los responsables de tal evento. Como podrían ser desde una llamada de atención, pérdida del empleo, hasta una sanción administrativa o penal.

54.- ¿Qué métodos se usarán para crear cuentas y finalizar accesos?

Los métodos que se usarán para crear cuentas y finalizar accesos es crear cuentas locales en el servidor del sistema. Otro es crear cuentas y dar de alta a los usuarios y equipos que accesarán a estos sistemas en el sistema de seguridad.

En el sistema de seguridad se deberán considerar los métodos de autentificado.

En los sistemas de información los administradores de las aplicaciones (bases de datos, hojas de marcha, sistema de administración de datos en tiempo real, sistema de gestión de flujo de trabajo, etc.) serán los que lleven el control del número de sesiones permitidas así como la duración de las mismas.

Para reducir errores cometidos por el administrador del sistema por los que se pueden producir puntos vulnerables en la seguridad se deben tener procedimientos bien documentados de la creación de cuentas.

55.- En la política se descartará que la contraseña inicial sea igual al nombre del usuario, o que se quede en blanco. Así como seguir un control de asignación de contraseñas.

Por control en los sistemas de información el usuario asigna su contraseña la cual debe ser de un mínimo de ocho caracteres alfanuméricos incluyendo caracteres especiales y sin escribir palabras que se encuentren en diccionarios (incluyendo otros idiomas), fechas de nacimiento, datos personales, la cual será reportada al administrador de passwords de cada usuario. El administrador de sistemas no dará necesariamente la contraseña, sin embargo sí las aprobará según los criterios para passwords. Como referencia existe una función automática en windows para este punto, es decir indica cómo generar passwords fuertes.

Se recomienda al usuario no anotar el password, si se llega anotar el password se debe tener en un lugar seguro, alejado del equipo que lo requiere como acceso.

No almacenar contraseñas encriptadas en un archivo clásico de contraseñas.

56.- ¿Se considerará un periodo para acceder a una cuenta sin que se inhabilite?
Sí, a los 15 días de inactividad en una cuenta se deberá reportar al administrador del sistema para tomar las medidas pertinentes.

57.- ¿Cuáles son los lineamientos acerca del uso de los recursos de red?
Se hará una lista de usuarios que están restringidos y cuáles son las restricciones. [Ver la hoja anexa de permisos]

58.- ¿Qué constituirá un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red?
El envío de correo electrónico en relación al uso con información no laboral.
El envío constante de ping.
Mantener conexiones abiertas a Internet.
Entrar a salas de chat.

59.- ¿Podrán los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas?
No. La contraseña será personal e intransferible.

60.- Política de contraseña de usuario: ¿Con qué frecuencia deberán cambiar de contraseña los usuarios y qué otras restricciones o requerimientos hay al respecto?

Lo que se refiere al sistema de seguridad las contraseñas se cambiarán cada mes por el administrador de seguridad. Para los sistemas de información los administradores de los mismos son los encargados (se hace la recomendación de que cambien mensualmente la contraseña tanto del sistema operativo como de sus aplicaciones, sin embargo el cambio no debe hacerse el mismo día de cada mes).

Las contraseñas son asignadas por el administrador del software que se tiene instalado en los equipos personales en común acuerdo con el usuario, el cual les recomienda que el password se cambie mensualmente y que estos a su vez reporten del cambio para la administración de password.

61.- ¿Los usuarios serán responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema?

Los usuarios serán los responsables de hacer los respaldos de su información en los servidores que se destinen para ello. En cuanto a aplicaciones y archivos de configuración tanto del sistema de seguridad como de los sistemas de información los administradores son los encargados de realizarlos diario o semanalmente.

Es necesario que los usuarios lleven un control de estos respaldos (fechas, etiquetar cintas, etc.). Toda la información respaldada se debe almacenar en lugares bajo llave y lejos de donde se obtiene.

62.- Consecuencias para los usuarios que divulguen información que pueda estar patentada, ¿Qué acciones legales u otros castigos pueden implantarse?

Se aplicarían sanciones a los responsables de tal evento, de acuerdo a las decisiones tomadas por la Gerencia de Sistemas de Información y Administración de Energía.

63.- ¿Qué hay al respecto a la privacidad del correo electrónico?

El correo electrónico es privado e intransferible.

64.- ¿Qué hay respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión?

Internamente se prohíbe el mal uso de correo electrónico como enviar cadenas, archivos de video (*.mpeg), archivos con virus o cualquier otro tipo de información que no tenga relación con el área de trabajo.

65.- Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

Estará prohibida cualquier modificación a la configuración de las cuentas de correo en el software que se utilice para este fin por el usuario. Cualquier cambio deberá solicitarse al administrador del correo.

El usuario deberá notificar si detectó algún correo falsificado.

66.- ¿Qué tienen que hacer los usuarios para protegerse a sí mismos y al sitio?

Activar un protector de pantalla con password.

Revisar con el antivirus actualizado todo tipo de archivos o programas nuevos. O bien, establecer un mecanismo que actualice en forma automática el antivirus, así como su aplicación a las PCs.

67.- ¿Qué podrá hacer la gente en Internet? ¿Pueden transferir archivos ejecutables al azar y ejecutarlos?

No se puede chatear, bajar protectores de pantallas, bajar información de sitios poco confiables, acceder a páginas XXX. No abrir sitios de juegos. Así como no pueden abrir archivos ejecutables de dudosa procedencia. Tampoco deben bajar paquetes que requieran licencia.

Como ejemplo de lo que sí puede hacer en Internet es: bajar información requerida en el área de trabajo para realizar pruebas de funcionalidad para su posterior adquisición o para bajar parches para la actualización de los equipos de la red.

Con respecto a los servicios de Internet:

CORREO ELECTRÓNICO

Se debe pensar e implantar una buena configuración adecuada para que en el caso de un ataque de negación de servicio solo se niegue el servicio de correo electrónico.

Usar una buena contraseña.

No aceptar la manipulación social. Es decir no aceptar o hacer caso de mensajes en que se pida cambiar la contraseña de forma específica aunque parezca de un administrador.

No debe aceptar abrir correos de personas que no se conozcan.

Revisar con antivirus los correos recibidos.

Revisar con un antivirus los archivos adjuntos que se envían.

No ejecutar programas si no se esperan o no se sabe en realidad lo que realizan.

No enviar datos personales o confidenciales.

Para evitar el SPAM: Si desea realizar una buena obra ('salvemos al mundo') usando el SPAM introduzca las direcciones electrónicas masivas de quienes envía en BCC o CCO. Sin embargo lo mejor que puede hacer es no responder a estos correos.

No enviar cadenas, juegos, cartas de felicitación o videos, estos pueden ser caballos de Troya.

Se debe tener en un sitio seguro el servidor de correo.

TRANSFERENCIA DE ARCHIVOS

No usar el FTP para obtener juegos de computadoras, software pirata e imágenes pornográficas porque tienden a ocupar una cantidad excesiva de tiempo y espacio en el disco. Además pueden ser troyanos.

Para instalar un FTP anónimo (“anonymous”), debe asegurarse que las personas que lo utilicen no puedan tener acceso a otras áreas o archivos del sistema, y que no puedan utilizar FTP para tener acceso al sistema en sí.

El servidor de FTP anónimo debe ser usado de forma apropiada, sólo para archivos de la empresa.

No proporcionar acceso a FTP fuera de su red. Los usuarios comunes no transfieren archivos con este protocolo.

Desconfiar de cualquier software que se obtenga por FTP.

ACCESO DE TERMINAL

Dar autenticación a inicios de sesión remotos.

"ON" coloca todas sus inspecciones de seguridad en el programa cliente, y cualquiera puede utilizar un cliente modificado que salte estas inspecciones, por lo que es totalmente inseguro para emplearse aun dentro de una red de área local protegida por un firewall (permite que cualquier usuario ejecute algún comando como otro usuario). Por ello debemos desactivar este servicio.

NOTICIAS DE USENET

Para las noticias de Usenet se deben configurar para que las inundaciones no afecten otros servicios. Las noticias asemejan una inundación cuando funcionan de forma normal.

Para instalar el servidor de noticias en el sitio debe determinar la forma más segura de que fluyan las noticias a los sistemas internos para que NNTP no pueda ser utilizado para penetrar el sistema principal.

Si se va a crear un grupo de noticias privado, hay que asegurarse de configurar NNTP con cuidado para controlar el acceso a estos grupos. Hasta este momento, por los problemas de seguridad que presenta no se considera como servicio a brindar en la red.

WORLD WIDE WEB

No agregar visualizadores.

No permitir que se cambien las configuraciones de los visualizadores, basándose en el consejo de extraños.

INFORMACIÓN SOBRE PERSONAS

"FINGER" puede proporcionar información valiosa a intrusos, por ejemplo, al identificar usuarios que rara vez se dan de alta. Quizá desee bloquear las solicitudes de finger que vienen de afuera de su red interna, o proporcionar sólo la información mínima

en respuesta a estas solicitudes. Las personas que usan finger en forma legítima no necesitan toda la información que les da finger.

Algunos sitios optan por escribir servidores que utilizan whois para distribuir información acerca de sus usuarios. si decide hacer esto, las preocupaciones comunes se aplican a los servidores para que no den demasiada información y par que no permitan que las consultas hagan que se ejecuten comandos arbitrarios.

SERVICIOS DE CONFERENCIA EN TIEMPO REAL

"TALK" puede ser muy engañoso para permitirlo a través de un firewall sin abrir involuntariamente otros agujeros de seguridad. Se recomienda configurar bien el firewall.

SERVICIO DE NOMBRES

No brindar más información de la pensada. No incluir información sobre el hardware y software que está ejecutando. No deseamos que un atacante conozca los nombres de todas las máquinas internas.

Configurar el servicio de nombres para tener disponible la información completa para los hosts internos, pero sólo en forma parcial para los solicitantes externos.

Usar un DNS interno y luego depender de los nombres de anfitrión para dar autenticación lo hace vulnerable a un intruso que puede instalar un servidor DNS mentiroso. Esto se puede manejar combinando algunos métodos, incluyendo:

-Usar direcciones IP en lugar de nombres de anfitrión, para dar autentificación a los servicios que deben ser más seguros.

-Dar autentificación a usuarios en lugar de anfitriones en los servicios más seguros, porque las direcciones IP también pueden falsificarse.

No es necesario ni aconsejable proporcionar servicio NIS/YP a máquinas externas, pues está diseñado para administrar un solo sitio, no para intercambiar información entre sitios, y es altamente inseguro. Por ejemplo, no sería posible proporcionar información de su anfitrión a sitios externos por medio de NIS/PY sin también proporcionar su archivo de contraseña, si ambos están disponibles internamente.

SERVICIOS PARA ADMINISTRACIÓN DE REDES

Para el ping y el traceroute es posible utilizar el filtrado de paquetes para evitar que estos se transmitan desde el sitio o se reciban de el.

SERVICIO DE HORA

Los relojes de radio adecuados para usarse como fuentes de hora NTP no son demasiado caros, cuando utilizamos NTP para sincronizar relojes para un protocolo de autentificación como Kerberos, se debe comprar los relojes y proporcionar internamente el servicio de hora en lugar de usar una referencia externa.

SISTEMAS DE VENTANAS

X11 no es seguro para usarse a través de Internet. Si se usa X11, hay que asegurarse que tanto el servidor como los clientes se debe tener encendida la opción de auntentificación.

SISTEMAS DE IMPRESIÓN

Las opciones para impresión remota son formas inseguras e ineficientes de transferir datos a través de Internet. No hay razón para permitirlo.

La Asociación de Correo Electrónico (EMA, Electronic Mail Association) recomienda que todo sitio debe tener una política acerca de la protección de la privacidad de los empleados. Las organizaciones deben establecer políticas que no se limiten al correo electrónico, sino que también abarque otros medios, como discos, cintas y documentos impresos. La EMA sugiere cinco criterios para evaluar cualquier política:

Estos son los siguientes puntos que se proponen como necesarios para la revisión de la política:

a) ¿La política cumple con la ley y con las obligaciones hacia otras empresas?

b) ¿La política evita el comprometer sin necesidad a los intereses del empleado, del patrón o de otras empresas?

c) ¿La política es funcional, práctica y de posible cumplimiento?

d) ¿La política aborda apropiadamente todas las formas de comunicación y mantenimiento de archivo en la oficina?

d) ¿La política fue anunciada por anticipado y aceptada por todos los interesados?

En caso de tener todas las respuestas afirmativas, esta política debe ser comunicada en forma oficial para su atención rigurosa por los miembros de la empresa. De lo contrario, se realizan las acciones debidas.

68.- ¿Podrá el administrador revisar o leer los archivos de un usuario por alguna razón?

Sí, sólo en caso de ser necesario y previa autorización del subgerente o gerente y que el archivo sea necesario para solucionar algún problema en los sistemas de información del centro de control de la empresa eléctrica.

68.1.-De ser afirmativa la pregunta anterior, ¿en qué grado tiene esa prioridad?

Cuando el usuario ya no puede bajar su correo por saturación en su espacio en disco del servidor de correo. También cuando el usuario tiene mucho tiempo sin revisar su correo.

69.- ¿Los administradores de la red tendrán el derecho de examinar el tráfico de la red o del host?

Sí tienen el derecho de examinar el tráfico para detectar qué tipo de información se intercambia entre usuarios (ej. Tráfico de UDP, TCP, Protocolos de comunicación, IPx, ethernet, etc.). Con el fin de detectar qué equipos introducen más tráfico a la red.

70.- ¿Cuáles serán las responsabilidades legales de los usuarios, los administradores del sistema y de la organización por tener acceso no autorizado a los datos privados de otras personas?

Se aplicarían sanciones a los responsables de tal evento. Como podrían ser desde una llamada de atención, pérdida del empleo, hasta una sanción administrativa o penal. Cabe señalar que para lo anterior necesariamente se necesita una modernización de la legislación tanto laboral como penal para la aplicación de alguna sanción en forma oficial.

Políticas para visitantes
Se requerirá que:

El visitante solicite por escrito la autorización de acceso.
Exista una bitácora para el control de acceso.

Y se recomienda que:

El acceso sea en horarios de trabajo (Seguridad)
El visitante siempre vaya acompañado por el personal de la empresa.
El visitante porte un gafete.
El personal de área de soporte porte su gafete.

Las políticas también se les debe dar a conocer a los foráneos:
En caso de requerir accesos a los sistemas de información para actualizar, configurar pruebas de conectividad de un producto que se requiere para realizar cambios en las aplicaciones de los sistemas de información y así brindar un mejor servicio a los usuarios. Todo ello bajo supervisión del administrador del sistema que se vea involucrado.

71.- ¿Qué lineamientos se tomarán para los usuarios internos que violen las políticas de seguridad de la organización?

Desde una llamada de atención hasta la restricción de acceso en los sistemas de información en caso de proporcionar información clasificada (confidencial) a personas foráneas que afecte la operación del Sistema Eléctrico a cargo serán removidas de su puesto de trabajo así como de las sanciones legales que la compañía considere necesaria.

72.- ¿Qué lineamientos se tomarán para los internos que violen las políticas de seguridad de un sitio remoto?

Se debe especificar en la política de seguridad que el violar las redes de otro sitio constituyen una violación de la política de la compañía. En este momento en la compañía se ha tratado como un acto de desconfianza para la persona que lo realiza y se le transfiere a otra área previo acuerdo de las partes laborales involucradas.

73.- ¿Qué lineamientos se tomarán para los usuarios foráneos que violan las políticas de seguridad dentro de la organización?

Desde revocación de contratos que la empresa eléctrica tenga con esa compañía hasta las secciones legales que la empresa eléctrica considere necesarias.

74.- ¿Ya se tomó en cuenta el monitorear las tendencias de violación?

Sí. Para este caso se cuenta con software que monitoreará y detectará intrusos que pretendan accesar a los sitios de información y que no están considerados en las políticas de seguridad.

75.- ¿Qué tipo de estrategia de respuesta se aplicaría a cada caso?

Se realizará una reconfiguración de permisos de acceso en los firewalls del sistema de seguridad, así como la aplicación de las sanciones antes mencionadas. Se revisan las políticas de seguridad para revisar si existe algún riesgo que no se haya considerado dentro de estas.

Las estrategias que se tienen son; “proteger y continuar”, “perseguir y demandar”.

Lineamientos auxiliares para elegir una estrategia:

a) La estrategia de proteger y continuar puede usarse en las siguientes circunstancias:

- Si los recursos de la red no están bien protegidos de los intrusos.
- Si la continua actividad del intruso pudiera resultar en daños y riesgos financieros considerables.
- Si existen considerables riesgos para los usuarios actuales de la red.
- Si en el momento del ataque no se conocen los tipos de usuario de una gran red interna.
- Si el sitio está sujeto a demandas judiciales por parte de los usuarios.

b) La estrategia de perseguir y demandar puede usarse en las siguientes circunstancias:

- Si los recursos del sistema están bien protegidos.
- Si el riesgo de la red es incrementarlo por los disturbios creados por las intrusiones presentes y futuras.
- Si se trata de un ataque concentrado y ya ha ocurrido antes.
- Si el sitio es muy notorio y ha sido víctima de ataques anteriores.
- Si el hecho de no demandar acarreará más intrusiones.
- Si el sitio está dispuesto a arriesgar los recursos de la red permitiendo que continúe la intrusión.
- Si puede controlarse el acceso del intruso.
- Si las herramientas de vigilancia están bien desarrolladas para crear registros adecuadas y recabar evidencias para la demanda.
- Si cuenta con personal capacitado interno para construir rápidamente herramientas especializadas.
- Si los programadores, administradores del sistema y de la red cuentan con los conocimientos necesarios acerca del sistema operativo, utilerías del sistema y los sistemas para que valga la pena el juicio.
- Si la administración de la empresa tiene disposición a demandar.

- Si los administradores del sistema saben qué tipo de evidencias presentar en un juicio y pueden crear los registros adecuados de las actividades del intruso.
- Si hay contactos establecidos con agencias judiciales conocedoras.
- Si existe un representante del sitio versado en las cuestiones legales relevantes.
- Si el sitio está preparado para las posibles acciones legales que emprendieran los usuarios si sus datos o sistemas se vieran comprometidos durante la demanda.
- Si se dispone de buenos respaldos.

76.- ¿Se tendrán los elementos suficientes para usar la estrategia "perseguir y demandar"?

En este momento no, ya que las leyes en México no están aprobadas en su totalidad por lo que sólo existen sanciones que se pueden aplicar a nivel interno de la empresa.

Considere las circunstancias para elegir el tipo de estrategia.

77.- ¿Existirá entre sus contactos organizaciones externas como el CERT de la UNAM y/u otras organizaciones?

CERT.- Equipo de respuesta a Emergencias de Cómputo. El objetivo de este equipo es abordar las preocupaciones acerca de seguridad de cómputo de los investigadores en Internet. Este equipo tiene la capacidad de hablar inmediatamente con expertos para diagnosticar y resolver problemas de seguridad. También pueden ayudar a establecer y mantener la comunicación entre un sitio y las autoridades del gobierno. Cuando no está dedicado a atender emergencias, el CERT sirve de centro de intercambio para identificar y reparar puntos vulnerables en los principales sistemas operativos. También puede proporcionar evaluaciones informales de sistemas existentes y orientar para mejorar la capacidad de respuesta a emergencias. Debido a esto, puede ayudarlo indirectamente a formular una política eficaz de seguridad de redes. También se sabe que este equipo ha trabajado con proveedores de sistemas de software para coordinar las soluciones a los problemas de seguridad.

78.- ¿Cuándo deberá ponerse en contacto con dependencias judiciales locales y federales, así como con las dependencias investigadoras?

En este caso en el sistema de seguridad estos criterios a la fecha no se han determinado.

79.- ¿Qué tipo de información podrá ser divulgada a las dependencias judiciales locales, federales, a las dependencias investigadoras y a la prensa?

En caso de que lo anterior aplicará, el criterio sería entregar la información mínima y necesaria para permitirles realizar su investigación, tanto a la prensa como a las dependencias judiciales y esta se determinaría de acuerdo a la gravedad y a las circunstancia.

80.- ¿Quiénes formarán el comité para interpretar y revisar las políticas?

El gerente de sistemas, los subgerentes y los administradores de los sistemas informáticos, así como el encargado de seguridad.

81.- ¿Cómo se propagará la cultura de seguridad informática?

Las computadoras personales deberán estar bajo la responsabilidad de cada usuario. Para que el usuario tome conciencia de la responsabilidad que tiene de sus equipos se le debe dar al usuario la capacitación previa y los procedimientos, los cuales deben ir firmados de recibido para evitar lagunas mentales. La capacitación es para todo usuario, es decir a cualquier nivel jerárquico que use una computadora. También se pueden realizar campañas de seguridad.

Es necesario que los usuarios estén alertas de no dejar ninguna sesión abierta mientras no estén presentes. Así también es útil usar protectores de pantalla con contraseña.

Los usuarios deben estar consientes que son responsables por cualquier actividad en el sistema, programa o red que ocurra bajo su USER ID Y PASSWORD, o cualquier componente de hardware que esté en sus manos.

82.- ¿Cómo va a dar la capacitación?

Por medio de cursos, campañas y acercamiento a los usuarios.

83.- ¿Tomó en cuenta a todos los usuarios? (Todos lo usuarios, incluye la alta gerencia). Sí.

84.- ¿Existen problemas de reducción de productividad con la puesta de la política?, de ser así, agregue recursos adicionales a la red para asegurarse de que los usuarios puedan realizar su trabajo sin pérdida de productividad.

No. todo marcha de acuerdo a lo establecido.

85.- ¿Cada cuando se harán los recordatorios de la política?

Tres veces al años o antes en caso necesario.

86.- ¿Habrá que considerar a los nuevos usuarios de la red para incluir la política en los paquetes de información de estos?

Sí, puesto que todo usuario de la red debe conocer las políticas para un buen funcionamiento de éstas.

87.- ¿Será necesario que los usuarios firmen la política para darse por enterados?

Sí.

88.- ¿A qué documento debe referirse la política para los administradores, es decir dónde se detallará y consultará la parte técnica?

Al documento de mantenimiento y plan de contingencia.

Después de tener una política de seguridad se debe tener también un plan de contingencia. El plan de contingencia son las recomendaciones o acciones que hay que tomar para recuperarse lo antes posible de daños informáticos y volver a la marcha normal de trabajo. En el plan de contingencia se puede incluir un ejemplo de análisis forense. El análisis forense se considera en el peor de los casos (cuando se ha perdido información importante y sólo queda el investigar).

En este documento no se incluyen el plan de contingencias y el análisis forense, puesto que, esta tesis se enfoca al diseño e implantación del sistema de seguridad, dejando para su estudio posterior el mantenimiento y recuperación de datos.

6.3. Conclusiones

Se ha dado respuesta a las dos preguntas más importantes que son formuladas para establecer un sistema confiable que son: ¿Qué es lo se debe proteger? ¿De quien hay que protegerse?

La respuesta a las preguntas anteriores son: Lo más importante es la información crítica, y los ataques pueden ser realizados por personas ajenas como por aquellas que pertenecen las políticas de seguridad adecuadas a las necesidades de la empresa eléctrica.

Después del estudio realizado, se da una propuesta a la empresa para cubrir las vulnerabilidades encontradas en los sistemas informáticos. Esta propuesta inicia con una lista que contiene el nombre de los responsables de los diferentes sistemas y departamentos. Esta lista debe encabezar las políticas dado que se necesitará de éstos contactos en el caso de que haya un incidente.

Las propuestas de las políticas y aún las políticas no cubren todos los riesgos, dado que existen algunos que no son evidentes. Sin embargo, sí reducirá en un mayor grado a éstos. Debido a lo anterior, cada que se descubran nuevas vulnerabilidades se deben agregar a las políticas.

Estas propuestas son parte esencial para la realización del sistema de seguridad por lo que se trató de realizar la redacción de la forma más clara posible, discutiéndola con los interesados del sistema de seguridad en la empresa, para que quedara entendida por todos y estuvieron en el mismo marco de discusión.

Con esta propuesta son asignados los ahora responsables del sistema de seguridad. Haciéndose cargo de ésta función una persona dedicada al sistema junto con auxiliares que aunque atienden otras tareas, también conocen el sistema, en caso que la persona encargada no esté disponible.

La política propuesta incluye desde el enfoque que se va a tomar considerando que éste da mayores facilidades para la administración; la forma en la que la política será usada hasta las sanciones contra las violaciones de ésta; la forma en la que deberá ser publicada; así como los alcances de ésta.

La política establece los documentos a utilizar y los procesos a seguir para tener un control sobre la conducta del personal hacia la información y un control de los recursos de la red de cómputo.

Para poder definir las políticas se tuvo que identificar los recursos y servicios de red a proteger, para reconocer amenazas que se presentaban en éstos y de aquí se desprende el buscar soluciones para prevenirlas. Mientras se termina de implementar la parte tecnológica, con las políticas que se proponen se pueden poner en servicio las que no precisan de esta y con esto agregar seguridad a la red.

Capítulo 7
Control de acceso: Firewalls

El control de acceso a los diferentes recursos de la organización es uno de los diferentes mecanismos referentes a la seguridad. Junto a otros componentes, como el control de contenido, IDS/IPS, antivirus y antispam contemplan casi todos los aspectos relacionados a seguridad.

Dado que el firewall es el componente básico para iniciar un sistema de seguridad, este capítulo describe ventajas y desventajas del uso de firewall y diferentes tipos de firewalls existentes.

7.1 Firewalls

Existen varias arquitecturas y configuraciones de firewalls, pero la idea básica detrás de éstos siempre es la misma. Esto es, un firewall separa una red protegida de una red sin protección, como lo es Internet. Es decir, somete a una revisión y filtra todas las conexiones que llegan desde Internet a la red protegida, y viceversa, a través de un solo control de seguridad concentrado. Un firewall previene que no se pueda alcanzar Internet desde una red interna, o esta última desde Internet, a menos de que se pase a través de este control (conocido como choke-hold firewall o firewall de bobina de control).

Pero incluso antes de definir qué tipo de firewall se adapta mejor a las necesidades particulares de la empresa eléctrica, se deberá analizar la topología de la red para determinar si los varios componentes de ésta, como los concentradores, ruteadores y el cableado son apropiados para un modelo específico de firewall.

Algunos firewalls pasan a través de todos los niveles del modelo OSI ya que actúan en los niveles sexto y séptimo, que son los niveles responsables del control de establecimiento de sesiones y aplicaciones. De esta manera, con un firewall se puede controlar el flujo de información a través del establecimiento de sesiones o incluso al determinar cuáles operaciones se permitirán o no lo harán.

La importancia de este capítulo está dada en el conocer las diferentes soluciones alternativas que se consideran para el diseño. Por ello se describirán los alcances y características de éstas.

7.2. Ventajas y desventajas de los firewalls

Hay que recordar que un firewall por sí solo no asegurará la red, sólo es parte de un área más amplia en la protección y la conectividad en la red en general. Se necesita determinar qué cosas se deben proteger, desarrollar una política de seguridad y establecer mecanismos para hacer cumplir la política y los procedimientos que van a

emplearse como prerrequisitos para implementar los firewalls. También existen mecanismos además del firewall que se pueden añadir para incrementar en gran medida el nivel de seguridad.

Un firewall puede implementarse en UNIX, NT, DOS o en alguna otra plataforma patentada. Se debe estudiar muy de cerca la plataforma que se elegirá, ya que ésta definirá definitivamente todos los proyectos futuros, el nivel de seguridad y en consecuencia, la política de seguridad que se está desarrollando. También se debe pensar en la fortaleza de cada sistema operativo; en la familiaridad, como un punto de suma importancia y en el conocimiento del ambiente que tienen los administradores con el sistema, pues son ellos quienes trabajarán con él; así como el soporte técnico que brindará la empresa de la plataforma.

Un firewall mejora en gran medida la seguridad de red y reduce los riesgos para los servidores en la red al filtrar inherentemente servicios inseguros. Como resultado, el entorno de red está expuesto a menores riesgos debido a que sólo los protocolos seleccionados son capaces de pasar a través de un firewall.

Un firewall puede ofrecer control de acceso a los sistemas de un sitio, por ejemplo, algunos servidores pueden ponerse al alcance de redes externas, mientras que otros pueden cerrarse de una manera efectiva al acceso no deseado.

Un riesgo que hay que esperar es el que los usuarios que reciben información de la red o de Internet, descarguen virus a través del correo electrónico y los diseminen en toda la red protegida.

Otra amenaza son los applets (principalmente los de Java, JavaScript y ActiveX), los cuales pueden iniciar procesos remotos en una estación de trabajo que podrían afectar a un servidor o incluso desactivar un firewall. Esto nos lleva a uno de los principales propósitos en los que una política de acceso es particularmente expresa para hacer cumplir: nunca se debe proporcionar acceso a servidores o servicios que no se requieran accesar; los hackers podrían explotarlos debido a que el acceso no es necesario.

Un firewall puede resultar menos costoso para la empresa eléctrica si todo (o la mayoría) el software modificado y el software de seguridad adicional se pueden localizar en el sistema de firewall que si se distribuye en cada servidor o máquina. En particular, los sistemas de contraseñas desechables y otro software de autentificación agregado puede localizarse en el firewall en lugar de situarlo en cada sistema al cual se necesite tener acceso desde Internet, también se debe de pensar en la seguridad interna. Frecuentemente, se da mucho énfasis al firewall, pero si un hacker irrumpe en el sistema, a menos que se tengan algunas políticas de seguridad internas en funcionamiento, la red quedará expuesta.

Otras soluciones para la seguridad de la red de la empresa eléctrica podrían involucrar modificaciones en cada sistema de servidor. Aunque vale la pena considerar muchas técnicas por sus ventajas y que probablemente son más apropiadas que los firewalls en ciertas situaciones, los firewalls tienden a ser más simples de implementar debido a que sólo el firewall necesita ejecutar software especializado.

La privacidad debe ser una gran preocupación para toda red de la empresa, debido a que lo que normalmente se consideraría información inofensiva en realidad podría contener pistas útiles para un hacker. Al usar un firewall, el sitio puede bloquear el acceso de servicios como Finger y el Servicio de Nombres de Dominio. Recordando que Finger despliega información sobre los usuarios tal como la hora de su última entrada al sistema, si han leído el correo entre otras cosas. Pero Finger también puede revelar información a los hackers sobre qué tan a menudo se utiliza un sistema, si se tienen usuarios activos conectados y si pudiese atacarse sin atraer la atención de los administradores y otros sistemas de supervisión.

Otra ventaja de usar un firewall en el sitio es que al pasar a través de un firewall todo el acceso hacia y desde Internet, se puede llevar una bitácora de los accesos y proporcionar estadísticas valiosas sobre el uso de la red.

Además de las bitácoras y las estadísticas, existen muchas otras ventajas de usar firewalls. A pesar de estas ventajas, se debería estar consiente de que también existen varias desventajas: cosas contra las cuales no pueden proteger los firewalls, como restricciones de acceso físico como lo es el robo de información por usuarios del sitio, amenazas de las puertas traseras (módems o servidores RAS (Remote Access Server) que omiten el acceso por el firewall) y vulnerabilidad a hackers internos, por nombrar unas cuantas.

Un firewall probablemente bloqueará ciertos servicios que los usuarios desean, por ejemplo Telnet, FTP, X Windows, NFS, etc. Estas desventajas no son únicas a los firewall solos; sin embargo, el acceso a la red también podría restringirse en el nivel de servidor, dependiendo de la política de seguridad del sitio. Una política de seguridad y las necesidades del usuario puede ayudar en gran medida a aliviar los problemas con acceso reducido a los servicios.

7.3. Componentes de los firewalls

Los componentes básicos en la construcción de un firewall incluyen:

- Políticas de seguridad
- Autentificación avanzada
- Filtrado de paquetes
- Gateways de aplicación

Los dos primeros componentes serán explicados en esta sección. Mientras que los dos últimos serán explicados en la siguiente sección dado que son los elementos principales para poder realizar una clasificación de firewalls.

7.3.1. Política de seguridad de la red

La decisión de instalar un firewall puede estar directamente influenciada por dos niveles de política de red.

La política de acceso a la red que define los servicios que se permitirán o negarán de manera explícita desde la red restringida es la política de más alto nivel, también define cómo se utilizarán estos servicios. La política de más bajo nivel define cómo el firewall restringirá en realidad el acceso y determinará los servicios especificados en la política de nivel superior. Sin embargo la política no debe volverse un documento aislado, olvidado; debe ser útil. Es necesario que la política de seguridad de red se vuelva parte de la política de seguridad de la compañía.

Hay que recordar que la política de seguridad de la red debe contener:

Política de flexibilidad: Internet por sí misma cambia cada día a una velocidad que nadie puede seguir. Conforme Internet se modifica, los servicios ofrecidos a través de la misma también cambian. Por eso, cualquier compañía necesita adaptarse a este desarrollo también, así que se debe estar preparado para editar y ajustar la política sin comprometer la seguridad y la consistencia.

Política de acceso a los servicios: La política de acceso a los servicios debe ser completamente realista, así cuando se realizan hay que concentrarse en los problemas de los usuarios de la compañía.

Política de diseño de firewall: Una política de diseño de firewall es específica para el firewall. Define las reglas de implementación de las políticas de acceso a los servicios. No se puede diseñar esta política sin entender las capacidades y limitaciones del firewall, así como las amenazas y los puntos vulnerables asociados con TCP/IP.

Los firewalls usualmente realizan una de las siguientes acciones:
- Permiten cualquier servicio a menos que se niegue expresamente.
- Niegan cualquier servicio a menos que se permita expresamente.

Un firewall que implementa la primera política permite a todos los servicios pasar a su sitio en forma predeterminada, excepto aquellos que la política de acceso a los servicios haya determinado que se les niegue el permiso. Con la segunda política, el firewall negará todos los servicios en forma predeterminada, pero luego permitirá aquellos que se hayan establecido como permitidos. La política de la cual se ha hablado es el componente más importante al instalar un firewall. Los otros tres componentes son necesarios para implementar y hacer cumplir la política.

Política de marcado al interior y exterior: Deberá forzar a los usuarios que llaman de fuera a pasar a través de la autentificación avanzada del firewall. Esto deberá enfatizarse en la política, así como la prohibición de módems sin autorización conectados a cualquier host o cliente, o que no pase a través de un firewall. La misma situación es para el PPP (Point-to-Point Protocol, protocolo punto a punto) y SLIP (Serial Line Internet Protocol, protocolo Internet para línea serie).

7.3.2. Autentificación avanzada

A pesar de todo el tiempo y esfuerzo invertido en escribir políticas e implementar firewalls, muchos incidentes resultan del uso de contraseñas débiles o permanentes.

Por otra parte, se debe estar consciente de que algunos servicios TCP o UDP sólo autentifican en el nivel de direcciones del servidor y no para usuarios específicos. Un servidor NFS, por ejemplo, no puede autentificar a un usuario específico en un servidor, debe otorgar acceso a todo el servidor. Para un hackeo por suplantación de IP es peligroso. Incluso a pesar de que la mayoría de los ruteadores pueden bloquear los paquetes enrutados de origen, aún es posible enrutar paquetes a través de firewalls de ruteador de filtrado si éstos no están configurados para filtrar los paquetes de entrada, cuya dirección origen está en el dominio local.

Los siguientes ejemplos de configuraciones son potencialmente vulnerables a aquellos ataques:

- Ruteadores a redes internas que aceptan varias interfaces externas.
- Ruteadores con dos interfaces que aceptan subredes en la red interna.
- Firewalls de proxy donde las aplicaciones de proxy utilizan la misma dirección IP origen para la autentificación.

Los ataques de suplantación de IP por lo general están dirigidos a las aplicaciones que utilizan autentificación en las direcciones IP origen. Cuando el hacker puede pasar el paquete, el acceso a datos no autorizados estará totalmente disponible para él. Hay que tener en mente que el hacker no tiene qué obtener de regreso un paquete de respuesta; este robo es posible aun sin él. Es más podría parecer que inhabilitar el ruteamiento de origen en el ruteador lo impedirá. Esto es falso, este enrutamiento no puede proteger la red interna de sí misma.

Si se tiene un ruteador hacia redes externas que acepte múltiples interfaces internas, se debería considerar la instalación de un firewall debido a que está expuesto a los ataques de suplantación de los hackers. Lo mismo se aplica a ruteadores con dos interfaces que aceptan subredes en la red interna, así como firewalls de proxy si las aplicaciones de proxy utilizan la dirección IP para la autentificación.

De acuerdo con el CERT, hay dos pasos que se pueden seguir con la finalidad de evitar este tipo de ataque:

- Instalar un ruteador de filtrado que restrinja la entrada en la interfaz externa, si ésta identifica que el origen del paquete está en el interior de la red. Aun si se trata de un paquete autentificado, no pasará.
- Filtrar los paquetes que salen para determinar si la dirección es diferente de aquella de la red interna, de tal manera que los ataques originados en el interior puedan impedirse.

Si la falta de seguridad es un riesgo, también lo es la excesiva complejidad en la configuración y los controles. Una de las primeras cosas que probablemente se dirá a los usuarios de Internet es que elijan contraseñas difíciles de adivinar. No obstante, la mayoría de los usuarios no seguirán este consejo, y aun si lo hicieran, los hackers pueden monitorear las contraseñas que se transmiten. Una de las alternativas más eficaces para pelear contra el hacker es adoptar medidas de autentificación avanzadas.

Algunos de los dispositivos de autentificación avanzada más populares en uso actualmente son los sistemas de contraseña desechable. Una tarjeta inteligente por ejemplo, genera una respuesta como autentificador en lugar de una contraseña tradicional. Trabaja junto con software y hardware. El sistema de autentificación avanzada del firewall debe localizarse en el firewall debido a que centraliza y controla el acceso al sitio. Se puede instalar en otro servidor, pero si se carga en un firewall es más práctico y manejable centralizar las medidas.

7.4. Clasificación de los firewalls.

Los firewalls se clasifican de acuerdo a sus componentes de filtrado de paquetes y/o gateways de aplicación. Por lo que se tienen firewalls de: Filtrado de paquetes, gateways de aplicación, híbridos que son lo que tienen ambos componentes y por último los de aplicación de segunda generación.

Firewalls de filtros de paquetes.

Éstos están basados en definir reglas o criterios de acuerdo al tipo de protocolo, puertos asociados, servicios o comandos que se permiten, tanto de entrada como de salida. Cuando un paquete quiere entrar a la intranet, el firewall revisa su lista de reglas y determina si puede pasar o no. Actualmente, la forma más común de implantar este tipo de firewalls, es a través de reglas de acceso en los propios ruteadores. Vea la figura 7.1.

Debilidades de los firewalls de filtrado de paquetes:

- El nivel de red es la única capa que comprenden, así que son vulnerables ante los ataques dirigidos a protocolos superiores a este nivel.
- El protocolo a nivel de red requiere conocimientos acerca de sus detalles técnicos, no todos los administradores los tienen. Por ello se vuelve más difícil de configurar.
- Exponen la red privada al exterior ya que no pueden ocultar la topología de red privada.
- Tienen capacidades de auditoría muy limitada.
- No todas las aplicaciones de Internet están soportadas por los firewalls de filtrado de paquetes.
- Estos firewalls no siempre soportan algunas de las cláusulas de las políticas de seguridad, tales como la autentificación de nivel de usuario y el control de acceso por horario.

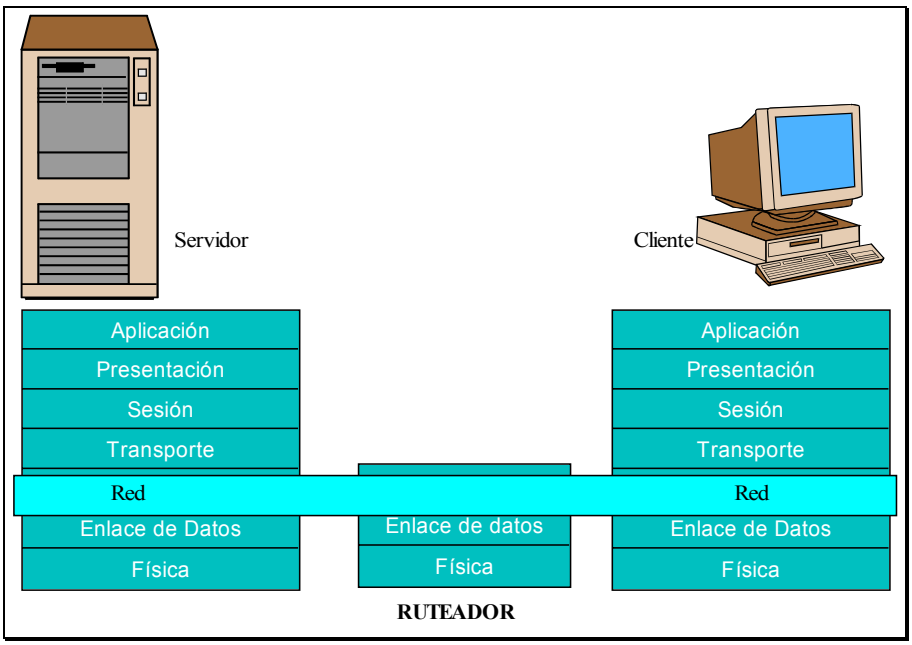

Figura 7. 1.- Firewall de filtro de paquetes

Firewalls basados en "proxies" (firewalls de nivel de aplicación).

Un Firewall de este tipo es aquél que está compuesto de uno o más "proxies", que actúan como intermediarios entre el usuario externo y las aplicaciones. Debido a su examen riguroso son más lentos y por ello no son transparentes al usuario. Vea la figura 7.2.

Ventajas de los firewalls de nivel de aplicación:

- Como entienden el protocolo de nivel aplicación pueden defenderse en contra de todos los ataques.
- No requieren que se conozcan todos los detalles acerca de los protocolos de los niveles más bajos, por ello es más fácil de configurar.
- Pueden ocultar la topología de la red privada.
- Tienen facilidades de auditoría con herramientas para supervisar el tráfico y manipular los archivos de gran tamaño que contienen información como el origen, las direcciones de red de destino, el tipo de aplicación, la identificación del usuario y la contraseña, el tiempo de acceso de inicio y de finalización, y la cantidad de bytes de información transmitidas en todas las direcciones.
- Pueden soportar más políticas de seguridad, incluyendo la autentificación de nivel de usuario y el control de acceso de hora del día.

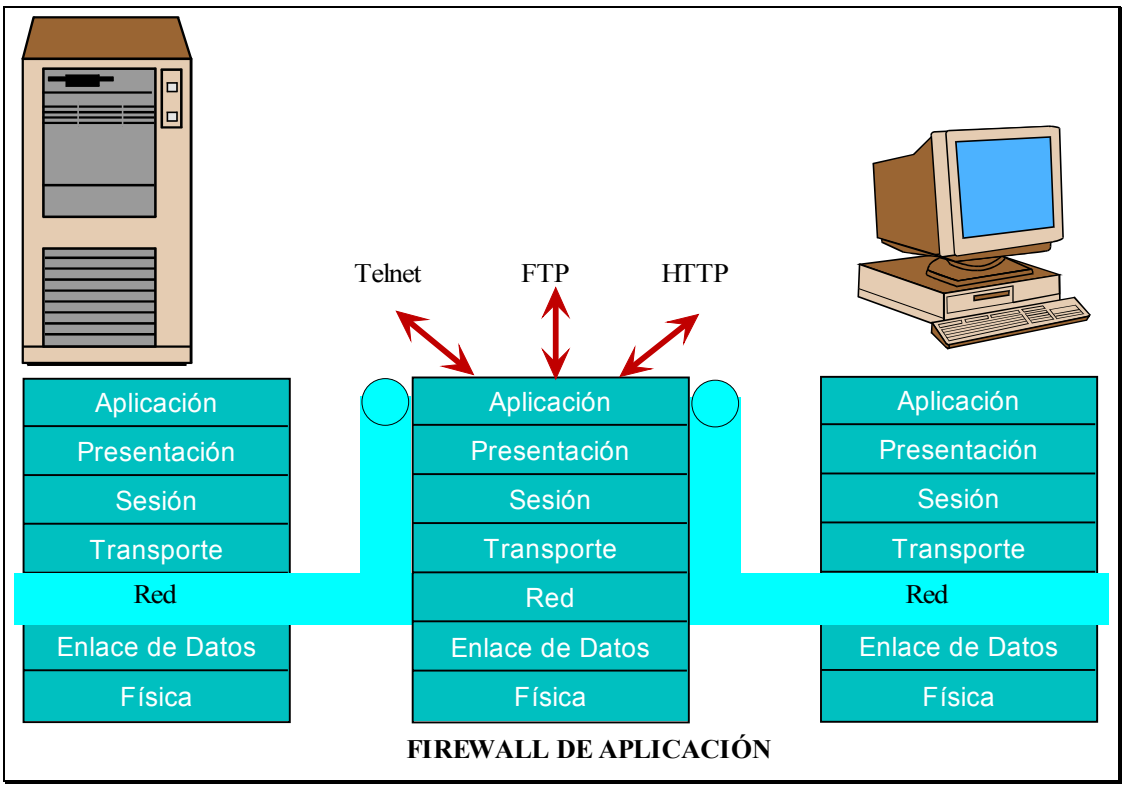

Figura 7. 2.- Firewalls de nivel de aplicación.

Después de haber definido los componentes básicos de los firewalls, algunos más avanzados se consideran como siguen:

Derivados de los componentes antes mencionados existen los siguientes tipos de firewalls:

Firewalls híbridos.

En esta clasificación quedan los firewalls que combinan ambas técnicas o que utilizan alguna de las técnicas anteriores con tecnologías adicionales, tales como la denominada “stateful inspection” de Check Point.

Firewalls de nivel de aplicación de segunda generación.

Sigue siendo un firewall de nivel de aplicación, pero esta generación resuelve el problema de transparencia que se presentaba en las versiones anteriores sin sacrificar el desempeño.

Ventajas de los firewalls de nivel de aplicación de segunda generación:

- Su transparencia y desempeño es mayor.

- Pueden proporcionar una completa traducción de direcciones de red además de que ocultan la topología de la red.
- Pueden soportar más mecanismos avanzados de autentificación de nivel de usuario.

7.5. Áreas a proteger

Existen por lo menos tres zonas distintas al menos para proteger. Estas zonas las podemos clasificar en “zona caliente”, “zona desmilitarizada” y “zona fría”.

Zona caliente.- Se denomina así a Internet y a los elementos que están fuera de la red.
Zona desmilitarizada.- DMZ (**De**-**mi**litarized **Z**one). Es una red expuesta que se establece como una barrera más de protección la cual brindará los servicios adicionales que aunado al firewall formarán un sistema integral de seguridad.
Zona fría.- Se denomina así a la zona de la red interna, y por tanto aquella que se quiere proteger mucho más. En esta zona están los servidores corporativos, minicomputadoras, ruteadores, PCs y toda la infraestructura que conforma la red de la organización.

7.6. Arquitecturas de firewalls

En esta sección se describirán algunas arquitecturas de firewalls las cuales servirán para decidir el tipo de arquitectura a usar en el diseño de la empresa eléctrica. Esta parte es muy importante también para conocer las características de algunos productos comerciales y así poder considerarlos para compararlos con arquitecturas que se construyan dentro de la empresa eléctrica en caso de que así se determine.

Para familiarizarse con estos productos se darán algunos conceptos que son usados por diferentes arquitecturas.

Traslación de direcciones de red (NAT). Con la NAT bidireccional se rescriben los identificadores de origen, de destino y de puerto de los paquetes en el tráfico de entrada y de salida de la interfaz. Esto es bastante útil para enrutar el tráfico a través de redes públicas empleando direcciones IP privadas. Vea la figura 7.3.

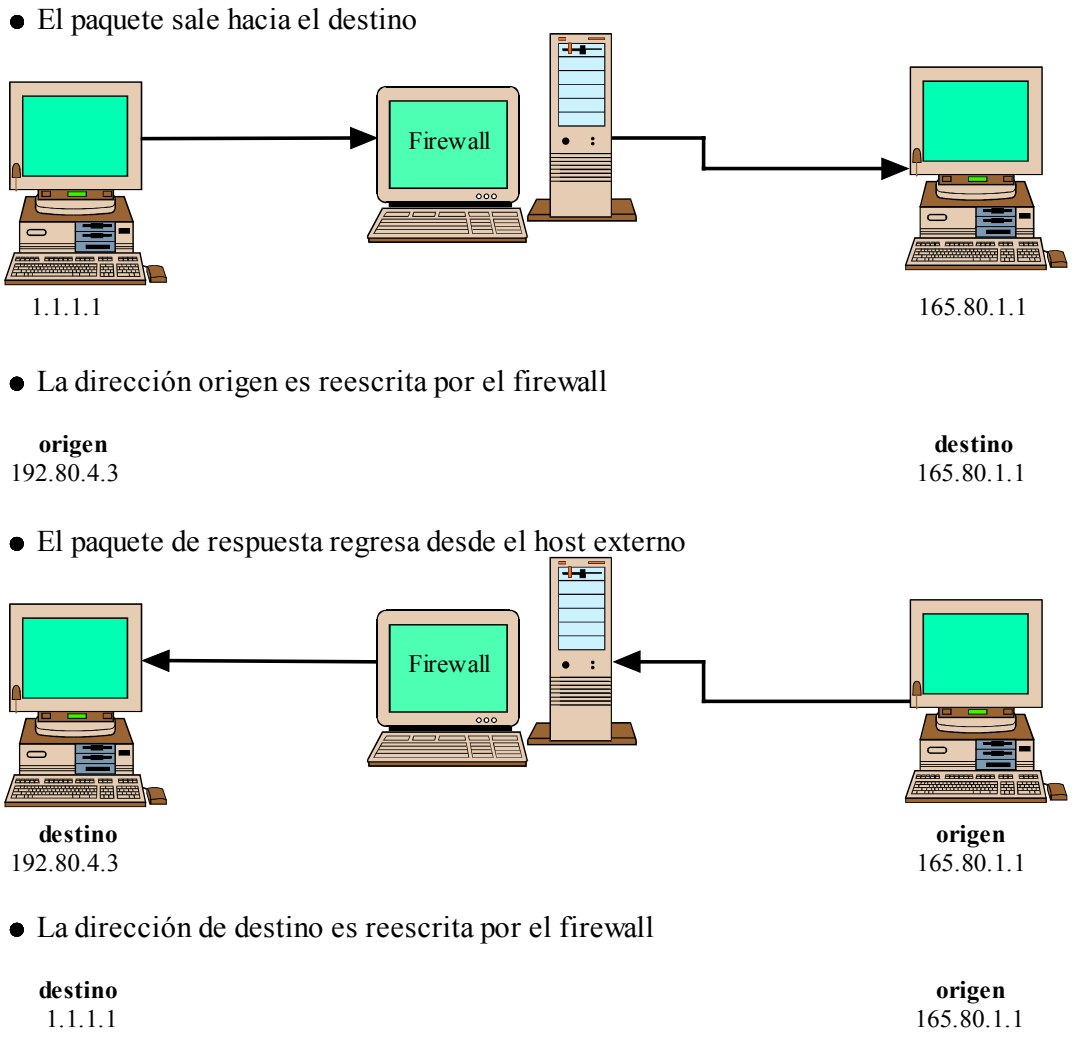

Figura 7. 3.- Traslación de direcciones de red.

Balanceo de la carga de operación en las conexiones. Es un proceso en el cual los paquetes son redirigidos hacia distintos hosts o redes por cada conexión concurrente.

Encriptado: IPSec. IPSec es un conjunto de estándares para la seguridad en Internet que garantiza un estándar abierto de conectividad de host a host, de host a firewall y de firewall a firewall. El estándar incluye dos partes: autentificación y encapsulamiento.

El *Authentication Header* (AH, encabezado de autentificación) ofrece un mecanismo por medio del cual el remitente firma los paquetes IP y el receptor verifica la firma.

El *Encapsulation Security Protocol* (ESP, Protocolo de Seguridad de Encapsulamiento) ofrece un mecanismo por medio del cual el remitente encripta los paquetes IP y el receptor los desencripta.

7.6.1. Tecnología Stateful Inspection

Check Point FireWall-1, desarrollado por Check Point, está basado en la arquitectura de *Stateful Inspection,* la cual fue inventada por Check Point. El *Inspection Module* de Firewall-1 analiza todos los niveles de comunicación de paquetes y extrae la información relevante sobre las comunicaciones y el estado de la aplicación.

El Inspection Module de FireWall-1 reside en el kernel del sistema operativo, debajo del nivel de red, en el nivel más bajo del software. Al revisar las comunicaciones en este nivel, FireWall-1 puede interceptar y analizar todos los paquetes antes de que lleguen al sistema operativo. Ver figura 7.4.

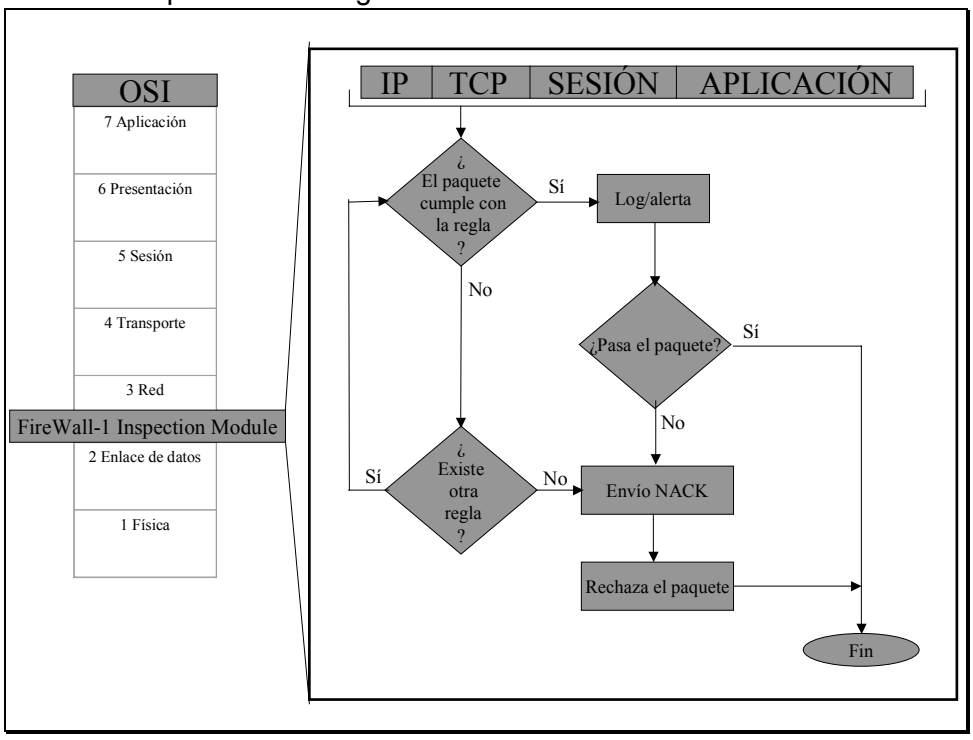

Figura 7. 4.- Firewall-1 Inspection Module

A menos que FireWall-1 verifique que los paquetes cumplen con las políticas de seguridad, dejará que se procesen en los niveles de protocolos arriba del de red. De lo contrario, ningún paquete será procesado en los protocolos más altos.

Conciencia completa del estado

El Inspection Module tiene acceso al mensaje completo. En FireWall-1 se pueden examinar los paquetes desde cualquiera de los niveles de comunicación. El Inspection Module examina las direcciones IP, los números de puertos e información necesaria para determinar si los paquetes cumplen con la política de seguridad. Se crean tablas de conexiones dinámicas en donde se almacena la información de estado y de contexto, las cuales se actualizan continuamente. Estas tablas proporcionan datos acumulativos con los cuales FireWall-1 revisa las comunicaciones siguientes.

El principio de seguridad de FireWall-1 es: “todas las comunicaciones que no están expresamente permitidas se rechazan”. Así, por default, FireWall-1 el tráfico es desechado cuando no ha sido aceptado explícitamente por la política de seguridad y en estos casos también genera alarmas de seguridad en tiempo real.

Protocolos de seguridad “sin control de estado”

Para los protocolos sin control de estado (como UDP y RPC) extrae los datos desde el contenido de la aplicación del paquete y los almacena en las tablas de estado las cuales proporcionan esta información cuando las aplicaciones no pueden hacerlo.

De forma más detallada, cada paquete de solicitud UDP entrante es verificado contra una lista de conexiones pendientes. Sólo se entrega el paquete cuando se trata de una respuesta a una solicitud pendiente. Debido a que no hay una solicitud pendiente, se rechaza el paquete UDP falsificado que pretende ser una respuesta a una solicitud. Si la respuesta no llega dentro del periodo especificado, la conexión se termina.

El lenguaje INSPECT

Utilizando el lenguaje INSPECT, Firewall-1 incorpora reglas de seguridad, conocimiento de la aplicación, información del contexto y datos de las comunicaciones dentro de un sistema de seguridad.

Utilizando la GUI (**G**raphical **U**ser **I**nterface, interfaz gráfica de usuario), INSPECT permite que el sistema se pueda incrementar, con lo cual se pueden agregar módulos, otras aplicaciones, servicios y protocolos al modificar una de las plantillas de script integradas en FireWall-1. Así como la administración es agradable desde esta interfaz intuitiva.

Stateful Inspection (la maquinaria interna)

Stateful Inspection de Check Point es capaz de acceder, analizar y utilizar: la información de los siete niveles en el paquete; el estado derivado de las comunicaciones previas; la información de estado derivada con respecto a otras aplicaciones y la manipulación de la información. Haciendo una comparación con otras arquitecturas de firewall, se tiene:

Capacidad del firewall	Filtros de paquetes	Firewalls de nivel de aplicación	Stateful Inspection
Información de la comunicación	Parcial	Parcial	Sí
Estado derivado de la comunicación	No	Parcial	Sí
Estado derivado de la aplicación	No	Sí	Sí
Manipulación de la información	Parcial	Sí	Sí

Stateful Inspection supera las limitaciones de los dos enfoques antes vistos al proporcionar conciencia completa en el nivel de la aplicación sin romper el modelo cliente/servidor a diferencia de como lo haría un firewall de aplicación. Con Stateful Inspection, el paquete es interceptado al nivel de red, pero después entra en acción el INSPECT Engine, como se ilustra en la figura 7.5. El INSPECT Engine obtiene la información de estado necesaria para la toma de decisión de seguridad de todos los niveles de aplicación y esta información la mantiene en las llamadas tablas de estado dinámico para evaluar los intentos de conexión siguientes.

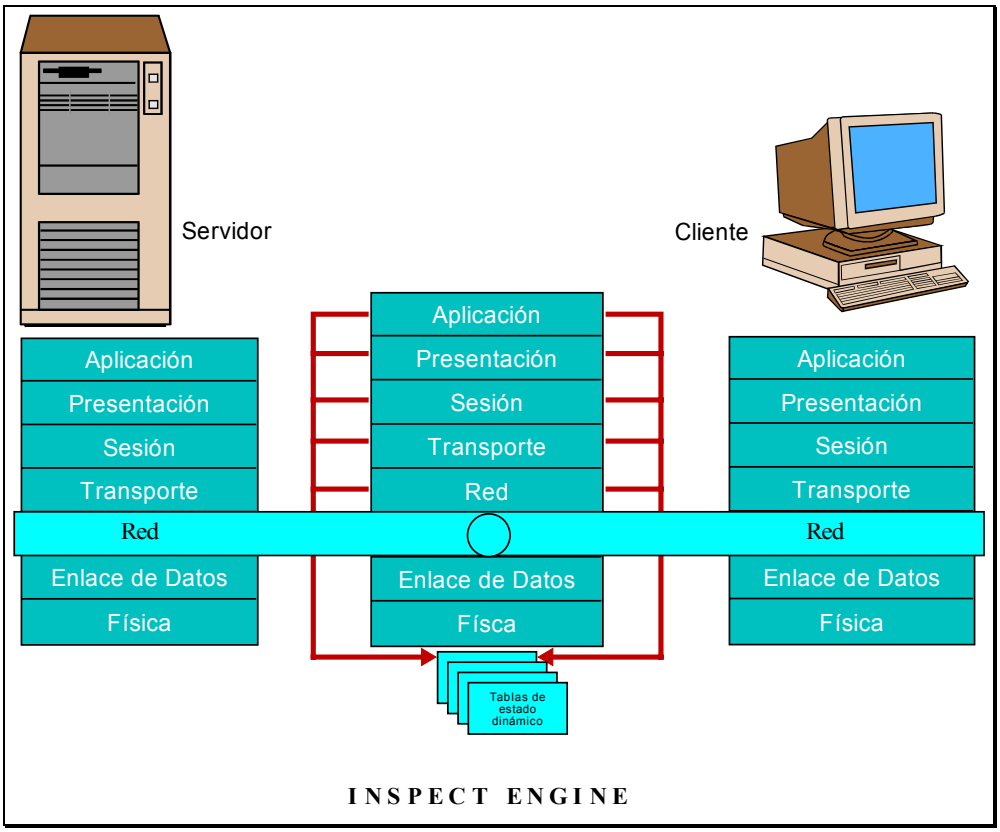

Figura 7. 5.- Inspect Engine

Stateful Inspection extensible

INSPECT Engine aplica la política de seguridad en la gateway en donde reside. Para incorporar nuevas aplicaciones, servicios y protocolos sin necesidad de instalar software adicional, el INSPECT Engine se puede programar utilizando el Lenguaje INSPECT de Check Point. Así para la mayoría de las aplicaciones nuevas, aún las desarrolladas por los usuarios, una modificación de algunas de las plantillas de script integradas en FireWall-1 a través de la GUI puede incorporar el comportamiento relacionado con las comunicaciones de la nueva aplicación.

El INSPECT Engine

El tráfico que pasa a través de las redes es controlado por el INSPECT Engine cuando se instala en una gateway. Debido a que FireWall-1 se ubica en el nivel más bajo del software, al inspeccionar desde este nivel, FireWall-1 asegura que el INSPECT Engine interceptará e inspeccionará los paquetes entrantes y salientes en todas las interfaces. El INSPECT Engine es capaz de activar o desactivar dinámicamente las conexiones según sea necesario; sin embargo el usuario puede desactivarlas si no son necesarias.

Los datos acumulativos de los estados de comunicación y de aplicación, de la configuración de la red y de las reglas de seguridad se utilizan para generar una acción apropiada que puede ser de aceptación, de rechazo, de autentificación o de encriptado de las comunicaciones.

La implementación de Stateful Inspection soporta cientos de aplicaciones, servicios y protocolos predefinidos.

Seguridad de las conexiones para los puertos asignados en forma dinámica

El rastreo simple falla para los puertos donde la asignación es dinámica y con frecuencia este señalamiento cambia a través del tiempo, así que INSPECT Engine de FireWall-1 rastrea en forma dinámica y transparente los números de los puertos RPC utilizando los servicios de mapa de puertos del sistema. El INSPECT Engine rastrea las solicitudes iniciales del portmapper y mantiene un espacio caché que mapea los números de los programas RPC hacia sus números de puerto y servidores asociados.

Cada vez que el INSPECT Engine examina una regla en la cual está involucrado un servicio basado en RPC, consulta al caché comparando los números de puertos del paquete y del caché, y verifica que el número del programa dirigido al puerto sea el que se especifica en la regla. Si el número de puerto del paquete no se encuentra en la caché, el INSPECT Engine genera su propia solicitud para el mapeador de puertos (portmapper) y verifica el número de programa que se encuentra en el puerto.

Entre otras características que se pueden encontrar en esta arquitectura como en la anterior, son la siguientes:

Incorporación de NAT.
Encriptado compatible con IPSec.
Autentificación avanzada.
Administración centralizada.
Supervisión e informes en tiempo real.
Múltiples niveles de registro en bitácoras y alarmas de notificación personalizadas.
Balanceo de carga.

7.6.2. Firewall Labyrinth de CYCON: el sistema “tipo Laberinto”

El firewall CYCON Labyrinth fue el primer sistema “tipo laberinto” que incorporó una NAT (**N**etwork **A**ddress **T**ranslation, translación de direcciones de red) bidireccional con un firewall de intelligent connection-tracking (ICT, rastreo inteligente de conexiones) para crear un dispositivo integrado de seguridad y administración de la red.

Los mecanismos de Stateful Inspection del firewall CYCON Labyrinth soportan todos los servicios basados en IP y siguen correctamente al tráfico TCP, UDP, ICMP y TCP SYN/ACK.

Así las diferencias que se pueden encontrar en esta arquitectura con Firewall-1 es que la autentificación se realiza a nivel de usuario y el soporte es hasta para seis interfaces de red.

Los firewalls Labyrinth utilizan un núcleo BSD Unix reescrito que incorpora estructuras optimizadas de datos y algoritmos diseñados para producir filtrado de paquetes de alta velocidad.

La regla de filtro no acepta los paquetes que se originan desde una interfaz externa que contengan direcciones de origen que coincidan con cualquier IP interna.

Los derechos de acceso posible se definen previamente por el administrador del firewall y pueden ser configurados para que expiren después de que termine un lapso predefinido.

7.63. Guardian Firewall System de NetGuard

La arquitectura del Guardian Firewall System de Netguard Ltd. está basada en un mecanismo original de inspección de estado a nivel MAC que lo vuelve inmune frente a las fallas en la seguridad del sistema operativo.

NetGuard ofrece a los administradores de redes, herramientas para el control de acceso a Internet. Algunas características de las herramientas más relevantes en Guardian son:

Indicador visual de la actividad de los agentes por toda la empresa. Con esta herramienta se puede administrar el firewall, incluyendo el análisis del ancho de banda asignado.

Amplia información de la gateway. Proporciona una interfaz para reunir toda la información de la gateway a través de un Agent Icon extendido. La información que se puede obtener de ahí es: total del ancho de banda disponible, total del consumo de ancho de banda, número de conexiones, número de usuarios activos y número total de usuarios.

La pantalla de supervisión de actividad. La pantalla Activity Monitoring de Guardian permite la autodetección de los usuarios activos.

Monitoreo de la conectividad de un usuario. Al seleccionar el icono de un usuario se puede obtener la información de conexiones de usuario en tiempo real como: Dirección IP y nombre del destino; tipo del servicio en uso; número de bytes recibidos y enviados; tiempo transcurrido con esta conexión; asignación de ancho de banda para cada sesión. La ventana Connection Monitoring permite funciones para que el administrador de la red cierre una conexión activa y permite que pueda crear reglas que determinan las condiciones bajo las cuales podrá operar el usuario.

El comando Cerrar Sesión en un cliente de autentificación. Para permitir la autentificación de los usuarios, Guardian requiere que al usuario se le asigne un periodo para iniciar una sesión y trabajar.

7.6.4. CyberGuard firewall: fortalecimiento del sistema operativo

La edición 3 de Cyberguard firewall es una solución de software e incluye un sistema operativo basado en UNIX, software integrado para la seguridad de la red y un administrador remoto basado en GUI.

La versión 4.2 combina el filtrado de paquetes y la seguridad proxy para las aplicaciones en una solución que se puede personalizar con el fin de permitir las comunicaciones bidireccionales, sólo de entrada o de salida mientras se bloquean los comandos de alto riesgo.

El sistema operativo confiable

En la solución de CyberGuard Firewall, el sistema operativo ha sido fortalecido con medidas de seguridad, por lo que los usuarios o las solicitudes sin autorización no podrán penetrar en el sistema operativo ni en la red. El sistema operativo de alto desempeño cuenta con la capacidad de manejar altos niveles de transferencia de datos sin presentar fallas que consuman mucho tiempo. CyberGuard está construido sobre un sistema operativo seguro que utiliza una extensión de seguridad para múltiples niveles llamada Multiple Virtual Secure Environment (MVSE, Ambientes Seguros Virtuales Múltiples). MVSE iguala el acceso a los datos con los privilegios de los usuarios, lo cual evita el robo o el acceso no autorizado a los datos sensibles a través de redes.

MVSE habilita a una red física sencilla para que pueda ser dividida en múltiples redes virtuales de acuerdo al nivel de seguridad deseado. Al mismo tiempo, los usuarios pueden dividir a sus equipos servidores de datos en múltiples servidores de datos virtuales, en donde cada uno tiene un nivel único de seguridad. MVSE asegura que los datos de un nivel de seguridad determinado sólo viajarán a través de redes con el mismo nivel de seguridad.

Interfaz gráfica de usuario (GUI)

CyberGuard Firewall en la plataforma Intel ofrece una GUI remota con una característica opcional que permite que un administrador controle y supervise en forma centralizada múltiples instancias de CyberGuard Firewall. Esta característica

proporciona un entorno gráfico integrado para la instalación, configuración, supervisión e informes.

Tecnología de reglas de control dinámico de estado

Una parte del enfoque de seguridad de CyberGuard radica en su tecnología de reglas de control dinámico de estado que extienden las capacidades comunes del filtrado de paquetes.

Con la tecnología de reglas de control dinámico de estado, cuando CyberGuard trabaja en la plataforma Intel puede identificar ataques como suplantación.

Este firewall para las plataformas Intel se ofrece en tres configuraciones:
Una opción de nivel básico que soporta 50 usuarios o menos.
Una opción para grupos de trabajo que soporta de 51 a 250 usuarios.
Una opción empresarial con soporte para un número ilimitado de usuarios.

7.6.5. El firewall de raptor: una arquitectura de nivel aplicación

Raptor Firewall 6.0 de AXENT para Windows NT y Solaris, contiene un conjunto de aplicaciones proxy. Basada en la arquitectura de firewall de nivel de aplicación, la familia Eagle incluye un conjunto de componentes modulares de software que proporciona seguridad de red en tiempo real para Internet, para los grupos de trabajo, para el equipo móvil y para los dominios de oficinas remotas dentro de una empresa.

Cumplimiento de la seguridad en todos los niveles de la red

Raptor Firewall ofrece una fuerte integración con Microsoft Windows NT empleando la Consola de administración basada en la Consola de administración de Microsoft para lograr una administración escalable.

Raptor Firewall ofrece soporte a alta disponibilidad utilizando Microsoft Cluster Server (MSCS) y productos de terceros fabricados por Veritas.

Como Eagle trabaja en los siete niveles de una aplicación basada en la red, cuenta con el acceso a toda la información contextual que se requiere para tomar las decisiones de autentificación y la autorización, incluyendo:

- El tipo específico de aplicación que se utiliza.
- Los comandos y los datos específicos de la aplicación que se activan o se desactivan.
- Los usuarios, grupos o periodos de uso permitidos para el servicio.
- Rangos de tiempo y fechas.
- Información de la autentificación.
- Registro de todas las conexiones permitidas o no.
- Mensajes de alerta a través de correo electrónico.

Raptor define cinco dominios de seguridad de la red para promover un enfoque integrado con el fin de proteger a la empresa:

- Seguridad para Internet.
- Seguridad para grupos de trabajo.
- Seguridad para usuarios móviles.
- Seguridad para el centro remoto.
- Seguridad integrada para la empresa.

Los firewalls de filtrado de paquetes autorizan el paso de los paquetes IP sobre una base de coincidencia con las reglas al primer intento.

A diferencia de los firewalls de filtrado de paquetes, el Eagle Firewall:

- Todas las conexiones son rechazadas a menos que se permitan explícitamente.
- Activa en forma automática la supervisión de actividad sospechosa.
- Realiza un registro exhaustivo para todas las conexiones.
- Coloca controles de acceso y restricciones de servicio muy detalladas.
- Activa la administración de reglas tipo “mejor coincidencia”.

El enfoque de mejor coincidencia de Eagle es que Eagle rechaza todo el tráfico de la red excepto el que debe aceptar explícitamente. En segundo lugar, las reglas que aplica el Eagle no dependen del orden, por lo que siempre elige una regla específica para el intento de conexión con el que se enfrenta. Para asegurarse de que la regla elegida es específica, Eagle siempre aplica el criterio de mejor coincidencia para aceptar o rechazar la conexión.

Mejoras en la administración del Raptor firewall 6.0 para NT

La Raptor Manager Console (RMC, Consola de Administración de raptor) ofrece administración escalable. RMC, empleando el marco de referencia de MicroSoft Management Console (MMC) en Windows, simplifica la administración al recolectar y desplegar una lista completa de los firewalls administrados en una ventana y los datos específicos del firewall en un panel adyacente. Una consola de administración local también se incluye para los firewalls Raptor basados en Unix.

Dependencia en proxys dedicados a la seguridad

El Eagle utiliza proxys para las aplicaciones con el fin de examinar cada intento de pasar los datos dentro o fuera de la red. Estos proxys ofrecen:

- Registros extensos de todas las actividades.
- Control detallado del sentido de comunicación del servicio, como las operaciones PUT y GET de FTP.

Utilización de la familia de firewalls Eagle de Raptor

Configuración gráfica de las políticas: Con la GUI de Eagle se utilizan ventanas para escribir las reglas y para definir los sistemas internos y externos, para especificar a los usuarios del firewall, para crear plantillas de autentificación y para realizar otras funciones. La ventana de supervisión de Eagle ofrece un panorama general de todos los intentos de conexión dentro de la red. La ventana de archivo de archivo de registro despliega información estadística de todas las conexiones en un instante.

Administración consistente: local o remota: Raptor ofrece la capacidad de Secure Remote Login (SRL, Sesiones Remotas Seguras) que permite que los administradores accedan en forma remota al sistema operativo para la configuración y el mantenimiento. SRL establecen una sesión TELNET encriptada y autentificada con el sistema del firewall.

Flexibilidad para permitir acceso transparente: Este nivel de acceso, permite que los usuarios "vean" y aparentemente se conecten directamente a ciertos sistemas. Estas conexiones siguen siendo manejadas por medio de un proxy por parte del Eagle, el cual continúa realizando registro en bitácoras y alertas de operaciones.

Redirección de direcciones: Para poder permitir a los usuarios que accedan a los datos de ciertos sistemas internos mientras que protege las identidades y las direcciones de estos sistemas.

Raptor Firewall soporta métodos populares para autentificación avanzada. Raptor Firewall también soporta contraseñas, NT Domain, TACACS y RADIUS.

La arquitectura proxy de aplicación de Eagle hace que el procesamiento de transacciones sea un mecanismo veloz, debido a que autoriza las conexiones al nivel de aplicación, cuenta con acceso a toda la información contextual en cada intento de conexión.

Control detallado de los túneles de VPN. La capacidad para aplicar filtros de paquetes dentro de túneles de VPN configurables, les proporciona a los administradores de Eagle un control detallado de los tipos y sentido del tráfico que se puede pasar entre los hosts. Este control permite especificar los niveles apropiados de encriptado para cada aplicación colocada en un túnel.

Capacidad integrada de bloqueo en la web. El software WebNOT integrado de Eagle ofrece la habilidad de restringir la navegación en al web en sitios que contienen material cuestionable.

En el capítulo siguiente se establecen en base a este estudio las particularidades con las que debe contar el firewall de la empresa eléctrica.

7.7. Conclusiones

Antes de decidir que la solución es la implantación de un firewall se analiza la topología de la red para determinar si es adecuada para los componentes de ésta.

Al analizar el tráfico que pasa por el firewall, éste resultó ser la solución a la mayor parte de la inseguridad informática, sin embargo también tiene sus desventajas. A la primera de ellas, que es el confiarse sólo de la tecnología, siempre se le dio un mayor énfasis. Por lo que el concientizar en cultura informática a los usuarios, y ellos den un buen uso a las políticas de seguridad debido a la importancia que tienen para lograr una buena implementación de un sistema integral de seguridad.

Las ventajas que brinda un firewall ante redes grandes como lo es la del caso de estudio es que brindan la facilidad de manejo, lo cual al reducir complejidades en la administración del sistema, también se reducen las vulnerabilidades en éste. Por ello tanto las políticas de alto como de bajo nivel deben ser flexibles y realistas.

El componente más importante de un firewall son las políticas de acceso, mientras que la autentificación avanzada, el filtrado de paquetes, las gateways de aplicación y otros módulos son los componentes necesarios para implementar y hacer cumplir la política.

El problema de la creación de passwords débiles se soluciona con tokens siendo un tipo de autentificación avanzada. Éstos generan un password distinto cada minuto, lo que garantiza que no se utilice nuevamente y éste no puede ser monitoreado en esa brevedad de tiempo.

El mejor firewall que se ajusta de acuerdo a los componentes de la red y a las necesidades de la empresa, como lo son el ocultar la topología, el requerir autentificación avanzada, y obtener la facilidad de administración con el fin de evitar complejidades y vulnerabilidades y brindar transparencia al usuario entre otros es clasificado como un firewall híbrido.

La razón para proponer una solución de firewall híbrido a las necesidades de la empresa eléctrica radica en que:

- La empresa hasta el momento de este estudio no contaba con ningún tipo de seguridad y es este tipo de firewall el que se adapta, de mejor manera, a la topología de red de la empresa eléctrica y además cumple con las necesidades de seguir el rastro a todos los paquetes de la familia TCP/IP en todas las capas.

De este capítulo se desprende la necesidad de diseñar el sistema de seguridad bajo un patrón de firewall centralizado, pues al ser diseñado de esta manera permite un ahorro significativo a la empresa eléctrica.

El diseñar un firewall centralizado, además de la ventaja antes mencionada, también tiene características adicionales tales como:

- Creación de bitácoras de acceso y uso de la red de cada uno de los usuarios. Mismos que brindan al administrador herramientas que le permitan proteger y verificar el buen uso de los recursos que brinda la red de la empresa eléctrica.

Algunas otras características del firewall que deben ser consideradas como esenciales para contar con una red confiable son:

- El uso de NAT que permite una mayor protección de la Intranet.
- Permitir un encriptado compatible con IPSec, mismo que permite la creación de VPN, que a la empresa eléctrica le reditúa en un ahorro considerable ya que no rentaría canales punto a punto.
- Y el balanceo de carga debido a que se trabaja con información en tiempo real.

Además, las zonas se tienen claramente identificadas que son la fría y la caliente, con el fin de brindar una mayor protección se determina el uso de una zona más, la zona desmilitarizada. En ésta se agregan los módulos que ayudan a la formación de un sistema integral de seguridad.

Capítulo 8
Diseño del sistema firewall

8.1. Consideraciones de diseño

Después de analizar algunos de los diferentes tipos de firewall que existen en el mercado es necesario establecer las funciones que debe de tener éste para proteger los sistemas de cómputo y comunicaciones de la empresa eléctrica.

Derivado del estudio precedido, algunas de las funciones fundamentales que se deben buscar en un firewall son las siguientes:

- Debe ser capaz de aceptar la política de diseño, que fue establecida específicamente para la empresa, sin forzarla y debe poder permitir servicios de red y aun así mantener el nivel de seguridad establecido para la compañía.

- Debe ser capaz de funcionar en forma continua sin interrupciones de este sistema ya que no se puede interrumpir el control y la supervisión de la red eléctrica nacional, por lo que deberá contar con alta disponibilidad.

- Debe ser flexible y escalable. Debe poder complementarse con módulos para que se ajuste a las necesidades de la política de seguridad de la compañía y adecuarse a los cambios organizacionales como el ser capaz de adaptarse a múltiples plataformas e instancias dentro de una red protegida. Esto incluye los sistemas operativos, las máquinas y las configuraciones para la seguridad.

- Debe tener medidas de autentificación avanzadas y debe ser expansible para acomodarse a estas autentificaciones en el futuro. Tales como autentificación de contraseñas y tarjetas de control de acceso.

- Debe emplear técnicas de filtrado de paquetes que permitan o nieguen el permiso a servicios específicos en los diversos sistemas según se requiera.

- La forma de configurar el filtrado de paquetes IP debe ser flexible, amigable y capaz de seleccionar tantos atributos como sea posible, incluyendo las direcciones IP (origen y destino), el tipo de protocolo, los puertos TCP/UDP (origen y destino), y las interfaces (de entrada y salida.)

- Debe contener la capacidad de centralizar el acceso SMTP con el fin de reducir las conexiones SMTP directas entre el sitio y los sistemas remotos. Esto dará como resultado una administración centralizada del correo electrónico del sitio.

- Debe adaptar el acceso público al sitio, de tal manera que los servidores de información pública queden protegidos mediante el firewall, pero puedan estar separados de los sistemas del sitio que no requieren acceso público.

- El firewall debe poseer mecanismos para registrar el tráfico y la actividad sospechosa, así como debe proporcionar informes estadísticos y de alarma. Por otro lado que contenga mecanismos para la reducción de bitácora, siendo así legibles y comprensibles.

- Si el firewall requiere un sistema operativo comercial, abierto como UNIX o NT, debe contar con una versión segura del sistema operativo en el cual funcionará el firewall, junto con otras herramientas de seguridad, según sea necesario para asegurar la integridad del servidor que opera como firewall.

- Debe desarrollarse de una manera tal que su solidez y exactitud puedan verificarse a través de auditorías. Así como debe tener un diseño simple, para facilitar su comprensión y mantenimiento.

- Debe tener garantía independiente acerca de la tecnología relevante del firewall que responda con el cumplimiento de las especificaciones, y de que se instaló en forma adecuada. Además, como es un sistema integrado con diferentes elementos tales como antivirus, autentificado dinámico, detector de intrusos el proveedor deberá conocer y ser certificado en este tipo de herramientas cualquiera que sea la marca ya que la importancia de los sistemas que protege son de alta seguridad ya que el control de la red eléctrica nacional es sustantiva para el funcionamiento de empresas, fabricas, alumbrado, suministro de energía doméstica, etc. En conclusión la instalación y puesta en marcha de este sistema debe ser realizado por expertos en la materia.

Consideraciones a las necesidades y usuarios:

- Debe existir transparencia a los usuarios ya que si se adopta un sistema confuso, los usuarios desarrollarán una resistencia en contra de él y buscarán formas de saltarse las políticas.

- Tanta tecnología requiere de un buen servicio de mantenimiento. Por ello debe contener soporte técnico, como el ofrecimiento de apoyo por parte del equipo técnico para la instalación, el uso y el mantenimiento, además de cursos de capacitación externos.

- Deberá ser lo bastante rápido como para que los usuarios no se quejen por la revisión de paquetes.

Este control, protege a la compañía de amenazas a la seguridad al declarar y hacer cumplir las especificaciones de lo que puede salir y entrar de la Intranet. Un elemento clave del control de acceso es estar consciente de todos los servicios y las aplicaciones subyacentes.

Existen otras cuestiones pero éstas ya se aplican de acuerdo a las situaciones de cada sitio. Hay que recordar que Internet es una red en constante cambio y en consecuencia pueden hacerse evidentes nuevas vulnerabilidades. La predisposición a los cambios es importante para una solución firewall así como se advirtió anteriormente con las políticas de seguridad.

8.2. Módulos adicionales a considerar

El firewall también debe contar como se mencionó con módulos adicionales a los ya especificados. Entre estos se encuentran:

- Módulo VPN para permitir una comunicación segura y cifrada de un firewall a otro.
- Módulo antivirus, que puede ser una adición del propio firewall o una liga con productos de terceros.
- Módulo de filtrado de URLs, para restringir la salida a sites no deseados.
- Módulo de filtrado de código portátil, permite revisar programas o componentes dañinos hechos en Java o ActiveX.
- Módulo detector de intrusos, detecta tareas sospechosas.
- Módulo de traducción de direcciones o NAT, hace la conversión entre las direcciones IP de la red de la empresa y las direcciones IP homologadas de Internet.
- Sistemas de autentificación y autorización, para permitir sólo usuarios autorizados.

Restricciones de diseño:

Para definir el tipo de firewall a utilizar en esta empresa eléctrica primero se analizó la topología de red de cómputo, en el que se determina el alcance de red y se hacen notar los equipos a asegurar.

De acuerdo a las políticas de seguridad de alto nivel previamente formuladas se obtienen las de bajo nivel para implantar al firewall.

El sistema debe ser escalable y permitir el agregar aplicaciones, servicios y protocolos.

El firewall a elegir debe poder interactuar con otros mecanismos de seguridad como lo son IDS (Intruder Detection System), antivirus, autentificación avanzada, VPNs, control de páginas web, encriptado compatible con IPsec para VPNs.

La acción que el firewall debe usar por ser la más conveniente de acuerdo a las políticas de seguridad es el: Negar cualquier servicio a menos que se permita expresamente.

En el diseño del firewall se agrega un ruteador para filtrar y bloquear todos los paquetes cuyas direcciones se originaron desde el interior de la red protegida.

El tipo de firewall a usar debe ser híbrido. Éste debe poder analizar todos los niveles de comunicación de los paquetes.

El firewall debe soportar todos los servicios basados en IP y seguir correctamente el tráfico stateless. Así como, debe permitir ocultar las direcciones internas de las externas no confiables.

También debe registrar las conexiones en modo regular y contener alarmas acerca de intento de conexiones no deseadas.

El firewall deberá soportar la arquitectura de cluster; para un balanceo de carga y seguridad del mismo con alta disponibilidad así como a los módulos de seguridad integrados. Se agrega un firewall por sistema crítico.

Las especificaciones técnicas para el sistema de seguridad de la empresa eléctrica son las siguientes:

8.3. Requerimientos mínimos obligatorios para la solución

Para ello es necesario adquirir e implantar la infraestructura que nos proporcione la seguridad requerida.

La solución debe incluir:

- Lo más reciente en hardware, software y servicios necesarios para la solución con las respectivas licencias del fabricante.
- Deberá contar con alta disponibilidad.
- Documentos en papel, medio magnético y/u ópticos y electrónicos.
- Personal calificado para la implantación de la solución.
- Diseño de la solución y proyecto detallado.
- Servicios de auditoría.
- Infraestructura de hardware y software, y desarrollo del portal.
- Implantación de los servicios que requiere la empresa eléctrica.
- Capacitación al personal que designe el centro de control de la empresa eléctrica.
- Garantía.
- Soporte técnico.

8.4. Diseño del firewall para la empresa eléctrica

El objetivo del diseño es proteger los sistemas de cómputo, y datos del centro de control de la empresa eléctrica contra accesos no autorizados para mantener la confidencialidad e integridad de los datos. Controlar el tráfico a o desde el centro de control de la empresa eléctrica por el sistema de seguridad propuesto.

8.4.1. Descripción de la arquitectura

La arquitectura de seguridad debe ofrecer doble nivel de validación con dos firewalls, basados en sistemas de alta disponibilidad. Un firewall a la entrada del centro de control de la empresa eléctrica y otro firewall para acceder a cada uno de los sistemas críticos:

- Sistema de administración de datos en tiempo real
- Sistema de administración eléctrica
- Sistema SM
- Sistema SMAR
- Sistema de gestión de flujo de trabajo

- Se deberá llevar a cabo la definición de políticas de acceso en cada uno de los segmentos de red a los que los sistemas críticos se encuentren conectados así como para el intercambio de información de dichos sistemas.

- Para la publicación de información del centro de control de la empresa eléctrica hacia Internet y/o Intranet se deberá desarrollar un portal, en un servidor WEB con una base de datos donde únicamente se depositará la información debida de los sistemas informáticos.

- Para el SMAR se asignará un método de autentificación dinámica para usuarios externos y una autentificación estática para usuarios internos. La información propia y confidencial de mercado debe depositarse únicamente en el Servidor de SMAR de manera segura. Cualquier otra conexión al resto de los Sistemas de Información empleará un mecanismo de autentificado estático.

- La arquitectura debe garantizar que ningún usuario pueda acceder a la red del sistema de administración de datos en tiempo real. Se debe asegurar que los usuarios tanto de Internet como de la Intranet de la empresa eléctrica que lo requieran sólo puedan depositar y/o consultar información al Servidor WEB del centro de control de la empresa eléctrica y a la base de datos.

- Los usuarios tanto de Internet como de Intranet de la empresa eléctrica sólo podrán realizar consultas de información a nivel Servidor WEB del centro de control de la empresa eléctrica.

- La arquitectura de seguridad deberá contar con una GUI amigable para su administración.

- Todos los componentes de hardware y software considerados dentro de los requerimientos que serán parte de la arquitectura deben contemplar servicios de soporte y mantenimiento renovables anualmente y dentro de un esquema de 7*24 incluyendo servicios de asesoría técnica vía telefónica, correo electrónico y en sitio.

- Se debe brindar capacitación técnica adecuada al personal del centro de control de la empresa eléctrica para llevar a cabo la administración y soporte técnico en el desarrollo y mantenimiento de la implantación.

8.4.2. Módulos para integrar en la arquitectura de seguridad.

- La arquitectura de Seguridad estará basada en una arquitectura SVN (Secure Virtual Network). Con la administración centralizada.

Firewall

- El firewall deberá poder analizar el mensaje en bruto, tener pleno conocimiento en todo momento del estado de las conexiones y aplicaciones para poder realizar un filtrado de contenido. Se debe tener el mínimo acceso al sistema operativo del firewall. El firewall deberá manejar el concepto de VPN, incluyendo la ocultación de IPs. La plataforma del firewall deberá poder integrar los controles de acceso, autentificados avanzados y encriptamiento.
- El firewall deberá permitir la realización de definición y creación de políticas de seguridad para filtrar a la familia completa de TCP/IP.
- La tecnología de autentificado permitirá verificar la identidad del usuario que esté haciendo uso de la VPN.
- La tecnología de firewall deberá soportar diversos métodos de autentificado, tanto estáticos como dinámicos.
- El proceso de encriptamiento deberá permitir que una vez que los usuarios del centro de control de la empresa eléctrica sean autentificados, la solución VPN proteja la privacidad de los datos que son transmitidos, incluyendo para esto el soporte estándar IPsec.

Alta disponibilidad

- La solución deberá trabajar bajo el concepto de alta disponibilidad.

Creación de reportes

- Deberá tener un módulo de creación de reportes en el cual se pueden analizar en bitácoras la información detallada. En estas bitácoras se deberá incluir información de intentos de acceso no autorizados, señalándolos como alarma.

Detección de intrusos

- Este módulo se deberá agregar para que de manera automática y en tiempo real se lleve a cabo el monitoreo del tráfico de la red, incluyendo eventos de auditoría y registro de bitácoras, reconfiguración del firewall para impedir cualquier ataque asociado con los protocolos TCP/IP notificando inmediatamente a los administradores. Estos módulos se deberán localizar en la entrada al sitio así como en cada uno de los equipos críticos.

Control de contenido

- Este mecanismo debe permitir el control de recursos URL con un control de accesos granular.

Protección antivirus

- Se debe integrar este mecanismo en la puerta de enlace de Internet para no dejar fluir tráfico con virus. Debe evitar el spam y realizar filtrado de mensajes con base al análisis de contenido. Esta protección antivirus también debe

prevenir de software malicioso reciente con la opción de deshacer cambios realizados por el software no deseado.

Autentificado dinámico

- Este sistema de seguridad deberá permitir a cualquier usuario el poder conectarse hacia la red con tarjetas de passwords de una sola vez (tokens). El autentificado dinámico deberá incluir: clave de asignación dinámica cada 60 segundos, con 6 dígitos y una duración de 3 años.

8.5. Desarrollo del portal del centro de control de la empresa eléctrica con acceso controlado a las aplicaciones.

El desarrollo del portal está asignado a los programadores de la empresa eléctrica, sin embargo aquí se presentan las características de éste ya que está aunado al proyecto de seguridad.

Seguridad de acceso al portal

- Se requiere que a nivel aplicativo se contemplen los certificados digitales tanto en el Servidor Web como en los clientes bajo los estándares de Infraestructura de clave pública (PKI, por sus iniciales en inglés), para de esta forma contar con un canal seguro desde el Servidor Web al usuario final cuando se requiera.
- La solución debe incluir facilidades de administración de usuarios: altas, bajas y cambios; así como para definir roles de usuarios.
- La transferencia de información entre los usuarios que cuentan con una conexión segura y el Web Server, deberá estar encriptada con la llave más larga permitida en México.
- La solución deberá contemplar al menos un certificado digital para el portal del centro de control de la empresa eléctrica emitido por una autoridad certificadora. En el proceso de obtención del certificado digital el centro de control de la empresa eléctrica proporcionará los datos requeridos por la autoridad certificadora.
- La solución deberá incluir al menos 250 certificados digitales para las plantas generadoras de energía.

Estadísticas

- Con el fin de saber la eficacia de las políticas de seguridad y de los sistemas críticos se debe incluir un sistema de estadísticas que permitirá evaluar puntos como los que siguen:

- Qué páginas son las más consultadas y por quiénes.
- Accesos por página, qué páginas son las menos consultadas y desde cuando.
- Qué software para navegar utilizan los usuarios y que versión.
- Qué equipos están accediendo, desde cuando y en qué momento lo dejaron de hacer.
- Cuál es el tráfico que genera en la red en un período determinado, cuántos archivos se transmitieron, en cantidad y en MB.
- Estadísticas de transmisión por día y hora.

Diseño

- Definición de un estilo acorde a la personalidad del centro de control de la empresa eléctrica, bajo el cual se publicará la información en el portal. La definición de estilo incluye:
  - Restricciones en uso de logotipos, e imágenes institucionales
  - Delimitación de uso de fuentes primarias y secundarias.
  - Delimitación de uso de colores, fondos e imágenes en general.
  - Restricciones en el uso de animaciones.

Categorización de la información

- La información publicada en el portal deberá estar categorizada para facilitar la comprensión de contenido, búsqueda de información, publicación de información y mantenimiento a las publicaciones.

Publicación de información

- El portal contará con los mecanismos necesarios para asegurar que las áreas de control puedan publicar en el portal de centro de control de la empresa eléctrica.

Software del portal para su construcción

- El software de construcción del portal debe estar basado en estándares JAVA más recientes. Contar con soporte para las especificaciones EJB 1.1 (Enterprise Java Beans).

Debe incluir los siguientes componentes:

- Facilidades de programación en JSP (Java Server Pages)
- Servidor de Servlets 2.1 o mayor.
- Servidor JSP 1.0 o mayor.
- Servidor de aplicaciones de arquitectura escalable con soporte para COM, DCOM, RMI y HTTP. Con facilidades de replicación automática, balanceo de carga, failover automático y seguridad basada en roles.
- Drivers JDBC 1.0 o 2.0 para DB2, Informix y Oracle.
- Deberá incluir licencias para un mínimo de 500 usuarios de Internet.

Software de base de datos

- Para la construcción del portal se debe incluir un manejador de base de datos con las siguientes características y facilidades:
  - Relacional.
  - Manejo de procedimientos almacenados
  - Facilidades para auditar usuarios.
  - Manejo de grandes volúmenes de información (del orden de Gigabytes.
  - Facilidad para respaldar bases de datos estando la base de datos activa.
  - Soporte a comunicación ODBC y JDBC.
  - Entorno operativo Unix
  - Deberá incluir licencias para un mínimo de 25 usuarios.

Aplicación despacho

- Esta parte del portal debe ofrecer:
  - Facilidades para publicar los requerimientos de energía a ser consultados por las plantas de energía.

- Facilidades para que la ofertas de las plantas, a través del servidor compartido, las reciba.
- Seguridad para que una planta no se entere de la oferta de las demás.
- Facilidades para publicar los resultados consultando en línea el repositorio compartido de datos.
- Seguridad par que los resultados solamente puedan ser vistos por la planta de energía a la cual va dirigida el resultado.

Servidor de datos para el portal

- La solución del portal deberá considerar la interfaz necesaria para publicar y o depositar datos del servidor de base de datos del centro de control de la empresa eléctrica existente. El servidor de base de datos centro de control de la empresa eléctrica es actualizado por sistemas internos.
- El centro de control de la empresa eléctrica proporcionará los modelos de datos para su utilización.

Seguridad de acceso a datos y aplicaciones

- El portal solamente accederá a la información del repositorio de datos para leer y construir respuestas.

Servicio

- El desarrollo del portal deberá incluir el servicio de soporte y mantenimiento en sitio por un año después de liberada la funcionalidad del portal. Entre las funciones a realizar están las siguientes:

- Mantener el software del servidor web en operación óptima.
- Participará de mantenimientos preventivos y correctivos.
- Mantener los niveles de servicio acordados.
- Elaborar reportes periódicos tales como bitácoras.
- Mantener y desarrollar nuevas formas y procesos de publicación de información.

8.6. Decisión de compra o desarrollo.

La decisión de comprar o construir un firewall depende de los recursos con los que dispone la compañía, tales como: el tiempo y la experiencia con la que se cuenta para diseñar, programar e implementar, el dinero para equipos y salarios que se requieren para invertir en el sistema de seguridad. De esta forma en el proceso de elección para saber si se debe construir el firewall dentro de la empresa o adquirir, se debe considerar si se cuenta con los medios necesarios para equipar, configurar, auditar, mantener y actualizar al sistema del firewall.

Así que, después de evaluar sus recursos humanos y económicos, la empresa concluye que los administradores no cuentan con el tiempo suficiente para desarrollar, implementar y administrar el firewall, ya que se requiere de manera inmediata proteger la información, por ello los fabricantes de decisiones optan por adquirir un firewall comercial. Por lo tanto, dicha compra se llevó acabo de una licitación atendiendo a cada una de las especificaciones mencionadas en los apartados anteriores.

En la siguiente sección se realizarán las especificaciones técnicas que incluyen la solución comercial.

8.7. Especificación técnica para la adquisición de firewall de la compañía eléctrica.

Tomando lo establecido en el estudio anterior se realizó el siguiente documento para la adquisición del sistema que protegería a los sistemas de información crítica de la compañía eléctrica.

Firewall primario (el nombre de "firewall primario" es únicamente para identificarlo dado que el concepto de cluster con balanceo de carga y tolerancia a fallos trabaja junto con otro firewall como si fuera únicamente uno solo.)

Este contiene las siguientes características en software:
- Módulo integrado de VPN
- Métodos y esquemas de autentificado
- Controles de acceso
- Incorporación de scaneo de virus
- Alta disponibilidad
- Network Address Translate (NAT)
- Detector de ataques
- Creación de reportes
- Interoperabilidad con cualquier módulo adicional (de seguridad)

Contiene las características en hardware:
- Un servidor con sistema operativo Unix.

Firewall secundario (el nombre de "firewall secundario" es únicamente para identificarlo dado que el concepto de cluster con balanceo de carga y tolerancia a fallos trabaja como si fuera únicamente un solo firewall.)
Este contiene las siguientes características en software:
- Módulo integrado de VPN
- Métodos y esquemas de autentificado
- Controles de acceso
- Incorporación de scaneo de virus
- Alta disponibilidad
- Network Address Translate (NAT)
- Detector de ataques
- Creación de reportes
- Interoperabilidad con cualquier módulo adicional (de seguridad)

Contiene las características en hardware:
- Un servidor con sistema operativo Unix.

Módulo control de URL
Contiene software para:
- Comunicación con firewalls
- Bloqueo de http

- Bloqueo de contenido

Módulo de autentificado dinámico
Contiene software para:
- Clave de asignación dinámica

Módulo antivirus
Contiene software para:
- Bloqueo de software maligno en SMTP, FTP y HTTP.

Módulo IDS
Contiene software para:
- La detección de intrusos.

Módulo de creación de reportes
Contiene software para:
- La creación de historiales en bitácoras.

Cinco firewalls para sistemas de información internos en software:
- Módulo integrado de VPN
- Métodos y esquemas de autentificado
- Controles de acceso
- Incorporación de scaneo de virus
- Network Address Translation (NAT)
- Detector de ataques
- Creación de reportes a través de bitácoras
- Interoperabilidad con cualquier módulo adicional (de seguridad)

Contiene las características en hardware:
- Cuatro servidores con sistema operativo Unix.

Nueve computadoras de escritorio
- Sistema operativo Windows NT.

Portal del centro de control:
Dos servidores en cluster.
Operación en alta disponibilidad

8.8. Características técnicas de la arquitectura de seguridad del centro de control de la empresa eléctrica a nivel software

CANTIDAD	SOFTWARE	CONCEPTO
1	Firewall primario y secundario Salida a Internet.	*Licencia ilimitada de usuarios. *Incluir Master CD-ROM y documentación. *Software suscripción para todos los productos (upgrades, service pack, patches) *Creación de VPN's entre firewalls y clientes. *Métodos de autentificación por usuario, cliente y sesión. *Controles de acceso que soporte más de 150 aplicaciones, servicios y protocolos. *Esquemas de autentificado por S/Key, SecurID, Tacacs, Radius y OS password. *Facilidad para incorporar scaneo de virus a través del protocolo CVP (Content Vectoring Protocol) junto con un Módulo de Antivirus adicional el cual deberá ser parte de la solución propuesta. *Utilización de NAT. *Alta disponibilidad utilizando fullcluster para balanceador de tráfico de carga. *Detección de ataques utilizando Elliptic Curve Cryptography 113. *Reporteo de los archivos de bitácora, generados en modo texto y gráfico de correos, servidores Web, impresoras, servidores FTP. *Instalación, configuración, puesta en marcha y entrenamiento práctico hacia el Firewall. *Interoperatibilidad con cualquier módulo adicional (encriptado, controlador URL's, antivirus, autentificado dinámico con tokens, alta disponibilidad, otros.) **CARACTERÍSTICAS GENERALES** * El software deberá contar con soporte técnico en el país * El tiempo de respuesta en el soporte deberá ser de 1 hora vía telefónica y correo electrónico, 4 horas en site. * Contar con la asesoría para la administración de cualquier módulo adicional (controlador URL's, antivirus, encriptamiento, autentificado dinámico, etc.) * Se deberán poder integrar módulos de otros fabricantes. * Garantía y actualizaciones por un año en los productos y servicios.

CANTIDAD	SOFTWARE	CONCEPTO
1	MÓDULO CONTROL DE URL	Licencia para 500 usuarios. Incluir: Master CD-ROM y documentación. Software de suscripción (upgrades, service pack, patches). Comunicación con firewall's a través del protocolos UFP. Bloqueo de http. Base de datos mayor a 1000000 de URL's. Bloqueo de contenido por usuario, grupo, por tiempo. Instalación, configuración, puesta en marcha y capacitación. Garantía y actualizaciones por un año en los productos y servicios.
1	MÓDULO DE AUTENTIFICADO DINÁMICO	Licencia para 100 usuarios. Incluir: Master CD-ROM y documentación. Un año de updates vía Internet. 100 tokens (25 estándar y 25 Key Fob para autentificación). Clave de asignación dinámica cada 60 segundos con 6 dígitos y duración de 3 años. Instalación, configuración, puesta en marcha y capacitación. Garantía y actualizaciones por un año en los productos y servicios.
1	MÓDULO ANTIVIRUS	Licencia para 500 usuarios Incluir: Master CD-ROM y documentación. Un año de updates vía Internet. Comunicación con firewall a través del protocolo CVP Instalación, configuración, puesta en marcha y capacitación. Garantía y actualizaciones por un año en los productos y servicios.
1	MÓDULO IDS	Incluir: Master CD-ROM y documentación. Un año de updates vía Internet. Instalación, configuración, puesta en marcha y capacitación. Garantía y actualizaciones por un año en los productos y servicios.

CANTIDAD	SOFTWARE	CONCEPTO
5	FIREWALLS PARA SISTEMAS DE INFORMACIÓN INTERNOS	Licencia para 250 usuarios. Incluir: Master CD-ROM y documentación. Software subscripción para todos los productos (upgrades, service pack, patches). Creación de VPN's entre firewalls y clientes. Métodos de autentificado por usuario, cliente y sesión. Controles de acceso que soporten más de 150 aplicaciones, servicios y protocolos. Esquemas de autentificado por S/key, Securid, Tacacs, Radius y OS password. Facilidad para incorporar scaneo de virus a través del protocolo CVP junto con módulo de antivirus adicional. Detección de ataques utilizando Elliptic Curve Cryptography 113. Utilización de NAT. Instalación, configuración, puesta en marcha y entrenamiento práctico del firewall. Interoperatibilidad con cualquier módulo adicional (encriptado, controlador de URL's, antivirus, autentificado dinámico con tokens, alta disponibilidad, etc.) **CARACTERÍSTICAS GENERALES** El software deberá contar con soporte técnico en el país. El tiempo de respuesta en el soporte técnico deberá ser de 1 hora vía telefónica y correo electrónico, 4 horas on site. Contar con asesoría para la administración de cualquier módulo adicional (controlador de URL's, antivirus, encriptamiento, autentificado dinámico, etc.) Se deben poder integrar módulos adicionales de otros fabricantes. Garantía y actualizaciones por un año en los productos y servicios.

8.9. Características técnicas de la arquitectura de seguridad del centro de control de la empresa eléctrica a nivel hardware

CANTIDAD	DESCRIPCIÓN
2	Equipos de cómputo que se describen como sigue: **SERVIDOR DEL SISTEMA DE SEGURIDAD (FIREWALL)** **UNIDAD CENTRAL** ARQUITECTURA: Sistema de procesamiento multisimétrico. **PROCESADOR** Procesador: RISC de 64 bits. Cantidad mínima: 2 procesadores. Velocidad mínima del procesador: 400MHz, 64 bits. Memoria caché mínima por procesador de 2 MB. Memoria RAM mínima 1GB con crecimiento a 2GB. **INTERFACES DE I/O** 4 Puertos Ethernet 10/100MB. 2 Puertos seriales 1 Puerto paralelo 1 Puerto Gigabit Ethernet. **ALMACENAMIENTO MASIVO** Almacenamiento interno: 2 discos de 18GB con capacidad de crecimiento a 108GB dentro del mismo gabinete. Discos de 10,000RPM hot-swap Ultra SCSI. **SOFTWARE** Sistema operativo UNIX SVR4 con 64 bits completos. Nivel de seguridad C2. NFS Versión 3.0 o superior, DNS, NIX, SMTP IEEE POSIX 1003.1 Y 1003.2 FIPS 151.2 Licencias ilimitadas de usuarios. Ambiente gráfico: X11R6 Windows System, MOTIF Window Manager, 1.2.4 OPEN GL. Protocolos de comunicaciones: NFS, TCP/IP, SNMP. Lenguajes de programación: ANSI C, C++, JAVA. **PERIFÉRICOS** Monitor de 17 pulgadas resolución mínima de 1280x1024 pixeles. Unidad de respaldo DAT 4MM DDS-3 con capacidad mínima de 12 GB. Unidad lectora de CD-ROM con velocidad 32X. **CARACTERÍSTICAS GENERALES** Estándares/Normas: NOM, UL.

	Garantías: 2 años en sitio directo del fabricante. **SERVICIOS ADICIONALES** (Mínimo durante la vigencia de la garantía) Soporte On-site, cuatro horas máximo de tiempo respuesta Entrenamiento completo para administración para 3 personas, con un mínimo de 40 horas por persona. El proveedor deberá incluir en su propuesta técnica y económica, la instalación, configuración y puesta en marcha después de entregados los equipos, de acuerdo a las especificaciones que en su momento indicará el centro de control de la empresa eléctrica. El fabricante deberá presentar escrito original en papel membretado en el que el fabricante se obliga a respaldar solidariamente al licitante en el plazo de entrega, garantía de los equipos, servicio, así como el cumplimiento de las especificaciones incluidas en la oferta técnica correspondiente.

5	**Servidor para la implantación de la arquitectura de seguridad.** **SERVIDOR DEL SISTEMA DE SEGURIDAD (FIREWALL).** **Unidad Central** Procesador RISC de 64 bits. Velocidad mínima del procesador 400MHz, 64 bits. Memoria caché mínima por procesador de 2MB. Memoria RAM mínima de 512 MB con crecimiento a 1GB. **INTERFACES DE I/O** 4 puertos ethernet 10/100 MB. 2 puertos seriales 1 puerto paralelo. 1 puerto gigabit ethernet. **ALMACENAMIENTO MASIVO** Almacenamiento interno: 18GB (enhanced IDE o SCSI) **SOFTWARE** Sistema operativo UNIX SVR4 con 64 bits completos. Nivel de seguridad C2. NFS versión 3.0 o superior, DNS, NIS, SMTP IEEE POSIX 1003.1 y 1003.2 FIPS 151.2 Licencias ilimitadas de usuarios. Ambiente gráfico: X11R6 window system, MOTIF window manager 1.2.4, open LG. Protocolos de comunicación: NFS, TCP/IP, SNMP. Lenguajes de programación: AMNSI C, C++, JAVA. **PERIFÉRICOS** Monitor de 17 pulgadas con una resolución mínima de 1280x1024 pixeles. Unidad lectora de CD-ROM con velocidad 32x.

	CARACTERÍSTICAS GENERALES Estándares/normas: NOM y UL. Garantías: 2 años en sitio directo del fabricante. Servicios adicionales por lo menos durante la vigencia de la garantía: *Soporte on-site, cuatro horas máximo de tiempo de respuesta. *Entrenamiento completo para administración y afinación del sistema para 3 personas, con un mínimo de 40 horas por persona. El proveedor deberá incluir en su propuesta técnica y económica, la instalación, configuración y puesta en marcha después de entregados los equipos, de acuerdo a las especificaciones que en su momento indicará el centro de control de la empresa eléctrica. El fabricante deberá de presentar escrito origina en papel membretado en el que el fabricante se obliga a respaldar solidariamente al licitante en el plazo de entrega, garantía de los equipos, servicio, así como el cumplimiento de las especificaciones incluidas en la oferta técnica correspondiente.
9	**COMPUTADORA DE ESCRITORIO** Deberá contar con procesador Intel Pentium III a 667 MHz. Con un bus 133MHz.- Deberá ser arquitectura isa/pci, con memoria RAM de 128 MB. RDRAM expandible al menos a 512 MB.- Deberá contar con memoria caché nivel 2 de 256 KB.- Con tarjeta de video de gráficos integrados Matrox Millenium G400-SG AGP con 16 MB SGRAM.- Con monitor de 15” SVGA con resolución de 1024*768, cumpla con normas energy star y mprii.-con unidad de diskette de 3.5’’ de 1.44MB.- Con unidad de disco duro smart III ultra ata de 13.5 GB.-Deberá contar con tarjeta de red PCI Fast Ethernet 10/100 BaseT, conector RJ45.- Deberá contar con dos puertos seriales, 1 paralelo, 2 USB, puerto de audio, con dos puertos minidin para teclado y mouse, con unidad de CD-ROM 40x o mayor. Deberá entregarse el software precargado de Microsoft NT versión 4.0 en inglés (incluyendo último service pack) con licencias de uso.- El teclado, CPU, monitor y mouse deberán ser la misma marca de fabricante.

8.10. Características técnicas del equipo para el portal del centro de control de la empresa eléctrica a nivel hardware.

Dos servidores en cluster: Sistema de procesamiento de transacciones en línea de alta disponibilidad.

Debe garantizar la operación con alta disponibilidad.

UNIDAD CENTRAL

PROCESADOR
Arquitectura del procesador: RISC de 64 bits.
Número de procesadores: 2x2 (cluster de dos servidores con al menos 2 procesadores cada uno.)
Velocidad mínima del procesador: 400MHz.
Memoria caché: 4MB.
Memoria RAM: 2GBx2 (4GB distribuidos, 2 GB en cada servidor.)

Capacidad mínima de crecimiento del sistema: 2x4 procesadores (8 procesadores en total), 2x4 GB (8GB en total) de memoria protegida con ECC (Error Correcting Code).

PUERTOS I/O
Cada servidor debe contar con los siguientes puertos:
1 puerto ethernet 100MB/s
1 puerto gigabit ethernet
2 puertos seriales
1 puerto paralelo.

Almacenamiento masivo
Almacenamiento interno: dos discos de 18GB Ultra SCSI hot-swap.
Dos arreglos de discos externos, tecnología fibre-channel (100MB/s), de 63 GB cada uno manejados en Raid 0+1 y que se conecten al servidor a través de puertos de fibra óptica (FC-AL) en configuración redundante. Fuentes de poder y de enfriamiento redundantes.

Capacidad de dispositivos (discos): 9GB mínimo por unidad de disco con características de hot-swap y hot plug.

SOFTWARE
Sistema operativo:UNIX SVR4 con 64 bits completos.
Multithreading en usuarios y kernel.
Que cumpla con la guía de portabilidad XPG3.
Nivel de seguridad C2.
NFS versión 3.0 o superior, DNS, NIS, SMTP.
IEEE POSIX 1003.1 Y 1003.2
FIPS 151.2
Licencias ilimitadas de usuarios.

Ambiente gráfico: X11R6 window system, MOTIF window manager 1.2.4, OPEN GL.

Protocolos de comunicaciones: NFS, TCP/IP, SNMP.
Lenguajes de programación: ANSI C, C++ y Java.

Administración de discos: software en ambiente gráfico para La administración de los discos duros.

PERIFÉRICOS
Cada servidor debe contar con:
1 monitor de 17 pulgadas, resolución mínima de 1280x1024.
1 unidad de respaldo del tipo DLT de 35 GB.
1 unidad lectora de CD-ROM velocidad 32x (mínimo)

CARACTERÍSTICAS GENERALES
Estándares/normas: NOM, UL.
Servicios adicionales por lo menos durante la vigencia de la garantía:
Soporte on-site, cuatro horas máximo de tiempo de respuesta.
Entrenamiento completo para administración y afinación del sistema para 3 personas, con un mínimo de 40 horas por persona.

El proveedor deberá incluir en su propuesta técnica y económica, la instalación, configuración y puesta en marcha después de entregados los equipos, de acuerdo a las especificaciones que en su momento indicará el centro de control de la empresa eléctrica.

El fabricante deberá presentar escrito original en papel membretado en el que el fabricante se obliga a respaldar solidariamente al licitante en el plazo de entrega, garantía de los equipos, servicio, así como el cumplimiento de las especificaciones incluidas en la oferta técnica correspondiente.

CARACTERÍSTICAS GENERALES DEL CLÚSTER.
Clúster con alta disponibilidad y topología de escalabilidad, deberá incluir todos los componentes de hardware y software necesarios para su óptimo funcionamiento en un ambiente de alta disponibilidad, soporte para la operación de base de datos oracle, monitor gráfico de componentes del sistema. Los discos, fuentes de poder y enfriamiento deberán tener las características de hot plug y hot swap.

La interconexión entre el arreglo de disco y los servidores deberá ser redundante de fibra óptica de 100 MB/s y con opción de conectar más arreglos de disco a través de hubs de fibra óptica.

Deberá soportar adición o remoción de nodos en forma dinámica.

8.11. Herramientas de desarrollo del portal

Ambiente de desarrollo para aplicaciones Web:

Manejador de Bases de Datos Relacional (RDBMS)
Opere en ambiente UNIX.

Ambiente de seguridad interna basado en uso de permisos y roles de usuario

Manejo de encriptamiento de passwords

CARACTERÍSTICAS GENERALES:

El software deberá contar con soporte técnico en el país.
Mantenimiento del software por 1 año (actualizaciones de software, asesoría telefónica, parches)

- El tiempo de respuestas en el soporte deberá ser de 1 hora vía telefónica y/o correo electrónico, 3 horas on site.

Debe incluir asesoría en la instalación y administración de módulos adicionales.
Debe incluir herramientas para conectarse con bases de datos del mismo y de otros fabricantes, en ambientes Unix

8.12. Implantación del firewall.

En esta sección se describirá el proceso que se llevó a cabo para la puesta en marcha del firewall. Así como las medidas preventivas para un buen uso y funcionamiento adecuado del hardware y software.

8.12.1. Configuración del sistema de seguridad

En siete servidores con plataforma Solaris se instala un firewall en cada uno de ellos. Únicamente en dos servidores que serán de alta disponibilidad es instalado el módulo que permitirá la distribución de carga entre éstos.

Enseguida se darán con más detalle los pasos que se siguieron para la instalación del firewall :

a) Instalación reciente del sistema operativo. Se realizan las particiones del disco duro de cada uno de los servidores para instalar los paquetes de End-User con un margen adicional que permita la descarga de parches de los paquetes antes mencionados.

b) Instalación y minimización del sistema operativo. Se instala, el End-User y se debe tener plena conciencia de que se han levantado servicios que no son necesarios para el firewall, mismos que serán dados de baja en el reforzamiento del sistema operativo y en las reglas del firewall.

Se descargan los parches y a través de éstos se realiza la actualización de los paquetes.

c) Reforzamiento del sistema operativo. Se deshabilitan todos los servicios que no brindará el firewall (Ej. se deshabilita el “Name Service Catching (NSC)”) y se establecen los permisos para cada uno de los usuarios quitándoles propiedades que pueden ser un riesgo de seguridad para la red al quedar habilitadas (Ej. Se edita el archivo de configuración destinado para tal efecto con el fin de modificar los permisos de los archivos cuando estos son creados para que sólo puedan ser modificados por el dueño).

El número de cuentas de usuarios debe ser el mínimo y éstas son únicamente para los administradores de seguridad así como cuentas de usuarios sin permisos de administrador. Son bloqueadas las cuentas innecesarias como lp y uucp en el archivo correspondiente.

Cada uno de los passwords debe ser de una longitud mínima de ocho caracteres, es decir, deben ser passwords fuertes con las características que se han mencionado en capítulo "propuestas de las políticas de seguridad". Los administradores de tareas sólo son asignados a los superusuarios y se niegan para todos los demás. Se eliminan los banners de algunos servicios (telnet y FTP), con el fin de no mostrar la versión del sistema operarivo, pues mostrar la versión es una vulnerabilidad.

La siguiente modificación del sistema operativo es para realizar la configuración de red. En la cual se asegura que no se realice la denegación de servicio por broadcast o/y multicast. Se agregan instrucciones para evitar un desbordamiento de pila. Se verifican los permisos de cada uno de los usuarios.

d) Reforzamiento del hardware. El equipo debe estar situado en lugares con entorno ideal de acceso restringido y con fuentes de alimentación redundantes.

Para tener la máxima disponibilidad se llevó a cabo la protección de la EEPROM exclusivamente a nivel “command” debido a que la máquina se encuentra físicamente protegida, se considera seguro el rearranque automático a favor de poder proporcionar un elevado tiempo de disponibilidad. Esta protección pide un password para modificar la EEPROM y se evita el establecer una contraseña de arranque del sistema.

e) Configuración de red de los sistemas de seguridad del CENACE.
Retomando el esquema básico de la colocación de un firewall, éste debe ser colocado entre la extranet (o Internet) y la Intranet como observa en la figura 8.1. Dicho concepto se tomó para la empresa eléctrica.

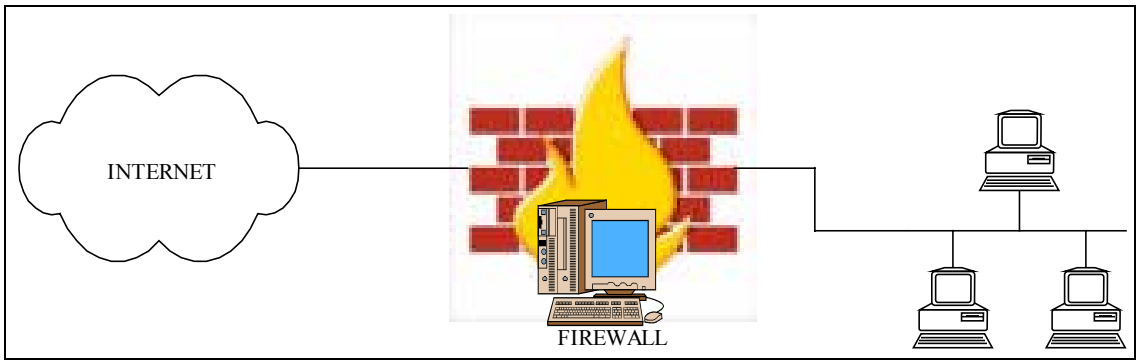

Figura 8. 1.- Colocación de firewall

Para garantizar la alta disponibilidad en la red de la empresa se hace uso de una arreglo en paralelo de los servidores que albergan los firewalls los cuales distribuyen la carga de tráfico (conocido como cluster) y en caso de falla o mantenimiento de alguno de ellos el firewall restante se hace cargo de todo el tráfico. Este arreglo es tomado como una sola identidad lógica.

Por otro lado se habilita la función de ruteo que es secundaria al firewall.

Para contar con un sistema de seguridad integral se utiliza el concepto de DMZ cuyas funciones a cumplir son:

a) Verificar que tanto el correo entrante como saliente de la Intranet no esté infectado con algún virus informático o que cualquier equipo envíe mensajes cuyo tamaño exceda la asignación establecida (4MB).

b) Establecer una bitácora de usuarios, intentos de acceso, peticiones a puertos y servicios, así como el origen de los mismos.

c) Autentificado dinámico a través de tokens.

d) El poder agregar otros servicios que se vayan requiriendo de acuerdo a las necesidades y recursos de la empresa. Ver figura 8.2.

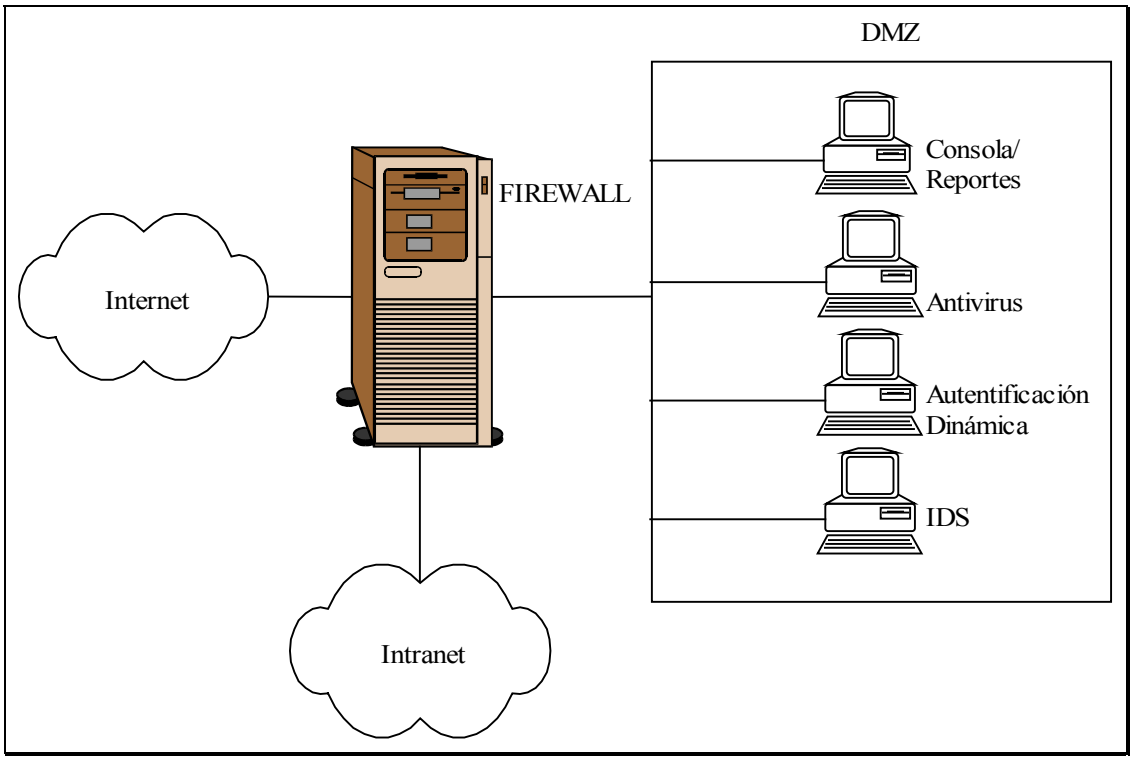

Figura 8. 2.- Diagrama de bloques.

Se establece la asignación de las direcciones IP para cada una de las interfaces de red en cada uno de los servidores destinados para contener el firewall. Como cada equipo cuenta con diferentes interfaces de red mismas que cuentan con una IP real y debido a la necesidad de que la red externa, la Intranet y la DMZ deben de enviar las peticiones y paquetes sólo a una interfaz común es necesario hacer uso del concepto de IP virtual.

La IP virtual permite que ambos equipos que funcionan como un cluster tengan la misma dirección para que sean reconocidos como sólo una entidad.

Así que, la configuración del servidor que contendrá al firewall está dada por:

- Dos direcciones IP externas relacionadas por una IP virtual. Véanse los puntos A (IP de la interfaz externa del firewall 1), A' (IP de la interfaz externa del firewall 2), AV (IP virtual) en la figura 8.3.

- Dos direcciones IP internas relacionadas por una IP virtual. Véanse los puntos B (IP de la interfaz interna del firewall 1), B' (IP de la interfaz interna del firewall 2), BV (IP virtual) en la figura 8.3.

- Dos direcciones IP que servirán para la DMZ relacionadas por una IP virtual. Véanse los puntos C (IP de la interfaz hacia la DMZ del firewall 1), C' (IP de la interfaz hacia la DMZ del firewall 2), CV (IP virtual) en la figura 8.3.

- Dos direcciones IP para permitir entre sus interfaces la carga distribuida. Véanse los puntos D y D' en la figura 8.3.

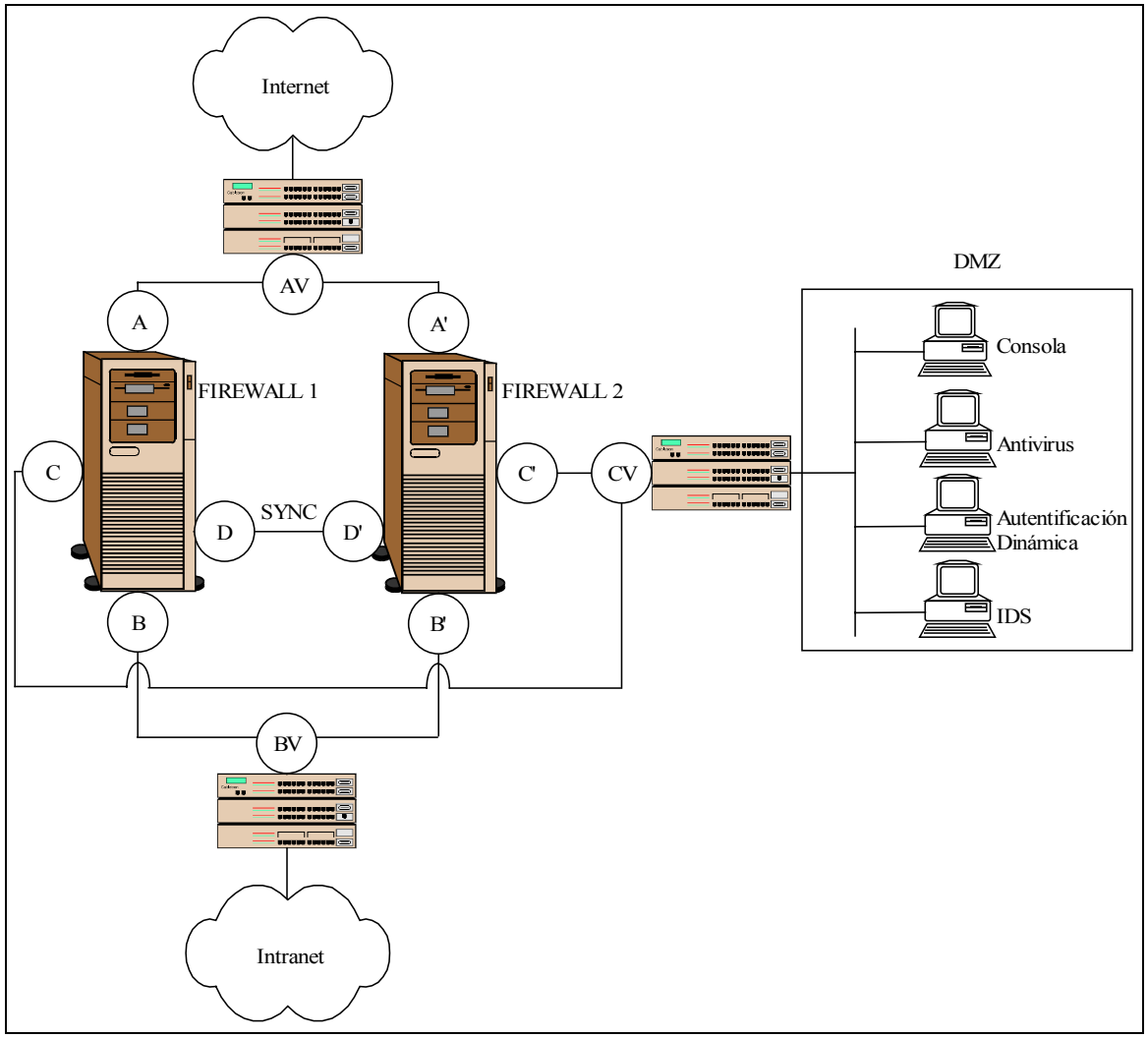

Figura 8. 3.- Configuración del firewall

f) Instalación y configuración de los firewalls.

La instalación del firewall comprende la parte de licencias y acuerdos, los cuales se aceptan.

Posteriormente se selecciona el producto y el tipo de instalación. En este caso se indica que es un stand-alone así como se realiza la identificación del firewall primario o secundario. Esto se debe a que uno tendrá prioridad en la configuración de la red.

Una vez que las opciones son validadas el sistema carga el software del firewall. Después de que la instalación está completa se ejecuta el comando cpconfig automáticamente, este comando permite reconfigurar el firewall.

Ahora se agrega un administrador y se introduce el nombre de éste. Se asigna el password y se confirma. Se agregan los derechos de administrador (leer/escribir).

Se selecciona clientes GUI, en la cual se agrega la IP del servidor asignado. Se despliega una sección que genera una semilla aleatoria para capacidades de encriptación, para ello se teclean caracteres aleatorios los cuales no todos son aceptados por el firewall. Después se inicializa la autoridad interna, de esta manera sólo este equipo podrá hacer las modificaciones.

Se toma nota del fingerprint del certificado que aparece. Posteriormente se teclea que no se quiere salvar el fingerprint a un archivo.

Finalmente se presiona la opción de que se quiere reiniciar el sistema. El sistema reiniciará para completar la instalación.

La instalación del servidor GUI se realiza en el equipo que contiene la IP antes asignada en el firewall. Se aceptan los términos de licencia. De manera similar a la instalación anterior se elige el producto. Se acepta el inicio de instalación. Se acepta el directorio por default. Aparece una ventana donde se seleccionan los componentes de la GUI. Se elige el siguiente paso para continuar con la instalación. Aparece una ventana de información posterior a la notificación de que la instalación está terminada.

Después de la instalación sigue la configuración del firewall para el cual se realizan las siguientes modificaciones en las propiedades del setup:

1. Dentro de setup/security_policy se habilitan las opciones de aceptar réplicas de UDP y aceptar paquetes salientes.
2. Dentro de setup/services se permite respuesta de las conexiones de datos FTP. Para que sea el código Inspect el que administre de forma segura y automática las sesiones de datos de FTP.
3. En setup/log_and_alert se selecciona la opción de ninguno. Se desactiva la opción que registra paquetes TCP establecidos, para no dejar rastro en el log de las conexiones que ya están establecidas o que se han perdido por timeout de la sesión TCP.

Finalmente se instala y se configura el software del cluster.

g) Reglas de Configuración de las políticas de seguridad

Para que el firewall cumpla su función se deben tomar en cuenta los siguientes tres puntos:

1. El orden de las políticas es de extrema importancia debido a que la revisión de las reglas por el firewall se realiza de manera secuencial. Una colocación inadecuada de alguna regla permitirá tráfico indeseado.
2. Al establecer las reglas se debe prestar cuidado especial de a quién está permitido el acceso en éstos, principalmente cuando es hacia cualquiera (any) en los campos de origen (source), destino (destination) o servicio (service).
3. Con el fin de llevar un control adecuado es importante realizar comentarios seguidos de la regla, por quién y cuándo fue habilitada así como indicar el servicio con el que está relacionado.

g.1) Políticas implantadas en el firewall.

Dentro del diseño y la implementación del firewall se cumplen las siguientes políticas de seguridad, establecidas en el capítulo 6.

Las políticas enumeradas 3, 6, 17, 19 y 20 establecen que sólo el administrador tendrá acceso lógico a la configuración del firewall y sólo él podrá realizar cambios a la misma. Además establecen una jerarquización de usuarios a través de asignación a grupos, dependiendo de la función que cada uno de ellos cumpla con la empresa. Lo anterior se observa en las figuras 8.4 y 8.5.

Figura 8. 4.- Autentificación del administrador al firewall.

La política número 4 establece el enfoque para el firewall que es “lo que no está expresamente permitido está prohibido” misma que se encuentra reflejada en la configuración actual de las políticas del firewall así como en la última regla que se establece para cada uno de éstos. Véase en la figura 8.5.

SOURCE	DESTINATION	SERVICE	ACTION
* Any	* Any	* Any	drop

Figura 8. 5.- Política de negación de servicios.

Las políticas que a continuación se enuncian 5, 20, 21, 22, 29, 30, 31, 32, 42, 43, 44, 54, 55, 56, 57, 60 y 63, establecen el estricto control que debe tener el sistema en lo que respecta a la jerarquización de recursos y autentificación de usuarios todo esto a través de la asignación y validación de logins, contraseñas y asignación de usuarios a grupos que vayan de acuerdo a la función, petición a servicios y trabajo que realizarán cada uno de ellos. Estas políticas se ven reflejadas en el uso de programas que permiten la autentificación de sesiones y usuarios (authen client, authen user, authen session). Mismos que están inherentes al establecer sesiones remotas con el software correspondiente así como en las reglas del firewall central. Véanse las figuras 8.6 y 8.7.

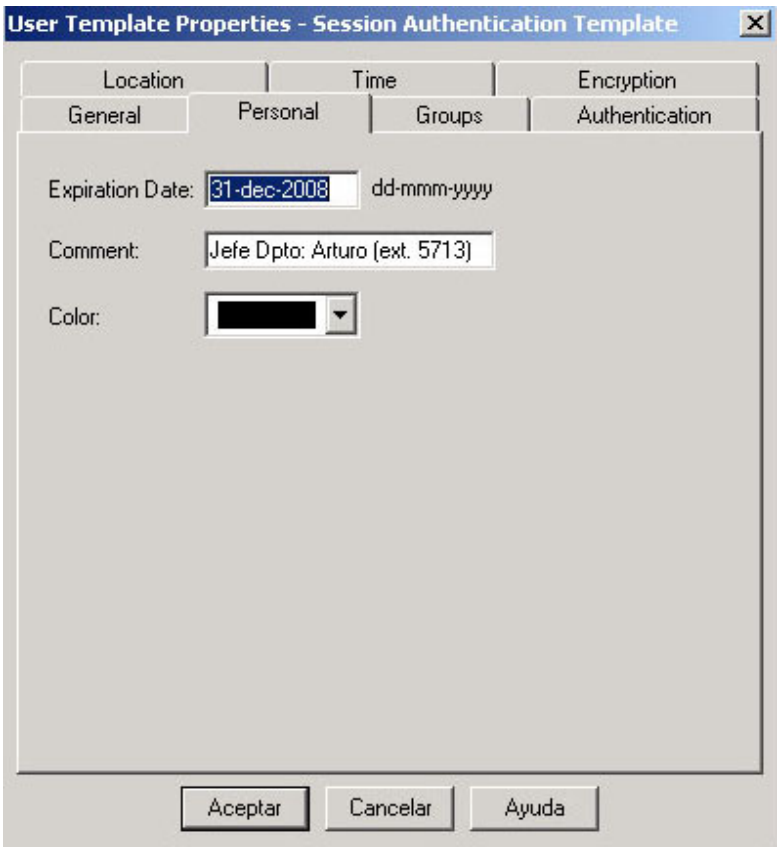

Figura 8. 6.- Características de grupos.

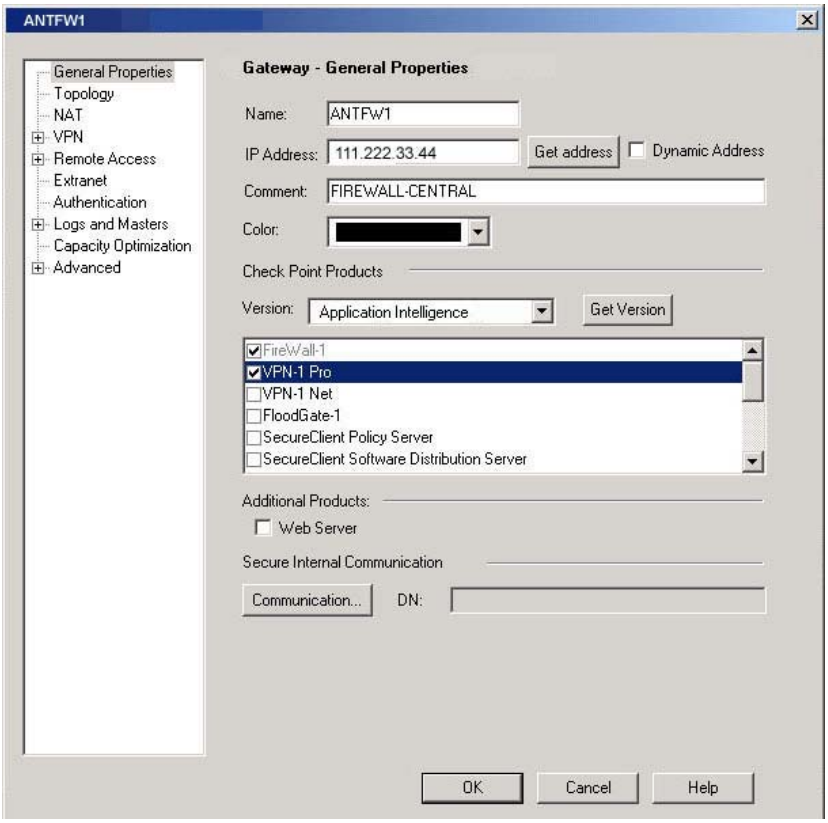

Figura 8. 7.- Configuración de autentificación.

Todo lo anterior funcionará de forma óptima siempre y cuando el usuario cuente ya con una conciencia sólida en seguridad informática.

Las políticas 16, 58 y 67 dictan que sólo se hará uso de la red para fines laborales y esto se lleva a cabo en las reglas del firewall que redireccionan hacia páginas y servicios que cumplan con los fines antes mencionados. Éste bloque de políticas pueden ser reforzado con el módulo de control de contenido que se donsidera en el diseño, no así en su implementación.

La política 33 establece que sólo con el uso de software de autentificación, la asignación de contraseñas de una sola vez (tokens), uso de VPNs, la jerarquización de usuarios y recursos será permitido al tener proyectos en común con ello se cumplirá el estricto control que se estableció para la red. Mismas que se muestran en la figura 8.8.

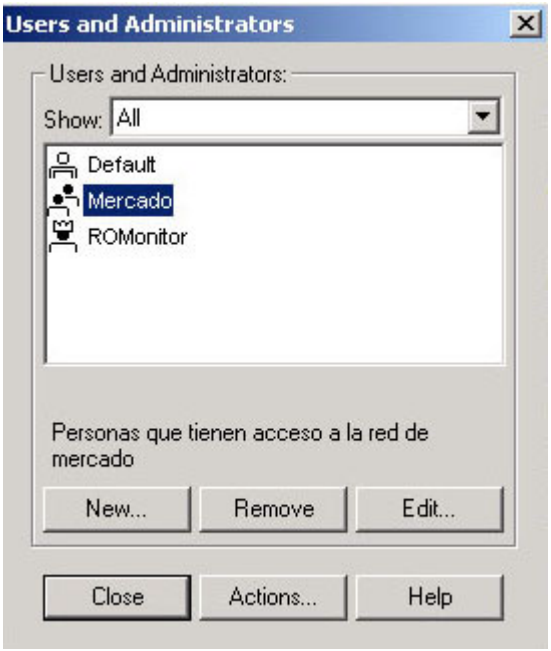

Figura 8. 8.- Definición de grupos de usuarios.

Los límites de protección de la red son establecidas en las políticas 7, 8 y 23 mismas que mencionan que sólo la Intranet es protegida y que la información definida como crítica requerirá una doble validación para hacer uso de ella a través de firewall central y los firewalls departamentales.

Las políticas 8, 9, 33, 34, 45 (tokens), 46, 48 y 54 han sido cubiertas ya al establecer políticas de autentificación. Véase en la figura 8.9. Para evitar que sea husmeada y/o modificada la información al ser transmitida por la Intranet se hace uso de VPNs. Véase en la figura 11.

Figura 8. 9.- Política de autentificación

Las políticas 15, 49, 67 y 74 establecen que se debe contar con una DMZ misma que tendrá a su cargo el control de correo entrante y saliente libre de virus, la creación de reportes de intentos de acceso y de las acciones consideradas como intromisiones. Ver figuras 8.10 y 8.11.

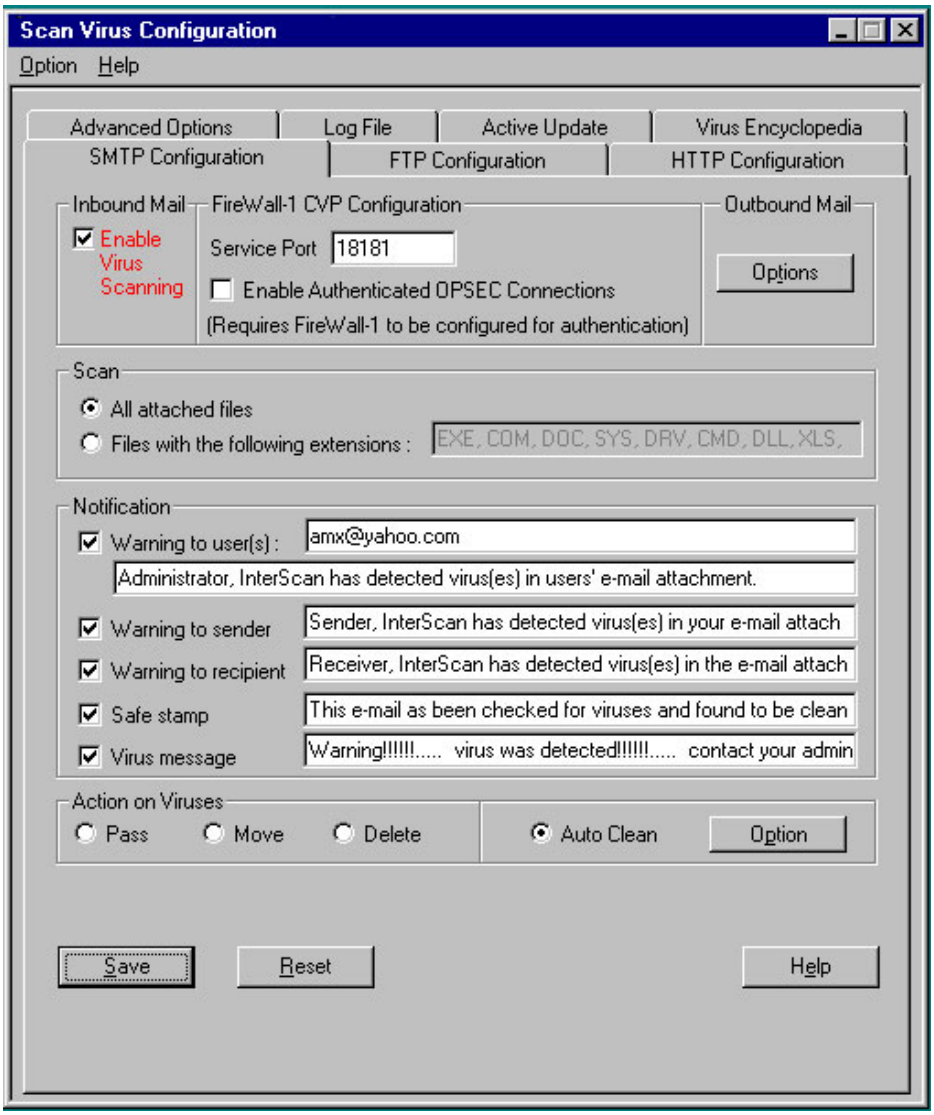

Figura 8. 10.-Configuración del antivirus desde la DMZ.

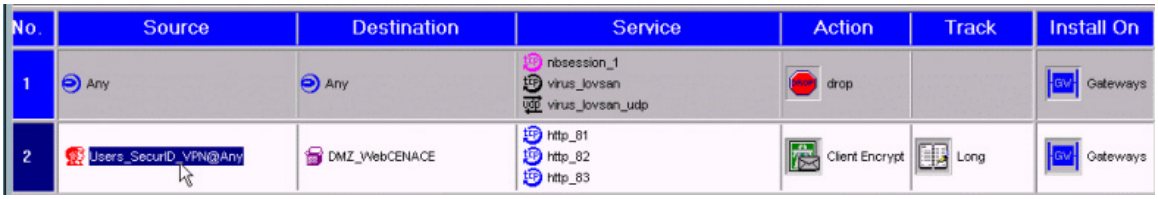

Figura 8. 11.- Políticas de seguridad del la DMZ.

La política número 27 se cumple al hacer uso de validaciones dinámicas para usuarios externos e internos que hagan uso del sistema crítico, esto hace más difícil el decifrado de contraseñas. Ver figuras 8.12 y 8.13.

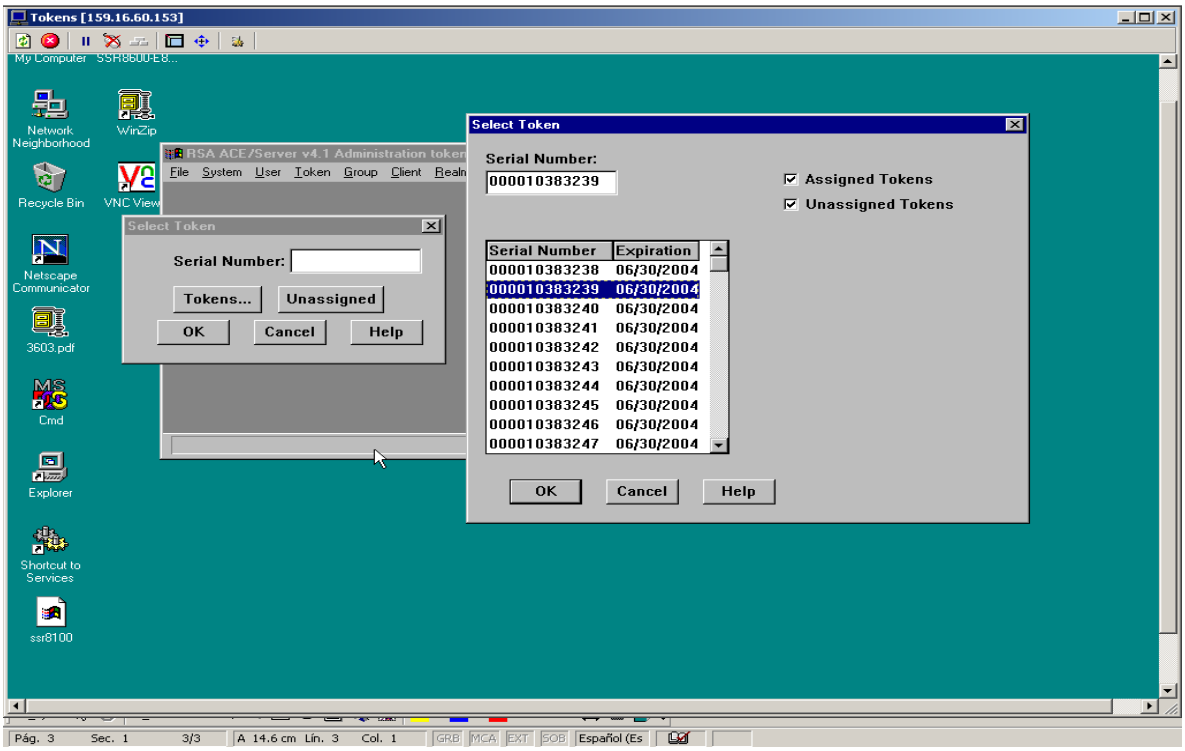

Figura 8. 12.- Asignación de tokens.

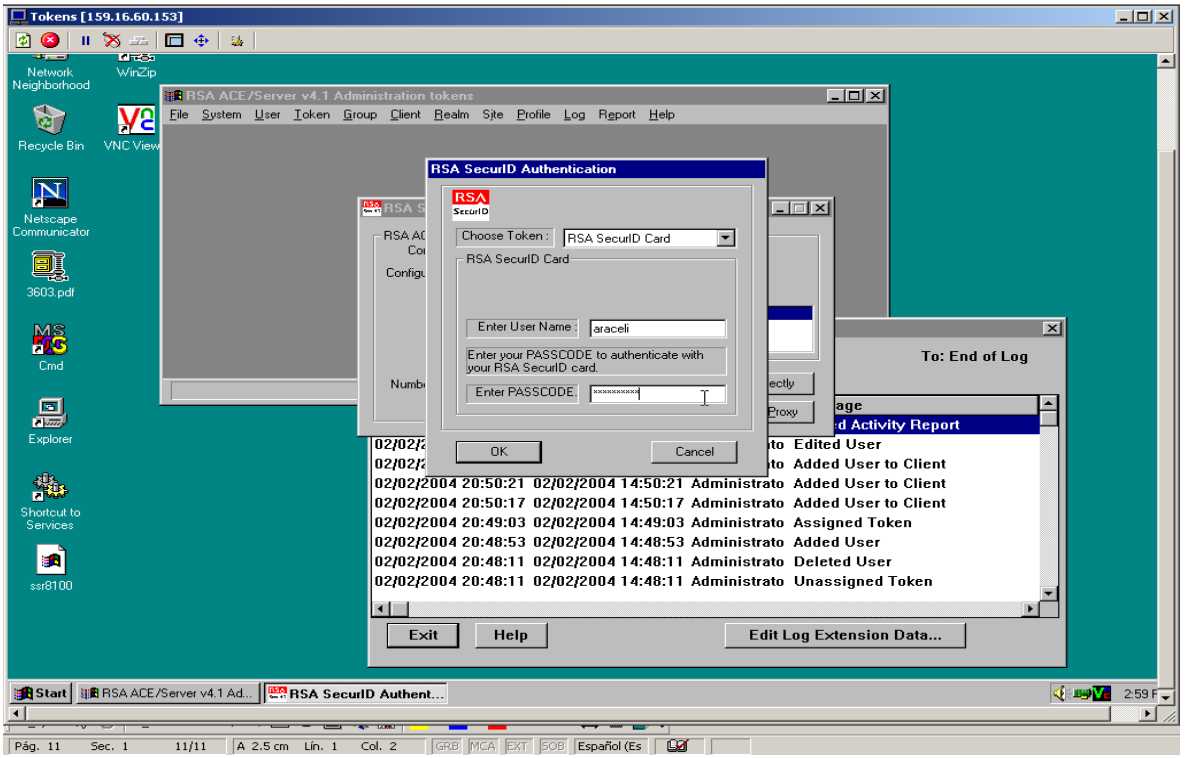

Figura 8. 13.-Autentificación por Token.

Para cumplir con la política 38, misma que establece una administración centralizada, se hace uso de un firewall central, el cual será configurado por medio de una consola que sólo tendrá esa labor.

En la política 67 se establece de manera particular y puntual que las restricciones para cada uno de los servicios de Internet así como las obligaciones y derechos que adquieren los usuarios al hacer uso de estos servicios. Misma que es cumplida al llevar a cabo el reforzamiento del sistema operativo en el cual son dados de baja los servicios inútiles y riesgosos para la empresa.

g.2) Las políticas que no pueden ser directamente aplicadas al firewall debido a sus características pero sí fueron establecidas de acuerdo a su función son llamadas en este trabajo "políticas alternas" catalogadas en cuatro rubros: a) Físicas, b) en contra de ingeniería social, c) concientización de usuarios, d) de administración y auditorías.

Las políticas físicas establecidas en la política número 3 establece que sólo el administrador de seguridad tendrá acceso físico al equipo donde se encuentra residente el firewall de la red.

En contra de la ingeniería social se establece que no se debe dar información de la red como logins y contraseñas vía correo o telefónica.

Las políticas 12, 36, 49, 58, 59, 60, 61, 63, 64, 65, 66, 67 y 82 hablan acerca de la concientización de la seguridad informática de los recursos humanos de la empresa eléctrica misma que reforzará el sistema de seguridad.:

Finalmente las políticas de administración y auditorías: 10, 11, 13, 16, 37, 39, 40, 41, 50, 51, 52, 53, 61, 68, 69, 70, 71, 72, 73, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87 y 88.

h) Mantenimiento del firewall

1. Situar las reglas de acceso más comunes al principio de la política de seguridad.
2. Mantener el juego de reglas lo más reducido posible.
3. Deshabilitar las conexiones de control de firewall siempre que sea posible y agregarlo en las reglas explícitas.
4. Deshabilitar en las propiedades "Decrypt on accept" si no se está usando la encriptación.
5. Para maximizar el rendimiento del firewall se realizan las siguientes modificaciones al sistema operativo Solaris:

   5.a. Hacer que cada puerto de las tarjetas de red tenga su propia dirección MAC con el comando

   #eeprom local-mac-address?=true

   5.b. Forzar todas las interfaces de red para que se conecten a la máxima velocidad deshabilitando la autonegación de las interfaces.

ndd –set/dev/hme adv_autoneg_cap 0 → deshabilita la autonegación
ndd –set/dev/hme adv_100fdx_cap 1 →forza la tarjeta a 100Mbits full duplex.

ndd –set/dev/hme adv_100hdx_cap 0 →deshabilta la tarjeta a 100Mbits half duplex.
ndd –set/dev/hme adv_10fdx_cap 0 →deshabilita la tarjeta a 10Mbits fullduplex.
ndd –set/dev/hme adv_10hdx_cap 0 →deshabilita la tarjeta a 10Mbits half duplex.

5.c. Aumentar el buffer de transmisión y recepción de TCP.
ndd –set/dev/tcp tcp_xmit_hiwat 65535→por defecto es 8192
ndd –set/dev/tcp tcp_recv_hiwat 65535→por defecto es 8192

5.d. Instalar las versiones actuales de parches recomendadas por el fabricante del sistema operativo.

6. Se recomienda depurar periódicamente los registros “system” y ”application” en el Event Viewer del sistema operativo windows, ya que, si se llegaran a llenar el servicio de los módulos puede verse afectado.

NOTA: Al realizar las actualizaciones a través de parches es necesario verificar y reconfigurar el reforzamiento del sistema operativo.

i) Procedimiento para hacer un respaldo del firewall.

En este procedimiento se quitan los nombres de comandos y archivos para no publicar lo que debe ser confidencial.

- Detener el firewall desde una sesión de sistema operativo.
- Copiar a otro directorio el directorio que contiene los archivos críticos en Solaris.
- Comprimir la información y guardarla en un diskette o CD.
- Iniciar el firewall.

j) Plan de contingencia.

Se realiza un respaldo manual cada tercer día de la configuración del firewall durante la instalacion y puesta en marcha. Dicho respaldo es transmitido por FTP hacia la máquina del administrador. Esto se lleva a cabo a través del administrador de tareas. Posteriormente, los respaldos son periodicos y de acuerdo a los cambios de configuración que permitan asegurar la funcionalidad inmediata.

Se llevó a cabo la sincronización de los firewalls a través de fuentes externas por medio de NTP. La política del firewall contempla la aceptación de este servicio.

Al llevar a cabo las actualizaciones en especial la del kernell se habilitan servicios los cuales modifican el reforzamiento inicial, por lo que se debe realizar nuevamente.

En los servidores que cuentan con sistema operativo Windows NT, Windows 2000 Advanced Server se habilitan sólo aquellos servicios que son necesarios. Siendo

configurados como Stand Alone Server lo cual permite un mayor control tanto de usuarios como de grupos de trabajo.

Se amplió la memoria cache de los registros “system” y “application”, ya que pueden alojar eventos en estos registros.

8.13. Consideraciones posteriores al diseño.

Ser realista. En ocasiones se piensa en la tecnología como solución a todos los problemas. Aquí no es el caso. La tecnología termina siendo una herramienta más para el objetivo de esta tesis, es decir, el asegurar una red no depende de la tecnología, depende de las necesidades de la compañía.

Administración. La tecnología no trabaja por sí sola, tiene que haber personas que la gestionen. Se puede implantar la mejor tecnología y tener la más segura, pero si el personal no está lo suficientemente capacitado para manejarla podría ser un error poner herramientas confusas con las cuales en lugar de ayudar a asegurar podría ser solo una carga más de trabajo sin cumplir con las expectativas de seguridad informática. Como resultado la cual se podrían generar más riesgos.

Revisar las bitácoras y las alarmas que genera el firewall. El firewall tiene bitácoras en las que se registran actividades, algunas pueden ser alarmantes, otras no. Sin embargo es información útil que se debe estar revisando y no dejarse al olvido. Con base a la bitácora, se ha de desarrollar un procedimiento en el que haga un seguimiento de qué se debe hacer si se detecta un acto delictivo.

Actualizar y revisar que el firewall esté bien configurado. El firewall y cualquier sistema operativo correspondiente debe actualizarse y mantenerse oportunamente con parches al mismo y correcciones a errores de programación. También se debe documentar y entender la información de cómo quedó configurado el firewall. Posteriormente se deben realizar pruebas.

Restringir las modificaciones a la configuración del firewall. No es conveniente que cualquier persona de soporte técnico pueda modificar la configuración. Si no se planean los cambios al sitio y a los servicios internos y externos, es fácil que se tengan urgencias que obliguen a realizar cambios de último momento. Por ello se hace la recomendación de tener un proceso mínimo de control de cambios.

8.14. Conclusiones

Conociendo las necesidades de la intranet de la empresa, se sabe que éstas se deben satisfacer. Por lo que con el conocimiento en productos comerciales se resaltan las principales características para cubrir dichas necesidades. De aquí también se busca la mejor solución para el diseño, que puede ser la de construir o adquirir un firewall.

En este capítulo se contó con las condiciones de diseño, las cuales fueron importantes para dar la mejor solución. Junto con éstas condiciones y otras

consideraciones como lo son el análisis de la topología, se evaluó si el sistema sería comprado o fabricado por la empresa eléctrica.

Posteriormente se realiza una lista con las características que debe cubrir este firewall. Esta lista se da al departamento que le compete la compra de equipo para que se le asigne un presupuesto. Por otro lado se considera la opción de construir uno. Sin embargo, no se dispone del tiempo suficiente ni los recursos humanos para la construcción del firewall, ni el conocimiento, además de que esta no es función del àrea que lo necesita. Por lo que se espera la propuesta del departamento de compra.

Para lograr la implantación del firewail interviene tanto el análisis de la topología de red, así como las necesidades de la empresa, las necesidades laborales de los usuarios, la aplicación de políticas y conceptos de seguridad, además de los conocimientos de los distintos tipos de incidentes e intrusiones en la seguridad de redes de cómputo. Los cuales fueron conceptos adquiridos de una ardua investigación.

Con el análisis de la red los elementos confiables se ubican de forma estratégica logrando un sistema integral de seguridad en el que el firewail será parte importante de éste. Así el filtrado de paquetes se complementa con módulos adicionales al firewail los cuales trabajan en conjunto con las siete capas del modelo OSI.

Por lo que para contar con una seguridad integral es necesario contar con elementos adicionales a un firewail centralizado híbrido, entre los distintos elementos desprendidos en los antecedentes de esta tesis se cuenta con el uso de una Zona Desmilitarizada (DMZ).

Una arquitectura de DMZ cuenta con servidores expuestos a Internet y es a través de ellos que es posible aislar a la intranet, con el objetivo de si el firewail es vulnerado, la seguridad de la red interna no sea comprometida.
Para el caso particular de la empresa eléctrica se estableció que la seguridad además de contar con un firewail centralizado debe estar fortalecida por una DMZ, misma uque debe estar constituida por:

- Un detector de intrusos, que tendrá la tarea de generar una bitácora de los accesos tanto válidos con los que no lo hallan sido, además de que alertará ante posibles procesos que sean un patrón para la intromisión.
- Un servidor que tendrá como función principal la de revisar el contenido del correo electrónico tanto del destinatario como remitente.
- Y una consola donde sea posible llevar la administración centralizada y conjunta de cada uno de los firewalls que forman el sistema de seguridad de la empresa eléctrica que protegen a los sistemas críticos.

Debido a las necesidades de la empresa eléctrica que no se puede dejar de trabajar se necesitó del concepto de alta disponibilidad. Por lo que la redundancia se usa para aplicar este concepto alcanzando una disponibilidad de 7 días a las semana, las 24 horas del día durante los 365(366) días del año. Esto se consiguió a través de otro concepto de distribución de carga conocido como cluster.

Como el firewall debe trabajar de acuerdo a los anteriormente expuesto, se estudia más afondo el producto obtenido para realizar su configuración y un vaciado de políticas de alto nivel y convertirlas a uno de bajo nivel dentro del firewall.

Para obtener el éxito del sistema de seguridad se le debe dar el cumplimiento a las políticas de alto nivel así como el mantenimiento debido a éstas. Por lo que se preveé con revisiones periódicas de las políticas, las cuales se van modificando de acuerdo a los resultados obtenidos y a las modificaciones hechas de acuerdo a las necesidades que se siguen generando en la empresa.

Por otro lado lo más importante y lo que realmente va a hacer funcionar el sistema integral de seguridad es la aceptación del proyecto y su cumplimiento por parte de los recursos humanos.

Cada parte del proyecto queda escrita de forma detallada para la empresa. Con ello se aporta la apertura de la capacitación en cultura de la seguridad informática dentro de la empresa eléctrica, así como queda documentado cada paso para darle el debido seguimiento a los cambios de acuerdo a la evolución que se vaya dando en esta tecnología.

Los dispositivos y software de seguridad se adquirieron de acuerdo al diseño del sistema de seguridad. El proceso de implementación aquí citado se llevó acabo. Desde el término de la implantación se ha mantenido funcionando el sistema de seguridad con la misma topología durante tres años, dando buenos resultados en el control de accesos de tráfico de la red hacia los sistemas críticos, en la prevención de ataques informáticos, en la anticipación a la propagación de virus y gusanos de la red externa, al lograr confidencialidad, consistencia e integridad de la información y de los sistemas críticos. La alta disponibilidad ha dado buenos resultado puesto que el sistema ha trabajado ininterrumpidamente siempre dando la oportunidad del mantenimiento técnico. Por lo que se hacen las actualizaciones de software y de las reglas del firewall sin consecuencias desfavorables para los objetivos de la empresa eléctrica.

Conclusiones y beneficios

CONCLUSIONES:

Antes de diseñar este sistema de seguridad en el centro de control de la empresa eléctrica se trabajaba con cuentas de usuario que permitían el acceso sin restricciones a los diferentes sistemas de información, además de no tener un control de ello. Lo cual evidentemente no garantizaba la confidencialidad, ni integridad de datos y menos disponibilidad entre otros. Es decir, la información podía ser alterada, robada o dañada debido al mal uso de ésta.

Se identificaron los puntos críticos que contienen la información de adquisición de datos en tiempo real del sistema eléctrico.

Se dio la seguridad a lo anterior garantizando que sólo el personal autorizado puede hacer uso de ella.

Se diseñó un sistema de seguridad que consiste tanto de hardware como de software que es configurado tomando como base las políticas de seguridad y éstas resultan ser a su vez una herramienta extremadamente útil para las empresas que manejan información que no desean compartir sin autorización.

Se han evitado múltiples ataques de intrusos así como se han detectado virus y hasta la fecha la red ha estado exenta de virus no así algunas de las otras redes de la compañía.

BENEFICIOS:

En la implementación del sistema de seguridad en el centro de control de la empresa eléctrica se puede concluir que los beneficios que se generan en ésta son:

Buen uso de la red de cómputo.

Mediante la capacitación se logra una de la propuestas de la política de seguridad que es el concientizar a los usuarios de la importancia de la cultura de la seguridad, dando un buen uso de la red y medidas y preventivas, por lo que es una herramienta para lograr una red confiable. Por ello se elabora material de apoyo para capacitaciones futuras.

Documentación.

En la cual queda registrado cada paso desde el inicio hasta el final de la implementación para modificaciones futuras.

Control.

Mismo que se con la definición de políticas de seguridad, las cuales establecen lo que se permite o se niega en la empresa. Éstas son informadas a los usuarios del Intranet, los cuales firman para darse por enterados.

Otro punto de control es el firewall, el cual, se configura con la filosofía de todo lo que no se permite expresamente, está prohibido. Es decir, los paquetes que entran o salen deben cumplir con las políticas de seguridad. Con ello se logra un control de acceso del tráfico de datos, servicios y puertos. Este filtrado es la base para sostener los módulos que se enumeran a continuación:

- IDS
- Antivirus
- Reportes
- Autentificado
- VPNs

Autorización.

Se tiene una lista de los usuarios, la cual define a qué sistema de información tienen permitido acceder y que rol tendrán en el mismo, permitiendo al administrador un mayor control de los usuarios y con ello brindarles una mayor seguridad para el intercambio de información. Esto se logra con base en la implementación de políticas de seguridad y se fortalece con el autentificado.

Autentificación.

En la consola destinada a la autentificación se realiza autentificado dinámico con tokens (tarjetas con tecnología de passwords de una sola vez) en el sistema de seguridad de autentificado dinámico destinado para usuarios de sitios remotos. Mismo que se garantiza que el dueño de la llave pueda acceder y enviar información sumamente importante, lo que garantiza la confiabilidad de la información depositada.

Auditoría.

Cada actividad realizada por los usuarios de la empresa así como las de personas no autorizadas queda registrado en archivos de bitácora y el sistema advierte con alarmas las actividades que podrían ser consideradas como delictivas con base a las políticas establecidas por el administrador.

Disponibilidad y consistencia.

Se implementa un antivirus para el servicio de correo electrónico y de ftp para garantizar que la información que se envía por estos medios sea confiable y por ello no dañe la infraestructura interna ni la información de la red de cómputo. Anteriormente no se tenía este control por lo que era difícil detectar los virus que afectaban la productividad de esta empresa.

Confidencialidad e integridad de datos.

Otro beneficio es el que ahora es posible observar y rechazar los intentos de accesos no autorizados, ya que antes de la implantación de éste sistema no era posible llevar a cabo esta acción.

Donde las actividades delictivas son definidas a través de plantillas de patrones típicos de intentos de intromisión y también por las establecidas en las políticas de seguridad.

El sistema reconoce más de 300 tipos de ataques y responde reconfigurando automáticamente el firewall para cancelar las conexiones y protegerse ante diversos ataques. Éstas plantillas pueden ser modificadas por el administrador haciéndolas tan rigurosas como se quieran.

Para garantizar la confidencialidad de la información, también, se realiza la implementación de VPNs en el sistema de seguridad. Las VPNs nos permiten el intercambio de información de forma encriptada de un lugar remoto a los sistemas de información.

Lo anterior sirve para que los administradores o gerentes consulten y/o modifiquen información y para que ésta no pueda ser alcanzada por personas ajenas y aún cuando lo hiciesen no puedan leerla. Otra ventaja de las VPNs es que no son líneas dedicadas las cuales tendrían un costo adicional a la empresa.

Integridad del diseño

La zona desmilitarizada (DMZ, por sus siglas en inglés) permite tener implementado todo el sistema de seguridad y a la que sólo se le permite acceder al administrador de éste. Lo que beneficia el mantener la integridad del diseño.

Alta disponibilidad

Para lograr la alta disponibilidad fueron implementados en el firewall un sistema cluster, el cual balancea tanto la carga de información de entrada como la de salida, además proporciona conectividad de forma transparente si hay un fallo en una pasarela.

Escalabilidad

El firewall elegido proporciona una plataforma abierta para ofrecer integración y operabilidad. El diseño permite la elección de entre más de 200 compañías para agregar soluciones de seguridad informática en futuros desarrollos. Con lo que se pueden añadir más módulos de diferentes fabricantes al firewall.

El hardware y el software no son únicamente la solución, detrás de todo esto hubo un trabajo de investigación que permitió adecuar el sistema de seguridad sin que se viera afectado en forma alguna el desempeño de la red de empresa eléctrica.

Con esto damos por concluido el implantación del sistema de seguridad que como se puede observar los beneficios son realmente significativos para la empresa.

En lo personal, fue de utilidad ya que me permitió conocer un campo de conocimiento que se encuentra en la punta tecnológica y esta dentro de las necesidades actuales de muchas empresas.

También, me permitió sirvió de apoyo para especializarme en una área en la cual hoy laboro.

Anexo A

Hojas de trabajo

Hoja de trabajo para desarrollar un planteamiento de seguridad[1]

Recursos de la fuente		Tipo de usuario del que hay que proteger al recurso	Posibilidad de amenaza	Medidas que se implementarán para proteger al recurso de la red.
Nombre	Importancia del recurso			

[1] Esta hoja de trabajo fue tomada del libro Firewalls y la seguridad en Internet de Karanjit Siyan y Chris Hare, de la página101.
La escala que se ha tomado es de 0 a 10.

Hoja de trabajo para el análisis de riesgo de seguridad de la red.[2]

Recursos de la red (Nombre del recurso)	Riesgo de los recursos de la red (Ri)	Peso(Importancia) del recurso (Wi)	Riesgo evaluado (Ri*Wi)

[2] Esta hoja de trabajo fue tomada del libro Firewalls y la seguridad en Internet de Karanjit Siyan y Chris Hare, de la página 105.

Hoja de trabajo para otorgar acceso a recursos del sistema y la red

Recursos de una red (Nombre del recurso)	Tipo de acceso	Permiso de sistema operativo UNÍX: rwx

Esta hoja de trabajo fue tomada del libro Firewalls y la seguridad en Internet de Karanjit Siyan y Chris Hare, de la página114.

REGISTRO DE SOLICITUD PARA ACCESOS AUTORIZADOS A USUARIOS A LA RED DEL CENTRO DE CONTROL DE LA EMPRESA ELÉCTRICA

Área usuaria: _____ **Fecha:**_____

Responsable(s) del Área:_____

_____

Vigencia(día/mes/año)**: De ____/____/____ al ____/____/____.**

Nombre del Servidor Destino	Dirección IP Servidor Destino	Dirección IP Fuente	Localización Física	Servicios Requeridos

FINALIDAD:_____
_____.

AUTORIZO:
AREA SOLICITANTE

AUTORIZA:

Vo. Bo.

_____ _____ _____

XXXXXXXXXXXXXXXXXXXXX
S U B G E R E N T E DEL ÁREA

XXXXXXXXXXXXXXXXXX
S U B G E R E N T E
DE EQUIPOS Y
PROCESO DIGITAL.

ING. FRANCISCO L. HOLGUIN R.
GERENTE DE SIST. DE
ADMON. DE ENERGIA.

Anexo B
Preguntas para un relevamiento

Antes de escribir e implantar las políticas de seguridad se debe realizar un estudio del nivel de seguridad con el cual cuenta el centro de control de la empresa eléctrica, con el fin de conocer las medidas preventivas y correctivas de seguridad que se llevan a cabo, con el propósito de fortalecerlas y en caso de que no hayan medidas básicas de seguridad introducirlas en las políticas.

Encuesta del nivel de seguridad para iniciar la implantación de políticas

1.- ¿Hay alguien responsable de la seguridad informática?

2.- ¿Se tiene alguna política de seguridad?

3.- ¿Los servicios y accesos a la red se restringen de alguna forma a los usuarios?

4.- ¿Existen antecedentes de intrusión a los sistemas?

5.- ¿El centro de control de energía tiene muchos sitios?

5.1.- En caso de ser afirmativo ¿cada uno cuenta con sus propias redes? De ser afirmativa la respuesta, ¿cada sitio maneja su seguridad o la seguridad es centralizada?

6.- ¿Qué recursos están protegidos?

7.- ¿Qué recursos se quieren proteger?

8.- ¿Ha protegido estos recursos anteriormente?

9.- ¿Actualmente, de quienes se protegen los recursos?

10.- ¿Qué tan posibles son las amenazas?

Ver hoja de trabajo en el anexo A para desarrollar un planteamiento de seguridad.

11.- ¿Qué tan importantes son los recursos de la red?

Ver hoja de trabajo para desarrollar un planteamiento de seguridad en el anexo A.

12.- ¿Qué medidas lleva a cabo para proteger sus bienes de forma económica y oportuna?

13.- ¿Qué recursos informáticos se identificaron?

14.- ¿Qué amenazas y vulnerabilidades se identificaron?

15.- ¿Quién está autorizado para usar los recursos?

16.- ¿Se tiene algún documento para saber cuál es el uso adecuado de los recursos?

17.- ¿Quién está autorizado para conceder acceso y aprobar el uso de los servicios de la red?

18.- ¿Quién puede tener privilegios de administración del sistema?

19.- ¿Cuáles son los derechos y responsabilidades de los usuarios?

20.- ¿Cuáles son los derechos y las responsabilidades del administrador del sistema, en comparación con los de los usuarios?

21.- ¿Qué hacen los administradores y los usuarios con la información delicada?

22.- ¿Quién puede instalar módems para entrar a la red?

23.- ¿Hay algo especial acerca de las líneas PPP (point to point protocol), SLIP (serial line Internet protocol) o ISDN (Integrated Services Digital Network)?

24.- ¿Se permite introducirse a las cuentas de otros usuarios?

25.- ¿Se permite descifrar las contraseñas?

26.- ¿Se permite interrumpir servicios?

27.-¿Los usuarios suponen que, si un archivo tiene permiso general de lectura, eso los autoriza a leerlo?

28.- ¿Se permite que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura?

29.-¿Los usuarios comparten cuentas?

30.- ¿Qué hay de los proyectos en común, es necesario compartir cuentas?

31.- ¿Se permiten cuentas para compartir con los miembros de la familia?

32.- ¿Se comparte una cuenta si permite que alguien tome prestada por un momento una ventana en su máquina?

33.- ¿Cómo se maneja la legalidad de software?

34.- ¿Quién es la autoridad a la cual le rinden cuentas las personas que tienen privilegios?

35.- ¿Qué debe hacer la gente antes de conectar una computadora a la red principal?

36.- ¿Qué tan seguras son las computadoras para conectarse a una red sin protección con acceso a Internet?

37.- ¿Cómo se protege la información financiera?

38.- ¿Cuándo pierde la gente el derecho de tener una cuenta y qué se hace al respecto?

39.- ¿Qué pasa si la gente se va o se le niega el acceso a las instalaciones de la organización?

40.- Si tiene sitios remotos ¿Cómo se restringe el acceso hacia su red principal?

41.- ¿Existen conexiones a equipos remotos?
41.1.-¿Cómo se aseguran estas conexiones?

42.- ¿Se tiene acceso seguro a su red?

43.- ¿Cómo tiene acceso a la red la gente que viaja?

44.- ¿Qué información de la compañía se considera confidencial?
44.1.-¿Cómo es protegida?
44.2.-¿Puede enviarse fuera del sitio por medio del correo electrónico?

45.- ¿Qué precauciones toma contra los virus de las computadoras personales?

46.- ¿Qué se hace para la seguridad física de las redes de computadoras?

47.- ¿Quién se puede conectar a su sitio con redes externas y qué es una red externa?

48.- ¿Es correcto que un administrador de proyecto conecte su sitio a otro sitio específico?

49.- ¿Qué pasa si establecen una segunda conexión a Internet?

50.- ¿Cómo se protege la información confidencial (datos personales) de la gente de la empresa?

51.- ¿Qué métodos se usan para crear cuentas y finalizar accesos?

52.- ¿Hay alguna política que descarte donde la contraseña inicial sea igual al nombre del usuario, o que se quede en blanco?

53.- ¿Cuál es el periodo que se da para acceder a una cuenta sin que se inhabilite?

54.- ¿Qué se tiene para los lineamientos acerca del uso de los recursos de red?

55.- ¿Qué constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red?

56.- ¿Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas?

57.- Política de contraseña de usuario: ¿Con qué frecuencia cambian de contraseña los usuarios y qué otras restricciones o requerimientos hay al respecto?

58.- ¿Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema?

59.- Consecuencias para los usuarios que divulguen información que pueda estar patentada, ¿Qué acciones legales u otros castigos se llevan a cabo?

60.- ¿Existe una declaración sobre la privacidad del correo electrónico?

61.- ¿Existe una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión?

62.- ¿Existe una política sobre comunicaciones electrónicas, tales como falsificación de correo?

63.- ¿Qué hacen los usuarios para protegerse a sí mismos y al sitio?

64.- ¿Qué puede hacer la gente en Internet?

65.-¿Pueden transferir archivos ejecutables al azar y ejecutarlos?

66.- ¿Puede el administrador revisar o leer los archivos de un usuario por alguna razón?
66.1.-De ser afirmativa la pregunta anterior, ¿en qué grado tiene esa prioridad?

67.- ¿Los administradores de la red tienen el derecho de examinar el tráfico de la red o del host?

68.- ¿Cuáles son las responsabilidades legales de los usuarios, los administradores del sistema y de la organización por tener acceso no autorizado a los datos privados de otras personas?

69.- ¿Existe algún control de seguridad o políticas para los visitantes?

70.- ¿Ya se tomó en cuenta el monitorear las tendencias de violación?

71.- ¿Qué tipo de estrategia de respuesta aplica a cada tendencia de violación?

72.- ¿Existe entre sus contactos organizaciones externas como el CERT de la UNAM y/u otras organizaciones?
CERT.- Equipo de respuesta a Emergencias de Cómputo. El objetivo de este equipo es abordar preocupaciones acerca de seguridad de cómputo de los

investigadores en Internet. Este equipo puede comunicarse inmediatamente con expertos para diagnosticar y resolver problemas de seguridad. También pueden ayudar a establecer y mantener la comunicación entre un sitio y las autoridades del gobierno. Cuando no está dedicado a atender emergencias, el CERT sirve de centro de intercambio para identificar y reparar puntos vulnerables en los principales sistemas operativos. También puede proporcionar evaluaciones informales de sistemas existentes y orientar para mejorar la capacidad de respuesta a emergencias. Puede ayudar indirectamente a formular una política eficaz de seguridad de redes. También se sabe que este equipo ha trabajado con proveedores de sistemas de software para coordinar las soluciones a los problemas de seguridad.

73.- ¿Se pone en contacto con dependencias judiciales locales y federales, así como con las dependencias investigadoras (esta pregunta es para saber qué hacen en caso de un incidente)?

74.- ¿Qué tipo de información puede ser divulgada a la dependencia investigadora y a la prensa cuando existe algún incidente?

75.- ¿Existe algún plan de contingencia en caso de algún incidente?

GLOSARIO

A

Access Control Control de acceso. Los mecanismos de poner límite al acceso a ciertos elementos de información o a ciertos controles basados en la identidad de los usuarios y su pertenencia a ciertos grupos predefinidos. El control de acceso se utiliza típicamente por administradores de sistemas para controlar el acceso de los usuarios a recursos de la red, tales como servidores, directorios y archivos.

ACK Abreviatura de acknowledgement (acuse de recibo). Un mensaje enviado por la unidad receptora a la estación o computadora emisora indicando o bien que la unidad está lista para recibir la transmisión o que una transmisión fue recibida sin error.

ACL Ver LCA

Administrador de red El término "administrador" se utiliza para cubrir a toda esa gente que sea responsable de la operación cotidiana de los recursos del sistema y de la red. Esto puede ser un número de individuos o una organización.

Administrador de seguridad El término "administrador de seguridad" se utiliza para cubrir a toda esa gente que sea responsable de la seguridad de la información y de la tecnología de información. En algunos sitios esta función se puede combinar con el administrador (arriba); en otros, esto será una posición separada.

Administrador de sistema Supervisor de los grandes sistemas de ordenadores encargado de que todo funcione correctamente en ellos.

Alteración o falseo de datos Ataque en el cual el agresor cambia los datos mientras se dirigen de su origen a su destino.

Análisis forense Análisis de un equipo atacado para averiguar el alcance de la violación, las actividades de un intruso en el sistema, y la puerta utilizada para entrar; de esta forma se previenen ataques posteriores y se detectan ataques a otros sistemas de la propia red. Cuando la prevención y los IDS(sistemas de detección de intrusos fallan entonces se realiza un análisis forense.

Anchor Ancla. Marca HTML que nos indica un encadenamiento de hipertexto o su destino.

Antivirus Programa diseñado con el objeto de detectar y eliminar los virus que esté infectando a un ordenador o a un sistema. El programa puede actuar una vez que el ordenador está infectado o permanecer residente en memoria para evitar que ningún virus entre en el sistema. Estos programas necesitan de actualizaciones continuas debido a que permanentemente están apareciendo nuevos virus.

Aplicación Programa que permite hacer algo útil con la computadora (comparadas con las utilerías, que sólo ayudan a su mantenimiento), como escribir o llevar la contabilidad.

Ataque Un incidente cuyo objetivo es causar daño a un sistema o utilizar los recursos de forma no autorizada.

Ataque de diccionario Una forma de ataque en el cual un agresor utiliza un gran conjunto de combinaciones probables para adivinar un secreto.

Auditoría 1. En referencia a computación, un examen de equipamiento, programas, actividades y procedimientos para determinar cuán eficiente funciona el sistema en conjunto, especialmente en términos de asegurar la integridad y seguridad de los datos. 2.El proceso que un sistema operativo utiliza para detectar y grabar los sucesos relativos a la seguridad, tal como un intento de crear, acceder o borrar objetos tales como archivos y directorios. Los registros de tales sucesos se almacenan en un archivo conocido como registro de seguridad, cuyo contenido está disponible sólo para aquellos con la acreditación adecuada.

Autentificación En un sistema operativo multiusuario o de red, el proceso mediante el cual el sistema intenta asegurarse que la persona que está iniciando sesión es la misma para quien se emitió una cuenta.

Autorización en referencia a computación, especialmente con computadoras remotas en una red, el derecho concebido a un individuo para utilizar el sistema y los datos almacenados en él. La autorización típicamente se configura por un administrador de sistemas y se verifica por la computadora basado en alguna forma de identificación de usuario, tal como un número de código o contraseña. También llamado privilegios de acceso, permiso.

B

BS7799 British Standards Institute Code of Practice for Information Security Management. BS7799 especifica aspectos de un programa de protección de la información adecuado a las necesidades de los negocios y la industria. La protección en BS7799 está basado en la seguridad de la integridad, disponibilidad y confidencialidad de activos de la información de corporaciones.

C

Caballo de Troya (o troyano) Son aquellos que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final; esto es, que se presentan como información perdida o "basura", sin ningún sentido. Pero al cabo de un tiempo, y esperando la indicación programada, "despiertan" y comienzan a ejecutarse y a mostrar sus verdaderas intenciones. En general estos virus son destructores de la información contenida en los discos.

CERT Computer Emergency Response Team. (Equipo de Respuesta a Emergencias de Cómputo). El objetivo de este equipo es abordar las preocupaciones acerca de seguridad de cómputo de los investigadores en Internet. Este equipo tiene la capacidad de hablar inmediatamente con expertos para diagnosticar y resolver problemas de seguridad. También pueden ayudar a establecer y mantener la comunicación entre un sitio y las autoridades del gobierno. Cuando no está dedicado a atender emergencias, el CERT sirve de centro de intercambio para identificar y reparar puntos vulnerables en los principales sistemas operativos. También puede proporcionar evaluaciones informales de sistemas existentes y orientar para mejorar la capacidad de respuesta a emergencias. Debido a esto, puede ayudarlo indirectamente a formular una política eficaz de seguridad de redes. También se sabe que este equipo ha trabajado con proveedores de sistemas de software para coordinar las soluciones a los problemas de seguridad.

Cliente Aplicación de software que trabaja en beneficio de usted para extraer un servicio en particular de un servidor en alguna parte de la red. El software cliente es la interfaz del usuario.

Cliente-Servidor Esquema de operación formado por nodos cliente que consumen los servicios ofrecidos por un servidor dentro de una red.

Clipper Chip Es un chip de codificación desarrollado por la NSA y el Gobierno de los Estados Unidos, este chip desde su origen tuvo una puerta trasera.

Clúster Un grupo de servidores de red independientes que funcionan -y parecen desde el punto de visa de los clientes- como si fuesen una sola unidad. Una red de clústers está diseñada para mejorar la capacidad de la red mediante, entre otras cosas, permitir a los servidores de un clúster intercambiar trabajos para balancear la carga del sistema. Al permitir que un servidor realice el trabajo de otro, una red de clústeres también mejora la estabilidad y minimiza o elimina el tiempo que el sistema permanece parado debido a fallos de aplicaciones o del sistema.

Contraseña Herramienta de autentificación empleada para identificar a los usuarios autorizados de un programa o una red para determinar sus privilegios, como el de sólo lectura, el de lectura y escritura, o el de copiado de archivos.

Correo electrónico Email- Forma de comunicación tipo batch, en la que los usuarios se envían mensajes escritos (con posibles anexo multimedia) a través de Internet. La comunicación por correo electrónico requiere de la existencia de direcciones estandarizadas, conocidas por lose servidores de correo a lo largo y ancho de la red global, y manejadas por los ruteadores.

Cuenta Un registro mantenido por redes de área local y sistemas operativos multiusuario para cada usuario autorizado del sistema, por motivos de identificación, administración y seguridad. Las cuentas de una red local las crean los administradores y se usan tanto para validar usuarios como para administrar las políticas del sistema que afecten a cada usuario, como por ejemplo los permisos.

D

DMZ De las siglas De-Militarized Zone. Es una red agregada entre una red de protección y una red externa a fin de proporcionar una capa adicional de seguridad. También llamada Red de perímetro.

DNS Domain Name Service: servicio de nombres de dominio. Protocolo de resolución de nombres, empleado en Internet. Convierte los nombres simbólicos contenidos en las direcciones URL a direcciones IP, y viceversa, con lo cual se puede tener acceso a las páginas Web.

E

EDI (Electronic Data Interchange) Intercambio electrónico de datos. Es el intercambio electrónico de datos comerciales en formato estandarizado, entre las aplicaciones informáticas de empresas relacionadas comercialmente a través de redes de valor agregado.

EMA (Electronic Mail Association) Asociación de correo electrónico

E-mail (Ver correo electrónico)

F

Firewall Protección contra flujos de tráfico no identificados en Internet. Existen diversos esquemas de hardware y software para crear estas "barreras" en los sitios de Internet. El firewall analiza los paquetes y sólo permite el ingreso de los provenientes de direcciones IP conocidas, o aquellos que cumplen ciertas reglas preespecificadas sobre sus contenidos.

FTP (File Transfer Protocol: protocolo de transporte de archivo) Protocolo de software para transportar archivos entre nodos de Internet. Empleando un lenguaje especial para sincronizar los sockets del cliente y del servidor, establece la comunicación y envía los paquetes de datos por el canal. Similares a los sitios Web, existen sitios FTP (cuyos URL inician con ftp://) dedicados a la transferencia de (grandes) archivos, y que ofrecen diversos tipos de acceso y servicio a usuarios "anónimos" o registrados.

FTP anónimo Servicio FTP que sirve a cualquier, no sólo a aquellos que tienen cuentas en el sitio. FTP anónimo por lo general permite descargar (bajar) todos los archivos pero sólo permite cargarlos (subirlos) en un directorio llamado /incoming.

Gateway Puerta de enlace o pasarela. Un dispositivo que conecta redes utilizando diferentes protocolos de comunicaciones de forma que la información puede pasarse de una a otra. Una pasarela transfiere la información y la convierte a un formato compatible con los protocolos utilizados por la red receptora.

GUI (Graphical User Interface: interfaz gráfica de usuario) Interfaz estándar para el manejo de las computadoras personales, que ofrece un ambiente visual más rico y supuestamente más sencillo de utilizar que los lenguajes de control.

H

Host 1. La computadora principal de un sistema de computadoras conectadas por enlaces de comunicaciones. 2.En redes locales basadas en PC, una computadora que proporciona acceso a otras. 3.En Intenet o en redes locales de gran tamaño, un servidor que proporciona acceso a otras computadoras de la red. Un host proporciona servicios, como por ejemplo grupos de noticias, correo o datos a computadoras que se conectan a él.

HTML Acrónimo de HyperText Markup Language (Lenguaje descriptor de hipertexto) dícese del formato estándar de los documentos que se utilizan en Word Wide Web desde el año 1989. En un documento HTML aparecen dos tipos de información: la que directamente se muestra en pantalla y una serie de códigos, transparentes al usuario, que indican como mostrar dicha información. En el documento existen etiquetas que muestran los atributos del texto. Otra función es indicar al sistema cómo responder a las peticiones del usuario. Existen otras etiquetas que son los enlaces que puede contener el documento con otros documentos que pueden estar situados en el mismo servidor o en cualquier otro servidor de la WWW. En el HTML pueden aparecer también ciertas marcas para rellenar formularios con los que enviar la información necesaria para realizar consultas en las bases de datos o para comprar o solicitar determinados servicios.

HTTP Acrónimo de Hypertext Transport Protocol (Protocolo de transporte de hipertexto). Protocolo de Internet que define cómo un servidor Web debe responder a las solicitudes de los artículos que se le hacen vía anchor y URL's.

I

Incidente Un evento que pone en riesgo la seguridad de un sistema de cómputo.

Internet Conjunto de redes y puertas de enlace a nivel mundial que usan la colección de protocolos TCP/IP para comunicarse entre ellas. En el núcleo de Internet se encuentra una red troncal de líneas de comunicación de datos a alta velocidad entre los nodos principales o computadoras host, consistente en miles de sistemas informáticos comerciales, gubernamentales, educativos y de otra naturaleza que se encargan de dirigir los datos y mensajes. Es posible que uno o más nodos de Internet puedan quedar fuera de línea sin que ello suponga un peligro para la globalidad de Internet, ni causar interrupción en el tránsito de datos en la red, dado que no existe ninguna computadora ni red específica que tenga el control.

Intruso Aquella persona que con una variedad de acciones intenta comprometer un recurso, puede ser por hardware o software.

IP Internet Protocol Acrónimo de Internet Protocolo. Protocolo de TCP/IP que gobierna la división de mensajes de datos en paquetes, el direccionamiento de paquetes desde el remitente hasta la red y estación de destino y el ensamblado posterior de los paquetes en dicho destino para reconstruir el mensaje original. IP es la parte sin conexiones de los protocolos TCP/IP.

IRC Acrónimo de Internet Relay Chat. Servicio que permite al usuario de Internet participar en una conversación en línea, en tiempo real, con otros usuarios. El IRC requiere un programa cliente, el cual despliega una lista de los canales IRC activos. Un canal IRC, mantenido por un servidor IRC, se encarga de transmitir el texto escrito por cada usuario conectado al canal a los demás usuarios que se encuentran en ese mismo canal. El cliente IRC se encarga de mostrar los nombres de los canales que se encuentran activos en cada momento, permitiendo al usuario unirse a un canal y muestra, en tal caso, las palabras o líneas de texto de los demás participantes para que el usuario pueda responder.

ISO 1799 Estándar de seguridad basado en el BS7799. ISO 17799 es el estándar de seguridad más reconocido internacionalmente. Es un conjunto completo de controles que se compone por buenas prácticas de seguridad.

K

Kerberos Sistema de autentificación de anfitrión confiable de terceros concebido en el MIT dentro del proyecto Athena. El servidor de autentificación Kerberos es un sistema central que conoce a cada responsable y sus contraseñas.

L

LCA o ACL (Listas de control de acceso) Generalmente se componen de una lista de responsables, una lista de recursos y una lista de permisos. Una lista asociada con un archivo que contiene información sobre qué usuarios o grupos tienen permiso para acceder o modificar un archivo.

Llave de sesión Clave simétrica temporal que sólo es válida por un breve periodo. Las llaves de sesión por lo general son números aleatorios que pueden elegirse ya sea por una de las partes que participan en una conversación, ambas partes en cooperación una con la otra o por un tercero confiable.

Llave privada Clave que pertenece a un responsable y nunca se revela a nadie. Un responsable la utiliza para descifrar los mensajes que se le envían y que están cifrados con la llave pública del responsable. Además se utiliza para cifrar una síntesis de mensajes enviado por el responsable a alguien más. Esto proporciona garantía de no recibir o sin posibilidad de rechazo, ya que cualquiera puede usar la llave pública del responsable par descifrar el compendio y asegurarse de que el mensaje fue originado por el responsable.

Llave secreta Llave utilizada por un algoritmo simétrico para cifrar y descifrar datos.

Login Inicio de sesión. En una red de computadoras, el proceso de autentificación donde un usuario proporciona un nombre de inicio de sesión y una contraseña.

Lotus Domino Servidor basado en Internet para el software Lotus Notes propiedad de Lotus, que lleva funciones de groupware (incluyendo correo electrónico, colaboración y calendarización) a redes empresariales. Domino es un producto de plataforma cruzada que incluye soporte para Unix y OS/2.

Lotus Notes Aplicación de groupware propietaria que ofrece funciones ocmo seguimiento de discusiones, correo electrónico, calendarización de grupo y capacidad de compartir bases de datos en grupos de trabajo grandes y pequeños. Lotus Notes incluye un elaborado lenguaje de desarrollo de aplicaciones que permite adecuarlo a las necesidades de un grupo de trabajo particular. Una versión compatible con Internet de Notes, Lotus Domino, lleva las funciones de notes a redes basadas en TCP/IP.

M

MMS Acrónimo de Manufacturing Message Specification. El MMS es un sistema internacional estandarizado de mensajes para el intercambio de datos en tiempo real y la supervisión y control de la información entre dispositivos de red y/o aplicaciones informáticas independientes de la función de la aplicación y del fabricante del dispositivo o aplicación. El MMS se ha usado como un protocolo de comunicación para dispositivos industriales como: robots, unidades terminales remotas (UTR), Sistemas de Gestión de energía (EMS), dispositivos electrónicos inteligentes (IED).

Módem Acrónimo de MODulator/DEModulator (Modulador/Demodulador). Nombre genérico con el que se designa al dispositivo electrónico que conecta un ordenador a una línea telefónica y transmite datos a través de ella a otro ordenador en una señal portadora analógica que transmite por la línea telefónica, y viceversa, cuando recibe la señal de otro módem.

Multiplataforma o plataforma cruzada Capaz de operar en una red en la cual las estaciones de trabajo son de diferentes tipos (por ejemplo, Macintoch, sistemas con windows y computadoras Unix.)

N

Navegador Programa de navegación para el Web, intenta proporcionar una interface transparente para una gran variedad de información a través de una amplia variedad de mecanismos. Permite el ir de un documento a otro en Internet.

Negación de servicio Ataque en el cual un agresor inunda el servidor con solicitudes falsas o con solicitudes legítimas de entradas. A pesar de que el agresor no se beneficia, el servicio se niega a los usuarios legítimos.

Nodo Término genérico usado para dispositivos que forman parte de una red. Los nodos incluyen computadoras de propósito general, de propósito especial, switches, rourters, bridges, etc.

P

Password (Ver contraseña)

Ping Programa utilizado par probar la accesibilidad de los destino al enviarles una solicitud de eco ICMP y esperar una respuesta.

Plataforma Término con el que se designa al procesador o al sistema operativo sobre el que un programa o aplicación puede ser ejecutado. Existen programas que sólo se pueden ejecutar sobre una plataforma y otros programas que son multiplataforma, es decir, se pueden ejecutar sobre diversos sistemas operativos.

Procesamiento distribuido

1.El procesamiento distribuido en Internet se basa en la utilización de infraestructura que provee Internet, haciendo uso de sus comunicaciones, protocolos y máquinas interconectadas, para distribuir trabajos de procesamiento entre los distintos nodos, que generalmente son computadoras personales a las que se les asigna una pequeña parte de un problema mayor para contribuir a su solución. Además, en este esquema, es necesario la utilización de equipos centrales o servidores que se encarguen de enviar estas pequeñas porciones de problema y recibir los resultados, para luego unirlos y obtener la solución. El procesamiento distribuido puede acelerar los resultados disminuyendo los costos, siendo una alternativa claramente superior ante la utilización de equipos de alto poder de cálculo, a la hora de lograr mayor potencia de procesamiento. 2.-Sistema de computación diseñado para múltiples usuarios que proporciona a cada uno una computadora funcionalmente completa. En computación personal, el procesamiento distribuido toma la forma de redes de área local (LAN), en las cuales las computadoras personales de un departamento u organización se enlazan mediante conexiones de cables de alta velocidad. El procesamiento distribuido ofrece algunas ventajas sobre los sistemas multiusuario. Si la red falla, el usuario puede seguir trabajando. También puede seleccionar software de acuerdo con sus necesidades. Un sistema de procesamiento distribuido se puede implementar con una inversión inicial modesta; basta con dos o tres estaciones de trabajo y, si se desea, un supervisor de archivos central.

Protocolo

Forma estándar de regular la transmisión de datos entre ordenadores. Se define el protocolo como el conjunto de reglas ya aprobadas que posibilitan la comunicación entre ordenadores o entre programas que de otra forma serían incompatibles. Los protocolos controlan un amplio campo de aspectos de comunicaciones, tales como las reglas para abrir y mantener una conexión, el orden de transmisión de los bits, el formato de los mensajes de correo electrónico, etc.

Puerto

En Internet, un puerto es un canal lógico a través del cual se rutea cierto tipo de datos de aplicación para decodificar datos entrantes y rutearlos al destino correcto. Cada tipo de servicio de Internet, como FTP o IRC, tiene cierto número de puerto asociado. La Autoridad de Números Asignados de Internet (IANA) controla la asignación de números. El número de puerto es el número que permite el envío de paquetes IP a un proceso determinado sobre una computadora conectada a Internet. Algunos números de puerto, se encuentran permanentemente asignados; por ejemplo, los datos de correo electrónico bajo SMTP van al puerto número 25. TCP permite el empleo de un total de 65,535 números de puertos, y el mismo número se encuentra disponible para UDP.

R

Red

Una red de computadoras es un conjunto de terminales, nodos, servidores y elementos de propósito especial que interaccionan entre sí con la finalidad de intercambiar información y compartir recursos.

Remoto Que no se encuentra en la vecindad inmediata, como una computadora u otro dispositivo que están situados en un lugar (una habitación, un edificio o una ciudad), a lo que se accede por medio de algún tipo de cable o enlace de comunicaciones.

RFC (Request For Comment, Solicitud de comentarios) Serie de documentos, que comenzó en 1969, la cual describe el conjunto de protocolos Internet y experimentos relacionados. Una RFC es un documento en el que se detalla o se propone un estándar de Internet.

RFC 2196 Es una guía para el desarrollo de políticas de seguridad y procedimientos para sitios que tienen sistemas en Internet. El propósito del documento es proveer una guía práctica para administradores que tratan de asegurar su información y servicios. Los temas cubiertos incluyen la formación y contenido de políticas de seguridad, seguridad de redes y respuestas a insidentes de seguridad.

rlogin Servicio ofrecido por UNIX de Berkeley que permite a los usuarios de una máquina conectarse a otros sistemas UNIX (par los cuales tiene autorización) e interactuar como si sus terminales estuvieran conectadas directamente. Similar a Telnet.

Ruteador Dispositivo intermedio en una red de comunicaciones que se encarga de la distribución de mensajes. Un ruteador es un dispositivo electrónico que examina cada paquete de datos que recibe y luego decide de qué manera enviarlo a su destino, siguiendo la ruta más eficiente disponible. En un conjunto de redes de área local (LAN) interconectadas donde se utilizan los mismos protocolos de comunicaciones, un ruteador actúa como enlace entre las LAN, haciendo posible que puedan enviarse mensajes de una a otra.

S

Sala de chat Término informal para un canal de comunicación que enlaza computadoras y permite a los usuarios "conversar" mediante el envío de mensajes de uno a otro en tiempo real.

Servicio 1. Función basada en cliente u orientada a usuario, tal como soporte técnico o suministro de red. 2. En relación con programación y software, se denomina servicio a un programa o rutina que da soporte a otros programas, particularmente a bajo nivel (cercano al hardware). 3. En redes, funcionalidad especializada basada en software proporcionada por los servidores de la red.

Servidor El servidor es una computadora multiusuario que recibe y atiende pedidos de información provenientes de muchas otras máquinas (usualmente de tipo personal). Cuando finalmente la información solicitada llega al sistema cliente, es procesada (y consumida) allí en forma local. Los sistemas de información que funcionan bajo Internet ya no requieren necesariamente de un cliente completo (es decir, una computadora con grandes capacidades de disco y memoria), sino que a veces basta con una máquina pequeña, o incluso un sistema de bolsillo; esto es debido al uso de HTML, y se conoce como thin client.

Sesión 1. Tiempo en el que un programa se encuentra en ejecución. En la mayoría de los programas interactivos, una sesión es el tiempo durante el cual el programa acepta entradas y procesa la información. 2. En comunicaciones, se denomina sesión al tiempo durante el que dos computadoras mantienen una conexión. 3. Una capa específica de protocolo en el modelo ISO/OSI que administra la comunicación entre usuarios o procesos remotos.

Shell Intérprete de comandos en Unix, él no es parte del sistema operativo, hace uso extenso de muchas características del sistema. Es la interfaz principal entre un usuario sentado frente a una terminal y el sistema operativo.

Sistema 1. Conjunto formado por un ordenador y todos sus periférico. 2.Dícese de cualquier colección o combinación de programas, procedimientos, datos y equipamiento utilizados en el proceso de la información.

Sistema operativo Término que se utiliza para referirse al programa, o más bien al conjunto de programas interrelacionados, que se dedican a controlar las funciones básicas del sistema, las operaciones de bajo nivel y el manejo de archivos sin necesidad de que intervenga un operador.

Sitio 1.Un "sitio" es cualquier organización que posea computadoras o recursos de redes. Estos recursos pueden incluir computadoras host de los usuarios, los ruteadores, los servidores terminales, PCs u otros dispositivos que tienen acceso a Internet. Un sitio puede ser un usuario final de servicios de Internet. 2.-Dícese del host de Internet que permite acceso remoto a través de FTP, telnet, gopher, etc.

SMTP Simple Mail Transport Protocol. Protocolo Simple de Transporte de Correo. Protocolo de Internet que dirige la transmisión de correo electrónico en redes de computadoras. En realidad, SMTP es simple ya que no soporta la transmisión de datos que no sean de texto. Por esta razón, las "Extensiones Multipropósito de Correo de Internet (MIME)" soportan archivos binarios de muchos tipos, y S/MIME soporte correo electrónico encriptado.

smurf Este ataque es bastante simple y a su vez devastador. Consiste en recolectar una serie de direcciones de broadcast para a continuación mandar una petición de echo ICMP a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. Este paquete maliciosamente manipulado, será repetido en broadcast, y cientos o miles de hosts (según la lista de direcciones de broadcast disponible) mandaran una respuesta de echo a la victima cuya dirección IP figura en el paquete ICMP.

SNMP Acrónimo de Simple Network Management Protocol (Protocolo de manejo simple de red). Protocolo perteneciente al entorno TCP/IP en el que se especifican la forma de comportarse los nodos de una red cuando se utilizan agentes para monitorizar el tráfico de la red y mantener una base de datos sobre dicho manejo.

Spam El acto de arrojar grandes cantidades de mensajes electrónicos a través de correo electrónico o grupos de interés a personas que no desean recibirlos.

SQL Siglas de Lenguaje de Consultas Estructurado. En sistemas de administración de bases de datos, lenguaje de consultas desarrollado por IBM que se ha vuelto el estándar de facto para consultas de bases de datos en una red cliente/servidor. Las consultas SQL se aproximan a la estructura de una consulta de lenguaje natural en inglés. Los resultados de una consulta se muestran en una tabla de datos que consta de columnas (correspondientes a los campos de los datos) y filas (correspondiente a los registros de datos.)

Suplantación de direcciones Tipo de ataque en el cual el agresor roba de un sistema una dirección legítima de red (por ejemplo, IP) y la utiliza para suplantar al sistema al cual pertenece la dirección.

SVN Secure Virtual Network. Es una arquitectura que provee una estructura íntegra para desarrollar y controlar una implementación de seguridad.

T

TCP Acrónimo de Transmission Control Protocol (Protocolo de Control de Transmisión). Protocolo de transmisión de la red ARPAnet que forma parte del TCP/IP. Este protocolo funciona en el nivel de transporte del modelo OSI, es decir, se encarga del establecimiento y verificación de la conexión de los datos. Se utiliza en las redes basadas en UNIX.

TCP/IP Acrónimo de Transmission Control Protocol/Internet Protocol (Protocolo de control de transmisión/protocolo Internet).Es un conjunto de protocolos de comunicaciones de datos. Estos protocolos permiten el enrutamiento de información de una máquina a otra, la entrega de correo electrónico y noticias, e incluso la capacidad de conexión remota. Estos protocolos pueden correr en cualquier hardware o sistema operativo.

El término TCP/IP se refiere a los dos protocolos principales, el Protocolo de Control de Transmisión y el Protocolo Internet (Transmission control Protocol/Internet Protocol). Si bien existen muchos otros protocolos que ofrecen servicios que operan sobre TCP/IP, estos son los más comunes.

Telnet Protocolo que permite a los usuarios de Internet iniciar una sesión en otra computadora conectada a Internet, incluyendo a aquellos usuarios que no se pueden conectar directamente con los protocolos TCP/IP de Internet. Telnet establece una terminal de computadora simple llamada terminal virtual de red.

TIS FWTK Juego de herramientas TIS Internet Firewall (FWTK) de Trusted Information Systems. TIS Internet Firewall Toolkit.

Token Dispositivo de hardware utilizado para aumentar la autentificación basada en contraseñas al retar a un responsable a que pruebe que posee la seña.

Token-Autentificado dinámico En sistemas de autentificación, cierto tipo de dispositivo físico (como una tarjeta con banda magnético, una tarjeta inteligente o un dispositivo parecido a una calculadora que genera una contraseña) que debe estar en posesión del individuo para tener acceso a una red. El dispositivo por sí solo no basta; el usuario también debe proporcionar algo memorizado, como un número de identificación personal (PIN).

U

UDP Acrónimo de User Datagram Protocol-Protocolo de datagrama de usuario. El protocolo sin conexión dentro de TCP/IP que corresponde a la capa de transporte en el modelo ISO/OSI. UDP convierte los mensajes de datos generados por una aplicación en paquetes a enviar mediante IP, pero no comprueba que el mensaje se haya enviado correctamente.

UPS Uninterruptible Power Supply. Sistema de alimentación ininterrumpida. Batería capaz de suministrar energía eléctrica contínua a un sistema de computación en caso de interrupción eléctrica. La batería, que se carga mientras la computadora está encendida, se activa cuando ocurre una interrupción eléctrica y suministra energía durante 10 minutos o más, tiempo suficiente para guardar los archivos y apagar la computadora para preservar la integridad de los datos.

V

VAN Value Added Network. Red de valor agregado. Es un intermediario entre sociedades comerciales electrónicas.

Virus Un virus de computadora es una pieza de código ejecutable, regularmente escondido en documentos, con habilidad para reproducirse. Muchos virus causan problemas al ocupar espacio de almacenamiento, destruir datos y al reducir el desempeño del sistema. Anteriormente los virus eran esparcidos a través de discos flexibles y archivos ejecutables, sin embargo, hoy en día es más común que los virus se diseminen más rápidamente vía Internet.

VPN Virtual Private Network. Usa infraestructura de una red pública haciendo conexiones entre nodos geográficamente dispersos. Para los usuario una VPN luce como una red privada, aun cuando está compartiendo cables de web con el tráfico de cientos o miles de otros usuarios al mismo tiempo. Tiene todas las características de una red privada.

W

WAN Acrónimo de wide area network (red de área extensa). Una red extendida geográficamente, que se basa en las capacidades de comunicación para unir los diversos segmentos de la red. Una WAN puede ser una red local grande, o puede estar formada por una serie de LANs (redes de área local)conectadas entre sí.

WWW (World Wide Web) Red de amplitud mundial. También se le conoce como Web. Está compuesta por un conjunto de documentos de hipertexto interconectados que se encuentran en diferentes servidores Web y otros documentos, menús y bases de datos que se encuentran disponibles a través de los URL (localizadores de recursos uniformes). Todos estos documentos están realizados y enlazados con el HTML y los servidores utilizan el HTTP para distribuir las páginas.

BIBLIOGRAFÍA

A Prueba de Hackers
Lars Klander
Anaya Multimedia

Web security and commerce=
Seguridad y comercio en el Web
Simson Garfinkel y Gene Spafford
(Riesgos, tecnologías y estrategias)
Mc Graw-Hill, 1999.

Construya Firewalls para Internet
Brent Chapman y Elizabeth D. Zwicky
McGraw-Hill

Diccionario de Informática e Internet
Microsoft
McGraw-Hill. Interamericana

Entér@te.
UNAM., Suplemento mensual.
29 de agosto del 2002., No. 11.

Guía de Seguridad e Integridad de Datos
Marc Farley, Tom Stearns y Jefrey Hsu
McGraw-Hill

Firewalls y la Seguridad en Internet
Karanjit Siyan y Chris Hare
Prentice-Hall, 2a Ed., 1997.

Manual de Firewalls
Marcus Goncalves
Mc Graw-Hill., 2001.

Practical UNIX& Internet Security
Simson Garfinkel y Gene Spafford

Redes de Computadoras. Protocolos, normas e interfaces.
Uyless Black
Computec y ra-ma , 2ª ed. 1997.

Seguridad en Unix y Redes
Antonio Villalón Huerta
V1.2., octubre 2002.

Virus Informáticos
Arturo Hernández Hernández
DGSCA-UNAM., 2000.

Referencias de Internet

http://www.magasecurity.org/trojans/kuang/

http://www.criptored.upm.es/guiateoria/gt_m189a.htm

http://www.vsantivirus.com/hoax-carlson.htm

http://www.checkpoint.com

http://www.checkpoint.com/products/downloads/firewall-1_statefulinspection.pdf

http://www.ietf.org/rfc/rfc2196.txt?Number=2196

http://andercheran.aiind.upv.es/toni/personal/

http://www.trendmicro.com/

http://www.iss.net

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/network/authen.asp

http://www.ipa.go.jp/security/english/anti-virus-e.html

http://www.icsalabs.com/surveysponsor/