REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES

TESIS

SEGURIDAD EN EL PERÍMETRO DE LA RED PETROINDUSTRIAL

Tesis presentada como requisito para optar al Título de Máster en Seguridad y Desarrollo con Mención en Gestión Pública y Gerencia Empresarial

Autora: Ing. Sistemas Nancy Guzmán Garzón
CPNV. EMC. Galo Alemán R.

Quito, Junio 2005

INDICE GENERAL

CAPITULO I

AMENAZAS DE LA INFORMACION

INDICE GENERAL

CAPITULO II

SEGURIDAD DE LA INFORMACION

CAPITULO III

SEGURIDAD PETRIMETRAL

CAPITULO IV

ANALISIS ACTUAL DE PETROINDUSTRIAL

CAPITULO V
PROPUESTA

SEGURIDAD EN EL PERIMETRO DE LA RED DE PETROINDUSTRIAL

Autor : ING. NANCY GUZMAN GARZON
Asesor: CPNV. GALO ALEMAN
Año : 2005

Resumen

El grado de dependencia que tiene Petroindustrial respecto de su información, la misma que se encuentra en un alto porcentaje en los equipos de computación y que es manejada bajo la red tecnológica que dispone actualmente la empresa, conlleva a una serie de riesgos y vulnerabilidades, que son necesarios identificarlos para establecer pautas que garanticen la inalterabilidad, confidencialidad y disponibilidad de la información.

El análisis realizado evidencia importantes debilidades en el esquema de la seguridad de la información de Petroindustrial, es urgente realizar acciones preventivas y correctivas que ayuden a mitigar los efectos negativos que pueden derivarse de estas debilidades identificadas, por lo que se plantea:

- Propuesta de Gestión, contempla una reestructuración de la Unidad de Sistemas, la creación de un Comité de Seguridad de la Información que gestione la seguridad de la información de Petroindustrial, recomienda un procedimiento de creación de políticas organizacionales y describe un conjunto de políticas organizacionales prioritarias, así como un modelo de gestión que permita un trabajo continuo a través del cual se vayan solucionando y elevando el nivel de seguridad de la información de Petroindustrial.
- Propuesta Técnica, dado que los requerimientos de seguridad planteados por la empresa se enmarcaron en el perímetro de la red de Petroindustrial Matriz la misma plantea una alternativa prioritaria a ser adoptada y pautas para llevar a cabo un rediseño de la estructura de seguridad perimetral.

Las recomendaciones se enfocan a dos tipos de acciones, las urgentes y las necesarias. Dentro del esquema de las urgentes se detallan acciones que deben implementarse inmediatamente para asegurar un mínimo necesario de seguridad. Las recomendaciones necesarias son las recomendaciones que por su naturaleza o gestión, deberán implementarse en una segunda fase no menos urgente pero generadas bajo una estructura que trabaje en forma planificada, continua y sobre todo que intervengan representantes de los diferentes distritos de Petroindustrial y de la oficina matriz.

CAPITULO I

2.7. AMENAZAS DE LA INFORMACION

1.1 INTRODUCCION

El grado de dependencia que tiene Petroindustrial respecto de su información, combinado con el repunte tecnológico mundial, mismo que conlleva inmerso una serie de riesgos de ataque y vulnerabilidad crítica de la empresa, determina la necesidad de establecer controles suficientes que garanticen la inalterabilidad, confidencialidad y disponibilidad de la información.

Petroindustrial conciente de que la aplicación ordenada de de controles y estándares administrativos, operativos y tecnológicos para asegurar la información de Petroindustrial, minimizan el riesgo de pérdida, accesos no deseados, errores y daños voluntarios e involuntariosa a la información apoyó el desarrollo este trabajo, el mismo que se orienta al análisis y propuestas administrativas operativas apropiadas a la realidad y estructura de Petroindustrial Matriz, que permitan asegurar adecuadamente a la información que se encuentra en la infraestructura tecnológica de Petroindustrial.

Dada la estructura organizacional de Petroindustrial distribuida en 3 distritos y la oficina matriz y considerando que maneja sistemas de información similares auque en diferentes tamaños y proporciones, pese a que el estudio se centralizara en la Matriz-Quito, la propuesta podría aplicarse en parte posteriormente en los distritos de Petroindustrial.

1.2 OBJETIVOS

OBJETIVO GENERAL

Mejorar la seguridad de la información y proponer un diseño de seguridad en el perímetro de la Red de Petroindustrial Matriz.

OBJETIVOS ESPECIFICOS

- Identificar los factores que están afectado a la seguridad de la información de Petroindustrial Matriz
- Proponer un esquema administrativo operativo que combine las mejores prácticas empresariales con las necesidades particulares de Petroindustrial para asegurar la información.
- Identificar mecanismos existentes en el mercado que permitan elevar el nivel de seguridad de la información en el perímetro de la Red de Petroindustrial.
- Proponer un diseño de seguridad en el perímetro de la Red de Petroindustrial.

1.3 EVOLUCION DE LA SEGURIDAD INFORMÁTICA

Los conceptos y principios de seguridad han seguido un patrón de evolución dentro de la organización social, desde la familia a una tribu, reino y estado. Muy pronto fue claro que los grupos eran menos vulnerables a las amenazas que las personas individuales, proveían una disuasión/intimidación. Los seres humanos aprendieron rápidamente que la mera existencia de medidas protectoras era frecuentemente suficiente para persuadir a los adversarios.

Los conceptos de alertar, evitar, detectar, alarmar y reaccionar son tan viejos como la vida misma, siendo una parte esencial de la pugna diaria por la vida, y están fundados en el instinto básico de supervivencia.

La actual tecnología informática, la miniaturización, los nuevos sistemas de comunicación entre otros avances, han generado nuevos ingredientes en los temas de seguridad, ingredientes que han permitido que la seguridad sea un tema amplio y complejo.

La Seguridad Informática implica conocer las características de lo que se pretende proteger: la Información. Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Los sistemas informáticos más seguros del mundo son los que están completamente aislados de los usuarios y de otros sistemas. Sin embargo, en el mundo real normalmente necesitamos sistemas informáticos compartidos que funcionen en red.

La mayoría de empresas desconoce la magnitud del problema con el que se enfrenta el mundo informático y, generalmente no se invierte en el capital humano ni económico necesario para prevenir el daño y/o pérdida de la información que es el conocimiento con que se cuenta.

1.4 RELACIÓN OPERATIVIDADï SEGURIDAD

Para establecer la relación entre la operatividad y la seguridad se debe analizar las características y conceptos de la información en el entorno informático:

- *Crítica***,** los sistemas pueden contener información crítica*,* la misma que puede ser indispensable para garantizar la continuidad de la operatividad de las actividades de una empresa.
- *Valiosa,* la información puede tener esta característica por su importancia y valor de haberla generado.
- *Sensitiva*, por su relación con la confidencialidad y privacidad de la misma, debe ser conocida sólo por personas autorizadas*.*
- *Integridad,* característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado.
- *Disponibilidad u Operatividad* es la capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que el hardware y el software funcione perfectamente.
- *Privacidad o Confidencialidad* es la necesidad de que la misma sólo sea conocida por personas autorizadas.
- *La Autenticidad* esta propiedad también permite asegurar el origen de la información, validación el emisor.

La Amenaza en el entorno informático se da con cualquier elemento que comprometa a la operatividad y disponibilidad de los recursos informáticos.

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos

conformarán políticas que garantizarán la seguridad de los recursos informáticos.

El riesgo es ñla proximidad o posibilidad de dañoò, el análisis y el desarrollo de políticas de seguridad permitirá: minimizar la posibilidad de su ocurrencia, reducir al mínimo el perjuicio producido, diseñar métodos para una rápida recuperación de los daños experimentados y corrección de las medidas de seguridad en función de la experiencia recogida.

La seguridad total en el ámbito Informático es muy difícil de conseguir en un 100% por lo que se habla de Fiabilidad y se define como la probabilidad de que un sistema se comporte tal y como se espera de él. Luego para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer ñqué es lo que queremos protegerò y ñde quién lo queremos protegerò, para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos.

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos; los datos de un sistema son los más importantes y lo más difícil de recuperar.

El nivel de seguridad dependerá del análisis de riesgos a que está expuesto los recursos, los costos a los que se esté dispuestos a incurrir y de las medidas a tomar para mantener la operatividad de los recursos informáticos.

1.5 SEGURIDAD FÍSICA

La Seguridad Física implica la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos. Los controles y mecanismos de seguridad dentro y alrededor de un Centro de Cómputo así como en los medios de acceso remoto al y desde el mismo, se implementan para proteger el hardware y la información almacenada.

Es importante considerar que cada sistema es único debido a las características especiales que le rodean, por lo que es necesario analizar los peligros más importantes y aspectos que deben considerar:

1.5.1 Incendios

El fuego es una de las principales amenazas contra la seguridad. Es considerado el enemigo número uno de las computadoras ya que puede destruir fácilmente los archivos de información y programas, por lo que es necesario considerar los siguientes aspectos para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos:

- El área en la que se encuentran las computadoras debe estar libre de materiales combustible o inflamable.
- Las paredes deben ser de materiales incombustibles.
- Debe construirse un ñpiso falsoòinstalado sobre el piso real, con materiales incombustibles y resistentes al fuego.
- No se debe permitir fumar.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles.

- El piso y el techo del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables, estas áreas deben contar con mecanismos de ventilación y detección de incendios adecuados.
- La temperatura no debe sobrepasar los 18º C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales y/o automáticos.

1.5.2 Inundaciones y condiciones climatológicas

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior, para lo que se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

La frecuencia y severidad de su ocurrencia de desastres naturales deben ser consideradas en las estrategias de seguridad.

1.5.3 Instalación eléctrica

Trabajar con computadoras implica trabajar con electricidad y en la medida que se desarrolle la estructura de las redes y la disponibilidad recursos tecnológicos, la infraestructura eléctrica se vuelve más compleja y debe ser manejada por un especialista, quien debe evaluar los riesgos y aplicar soluciones de acuerdo con las normas de seguridad recomendadas.

El cable de red es un nuevo frente de ataque, los intrusos intentan acceder a los datos ubicados en una red de computadoras a través del desvío o estableciendo una conexión no autorizada en la red, los datos que fluyen a través del cable pueden estar en peligro.

1.5.4 Acciones hostiles

- ROBO, las computadoras son posesiones valiosas de las empresas y están expuestas al robo, esta situación se agrava con la facilidad actual con la que se puede copiar los datos, software, e incluso discos duros son fáciles de sustraer sin dejar ningún rastro.
- FRAUDE, cada año, millones de dólares son sustraídos de empresas y, en muchas ocasiones las computadoras han sido utilizadas como instrumento para dichos fines.
- SABOTAJE, es uno de los peligros en los centros de procesamiento de datos, la protección contra el saboteador es uno de los retos más duros ya que puede ser un empleado o un sujeto ajeno a la propia empresa, quienes intentan desaparecer información o alterarla.

1.5.5 Control de accesos físico

El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

El uso de credenciales de identificación es uno de los puntos importantes del sistema de seguridad, a fin de poder efectuar un

control eficaz del ingreso y egreso del personal a los distintos sectores de la empresa. En este caso la persona se identifica con algo que posee. Las personas también pueden acceder mediante algo que saben (un número de identificación) que se solicitará a su ingreso.

1.4.6 Utilización de Sistemas Biométricos

La Biometría es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas, es la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos. La tecnología biométrica es beneficiosa porque Pueden eliminar la necesidad de poseer una tarjeta para acceder, y principalmente porque las características biométricas de una persona son intransferibles a otra. Sus utilizaciones más frecuentes son:

- La HUELLA DIGITAL, basada en el principio de que no existen dos huellas dactilares iguales, este sistema es utilizado con excelentes resultados.
- La VERIFICACIÓN DE VOZ, este sistema es muy sensible a factores externos como el ruido, el estado de ánimo y enfermedades de la persona, el envejecimiento, etc.
- VERIFICACIÓN DE PATRONES OCULARES, se basa en los patrones del iris o de la retina y hasta el momento son los considerados más efectivos (en 200 millones de personas la probabilidad de coincidencia es casi 0). Su principal desventaja reside en la resistencia por parte de las personas a que les analicen los ojos, por revelarse enfermedades que en ocasiones se prefiere mantener en secreto.

1.6 SEGURIDAD LÓGICA

A medida que aumenta la interconexión global del planeta, se está convirtiendo en realidad el sueño futurista de disponer de la información en cualquier lugar, en cualquier momento y en cualquier dispositivo.

Las empresas y sus clientes sólo almacenarán sus datos confidenciales en un entorno que le garanticen un alto nivel de seguridad. Las encuestas sobre delitos y seguridad informáticos indican un alto porcentaje de intentos de ataques o infracciones de seguridad. Los promedios de pérdidas anuales son altos, muchos de ellos a través de Internet y a equipos con el sistema operativo Microsoft Windows, por lo que el conocer y desarrollar los temas de seguridad son prioritarios.

Los administradores de red, actualmente deben enfrentar continuos ataques a los sistemas informáticos, por lo que la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos de la red privada.

La Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo, implica:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos y por el procedimiento correcto.

- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.6.1 Control de Acceso Lógico

Los controles de acceso se utiliza para restringir los accesos a la información y los recursos únicamente a personal autorizado. La identificación y autentificación, es una línea de defensa para la mayoría de los sistemas computarizados, es la base para los controles de acceso y para el seguimiento de las actividades de los usuarios.

Existen cuatro tipos de técnicas que permiten realizar la autenticación del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Password o palabra clave que solamente el individuo conoce.
- Por medio de una tarjeta magnética.
- A través de una identificación física del individuo, por ejemplo las huellas digitales o la voz.
- A través de patrones de escritura.

La Seguridad Informática se basa en la efectiva administración de los permisos de acceso a los recursos informáticos, esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios.
- Identificación de los usuarios de acuerdo con una norma homogénea para toda la organización.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos.
- Las revisiones deben orientarse a verificar los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso.
- Detección de actividades no autorizadas, auditorias y seguimiento de los registros de transacciones; para detectar la ocurrencia de actividades no autorizadas.
- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización.
- El acceso a la información también se realiza a través de funciones o roles de usuarios, como por ejemplo un rol para programadores, el cual le permita realizar ciertas actividades de a cuerdo a su trabajo permitido. En este caso los derechos de acceso pueden agruparse de acuerdo con el rol de los usuarios.
- Los controles y asignaciones de permisos también pueden ser a nivel de aplicación, restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema, por ejemplo cuando una organización dispone de licencias limitadas de un determinado

producto de software, no permita la utilización del producto cuando se a superado el número de usuarios permitidos.

1.6.2 Control de acceso externo

Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos y conexiones con redes externas, exponen a los sistemas a niveles mayores de riesgo. Asegurar todos los enlaces de una red para que disponga de adecuados niveles de seguridad permite proteger la información de un ataque; por lo que es importante determinar:

- Elementos de la red que pueden ser accedidos
- Procedimiento de autorización para la obtención de acceso
- Controles para la protección de la red
- Encriptación de los datos
- Concienciación de usuarios
- Control de los dispositivos de control de puertos, estos dispositivos autorizan el acceso a un puerto determinado y pueden estar físicamente separados o incluidos en otro dispositivo de comunicaciones, como por ejemplo un módem.
- Control Firewalls o puertas de seguridad, que filtrar el acceso entre dos redes, usualmente una privada y otra externa.

1.7 ELEMENTOS DE LA RED

1.7.1 Protocolos de Red

Las comunicaciones en las redes, se realiza a través de sistemas operativos y hardware especial, que utilizan sistemas de comunicación o lenguaje llamado protocolo. Los protocolos de cada capa tienen una interfaz bien definida y sólo poseen conocimiento de las capas directamente inferiores. Esta división de los protocolos ofrece abstracción de los mecanismos de bajo nivel responsables por la transmisión de datos sobre las informaciones intercambiadas. Por lo tanto un Protocolo es el conjunto de normas que rige cada tipo de comunicación entre dos computadoras

Algunos protocolos se encargan de transportar datos, mientras que otros se encargan de la comunicación entre computadoras, y otros de convertir correctamente los datos. Ejemplos de Protocolos:

- Capa 1: Nivel físico
  - Cable coaxial
  - Cable de fibra óptica
  - Cable de par trenzado
  - Microondas
  - Radio
  - Palomas
  - RS-232
- Capa 2: Nivel de enlace de datos
  - Ethernet, Fast Ethernet, Gigabit Ethernet
  - Token Ring
  - FDDI
  - ATM
  - HDLC
- Capa 3: Nivel de red
  - ARP, RARP

  - IP (IPv4, IPv6)
  - X.25
  - ICMP
  - IGMP
  - NetBEUI
  - IPX
  - Appletalk

- Capa 4: Nivel de transporte

  - TCP
  - UDP
  - SPX

- Capa 5: Nivel de sesión

  - NetBIOS
  - RPC
  - SSL

- Capa 6: Nivel de presentación

  - ASN.1

- Capa 7: Nivel de aplicación

  - SNMP
  - SMTP
  - NNTP
  - FTP
  - SSH
  - HTTP
  - SMB/CIFS
  - NFS
  - Telnet
  - IRC
  - ICQ
  - POP3
  - IMAP

A continuación se describe algunos de los protocolos:

- NETBIOSï NETBEUIï NWLINKï WINS Network Basic Input Output System, es el protocolo más sencillo. Está compuesto por menos de 20 comandos que se ocupan del intercambio de

datos. Se ha perfeccionado y ampliado recibiendo el nuevo nombre NetBEUI (NetBIOS Extended User Interface), se amplio nuevamente recibiendo el nombre de NWLink (NetWare Link). NetBIOS toma el puerto 137ï 139 en computadoras que utiliza el sistema operativo Windows. Está considerado el protocolo más fácilmente vulnerable, por lo que se recomienda no utilizarlo.

- TCP/IP, actualmente se utiliza ampliamente, sus estándares soporta autenticación, integridad y confidencialidad a nivel de datagramas, se basa en las capas del modelo OSI, contempla un conjunto de protocolos de TCP/IP, que consta de 4 capas principales y que se han convertido en un estándar a nivel mundial. Utiliza el puerto 21 TCP.
- IP, Internet Protocol define la base de todas las comunicaciones en Internet, es utilizado por los protocolos del nivel de transporte (como TCP) para encaminar los datos hacia su destino. IP tiene únicamente la misión de encaminar el datagrama sin comprobar la integridad de la información que contiene. Para ello se utiliza una nueva cabecera que se antepone al datagrama que se está tratando. Este protocolo no garantiza la llegada de los paquetes a destino, ni su orden; tan solo garantiza la integridad del encabezado IP. La fiabilidad de los datos deben garantizarla los niveles superiores. El protocolo IP identifica a cada equipo que se encuentre conectado a la red mediante su correspondiente dirección, esta dirección es un número de 32 bits que debe ser único para cada Host, normalmente suele representarse en cuatro cifras de 8 bits separadas por puntos (por ejemplo: 205.025.076.223). En este número se ha establecido cuatro clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:
    - Clase A: son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas

direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de las computadoras (Hosts) que pertenezcan a esta misma red. Esto significa que podrán existir más de dieciséis millones de Hosts en cada una de las 126 redes de esta clase. Este tipo de direcciones es usado por redes muy extensas.

- Clase B: estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, debiendo ser un valor entre 128.001 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador de la computadora permitiendo, por consiguiente, un número máximo de 64.516 ordenadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes.
- Clase C: el primer byte está entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.001.001 hasta 223.254.254. Un byte se usa para el Host, permite que se conecten un máximo de 254 computadoras en cada red.
- Clase D: esta clase se usa con fines de multidifusión a más de un dispositivo. El rango es desde 224.0.0.0 hasta 239.255.235.255.

- IPXï SPX, Internetwork Packet Exchangeï Sequenced Packet Exchange es el protocolo de nivel de red propietario de

NetWare (para su sistema operativo Novell) es utilizado en las redes tipo LAN.

- FTP, File Transfer Protocol se incluye como parte del TCP/IP, estando destinado proporcionar el servicio de transferencia de archivos. El FTP depende del protocolo TCP para las funciones de transporte, y guarda alguna relación con Telnet (protocolo para la conexión remota). FTP utiliza dos canales de conexión separados: uno es el canal de comandos que permanece abierto durante toda la sesión y el otro es el canal de transmisión de archivos.
- SMTP El servicio de correo electrónico se realiza a través del protocolo Simple Mail Transfer Protocol, (empleando redes TCP/IP) y permite enviar mensajes a otros usuarios de la red. Los mensajes de correo electrónico generalmente no se envían directamente a las computadoras personales de cada usuario, sino a un servidor de correo que actúa como almacén de los mensajes recibidos. Los mensajes permanecerán en este sistema hasta que el usuario los transfiera a su propio equipo para leerlos de forma local (vía POP). El cliente de correo envía una solicitud a su eï mail Server (al puerto 25) para enviar un mensaje (y almacenarlo en dicho servidor). El Server establece una conexión SMTP donde emisor y receptor intercambian mensajes de identificación, errores y el cuerpo del mail. Luego de esto el emisor envía los comandos necesarios para la liberación de la conexión.

- POP, Post Office Protocol fue diseñado para la recuperación de correo desde el eï mail Server hacia la computadora destinataria del mensaje.

  Al igual que sucede con SMTP, inicialmente el proceso escucha los puertos 109 y 110 en TCP y cuando el emisor solicita el

mensaje se establece una conexión full duplex donde se intercambian los mensajes Emisorï Server para luego finalizar la conexión cuando se hallan enviado cada uno de los mails almacenados en el servidor.

Actualmente el protocolo POP se encuentra en su tercera implementación por lo que generalmente se escuchará sobre POP3.

- NNTP, Network News Transfer Protocol fue diseñado para permitir la distribución, solicitud, recuperación y envío de noticias (News).
- SNMP, Simple Network Management Protocol se utiliza para monitorizar, controlar y administrar múltiples redes físicas de diferentes fabricantes, donde no existe un protocolo común en la capa de Enlace. La estructura de este protocolo se basa en utilizar la capa de aplicación para evitar el contacto con la capa de enlace y, aunque es parte de la familia TCP/IP no depende del IP ya que fue diseñado para ser independiente, ejemplo, IPX de Novell. Permite la gestión remota de dispositivos de red, tales como switches, routers y servidores.
- TELNET, protocolo diseñado para proporcionar el servicio de conexión remota (remote login). Forma parte del conjunto de protocolos TCP/IP y depende del protocolo TCP para el nivel de transporte. Es un emulador de terminal que permite acceder a los recursos y ejecutar los programas de un equipo remoto en la red, de la misma forma que si se tratara de una terminal real directamente conectado al sistema remoto. Una vez establecida la conexión el usuario podrá iniciar la sesión con su clave de acceso. El sistema local que utiliza el usuario se convierte en una terminal "no inteligente" donde todos los caracteres pulsados y las acciones que se realicen se envían al Host remoto, el cual devuelve el resultado de su trabajo. Este

programa utiliza TCP para conectarse utiliza el puerto 23 (por defecto). Una vez que se establece la conexión, Telnet actúa como un intermediario entre el cliente y el servidor. Estas conexiones suelen ser más económicas pero más lentas. Su mayor problema es de seguridad, ya que todos los nombres de usuario y contraseñas necesarias para entrar en las máquinas viajaban por la red sin cifrar (en ``texto claro). Esto permite que cualquiera que espíe el tráfico de la red pueda obtener los nombres de usuario y contraseñas

- POP3 (Post Office Protocol 3). Tercera versión del protocolo diseñado para la gestión, el acceso y la transferencia de mensajes de correo electrónico entre dos máquinas, habitualmente un servidor y una máquina de usuario. Los servidores POP3 permiten tener acceso a una sola bandeja de entrada a diferencia de los servidores IMAP, que proporcionan acceso a múltiples carpetas en los servidores.
- IMAP es un acrónimo inglés de Internet Message Access Protocol. Protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una vez configurada la cuenta IMAP, puede especificar las carpetas que desea mostrar y las que desea ocultar, esta característica lo hace diferente del protocolo POP.
- Un DNS (Domain Name System) es un conjunto de protocolos y servicios que permiten a los usuarios utilizar nombres en vez de tener que recordar direcciones IP numéricas. Ésta es ciertamente la función más conocida de los protocolos DNS: la asignación de nombres a direcciones IP.
- NNTP, Network News Transport Protocol, protocolo de transferencia de noticias. Es el Protocolo de red utilizado por el

Usenet internet service. Es un Protocolo de red basado en tiras de textos, es usado para subir y bajar así como para transferir artículos entre servidores.

- HTTP es el protocolo de la Web (WWW), usado en cada transacción. Las letras significan Hyper Text Transfer Protocol, es decir, protocolo de transferencia de hipertexto. El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceder a una página web, y la respuesta de esa web, remitiendo la información que se verá en pantalla. HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. Al finalizar la transacción todos los datos se pierden. Por esto se popularizaron las cookies, que son pequeños ficheros guardados en el propio ordenador que puede leer un sitio web al establecer conexión con él, y de esta forma reconocer a un visitante que ya estuvo en ese sitio anteriormente. Gracias a esta identificación, el sitio web puede almacenar gran número de información sobre cada visitante, ofreciéndole así un mejor servicio.
- IRC significa Internet Relay Chat, que es un protocolo de comunicación en tiempo real basada en texto, la cual permite debates en grupo y/o privado, el cual se desarrolla en canales de chat que generalmente comienzan con el caracter # o &, este último solo es utilizado en canales locales del servidor. Es un sistema de charlas muy popular actualmente y ampliamente utilizado por personas de todo el mundo.
- ICQ ("I seek you" o "te busco") es un servicio de mensajería instantánea y el primero de su tipo en ser ampliamente utilizado en Internet, mediante el cual es posible chatear y enviar mensajes instantáneos a otros usuarios conectados a la red de

ICQ. También permite el envío de archivos, videoconferencias y charlas de voz. Los usuarios de la red ICQ son identificados con un número, el cual es asignado al momento de registrar un nuevo usuario, llamado UIN ("Universal Internet Number" o "número universal de Internet").

1.7.2 Puertos

Para acceder desde el nivel de red al nivel de aplicaciones no sirve simplemente indicar la dirección IP; se necesitarán más especificaciones para que el Host de destino pueda escoger la aplicación correcta. Un puerto se representa por un valor de 16 bits y hace la diferencia entre los posibles receptores de un mensaje. La combinación Dirección IP + Puerto identifican una región de memoria única denominada Socket. Al indicar este Socket, se puede trasladar el paquete a la aplicación correcta y, si además recibe el puerto desde donde fue enviado el mensaje, se podrá suministrar una respuesta.

Actualmente existe miles de puertos ocupados de los 216 = 65535 posibles, de los cuales apenas unos cuantos son los más utilizados y se encuentran divididos en tres rangos:

- Desde el puerto 0 hasta el 1023: son los puertos conocidos y usados por aplicaciones de servidor.
- Desde el 1024 hasta el 49151: son los registrados y asignados dinámicamente.
- Desde el 49152 hasta 65535: son los puertos privados.

1.7.3 Estructura Básica De La Web

La estructura básica de la World Wide Web (WWW) consiste en que el protocolo HTTP actúa como un transporte genérico que lleva varios tipos de información del servidor al cliente. Hoy en día las conexiones a servidores Web son las más extendidas entre usuarios de Internet, hasta el punto tal de que muchas personas piensan que este servicio es el único existente.

Cada entidad servidor se identifica de forma única con un Localizador de Recursos Universal (URL) que a su vez está relacionado unívocamente con una dirección IP.

El tipo más común de datos transportado a través de HTTP es HTML (HiperText Markup Language). Además de incluir directrices para la compresión de textos, también tiene directrices que proporcionan capacidades como las de enlaces de hipertexto y la carga de imágenes en línea.

La importancia de Internet no reside solamente en el número de máquinas interconectadas sino en los servicios y recursos que brinda (Gopher, News, Archie, WWW, etc.).

1.7. 3.1 IRC Internet Relay Chat

El Internet Relay Chat es un sistema de coloquio en tiempo real entre personas localizadas en distintos puntos de la red. Es un servicio basado exclusivamente en texto por teclado. Su gran atractivo es que permite las conversaciones en vivo de múltiples usuarios la mayor parte desconocidos entre sí. El IRC está organizado por redes, cada una de las cuales está formada por servidores que se encargan, entre otras cosas, de ofrecer canales de conversación y transmitir los mensajes entre usuarios. Para

acceder a un servidor de este tipo es necesario disponer de un programa cliente, siendo los cuatro más populares el mIRC, Pirch, Ichat y Microsoft Chat. La mayoría de los nombres de canales empiezan con ñ#ò Hay canales públicos, privados, secretos e individuales. Se suele entrar en las charlas con apodos (nick), de manera que los usuarios conserven el anonimato.

1.7. 3.2 Usenet

USENET Una de las áreas más populares de Internet son los grupos de discusión o NewGroups. El término UseNet surge de USER NETwork (red de usuarios) y se refiere al mecanismo que soportan los grupos de discusión. Los grupos se forman mediante la publicación de mensajes enviados (ñposteadosò) a un grupo en particular (generalmente de un tema específico). Es una red que no se centra en un único servidor que distribuye los mensajes, sino en una cadena de servidores que se pasan los mensajes de los grupos que soporta. La filosofía de las UseNet es la siguiente: Al dejar un mensaje, no sólo se queda en el grupo en cuestión, sino que también les llega a todos los usuarios suscritos al mismo, vía eï mail. Es útil para acudir a un grupo temático determinado para pedir ayuda.

1.7. 3.3 Habitantes del Ciberespacio

- Los hackers son las personas que han escrito programas de gran magnitud, con grandes capacidades que satisfacen necesidades de largo alcance, y los donan, de tal manera que cualquiera pueda utilizarlos, son personas que están siempre en una continua búsqueda de información, vive para aprender y todo para él es un reto; no existen barreras, y lucha por la difusión libre de información.

- GURÚS, considerados los maestros y los encargados de ñformarò a los futuros hackers.
- LAMERS O SCRIPTï KIDDERS, aficionados jactosos. Prueban todos los programas que llegan a sus manos. Generalmente son los responsables de soltar virus con el fin de molestar y que otros se enteren. Son aprendices que presumen de lo que no son aprovechando los conocimientos del hacker y lo ponen en práctica sin saber.
- COPYHACKERS, falsificadores sin escrúpulos que comercializan todo lo copiado (robado).
- BUCANEROS, comerciantes que venden los productos crackeados por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los copyhackers.
- NEWBIE, Son los novatos del hacker. Se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido.
- SAMURAI, hace su trabajo por encargo y a cambio de dinero. Estos personajes, a diferencia de los anteriores, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers.
- PIRATAS INFORMÁTICOS, copia soportes audiovisuales (discos compactos, cassettes, DVD, etc.) y los vende ilegalmente.
- PERSONAL (INSIDERS), los robos, sabotajes o accidentes relacionados con los sistemas informáticos, también pueden ser causados por el propio personal de la organización propietaria de dichos sistema. Estos pueden ser ex-empleados, curiosos o intrusos remunerados.

1.8 LOS ATAQUES

Es conocido que cualquier adolescente, sin tener grandes conocimientos, con una herramienta de ataque desarrollada por los hakers, es capaz de dejar sin servidor de información a una organización a través del Internet.

A través de los años se han desarrollado formas cada vez más sofisticadas de ataque para encontrar fallas en el diseño, configuración y operación de los sistemas.

Existen ataques Remotos, los mismos que se inician en contra una maquina sobre la cual el atacante no tiene control físico como:

- Ingeniería Social, es la manipulación de las para que revele todo lo necesario para superar las barreras de seguridad. Esta técnica es una de las más usadas y efectivas a la hora de averiguar nombres de usuarios y passwords. Por ejemplo, haciéndose pasar por administrador del sistema solicita la contraseña con alguna excusa.
- Ingeniería Social Inversa, los intrusos publican de alguna manera la posibilidad de brindar ayuda a usuarios, y estos acuden a ellos ante un imprevisto, situación que es aprovechara para pedir información confidencial que luego será usada por el intruso.
- Trashing (cartoneo), usualmente un usuario anota su login y password en un papel y luego, cuando lo recuerda, lo arroja a la basura, este es aprovechado por un atacante, el Trashing puede ser físico o lógico, como analizar buffers de impresora y memoria, bloques de discos, etc.
- Ataques de monitorización, este tipo observa a la victima y su sistema, con el objetivo de obtener información, establecer sus vulnerabilidades y posibles formas de acceso futuro.

- Decoy (señuelos), son programas diseñados con similar interfase que otro original. En ellos se imita la solicitud de un ingreso y el usuario desprevenido lo hace, el programa guardará esta información para futuros ataques.
- Scanning (búsqueda), método de descubrir canales de comunicación susceptibles de ser explotados, lleva mucho tiempo. La idea es recorrer tantos puertos de escucha como sea posible, y guardar información de aquellos que sean receptivos o de utilidad para cada necesidad en particular.
- Ataques de autentificación, tienen como objetivo engañar al sistema de la víctima para ingresar, este engaño se realiza tomando las sesiones ya establecidas por la víctima u obteniendo su nombre de usuario y clave. Muchos ataques de este tipo comienzan con Ingeniería Social, y los usuarios, por falta de cultura, facilitan a extraños sus identificaciones dentro del sistema. A continuación se mencionan algunas formas de ataques de autentificación:
    - Spoofingï looping, ingresa al sistema, tomar acciones en nombre de otro; obtiene información e ingresar en otro, luego utiliza este para entrar en otro, y así sucesivamente. Este proceso, llamado Looping tiene la finalidad de evaporar la identificación y la ubicación del atacante.
    - Spoofing, es un ataque sobre los protocolos, implica un buen conocimiento del protocolo en el que se va a basar el ataque. Los ataques más frecuentes son el IP Spoofing, el DNS Spoofing y el Web Spoofing.
    - IP Spoofing, el atacante genera paquetes de Internet con una dirección de red falsa en el campo From, pero que es aceptada por el destinatario del paquete, la víctima ve un ataque proveniente de una red falsa.

- Utilización de Backdoors, se denomina puertas traseras, son trozos de código en un programa que permiten a quien las conoce saltarse los métodos usuales de autentificación para realizar ciertas tareas. Habitualmente son insertados por los programadores del sistema para agilizar la tarea de probar código durante la fase de desarrollo. Esta situación se convierte en una falla de seguridad si se mantiene una vez terminado el producto ya que cualquiera que conozca el agujero o lo encuentre podrá saltarse los mecanismos de control.

- Denial Of Service, Los protocolos existentes actualmente fueron diseñados para ser empleados en una comunidad abierta y con una relación de confianza mutua. La realidad indica que es más fácil desorganizar el funcionamiento de un sistema que acceder al mismo; así los ataques de Negación de Servicio tienen como objetivo saturar los recursos de la víctima de forma tal que se inhabilita los servicios brindados por la misma. Más allá del simple hecho de bloquear los servicios del cliente, existen algunas razones importantes por las cuales este tipo de ataques pueden ser útiles a un atacante, por ejemplo cuando se ha instalado un troyano y se necesita que la víctima reinicie la máquina para que surta efecto a través de:

  - Jamming O Flooding, son ataques que saturan los recursos del sistema como: memoria o espacio en disco disponible, envía tanto tráfico a la red que nadie más pueda utilizarla.

  - Broadcast Store, este ataque es bastante simple y a su vez devastador, recolecta una serie de direcciones BroadCast para a continuación mandar una petición CMP (simulando un Ping) a cada una de ellas en serie, varias veces, falsificando la dirección IP de origen. La solución está en

manos de los administradores de red, los cuales deben configurar adecuadamente sus Routers para filtrar los paquetes de petición Indeseados (Broadcast)

- Mail Bombingï Spamming, el e-mail Bombing consiste en enviar muchas veces un mensaje idéntico a una misma dirección, saturando así el mailbox del destinatario. El Spamming, en cambio se refiere a enviar un eï mail a miles de usuarios.

- Ataques Con Javascript Y Vbscript, son dos lenguajes usados por los diseñadores de sitios Web para evitar el uso de Java, actualmente se utilizan para explotar vulnerabilidades específicas de navegadores y servidores.
- Ataques Mediante Activex, tecnologías potentes desarrollada por Microsoft que descargar código totalmente funcional de un sitio remoto. Es la respuesta de Microsoft a Java. Muchas veces cuando se descarga una página de internet pregunta si confía en el que expendió el certificado y/o en el control ActiveX. Si el usuario acepta, éste puede pasar a ejecutarse sin ningún tipo de restricciones de seguridad.

Considerando la forma en que proceden los ataques se puede definir los siguientes tipos:

- Interrupción, un sistema se pierde o desaparece o queda imposibilitado para su uso.
- Intercepción, se accede sin autorización.
- Modificación, además de acceder, se modifica alguna información.
- Generación, creación, invención de datos no autorizados

1.9 SPAM

El spam es el envío de mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

Los spammers (individuos o empresas que envían spam) utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su actividad, generalmente a través de programas automáticos que recorren internet en busca de direcciones. Algunas de las principales fuentes de direcciones para luego enviar el spam son:

- Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes cuando estos ingresan por ejemplo a foros.
- Los grupos de noticias, cuyos mensajes suelen incluir la dirección del remitente.
- Correos electrónicos con chistes, cadenas, etc. que los usuarios de internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje.
- Páginas en las que se solicita tu dirección de correo (o la de "tus amigos") para acceder a un determinado servicio o descarga.
- Compra de bases de datos con direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).
- Entrada ilegal a servidores.
- Por ensayo y error, se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes. Un método

habitual es hacer una lista de dominios, y agregarles "prefijos" habituales. Por ejemplo, para el dominio microsoft.com, probar info@microsoft.com, webmaster@microsoft.com, etc. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) por consumirse gran parte del ancho de banda en mensajes basura.

Todos sabemos del impacto negativo del correo no deseado en la empresa: mina la productividad del usuario, introduce una potencial responsabilidad jurídica y aumenta la carga de trabajo del personal, la infraestructura y el presupuesto de los centros informáticos.

Durante los primeros seis meses de 2004, Symantec reportó un aumento marcado en la cantidad de correo no deseado que se distribuía en Internet. De hecho, el correo no deseado, generalmente definido como correo electrónico no solicitado o correo basura que proviene de terceros, constituyó más del 60% de todo el tráfico de correo electrónico durante este periodo, según la última edición del Informe sobre las amenazas a la seguridad en Internet de Symantec. Nucleus Research concluyó que a comienzos de este año el costo promedio del correo no deseado por empleado en los Estados Unidos aumentó de $874 dólares americanos en Julio de 2003 a la asombrosa cifra de $1.934 en mayo de 2004.

Los creadores de spam también están diseñando nuevas formas de secuestrar computadoras para enviar correo no deseado, como lo demostraron recientes gusanos informáticos de correo electrónico masivo, como Sasser, Netsky y SoBig. Los análisis iniciales sugieren que aunque los gusanos no tenían una carga útil especialmente nociva, instalaban un programa de correo en las computadoras de las víctimas que creaba las condiciones

para implementar una red inmensa de conductos de identidades ocultas a través de los cuales el correo no deseado se podía retransmitir.

Además, se espera que el correo no deseado y las amenazas asociadas a él continúen aumentando en los próximos meses. En particular, Symantec ha pronosticado un aumento en el uso del correo no deseado como herramienta en los nuevos ataques sofisticados de estafa electrónica o ñphishingò. Estos ataques utilizan direcciones de correo electrónico falsificadas y sitios Web fraudulentos diseñados para engañar a los destinatarios para que divulguen información financiera personal como números de tarjetas de crédito, nombres de usuario, contraseñas de cuentas, así como otros códigos de identificación personal.

El negocio del correo no deseado está en pleno desarrollo, la última generación de correo no deseado incorpora tácticas sofisticadas como aleatoriedad extrema, ocultamiento del origen y evasión de filtros mediante el uso de HTML. Y los creadores de spam continúan apostando fuerte al diseñar formas de evadir los filtros y de lucrarse con sus actos.

A pesar de los grandes esfuerzos que hacen las empresas y consumidores, el correo no deseado continúa proliferando porque el aspecto económico de éste sigue siendo muy atractivo. Como numerosos comentaristas han señalado, lo que necesitan los creadores de spam para obtener ingresos mensuales de $1 millón de dólares americanos, es que uno de cada 2.000 ñvíctimas del correo no deseadoòles compre $20 dólares, es decir que necesitan un promedio de 0,05% respuestas. El aspecto económico del correo no deseado sigue siendo difícil de combatir y genera los siguientes problemas:

- Obstruye los servidores y equipos de escritorio, al usar los recursos informativos.
- Afecta la productividad del usuario - toma tiempo separar el correo malo del bueno y le toma tiempo lo que implica costos adicionales para la empresa.
- El correo electrónico no deseado es molesto y el correo ofensivo puede ser perturbador.
- La naturaleza gráfica y obscena de muchos correos electrónicos indeseables genera preocupación.

1.10 CODIGO MALICIOSO

El código malicioso se propaga dentro de las organizaciones y entre ellas, es un código deliberadamente ejecutado con fines dañinos. El código malicioso se puede clasificar básicamente en cuatro tipos principales:

- Virus, infecta a otro programa, sector de inicio, sector de partición o archivo que admite macros insertándose o adjuntándose a ese medio. Luego se replica a otros equipos a partir de ese punto. Es posible que los virus sólo se repliquen, pero muchos también dañarán los sistemas que infecten.
- Gusano, se copia a sí mismo de una unidad de disco a otra o a través de la red mediante el correo electrónico u otro mecanismo de transporte. No necesita modificar su host para propagarse. Puede dañar y poner en peligro la seguridad del equipo.
- Caballo de Troya, no se replica por sí mismo, pero su funcionalidad maliciosa está escondida en otros programas que parecen tener alguna utilidad, por lo que suele pasarse a otros equipos (a menudo puede presentarse en forma de programa de broma). Una vez presente en un sistema, dañará o pondrá

en peligro la seguridad del equipo, lo que puede ser el primer paso para permitir el acceso no autorizado.

- Otros tipos como por ejemplo un código ejecutable que dañe el entorno, ya sea de forma intencionada o no. Un ejemplo es un archivo de comandos que realiza bucles y en cada uno de ellos utiliza recursos del sistema hasta que el equipo no puede funcionar normalmente.

1.11 ESCASEZ DE PERSONAL DE SEGURIDAD DE LA INFORMACIÓN

Encontrar personal cualificado en seguridad de la información es una labor difícil, y este seguirá siendo en el futuro cercano. Aspectos como la inmadurez de las soluciones de los proveedores de seguridad de la información, el número limitado de personal cualificado disponible y el desarrollo de habilidades requeridas para la seguridad de la información constituyen el desafío para las instituciones. Los ejecutivos empresariales deberán trabajar más en esta área para superar estos retos.

Debido la inmadurez del mercado, la carencia de estándares y la gran cantidad de soluciones aisladas, la falta de entrenamiento es un problema para el personal de seguridad. Además, los desafíos de la seguridad de la información siguen aumentando a gran velocidad y expanden constantemente la lista de tecnología que se debe implantar, para lo que el personal de seguridad de la información no está preparado. Esto se traduce en más tiempo y dinero para entrenar al personal en los productos comercialmente disponibles.

Para obtener las credenciales necesarias para la seguridad de la información se requiere un entrenamiento y experiencia considerables. La credencial CISSP (Certified Information Systems Security Professionals) es una certificación acreditada internacionalmente que requiere la aprobación de un examen sobre gran variedad de temas de seguridad de la información, y tener una experiencia laboral mínima de cuatro años. La credencial relacionada SSCP (System Security Certified Practitioner) exige un año de experiencia además de la aprobación de un examen.

La certificación CISM (Certified Information Security Manager) también requiere un número mínimo de años de experiencia en seguridad de la información, además de haber aprobado satisfactoriamente un examen escrito. Todas estas certificaciones exigen entrenamiento continuo como parte de la certificación y las certificaciones GIAC (Global Information Assurance Certifications**)** exigen una evaluación periódica cada dos años. Los profesionales de la seguridad que disponen de estas certificaciones tienen gran demanda y los empresarios deben competir para contratarlos. La certificación CISA (Certified Information Systems Auditor**)** requiere un mínimo cinco años de experiencia laboral antes de poder presentarse a un examen.

Además de la capacitación técnica específica, el personal de seguridad de la información debe desarrollar habilidades para el cumplimiento de la seguridad que no forman parte de la formación profesional tradicional del personal. Existen pocos especialistas que hayan estado en el área de seguridad de la información más de dos años y posean la combinación requerida de habilidades técnicas en el cumplimiento de la seguridad.

CAPITULO II

SEGURIDAD DE LA INFORMACION

2.1 POLÍTICAS, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas, estándares y procedimientos para la seguridad de la Información son una serie de múltiples documentos interrelacionados que utiliza una organización para administrar y proteger la información de la que depende para sus operaciones actuales y futuras.

La siguiente ilustración muestra los grupos importantes de documentos de protección a la información:

FUENTE: **http://www.symantec.com**

- *Documento de la política de seguridad ï Por qué,* la política de seguridad de la información de una organización es un simple documento que articula la filosofía, los requerimientos reglamentarios y las creencias que la organización tiene en relación con la protección a los recursos de la información. Esta política explica con documentación el enfoque del medio ambiente, del personal y de los procesos en donde la aplica, así como las consecuencias de su incumplimiento. La Política de Seguridad de la Información es parte de un conjunto de políticas que generalmente cumplen las organizaciones. Otras políticas solucionan áreas críticas como los recursos humanos, las instalaciones y las finanzas. Estas otras políticas

deben ser complementadas y respaldadas con La Política de Seguridad de la Información.

- *Estándares ï Qué*, los estándares de seguridad de la información constan de documentos múltiples que se aplican a todas las áreas de la empresa que utilizan la información. Estos estándares abarcan controles de seguridad físicos, administrativos y técnicos que están diseñados para proteger la información.

- *Procedimientos* ï Cómo, los procedimientos de seguridad de la información establecen de manera detallada las operaciones que necesitan realizarse para satisfacer los requerimientos especificados en el Estándar que se aplica a una actividad determinada, proceso de seguridad o protección a un recurso de la información.

Solo cuando se aprecia el valor de la información, se puede determinar los esfuerzos necesarios para protegerla. La protección de la información requiere una inversión inicial y progresiva bien se trate del hardware, software, almacenaje o personal.

2.1.1. Diseño de Políticas de Seguridad

La clave para desarrollar con éxito documentos para un programa efectivo de seguridad de la información consiste en recordar que las políticas, estándares y procedimientos de seguridad de la información son un grupo de documentos interrelacionados. La relación de los documentos es lo que dificulta su desarrollo, aunque es muy poderosa cuando se pone en práctica. Muchas organizaciones ignoran esta interrelación en un esfuerzo por simplificar el proceso de desarrollo.

Una Política de Seguridad de la Información está conformada por unos pocos elementos como:

- Alcance de aplicabilidad
- Necesidad de adherirse a la política
- Descripción general de la política
- Consecuencias de no adherir a la política

La política de seguridad se implementará mediante los estándares y procedimientos de seguridad de la información. La Política de Seguridad simplemente ofrece compromiso y respaldo administrativo para que se brinde protección a la información.

Para que la política sea verdaderamente efectiva, debe ser aprobada por el gerente de la organización.

Las características principales de una Política de Seguridad de la Información son:

- Debe estar escrita en lenguaje simple, pero jurídicamente viable
- Debe basarse en las razones que tiene la empresa para proteger la información
- Debe ser consistente con las demás políticas organizacionales
- Debe hacerse cumplir - se exige y mide el cumplimiento
- Debe tener en cuenta los aportes hechos por las personas afectadas por la política
- Debe definir el papel y responsabilidades de las personas, departamentos y organizaciones para los que aplica la política

- No debe violar las políticas locales, estatales o federales
- Debe definir las consecuencias en caso de incumplimiento de la política
- Debe estar respaldada por documentos "palpables", como los estándares y procedimientos para la seguridad de la información, que se adapten a los cambios en las operaciones de las empresas, las necesidades, los requerimientos jurídicos y los cambios tecnológicos.

Para ayudar a las organizaciones a desarrollar estándares de seguridad de la información, un organismo de estándares han definido lo que deben considerar para la protección de la información, el Instituto de Estándares Británico publicó la norma BS-7799 en 1995. Este documento fue presentado a aprobación por la Organización Internacional de Estándares (ISO) para producir un estándar internacional de seguridad de la información. En el año 2000, la ISO publicó una versión internacional de la BS-7799, conocida como ISO-17799, que eliminó algunos elementos específicos de la ley británica.

2.2 NORMA ISO 17799

Debido a la necesidad asegurar la información que poseen las organizaciones se han desarrollado normativas que engloban todos los aspectos a tener en consideración por parte de las organizaciones para protegerse eficientemente frente a todos los probables incidentes que pudiesen afectarla, ante esta disyuntiva apareció el BS 7799, o estándar para la gestión de la seguridad de la información, un estándar desarrollado por el British Standard Institute en 1999 en el que se engloban todos los aspectos relacionados con la gestión de la seguridad de la información

dentro de la organización. Esta normativa británica acabó desembocando en la actual ISO/IEC 17799 ï Code of practice information security management.

En un principio se consideraba por parte de las empresas que tenían que protegerse de lo externo, de los peligros de Internet, pero con el paso del tiempo se están percatando de que no sólo existen este tipo de amenazas sino que también hay peligros dentro de la organización y todos éstos deberían ser contemplados. La aparición de esta normativa de carácter internacional ha supuesto una buena guía para las empresas que pretenden mantener de forma segura sus activos.

La ISO 17799 considera la organización como una totalidad y tiene en consideración todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que puedan producirse. Esta norma estructurada en 10 áreas o dominio los mismos que están asociados a uno o varios objetivos de seguridad, y cada objetivo se define a su vez, en uno o más controles de seguridad cuya implantación debe traducirse en la consecución del objetivo de seguridad asociado. Las áreas o dominios son:

1. Política de seguridad.
2. Aspectos organizativos para la seguridad.
3. Clasificación y control de activos.
4. Seguridad ligada al personal.
5. Seguridad física y del entorno.
6. Gestión de comunicaciones y operaciones.
7. Control de accesos.
8. Desarrollo y mantenimiento de sistemas.
9. Gestión de continuidad del negocio.
10. Conformidad con la legislación.

Fuente : NORMA ISO 17799

POLÍTICA DE SEGURIDAD

- Dirigir y dar soporte a la gestión de la seguridad de la información.

Contempla la documentación de Política, la misma que debe ser comunicada o publicada por la Dirección de la empresa. En este nivel se revisa y evalúa los nuevos riesgos, efectividad de la Política, Costes y el impacto de Controles en la eficiencia del negocio y cambios tecnológicos.

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

- Gestiona la seguridad de la información dentro de la organización.

- Mantener la seguridad de los recursos de tratamiento de la información y de los activos de información de la organización que son accedidos por terceros.

CLASIFICACIÓN Y CONTROL DE ACTIVOS

- Mantener una protección adecuada sobre los activos de la organización.

- Asegurar un nivel de protección adecuado a los activos de información.

SEGURIDAD LIGADA AL PERSONAL

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios.

- Asegurar que los usuarios son conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo.

- Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

SEGURIDAD FÍSICA Y DEL ENTORNO

- Evitar accesos no autorizados, daños e interferencias a la información de la organización.

- Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.

- Prevenir las exposiciones a riesgo o robos de información y de recursos de tratamiento de información.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

- Asegurar la operación correcta y segura de los recursos de tratamiento de información.

- Minimizar el riesgo de fallos en los sistemas.

- Proteger la integridad del software y de la información.

- Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- Evitar daños a los activos e interrupciones de actividades de la organización.
- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre organizaciones.

CONTROL DE ACCESOS

- Evitar accesos no autorizados a los sistemas de información.
- Protección de los servicios en red.
- Evitar accesos no autorizados a ordenadores.
- Evitar el acceso no autorizado a la información contenida en los sistemas.
- Detectar actividades no autorizadas.

DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- Verificar que la seguridad está incluida dentro de los sistemas de información.
- Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.
- Proteger la confidencialidad, autenticidad e integridad de la información.
- Mantener la seguridad del software y la información de la aplicación del sistema.

GESTIÓN DE CONTINUIDAD DEL NEGOCIO

- Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente grandes fallos o desastres.

CONFORMIDAD

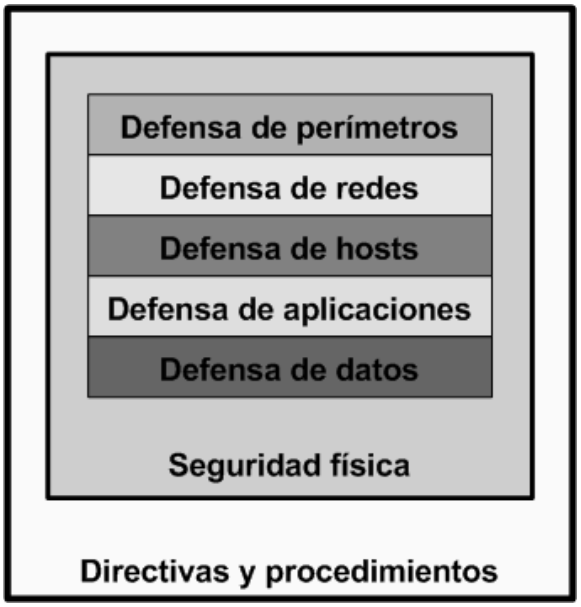
- Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad.

- Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma.

2.3 DEFENSA EN PROFUNDIDAD

Según la guía de operaciones de seguridad para Windows 2000, para reducir el riesgo se debe usar una estrategia de defensa en profundidad para proteger los recursos de amenazas externas e internas. Las capas de seguridad que forman la estrategia de defensa en profundidad incluyen el despliegue de medidas de protección desde los enrutadores externos hasta la ubicación de los recursos, pasando por todos los puntos intermedios.

Con el despliegue de varias capas de seguridad, ayuda a garantizar que, si se pone en peligro una capa, las otras ofrecerán la seguridad necesaria para proteger sus recursos. Lo ideal es que cada capa proporcione diferentes formas de contramedidas para evitar a los intrusos.



La cantidad de medidas de seguridad que se pueda aplicar dependerá de la evaluación de riesgos y el análisis de costos y beneficios de la aplicación. Según el gráfico anterior son diferentes los niveles de defensa

- *Directivas y procedimientos*, respecto a los empleados resulta esencial que sean conscientes de las directivas de seguridad y de lo que está permitido y prohibido porque: inconscientemente pueden poner en peligro la seguridad del entorno.

- *Seguridad física*, considerar la seguridad física como un elemento fundamental para la estrategia de seguridad global, si alguien puede tener acceso a un edificio, puede tener oportunidades para llevar a cabo un ataque sin necesidad de conectarse a la red.

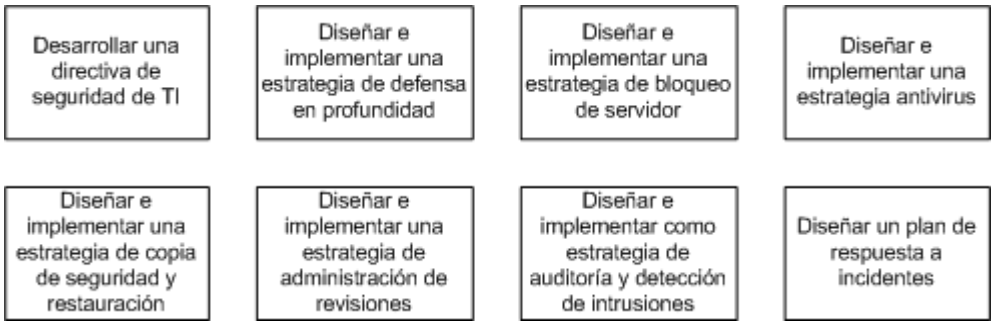
- *Defensa de datos*, uno de los recursos más valiosos de una empresa son los datos incluso de ellos depende la actividad misma de la empresa. Los datos se pueden proteger de varias

formas, incluido el cifrado de datos mediante o manteniendo claves de acceso.

- *Defensa de aplicaciones*, es una capa de defensa más, el refuerzo de las aplicaciones es una parte esencial de cualquier modelo de seguridad, es responsabilidad del programador incorporar la seguridad en la aplicación para proporcionar una protección adicional, además se debe probar en profundidad el cumplimiento de la seguridad de cada aplicación de la organización.

- *Defensa de hosts*, las directivas de host deben estar definidas para que limiten el uso a sólo a tareas autorizadas, de este modo, se crea otra barrera de seguridad que un atacante deberá superar antes de poder provocar algún daño. El diagrama que presenta l da a conocer los amplios y complejos aspectos que se debe considerar para configurar la seguridad un servidor y mantenerla.

Configuración de la seguridad a un servidor



Fuente: Guía de operaciones de seguridad para Windows 2000

- *Defensa de redes,* si se dispone de una serie de redes en la organización, se debe evaluarlas individualmente para asegurarse de que se ha establecido una seguridad

apropiada. Se debe examinar el tráfico y bloquear el que no sea necesario.

- *Defensa de perímetros,* la protección del perímetro de su red es el aspecto más importante para detener los ataques externos, la organización debe disponer de algún tipo de dispositivo de seguridad para proteger cada punto de acceso a la red. Es necesario evaluar qué tipos de tráfico se permiten y desarrollar un modelo de seguridad para bloquear el resto del tráfico. Los servidores de seguridad son una parte importante para asegurarse de minimizar los ataques externos.

2.4 ANTIVIRUS

Los antivirus son programas cuya función es detectar y eliminar virus informáticos y otros programas maliciosos.

Básicamente, un antivirus compara el código de cada archivo con una base de datos de los códigos de los virus conocidos, por lo que es importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado. También se les ha agregado funciones avanzadas, como la búsqueda de comportamientos típicos de virus (técnica conocida como heurística). Normalmente un antivirus tiene un componente que se carga en memoria y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados, en tiempo real. Es muy común que tengan componentes que revisen los adjuntos de los correos electrónicos salientes y entrantes.

Los virus informáticos no afectan directamente el hardware sino a través de los programas que lo controlan; causan daño al reproducirse y utilizar recursos escasos como el espacio en el disco, tiempo de procesamiento, hacen que el sistema se detenga, borre archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Un antivirus es una gran base de datos con la huella digital de todos los virus conocidos para identificarlos y también con las pautas que más contienen los virus. Los fabricantes de antivirus avanzan tecnológicamente casi en la misma medida que lo hacen los creadores de virus. Esto sirve para combatirlos, aunque no para prevenir la creación e infección de otros nuevos.

Debe tenerse en cuenta que un programa antivirus forma parte del sistema y funcionará correctamente si es adecuado y está bien configurado.

Las funciones de un antivirus son:

- *Detección,* debe poder identificar la presencia y/o accionar de un virus en una computadora. Adicionalmente puede brindar módulos de identificación, erradicación del virus o eliminación de la entidad infectada.
- *Identificación de un virus***,** existen diversas técnicas para realizar esta acción:
  - *Scanning,* técnica que consiste en revisar el código de los archivos (fundamentalmente archivos ejecutables y de documentos) en busca de pequeñas porciones de código que puedan pertenecer a un virus (sus huellas digitales). Estas porciones están almacenadas en una base de datos

del antivirus. Su principal ventaja reside en la rápida y exacta que resulta la identificación del virus.

- *Heurística,* búsqueda de acciones potencialmente dañinas perteneciente a un virus informático. Esta técnica no identifica de manera certera el virus, sino que rastrea rutinas de alteración de información y zonas generalmente no controlada por el usuario (Boot Sector, FAT, y otras). Su principal ventaja reside en que es capaz de detectar virus que no han sido agregados a las base de datos de los antivirus.

- *Chequeadores de Integridad,* Consiste en monitorear las actividades de la PC señalando si algún proceso intenta modificar sectores críticos de la misma. Su ventaja reside en la prevención aunque muchas veces pueden ser vulnerados por los supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvío y la posterior saturación de los servidores al existir millones de mensajes enviados.

2.5 SISTEMA DE DETECCIÓN DE INTRUSOS

Realizar la supervisión de una red de comunicaciones implica necesariamente realizar un estudio detallado y pormenorizado de todo el tráfico que circula por esta, locuaz resulta inviable filtrar toda la información que circula por red en tiempo real.

Si bien es cierto que es muy importante conocer que se ha recibido un intento de ataque, aún más importante es conocerlo a tiempo no sirve de nada conocerlo días o semanas después.

2.5.1. Intruder Detection Systems IDS

IDS - Intruder Detection Systems, el sistema de detección de intrusos es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, usan herramientas automáticas. En el mercado existen diferentes versiones, de Hardware y de Software como por ejemplo el Intrusion Detection de Computer Associates, SNORT (linux), en hardware esta de Symantec, el Security gateway (como modulo), entre otros.

El funcionamiento de estas herramientas se basa en el análisis pormenorizado del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, y/o comportamientos sospechosos, como puede ser el scaneo de puertos, paquetes, etc.

Sistemas de Detección de Intrusos o IDS (Intrusion Detection Systems), mecanismo de defensa que se ha debilitado por nuevas tecnologías como detección por firmas o patrones (Signature based) y detección de situaciones anómalas (Anomaly based). La IDS siempre ha estado con altos índices de ataques no detectados y ataques detectados erróneamente, además mantiene una administración compleja, por lo que la industria de seguridad informática ha impulsado el desarrollo de IPS.

Existen dos componentes básicos para cualquier sistema de detección de intrusos (IDS) que son los sensores y la consola. Los sensores de un IDS son elementos pasivos que examinan todo el tráfico de su segmento de red en búsqueda de eventos de interés. La consola de un sistema de detección de intrusos se

encarga de recibir toda la información de los sensores y presentarla al operador.

2.5.2. Network IDS ï NDIS

Los NIDS son IDS que trabajan con diferente arquitectura y según su l utilización de monitorización del tráfico de la red, se agrupa los NIDS en:

- Signature based NIDS: Al igual que muchos antivirus, estos IDS se basan en la búsqueda de patrones conocidos (firmas) en el tráfico de la red.
- Anomaly based NIDS: Se basan en analizar el tráfico de la red creando estadísticas y asignándoles pesos. Cuando se detecta tráficos sospechoso, se confronta con las estadísticas anteriores y en función del peso asignado y la cantidad de ocurrencias del evento se dispara una alarma o no.
- Protocol modeling NIDS: Estos sistemas de detección de intrusos buscan paquetes que contengan anomalías o configuraciones poco comunes de los protocolos de red (a fin de cuentas, los datos van encapsulados en distintos datagramas de distintos protocolos).
-

2.5.3. Distributed Intrusion Detection System - DIDS

Los sistemas DIDS (Distributed Intrusion Detection System), proporcionan el servicio de detección de intrusos para grandes redes las mismas que se encuentran en grandes organizaciones o universidades dónde un sistema IDS no proporciona la

flexibilidad necesaria para la heterogeneidad de los elementos disponibles.

Se diferencia del NIDS por la presencia de dos elementos nuevos en su arquitectura :

- Central Analysis Server: Es el centro del sistema DIDS y es el encargado de recibir toda la información procedente de los agentes y realizar un repositorio común de conocimiento. También realiza las funciones de control y sincronización de los diferentes nodos que forman parte del sistema.
- Co-operative Agent network: Es un sistema autónomo encargado de la monitorización de una red. Detecta posibles incidentes e informa al servidor central para que comunique a todos los nodos el ataque detectado así como las contra-medidas a realizar.
-

2.5.4. Intrusion Prevention System ï IPS

El sistema de prevención de intrusos (Intrusion Prevention System, IPS), es la tendencia actual de los sistemas de detección de intrusos, es un dispositivo (hardware o software) que tiene la habilidad de detectar ataques tanto conocidos como desconocidos y reaccionar a esos para impedir su éxito.

Los sistemas de prevención de intrusos pueden verse como la evolución de dos elementos que han dominados la seguridad en todas las redes informáticas del mundo:

- Firewall: garantiza o bloquea el acceso a los recursos de la red.
- IDS: mantiene el estado de las conexiones y examina el contenido de los paquetes que circulan por la red.

Los IPS pueden agruparse en cinco categorías dependiendo de su arquitectura y ubicación dentro de la red:

- Inline IPS: se caracterizan por colocarse entre dos tarjetas, la primera conectada a la red exterior y que no dispone de dirección IP. Su función es la de realizar bridging transparente entre la red y el IPS. Al no disponer de dirección IP, esta interface es totalmente invisible y no puede recibir ningún tipo de tráfico expreso (ni ser atacado). La segunda tarjeta está conectada a la red "segura" o interna y permite conectar al sistema IPS para su gestión y configuración.

  El sistema IPS procesa todo el tráfico entrante y saliente de manera que cada paquete puede pasar, eliminarlo o incluso rescribir el paquete eliminando elementos potencialmente peligrosos; por lo que estos sistemas deben ser muy sólidos, ya que si el IPS deja de funcionar (fallo hardware/software), se pierde el acceso a la red.
- Layer seven switches: Los switches son dispositivos de capa 2 del modelo OSI. En el caso de las redes IP, los diferentes protocolos para los distintos servicios (HTTP, FTP, ...) se sitúan en la capa 7 del modelo OSI, para poder inspeccionar paquetes IP de diferentes servicios se necesita un conmutador de nivel 7. Estos IPS contienen un componente hardware muy importante que le proporciona una velocidad de proceso en el filtrado de paquetes de red muy superior a los sistemas convencionales basados en un programa que se ejecuta en un ordenador. Su modo de funcionamiento se basa en un único puerto del switch encargado de mantener la conexión de red con el exterior, y el resto de puertos conectados a los distintos servidores monitorizar.

Como los otros sistemas de prevención de intrusos, es capaz de filtrar el tráfico, buscar patrones en la red y controlar las conexiones de entrada y salida.

- Application firewall/IDS: Este grupo de IPS son programas autónomos que corren en cada uno de los servidores a proteger. De esta forma, se encargan de proteger únicamente un ordenador o servicio concreto, y no una red o conjunto de ordenadores.
- Hybrid switches: Estos sistemas de prevención de intrusos se basan en combinar una parte de software y otra de hardware. La parte hardware es la encargada de filtrar el tráfico en tiempo real (debido a su mayor velocidad de proceso), limitar el numero de peticiones a los servidores y regular los anchos de banda de entrada y salida adecuándolos a las necesidades y demandas en cada momento. La parte software se instala en cada uno de los servidores a monitorizar.
- Deceptive applications: Este tipo de aplicaciones empezaron a utilizarse en el 98, reacciona proactivamente frente a la detección de intrusos. Su aplicación se divide en tres fases:
  1. En una primera fase se analiza todo el tráfico de la red con el objetivo de crear un modelo que represente todo el tráfico "normal" que circula por la red.
  2. En una segunda fase, el sistema monitoriza el tráfico y las peticiones que circulan por la red. Cuando observa peticiones a servicios que no existen o que no están disponibles, reacciona enviando como respuesta un paquete "marcado" simulando la existencia del servicio y anotando los parámetros de origen de la petición.
  3. La tercera fase se produce cuando el atacante utiliza los datos obtenidos en incursiones anteriores a la red (fase 2) para lanzar un ataque sobre servidores o servicios. En

este momento el sistema reconoce al atacante y bloquea su acceso a la red.

2.6 EVITAR SPAM

El correo electrónico no deseado (spam) o correo basura, continua sobrecargando las bandejas de entrada. Actualmente se envía más correo electrónico no deseado que nunca, lo que solía ser simplemente un fastidio, es ahora una epidemia que demora las redes empresariales y congestiona las bandejas de entrada.

La gran mayoría de Proveedores del Servicio de Internet (ISP) no permiten que sus clientes envíen correo electrónico no deseado según las políticas de uso, por lo que los remitentes de correo electrónico no deseado con frecuencia deben operar clandestinamente y utilizar otros recursos de redes, generalmente robados. Estos son los principales medios de envío del correo electrónico no deseado:

- *Retransmisores abiertos:* Los remitentes de correo electrónico no deseado identifican los retransmisores abiertos en Internet y utilizan estos servidores para enviar sus mensajes masivos disfrazando el origen y como un recurso "gratuito" de envío masivo de correo electrónico. Los dueños de estos retransmisores de correo son generalmente compañías legítimas que tienen servidores de correo configurados inadecuadamente.
- *ISP invasores:* Un "SpamHaus" genera ganancias con el envío de correo electrónico no deseado. Los remitentes de este tipo de correo se conectan a la troncal de Internet y pagan tarifas a las grandes empresas de telecomunicaciones como lo haría un ISP legítimo. Los remitentes de correo electrónico no deseado continuamente rotan los nombres de dominio y las subredes de IP para evitar ser detectados por los filtros y listas negras de

correo electrónico no deseado y envían gratuitamente el correo electrónico no deseado alrededor del mundo.

- *Cuentas que se usan una vez:* Los remitentes de correo electrónico no deseado por lo general se suscriben a cuentas de correo electrónico gratuito o de prueba con un ISP o proveedor importante de correo Web, como Yahoo y proceden a enviar correo electrónico no deseado desde esa dirección hasta que se las cierran - sólo para continuar con otra cuenta gratuita.
- *Proxis Web abiertos:* Si los proxis se configuran mal pueden permitir a los usuarios externos conectarse al servidor Web, por ejemplo a través del Puerto 80 y conectarse de manera anónima a un servidor de correo aleatorio para enviar el correo electrónico no deseado.
- *Conexiones a Internet inalámbricas:* Las conexiones inalámbricas prevalecen más que nunca y esto le da vía libre a los remitentes de correo electrónico no deseado para que tengan acceso a los recursos de las redes.

Lo que funciona para los remitentes de correo electrónico no deseado un día, puede no funcionar al día siguiente, lo mismo sucede con aquellas personas que son responsables de controlar el correo electrónico no deseado en la empresa. No hay una sola herramienta que elimine este correo por completo, a pesar de que hay muchos métodos variados para filtrarlo poco a poco. Puesto que la cantidad de correo electrónico no deseado aumenta y continúa obstruyendo las redes de la información, los administradores están buscando formas para detectar y bloquear este correo electrónico basura antes de que llegue a las bandejas de entrada de los empleados.

La manera más efectiva de proporcionar protección a largo plazo contra el correo electrónico no deseado es adoptar un

sistema de capas múltiples que maximice la detección y minimice los falsos positivos mediante tres capas de protección:

- Detección de correo electrónico no deseado que incluye:
  - Soporte a las listas negras múltiples en tiempo real
  - Motor heurístico que combate el correo electrónico no deseado
  - Listas negras personalizadas
  - Bloqueo del renglón del asunto

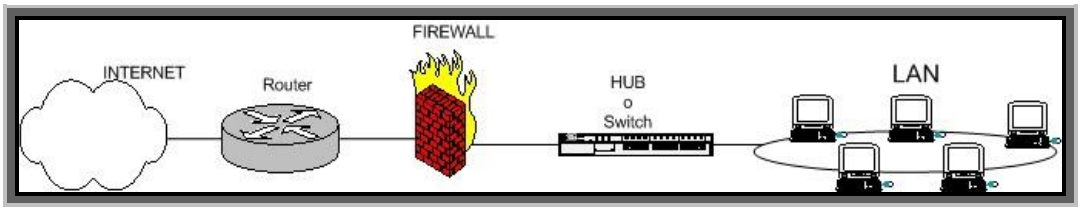
- Control de los falsos positivos que incluye:
  - Listas blancas personalizadas
- Prevención de falsos positivos
  - Identificación del renglón del asunto - lo que le permite al administrador filtrar a nivel del gateway y de la estación de trabajo
  - "Cuarentena" que enviará el correo electrónico sospechoso a una cuenta especial administrativa del correo electrónico

CAPITULO III

ASEGURAR EL PERÍMETRO DE LA REDLA

3.1. FIREWALL.

Un firewall es un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Para ilustrar esta definición podemos observar la siguiente figura.



Un Firewall impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina quien puede entrar para utilizar los recursos de red que pertenece a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información.

El firewall permite al administrador de la red definir un embudo, que permite mantener al margen de la red a usuarios no-autorizados fuera de la red y proporciona protección para varios tipos de ataques posibles. Además ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos.

3.2. BENEFICIOS DE UN FIREWALL

Un Firewall tiene las siguientes ventajas en la seguridad de la red:

- Son excelentes para reforzar la política de seguridad de una empresa.
- Son excelentes auditores, ya que registra el tráfico que pasa a travésde él.
- Protege de intrusiones, porque permite el acceso a la red sólo a direcciones autorizadas.
- Optimiza el acceso, ya que identifica los elementos de la red internos y optimiza la comunicación entre ellos.
- Protege información privada, permite el acceso solamente a quien tenga privilegios a la información de cierta área o sector de la red.
- Desde el punto de vista del internet tiene las siguientes ventajas:
- Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet, localiza con precisión cuellos de botella potenciales del ancho de banda.
- Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.
- Monitorea regularmente la red para detectar múltiples ataque a la red interna.

3.3. LIMITACIONES DE UN FIREWALL

Los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles pero no puede proteger:

- No puede prohibir que los espías corporativos copien datos sensitivos en algún dispositivo y substraigan estas del edificio.
- No puede proteger contra los ataques de la "Ingeniería Social", por ejemplo cuando se persuade a un usuario a que le permita usar su contraseña del servidor corporativo o que le permita el acceso temporal a la red.
- No puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software.
- No puede contra aquellos ataques que se efectúen fuera de su punto de operación. Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida.
- Sondeo del sistema para debilitar la seguridad, los hacker después que obtienen la información de una red de una determinada organización, tratan de probar cada uno de los servidores para debilitar la seguridad explorar individualmente los servidores residentes en una red para intentar conectarse a un puerto especificando el tipo de servicio que esta asignado al servidor. Par esto utilizan varias herramientas de dominio público, como el Rastreador de Seguridad en Internet o la Herramienta para Análisis de Seguridad para Auditar Redes (SATAN) , el cual puede rastrear una subred o un dominio y ver las posibles fugas de seguridad.

3.4. METODOS DE FIREWALL

Los firewall trabajan utilizando diferentes métodos para identificar intrusos :

- Filtrado de Paquetes
- Stateful Packet Inspection.
- Deep Packet Inspection DPI

3.4.1. Packet Filtering - Filtrado de Paquetes

El método más común del Firewall es el Filtrado de Paquetes. Cada paquete de información se analiza con respecto a una serie de filtros. Cuando un Firewall con Filtrado de Paquetes recibe un paquete desde Internet, checa la información contenida en la dirección IP del encabezado del paquete y la chequea contra la tabla de reglas de control de acceso para determinar si el paquete es aceptable o no.

El conjunto de reglas establecidas por el administrador del Firewall sirve como la lista de invitados. Estas reglas pueden especificar ciertas acciones a tomar cuando una dirección IP origen o destino o número de puerto es identificado. Por ejemplo, el acceso a un sitio pornográfico puede ser bloqueado al designar la dirección IP de dicho sitio como no una conexión no permitida (de entrada o de salida) para la computadora del usuario. Cuando el Firewall de Filtrado de Paquetes encuentra un paquete proveniente del sitio pornográfico, examina el paquete. Debido a que la dirección IP del sitio pornográfico está contenida en el encabezado del paquete, éste cumple las condiciones que específicamente niegan tal conexión y al tráfico de web no se le permite pasar.

A pesar que los Filtros de Paquetes son rápidos, también son relativamente fáciles de evadir. Un método de evitar a un Filtro de Paquetes es conocido como IP spoofing, en el cual los hackers adoptan la dirección IP de una fuente confiable, de esta manera engañando al Firewall haciéndolo pensar que el paquete del hacker de hecho viene de un sitio de confiar. El segundo problema fundamental de un Filtro de Paquetes es que permiten una conexión directa entre las computadoras origen y destino. Como resultado, una vez que la conexión inicial ha sido autorizada por el Firewall, la computadora origen se conecta directamente con la computadora destino, potencialmente exponiendo a un ataque a la computadora destino y a todas las computadoras que están conectadas a ésta.

3.4.2. Stateful Packet Inspection.

Un Segundo método utilizado por los Firewalls es conocido como Stateful Packet Inspection. Este método es una forma de filtrado de paquetes super-cargada. Éste examina no sólo los encabezados del paquete, sino también el contenido para saber más acerca del paquete que sólo su información de origen y destino. Se llama Stateful Paket Inspection porque examina en contenido del paquete para determinar cuál es el estado de la comunicación, por ejemplo se asegura que la computadora destino especificada ha solicitado previamente la comunicación actual. Esta es una forma de asegurar que toda comunicación es iniciada por la computadora original y toman lugar con fuentes que son conocidas y confiables a partir de interacciones previas. Adicionalmente a ser más rigurosas en su inspección de paquetes, los Firewalls de Stateful Inspection además cierran puertos hasta que una conexión hacia el puerto específico es solicitada. Esto

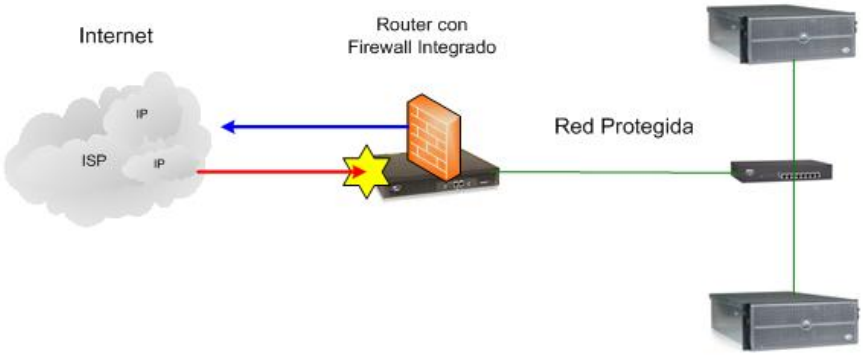
permite una capa adicional de protección contra la amenaza de un escaneo de puertos.

3.4.3. Deep Packet Inspection DPI

Deep Packet Inspection es un término utilizado para describir la capacidad de un sistema de Detección de Intrusos o un Firewall para mirar dentro de el segmento de datos de un paquete de aplicación o corriente de datos y llevar a cabo decisiones a partir del significado de los datos basándose en el contenido de éstos. El motor que lleva a cabo la Inspección Profunda de Paquetes típicamente incluye una combinación de tecnología de concordancia de firmas además de un análisis heurístico de los datos para determinar el impacto de dicha comunicación. La maquinaria de inspección debe utilizar una combinación de técnicas de análisis en base a firmas, así como técnicas estadísticas, o de análisis de anomalía. Éstas dos son tomadas prestadas directamente de la tecnología de Detección de Intrusos. Con el fin de identificar el tráfico con la velocidad necesaria para proveer el desempeño adecuado, este método está siendo incorporado a los Firewall´s actuales. Estas Unidades de Proceso de Red proveen una rápida discriminación del contenido dentro de los paquetes mientras que del mismo modo permiten la clasificación de los datos.

3.5. TIPOS DE FIREWALLS

Los cortafuegos o firewalls, son dispositivos o sistemas que



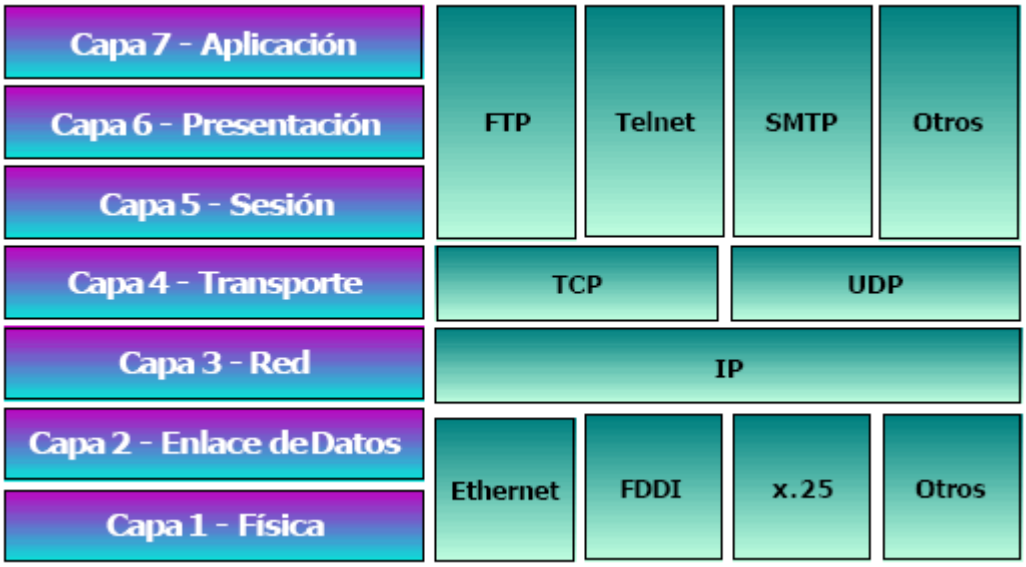
controlan el flujo de tráfico entre dos o más redes empleando ciertas políticas de seguridad para limitar, permitir o bloquear el tráfico entre dos redes en base a una serie de reglas. Su complejidad reside en las reglas que admiten y en como realizan la toma de decisiones en base a dichas reglas.

La tecnología empleada en los cortafuegos ha ido madurando a medida que la industria especializada avanzaba y ahora tenemos una amplia variedad de dispositivos que realizan esta función de distintas formas. Una forma práctica y sencilla de comparar las bondades de cada plataforma es examinando las capas del modelo OSI (Open System Interconnect) donde el cortafuegos interactúa.

La clasificación conceptual más simple divide los cortafuegos en sólo dos tipos:

- Cortafuegos a nivel de red (trabajan en las capas 2, 3 y/o 4 del modelo OSI).
- Cortafuegos a nivel de aplicación (trabajan en las capas 5,6 y/o 7 del modelo OSI).

Como regla general, podemos afirmar que cuanto más bajas sean las capas en las que el cortafuegos trabaja, su evaluación será más rápida y transparente su capacidad de acción ante ataques complejos es mayor.



Algunos de los servicios y protocolos más usados correlacionados sobre las capas del modelo OSI donde se desarrollan.

Existe otra clasificación dependiendo del acabado externo del producto, existe en el mercado cortafuegos que son meros servicios que se ejecutan sobre sistemas operativos robustos como: IPTables en el mundo Linux o CISCO Centri Firewall para tecnología NT, complejas herramientas modulares que pueden instalarse en varias máquinas como es el caso de Firewall-1 de Central Point, o puede tratarse de sistemas dedicados que incluyen dentro de una caja compacta el hardware, el sistema operativo y el software específico, todo ello completamente listo para trabajar es el caso del CISCO PIX Firewall.

Las últimas tecnologías no aportan claridad para distinguirlas hasta el punto que no está claro cual es mejor y cual es peor. Pero

en cualquier caso, se deberá prestar atención y poner mucho cuidado a la hora de instalar la que realmente se necesita en una organización e incluso se menciona otro tipo de firewalls:

- Nivel de red.
- Nivel de aplicación.

3.5.1. Firewalls a nivel de red

Generalmente, toman las decisiones basándose en la fuente, dirección de destino y puertos, todo ello en paquetes individuales IP. Los modernos firewall a nivel de red se han sofisticado ampliamente, mantienen información interna sobre el estado de las conexiones que están pasando, los contenidos de algunos datagramas y más cosas. Un aspecto importante que distingue a las firewall a nivel de red es que enrutan el tráfico directamente, tienden a ser más veloces y más transparentes a los usuarios.

3.5.1.1 Firewall de Red ï SymantecÊ Gateway Security 5400

SymantecÊ Gateway Security 5400 ofrece máxima protección incluso contra las amenazas a la seguridad en Internet más dañinas, al mismo tiempo que reduce la complejidad de la administración de la seguridad. Es uno de los firewalls empresarial más completo del mercado que integra motores de detección de intrusos y prevención de intrusos basados en anomalías de

protocolo y en firmas, un filtrado de contenidos basado en direcciones URL,antispam .

Funciones y ventajas importantes:

- Protección completa de la red en la conexión a Internet o a las subredes WAN y LAN.
- Administración centralizada que simplifica la administración de la seguridad de la red a través de la centralización de registros, alertas, informes y de la configuración de políticas.
- Satisface los requisitos de rendimiento de las organizaciones, cualquiera que sea su tamaño, con la opción de alta disponibilidad y balanceo de carga integrados.
- Modelo de alto rendimiento que proporciona velocidades de transferencia que van desde 200 Mbps hasta más de 3,5 Gbps en configuraciones agrupadas.
- Actualizaciones automáticas de seguridad mediante la tecnología LiveUpdateÊ de SymantecÊ Security Response, la primera organización mundial en investigación y soporte de la seguridad en Internet.
- Permite a los administradores configurar políticas granulares para obtener control completo de la información que entra y sale de la red, realiza una inspección profunda de los paquetes, para interrumpir y registrar los paquetes incorrectos, lo que permite bloquear sesiones específicas que contengan amenazas o bloquear direcciones IP específicas que sigan representando una amenaza.
- Si los paquetes están basados en HTTP, la tecnología de filtrado de contenidos compara la fuente IP con una lista de sitios Web prohibidos. Los contenidos prohibidos se interrumpen y se registran.

- A través de LiveUpdate de Symantec se obtienen oportunas actualizaciones automáticas de las nuevas definiciones de virus, firmas de ataques y listas de filtrado de URL para un despliegue rápido y fácil en toda la empresa.

3.5.1.2 FORTINET 1000

Fortinet fue fundada en el año 2000 por Ken Xie, la compañía tiene su central en Santa Clara, California , fue el primero en:

- Acelerar el proceso firewall mediante ASIC.
- Diseñar un dispositivo dedicado, más fácil de gestionar y mantener, con una gran acogida en el mercado.

El fundador de Fortinet dio un enorme paso más integrando antivirus, filtrado de contenido, tecnología IDP y antispam en un solo dispositivo, junto con el firewall y servidor VPN. Los procesos pesados son acelerados por un ASIC evolucionado, FortiASIC, que permite romper la barrera del procesado de contenidos en tiempo real.

En lo que respecta a certificaciones, FortiGate es el único Firewall Antivirus del mercado que ha recibido las cuatro certificaciones independientes ICSA:

- Firewall
- Antivirus
- IPsec VPN
- Detección de Intrusiones.

Infraestructura FortiProtect responder rápidamente y proactivamente a todas las amenazas basadas en virus, gusanos, troyanos, grayware (spyware, adware, etc.). FortiProtect Update Infrastructure, es un elemento clave en la estrategia global de seguridad de Fortinet para proporcionar una completa protección

ante virus e intrusiones. Esto asegura protección automática en tiempo y minimiza la exposición a infecciones de red y ataques.

FortiProtect Update Infrastructure opera de forma ininterrumpida (24*7) alrededor del mundo para identificar ataques nuevos y desarrollan firmas contra virus y ataques.

La infraestructura FortiProtect consta de tres elementos clave:

- FortiProtect Center
- Un portal de información actualizado ñal minutoòque proporciona todos los datos sobre nuevos virus y vulnerabilidades así como novedades y recursos en el campo de laseguridad de redes.
- FortiProtect Security Response Team. Un completo equipo de expertos en seguridad dedicados a la investigación de nuevas amenazas y el desarrollo de firmas que permitan a los dispositivos Fortigate detectar y prevenir nuevos ataques.
- FortiProtect Distribution Network, posee de una red de servidores de distribución de alta disponibilidad, que proporcionan actualizaciones automáticas e inmediatas a los firewall antivirus Fortigate en todo el mundo, tan pronto como El equipo FortiProtect Security Response Team desarrolla una nueva firma.

Especificaciones:

- Interfaces
  - 10/100 Ethernet Ports 4
  - Gigabit Ethernet Port 2
- System Performance
  - Concurrent sessions 600,000
  - New sessions/second 15,000
- Firewall throughput (Mbps) 1Gbps
- Antivirus, Worm Detection & Removal

- Scans HTTP, FTP, SMTP, POP3, IMAP, Å
- Quarantine infected messages Å
- NAT
- Routing mode
- VLAN tagging (802.1q) Å
- Access control list (Source IP, Destination IP,
- TCP port, and UDP port) Å
- User Group-based authentication Å
- H.323 NAT Traversal Å
- WINS support Å
- VPN
- PPTP, L2TP, and IPSec Å
- Encryption (DES, 3DES, AES) Å
- Dead peer detection Å
- Interoperability with major VPN vendors Å
- Content Filtering
- URL block Å
- Content profiles 32
- Blocks Java Applet, Cookies, Active X Å
- Email filtering (keyword, blacklist, exempt list) Å
- Intrusion Detection and Prevention
  - Detection for over 1300 attacks Å
  - Prevention for over 30 DoS and DDoS attacks Å
  - Customizable detection signature list Å
- Logging/Monitoring
  - Internal logging/removable HD 20G
  - Log to remote Syslog/WELF server Å
- Graphical real-time and historical monitoring Å
- SNMP Å
- Email notification of viruses and attacks Å

3.5.2 firewall de aplicación

Los firewalls de nivel de aplicación por lo general son hosts corriendo proxy servers, que no permiten el tráfico directo entre redes, manteniendo una auditoria del tráfico que pasa a través de él. Este tipo de firewall puede ser utilizado para realizar las tareas relativas al NAT (Network Address Translation), debido a que como las comunicaciones van de un lado hacia el otro se puede enmascarar la ubicación original.

Los filtros a nivel de aplicación permiten aplicar un esquema de seguridad más estricto. En estos firewalls se instala un software específico para cada aplicación a controlar; de hecho si no se instala los servicios relativos a la aplicación las comunicaciones no podrán ser enrutadas, de esta forma se garantiza que todas aquellas nuevas aplicaciones desconocidas no puedan acceder a la red. Otra ventaja es que permite el filtrado del protocolo, por ejemplo que impida navegar por el FS; esto es lo que hay se conoce como un FTP anónimo.

Dentro de este tipo están los Firewalls apropiados para los usuarios de casa, en el mercado existen varios proveedores de este software entre los más comunes tenemos:

Editor del Software	Producto
Microsoft	Firewall para Conexión a Internet
Symantec	Firewall Personal Norton 2002 (Symantec)
McAfee	Firewall Personal McAfee.com (McAfee)
Zone Labs	ZoneAlarm Pro (Zone Labs)

Sygate	Firewall Personal de Sygate PRO (Sygate Technologies)
Zero-Knowledge Systems	Firewall Personal Freedom (Zero-Knowledge Systems)
Internet Security Systems	Black Ice Defender (Internet Security Systems)

3.5.2.1 firewall de aplicación ï symantec enterprise 7.0

Symantec Enterprise Firewall ofrece el firewall enterprise 7.0, seguro y de alta velocidad el mismo que tiene las siguiente características:

- Es un firewalls que garantiza seguridad y rendimiento porque admite el algoritmo AES (Estándar Avanzado de Encriptación)
- Compatible con las soluciones integradas de balanceo de carga y alta disponibilidad, tanto de hardware como de software, para poder recuperarse en caso de error y proveer la máxima disponibilidad del servicio
- Permite la administración local y remota de Symantec Enterprise Firewalls dispositivos de seguridad.
- Se integra sin problemas con Symantec Enterprise para conectarse de manera segura con oficinas y usuarios remotos.
- Alternativas de autenticación sólida de usuarios que dan flexibilidad para seleccionar bases de datos de seguridad ya existentes.

- Endurecimiento automático del sistema que minimiza los riesgos y vulnerabilidades desactivando funciones del sistema operativo innecesarias, de manera inicial y en forma continua.
- Arquitectura completa para la administración de políticas de seguridad y configuración de normas.
- Sus amplias capacidades de registro e informes suministran información estadística detallada de las sesiones o análisis personalizados.
- Certificación ICSA que garantiza conformidad con las pruebas de penetración restrictivas y con los requisitos líderes de la industria para la protección de seguridad. Encriptación y autenticación que extienden las redes de la empresa.
- Respaldado por Symantec Security Response, la primera organización mundial en investigación y soporte de la seguridad en Internet.
- Además de proteger el sistema en todos los niveles de las capas TCP/IP de la red, ofrece un administrador intuitivo de múltiples plataformas, un desempeño con múltiples procesadores/subprocesadores, métodos de autenticación flexibles, un endurecimiento inicial y continuo del sistema operativo y de la red, y protección incorporada contra ataques de negación de servicio y amenazas combinadas.
- Además dispone de los siguientes servicios:
    - Servicios administrados de seguridad, que permiten que los clientes eviten los costos asociados con la administración de sus propios centros de operaciones de seguridad.
    - Servicios administrados de firewall, ofrece una protección ágil del perímetro con un mantenimiento, monitoreo e informes de administración de firewall ya probados.

- Servicios administrados de valoración de vulnerabilidades en internet, utiliza herramientas para ayudar a las organizaciones a eliminar las vulnerabilidades.

3.5.2.2 firewall de aplicación ï ISA Server 2004

Microsoft® Internet Security and Acceleration (ISA) Server 2004 Enterprise Edition ofrece una conexión a Internet segura, rápida y fácil de administrar. El servidor ISA integra un sofisticado firewall de empresa de múltiples capas preparado para la capa de aplicación. Se basa en la seguridad y el directorio de Microsoft Windows ServerÊ 2003 para obtener seguridad basada en directivas, aceleración y administración de interconexión a redes.

ISA Server 2004 Enterprise protege las redes contra el acceso no autorizado, realiza filtrado e inspecciona el estado y alerta de los ataques contra el firewall o la red protegida.

El filtrado del tráfico realiza a nivel de paquete, circuito y aplicación, filtrado e inspección con estado, gran compatibilidad con aplicaciones en red, una red privada virtual (VPN) perfectamente integrada, detección de intrusiones integrada, filtros de aplicación de capa 7 inteligentes, transparencia del firewall para todos los clientes, autenticación avanzada, publicación de servidor segura, además permite realizar las siguientes operaciones:

- Proteger las redes contra el acceso no autorizado.
- Defender los servidores web y de correo electrónico de ataques externos.
- Inspeccionar el tráfico de red entrante y saliente para garantizar la seguridad.
- Recibir alertas de actividad sospechosa.

- Minimiza los cuellos de botella de rendimiento y ahorra ancho de banda de red, ya que sirve contenido Web almacenado en caché local.
- Definición personalizada de los protocolos, puede controlar el número de puerto de origen y de destino de cualquier protocolo.
- Administración de VPN, incluye un mecanismo de redes privadas virtuales totalmente integrado, que se basa en las funciones de Microsoft® Windows ServerÊ 2003 y Windows® 2000 Server. Incluye : inspección y filtrado con estado para VPN y filtrado e inspección con estado a través de túnel VPN de sitio a sitio
- Filtrado HTTP regla a regla, permite al firewall realizar una profunda inspección con estado de HTTP (filtrado de capa de aplicación). La extensión de la inspección se configura regla a regla. Se pueden configurar restricciones personalizadas para el acceso HTTP entrante y saliente.
- Bloquear el acceso a todo el contenido ejecutable, la directiva se puede configurar para que bloquee todos los intentos de conexión al contenido ejecutable de Windows.

3.5.2.3 firewall de aplicación ï LINUX: IPTABLES

En Linux, el filtrado de paquetes se controla a nivel del kernel. Existen módulos para el kernel que permiten definir un sistema de reglas para aceptar o rechazar los paquetes o las comunicaciones que pasan por el sistema.
En versiones de Kernel anteriores a la 2.4 se disponía de los módulos IPCHAINS para montar firewalls, a partir del kernel 2.4 el modulo para filtrado de paquetes mucho más potente que IPCHAINS es IPTABLES.

Bastion-firewall es un firewall basado en iptables, funciona bajo cualquier versión de Linux con el kernel 2.4 o superior y tiene las siguientes características:

- Administración basada en ficheros de configuración en texto plano y tratados como código bash, permitiendo introducir código en los ficheros de configuración para la generación de los valores de las variables.
- Administración basada en web mediante bastion-firewall-interface que modifica los ficheros de configuración, habilitando al administrador a realizar una configuración mixta.
- Sistema de estadísticas del tráfico basadas en web y que contienen gráficas del tráfico.
- Sistema de separación del tráfico y de agrupación y ordenación de las reglas, servicios y protocolos para obtener una máxima velocidad en el tratamiento del tráfico.
- Sistema para bloquear direcciones IP permanentemente y para indicar que direcciones nunca se deben bloquear, estas direcciones pueden ser usadas desde un IDS o IPS para bloquear posibles atacantes sin peligro de provocar un ataque de denegación de servicio.
- Posibilidad de utilizar listas de IPs en cada lugar donde normalmente introduciríamos una dirección IP. bastion-firewall expandirá la lista de IPs y creará las reglas para cada IP.
- Sistema para detectar cambios en la configuración y elegir entre regenerar de nuevo las reglas o cargar las reglas en la cache.
- Permite para cada servicio especificar los flujos de tráfico entre los interfaces de entrada y salida y las IPs de la red local y la remota.

- Proteccion contra ataques contra el kernel, spoofing, ataques de denegación de servicio, ataques de llenado de los logs, escaneos de puertos.
- Creación de logs del funcionamiento del firewall y avisos de inicio y parada.
- Detección y posible bloqueo de trafico.
- Funcionalidad de proxy transparente, NAT, SNAT, DNAT o REDIRECT por medio de tablas y mediante fichero de configuración.

3.6. SEGURIDAD INTEGRADA

Aunque son efectivos proporcionando protección a nivel de red, firewalls, VPNs e IDSs no cubren las necesidades de protección actuales porque:

- Miran solamente las cabeceras del paquete, no miran el interior. No pueden comprobar el contenido del paquete en tiempo real y procesarlo para identificar virus, gusanos u otras amenazas, y por lo tanto son totalmente ineficaces contra ataques basados en el contenido. Consecuentemente, virus, gusanos y troyanos transmitidos por correo electrónico y tráfico http pasan fácilmente a través de cortafuegos y VPN, pasando a menudo desapercibidos por los sistemas de detección de intrusiones.
- No pueden ayudar contra el uso indebido de los recursos de la red, negando los paquetes que contienen material inapropiado, tal como pornografía o sitios Web inadecuados.

Firewalls, Servidores VPN e IDSs fallan a la hora de proporcionar protección completa, para solucionar las limitaciones de firewalling stateful inspection fue desarrollada una tecnología

conocida como Deep Packet Inspecion (DPI). DPI da una paso más llegando a analizar, además de las cabeceras, el contenido de los paquetes. Mientras un ataque pueda ser contenido en sólo unos pocos paquetes, DPI puede ser efectivo en su detección, como pueda ser el caso en ataques de denegación de servicio. La gran limitación de DPI es que no puede detectar amenazas que requieren muchos paquetes para ser transmitidas por Internet. En general, la mayor parte de virus y gusanos tienen docenas de Kbytes e incluso suelen estar en ficheros (documentos, programas, etc.) de millones de bytes, requiriendo así cientos o miles de paquetes para su transmisión. Como resultado de esto, la probabilidad de detectar virus y gusanos analizando el contenido de unos pacos paquetes es extremadamente pequeña.

Como resultado de las limitaciones de estos dispositivos, las organizaciones se han visto forzadas a implantar una amplia colección de soluciones parciales adicionales:

- Antivirus de pasarela
- Filtrado URL
- Filtrado antispam

Cada una de estas herramientas enfocada a una parte concreta del problema global.

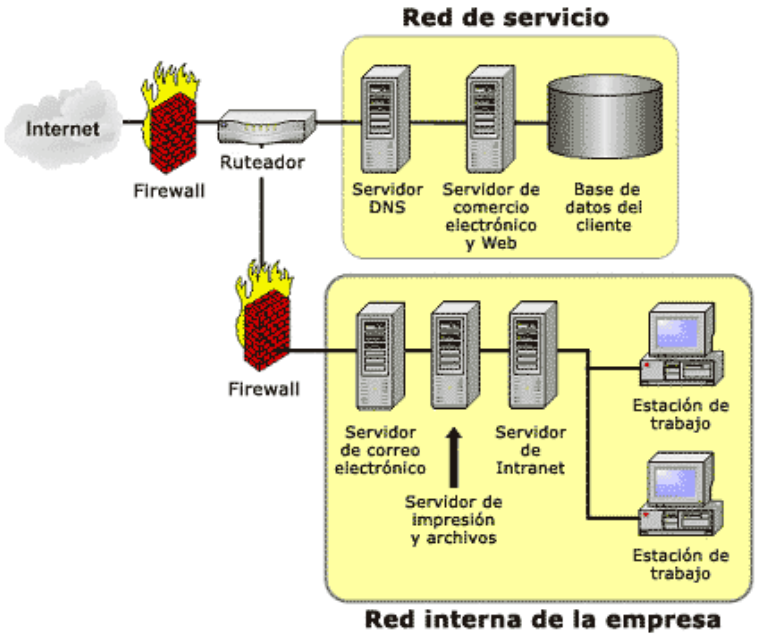
Los Firewall Antivirus deben proporcionar un amplio abanico de servicios de red ï firewall stateful inspection, VPN, detección y prevención de intrusiones (firmas para más de 1.400 ataques y detección de anomalías); así como servicios de nivel de aplicación tales como antivirus de correo electrónico y tráfico web, filtrado de contenidos y filtrado antispam, todo unificado en plataformas dedicadas y de fácil gestión.

Existe herramientas que escanean el tráfico de correo electrónico en búsqueda de virus, pero no escanean el tráfico Web en búsqueda de estas amenazas, ya que los sistemas antivirus convencionales basados en software agregan demoras inaceptables al tráfico en tiempo real. Y dado que la mayoría de ataques de hoy en día provienen de tráfico Web (HTTP), esto representa un vacío significativo a lo que hay que tomar en cuenta el momento de revisar las especificaciones de los equipos.

Dado a las características que han tomado los equipos que protegen la red perimetral muchos de los equipos que hay en el mercado ya no se refieren únicamente a los equipos que prestan estas soluciones como firewall sino como equipos o herramienta de gestión integrada de seguridad.

Una red segura requiere dedicación y acciones preactivas que permitan que las redes sean menos frágil a cada uno de los problemas de la seguridad. La seguridad de la red es un tema extenso en su conjunto, es necesario analizar todos los aspectos de la red que necesitan protección y cómo construir la red de manera que cada capa esté protegida por su respectiva capa de seguridad. Por lo que es necesario conocer lo que se tiene y lo que se necesita para protegerla.

Es importante separar los servicios de red y suministrar una capa de seguridad



para cada servicio.

Una forma de proteger a la red puede ser como muestra el gráfico siguiente, configurar dos redes distintas utilizando firewalls para proteger la red empresarial de Internet y otro firewall para separar la Intranet empresarial de los clientes externos .

En este gráfico se observa una división de la red en dos grupos, los componentes de la red pueden dividirse esencialmente en estas dos categorías principales:

- *Intranet*, contiene todos los servidores y las aplicaciones que son internos de la compañía. Este segmento de la red está separado de la Internet pública por dos firewalls para brindar mayor protección.
- *Red de servicio o de perímetro,* las redes de perímetro están entre Internet e Intranet en este nivel se pueden definir reglas para acceder a esta red específica.

Establecer redes separadas dentro de la compañía permite mayor control sobre el acceso a servidores y servicios.

Es importante tener en cuenta reglas de mejores prácticas tanto para cuando se diseñe la red, ya que esto puede ayudar a identificar graves problemas de seguridad con anticipación y reducir amenazas potenciales. En lo que se refiere a la seguridad en el perímetro de la red, la seguridad no se puede manejar unilateralmente, atacando problemas aisladamente, se debe cubrir diferentes aspectos como:: Análisis en el puerto, negación de servicio, no permitir falsificación de la dirección IP, no permitir Husmeo de la dirección IP, virus, gusanos, etc.; por lo que las empresas deben adoptar una estrategia integrada que responda a

la seguridad de la red en todos los niveles: en el gateway, servidor y cliente.

El firewall de perímetro tradicional ya no proporciona protección adecuada contra intrusiones y amenazas. En parte esto se debe a que la definición de "perímetro" se ha vuelto confusa. La adición de servidores de acceso remoto, conexiones de comunicación, los servidores VPN y los puntos de acceso inalámbrico implica que el anteriormente bien definido límite de la red ya no es tan claro. Existen ahora múltiples caminos externos para llegar a la red corporativa. Inevitablemente, estos están sujetos a que alguien burle el firewall para tener acceso inadecuado a los recursos de la red.

La seguridad integrada usa ampliamente los principios de protección y emplea funciones de seguridad complementaria en los múltiples niveles de la infraestructura. La seguridad integrada puede proteger más eficientemente contra una variedad de amenazas en cada nivel con el fin de minimizar los efectos de los ataques a la red. Las principales tecnologías de seguridad que se deben integrar son las siguientes:

- Firewalls de clase empresarial: Controlan todo el tráfico de la red al monitorear la información que entra y sale de la red para garantizar que no ocurran accesos no autorizados.
- Detección y respuesta a intrusos en tiempo real: Detecta accesos no autorizados y suministra alertas e informes que se pueden analizar para crear los patrones y establecer un planeamiento.
- Filtrado de contenidos: Identifica y elimina tráfico no deseado. El filtrado de contenidos ayuda a las organizaciones a hacer

cumplir políticas de uso aceptables para que no se utilicen indebidamente los recursos de la red.

- Redes privadas virtuales (VPN): Protegen las conexiones más allá del perímetro, permitiéndole a las empresas comunicarse en Internet de manera segura.
- Control de vulnerabilidades: Descubre los vacíos de seguridad y sugieren las mejoras.
- Protección antivirus: Protege contra virus, gusanos y caballos de Troya.

Con estas tecnologías de seguridad integradas en una sola solución, una empresa está en mejor posición para resistir una amenaza a la red moderna actual, sea un ataque de códigos maliciosos, un ataque de negación de servicios, acceso no autorizado (interno o externo) o amenazas combinadas.

Cuando las tecnologías de seguridad se integran en una solución única, ofrecen una protección más completa al mismo tiempo que ayudan a reducir la complejidad y los costos. Una solución integrada elimina la necesidad de administrar múltiples productos de muchos distribuidores o solucionar problemas de interoperabilidad. Además puesto que la seguridad integrada se puede implementar en todos los niveles de la red, ofrece mayor protección a los recursos patentados y reduce los riesgos para la continuidad de las empresas. Aparte de ello, el enfoque integrado hace que el personal informático se concentre en otras iniciativas estratégicas al mismo tiempo que se maximiza la productividad de los departamentos de informática, frecuentemente sobrecargados de trabajo. Hoy en día las organizaciones pueden mejorar la eficiencia de las funciones de la seguridad, minimizar el impacto de los ataques y mejorar su situación de seguridad con el esquema de seguridad integrada.

CAPITULO IV

ANALISIS ACTUAL DE PETROINDUSTRIAL

4.1. EL PETROLEO EN EL ECUADOR

Los derivados del petróleo y la industria que genera encierran miles de productos diferentes que tienen que ver con todos los aspectos de la vida humana a través de diversas mercancías de uso que el hombre necesita, tales como: combustibles de carros, barcos y aviones, kerosén, gas de cocina, abonos agrícolas, plásticos, caucho sintético, medicinas, cosméticos, ciertos tipos de telas, insecticidas, cera, tinta, aceites de motos, detergentes, colorantes, explosivos, perfumes, discos, películas, pintura, barnices, champús, grasa, etc.

El petróleo es un mineral energético por excelencia. Se trata de un hidrocarburo o compuesto orgánico, cuya formación se debe a la descomposición de residuos vegetales y animales a lo largo de muchísimos siglos, localizados en las profundidades de la tierra. Cuando el hidrocarburo es líquido aparece en forma de petróleo y cuando es gaseoso forma el gas natural que es otro energético; su estado sólido aparece en forma de asfalto, tan usado en la construcción de carreteras y calles, siendo además conocido en este último caso con el nombre de brea.

El petróleo al encontrarse en el interior de la tierra ya no está en el suelo o superficie sino en el subsuelo, se puede localizar en territorio continental o en el subsuelo del fondo marino. El sitio donde se localiza se denomina yacimiento y éste es su depósito. Son encontrados a través de la exploración, búsqueda o prospección que son los métodos o técnicas usados para este fin,

posteriormente se procede a la perforación con un taladro hasta llegar al lugar donde se encuentra y mediante procedimientos técnicos extraerlo; se conforma así lo que se llama un pozo de petróleo. Luego es transportado a las refinerías para que sea tratado con el fin de elaborar los múltiples productos para el uso de los consumidores. También puede ser depositado o almacenado en gigantescos tanques como reserva o para comercializarlo en los puertos de embarque, donde los barcos cisternas los trasladan a los países que lo compran.

La actividad de exploración petrolera en el Ecuador se inicia a principios de siglo a lo largo de la costa del Pacífico. El primer descubrimiento importante lo realizó la compañía Angla Ecuadorian Oilfields Ltda. En 1924 en la península de Santa Elena, dando inicio a la producción petrolera.

Los primeros trabajos de exploración hidrocarburífera en la Región Oriental se inician en 1921, cuando la compañía Leonard Exploration Co. de Nueva Cork obtuvo una concesión de 25 mil km2 por el lapso de 50 años.

En 1964 la Texaco Gulf obtiene una concesión de un millón quinientos mil hectáreas. Esta compañía en 1967 perfora el primer pozo productivo el Lago Agrio N.1. Posteriormente en 1969 siguieron los de Sacha y Shushufindi. A raíz de esto, se produce una serie de concesiones, que tuvieron el dominio absoluto de las compañías extranjeras, hasta que en junio de 1972 se crea la Corporación Estatal Petrolera Ecuatoriana (CEPE).
La producción propiamente de la Región Oriental se inicia en 1972 por parte del consorcio Texaco-Gulf.

El 6 de julio de 1974, CEPE adquiere el 25% de las acciones de este consorcio, creándose un nuevo consorcio CEPE-Texaco-Gulf.

En 1976 ante una serie de irregularidades cometidas por la empresa Gulf, CEPE adquiere esas acciones con lo que pasa a ser el accionista mayoritario del consorcio con el 62% de las acciones; posteriormente CEPE adquiere la totalidad de las acciones y pasa a tener el control de todas las fases de la producción petrolera. A partir de 1989 CEPE se convierte en PETROECUADOR con varias empresas filiales: Petroproducción, Petroindustrial, Petrocomercial y Petroamazonas.

El Ecuador actualmente y desde el boom petrolero financia la gran mayoría de sus gastos con la venta de petróleo, por lo que existe una elevada dependencia de los ingresos petroleros de la economía nacional y del Estado como se puede apreciar en el siguiente cuadro:

Balanza comercial petrolera y no petrolera en millones de dólares

Año	Petroleras	No Petroleras	Total	Petroleras	No Petroleras	Total	Petrolera	No Petrolera	Total
2001	1.900	2.778	**4.678**	250	4.731	**4.981**	1.650	-1.953	**-302**
2002	2.055	2.981	**5.036**	232	5.773	**6.006**	1.823	-2.792	**-969**
2003	2.606	3.432	**6.039**	597	5.501	**6.097**	2.010	-2.069	**-59**
2004*	3.585	2.664	**6.250**	621	5.258	**5.878**	2.965	-2.593	**372**

Fuente: Banco Central del Ecuador

4.2 PETROECUADOR

La administración y comercialización del petróleo es llevado a cabo por la Empresa Estatal Petróleos del Ecuador (PETROECUADOR), cuyo régimen jurídico está perfectamente tratado en la ley de hidrocarburos y en la ley de la Empresa Estatal

Petróleos del Ecuador, además tenemos una flota Petrolera Ecuatoriana (FLOPEC) creada con capitales ecuatorianos y japoneses.

Su importancia está dada por la constitución Polítcia:

ART. 247. Son de propiedad inalienable e imprescriptible del Estado los recursos naturales no renovables.... Estos bienes serán explotados en función de los intereses nacionales. Su exploración y explotación racional podrán ser llevadas a cabo por empresas públicas, mixtas o privadas, de acuerdo con la ley.ò

La ley de hidrocarburos:

ART. l. Los yacimientos de hidrocarburos y sustancias que lo acompañan, en cualquier estado físico, que se encuentren, en el territorio nacional, incluyendo las zonas cubiertas por las aguas del mar territorial, pertenecen al patrimonio inalienable e imprescriptible del Estado.
ART. 2. El Estado explotará y explorará los yacimientos señalados en el artículo anterior, en forma directa a través de la Empresa Estatal Petróleos del Ecuador (PETROECUADOR), la que podrá hacerlo por sí mismo (...) o constituyendo compañías de economía mixta con empresas nacionales o extranjeras de reconocida competencia, legalmente establecidas en el país (...).

ART. 3 ñEl transporte de hidrocarburos por oleoductos, poliductos y gasoductos, su refinación, industrialización, almacenamiento y comercialización, serán realizados por PETROECUADOR... Directamente o celebrando contratos de asociación, consorcios de operación o mediante otras formas contractuales vigentes en la legislación ecuatoriana. ... ò

ART. 5. Los hidrocarburos se explotarán con el objeto primordial de que sean industrializados en el país.

ART. 6. Corresponde a la Función Ejecutiva la formulación de la política de hidrocarburos. Para el desarrollo de dicha política, su ejecución y aplicación de esta Ley, el Estado obrará a través del Ministerio del ramo, de Petroecuador y del Ministerio de Defensa Nacional.

ART. 247 .Son de propiedad inalienable e imprescriptible del Estado los recursos naturales no renovables.... Estos bienes serán explotados en función de los intereses nacionales. Su exploración y explotación racional podrán ser llevadas a cabo por empresas públicas, mixtas o privadas, de acuerdo con la ley.ò

ART.58 Sólo el Estado o PETROECUADOR podrán en lo futuro, por sí mismos o mediante algunas de las formas contractuales (contratos) establecidas en esta ley, construir, operar y administrar oleoductos, gasoductos y otros medios similares de transporte de hidrocarburos (...)
ART. 66. El transporte marítimo de hidrocarburos y derivados deberá efectuarse preferentemente en naves de bandera nacional (...) y considerando la competencia internacional.

Ley de la Empresa Estatal Petróleos del Ecuador:

ART. l. NATURALEZA. Crease la Empresa Estatal Petróleos del Ecuador, PETROECUADOR, con personalidad jurídica, patrimonio propio, autonomía administrativa, económica, financiera y operativa, con domicilio principal en la ciudad de Quito (.. .).

ART. 2. OBJETIVO. (.. .), tiene por objeto el desarrollo de las actividades que le asigna la Ley de Hidrocarburos, en todas las

fases de la industria petrolera, lo cual estará orientado a la óptima utilización de los hidrocarburos, que pertenecen al patrimonio inalienable e imprescriptible del Estado, para el desarrollo económico y social del país, de acuerdo con la política nacional de hidrocarburos establecida por el Presidente de la República, incluyendo la investigación científica y la generación y transferencia de tecnología (.. .).

4.3. PETROINDUSTRIAL

PETROINDUSTRIAL pertenece al conjunto de filiales de la Empresa Estatal de Petróleos del Ecuador PETROECUADOR, es la empresa encargada de transformar los Hidrocarburos del país, mediante procesos de refinación para producir derivados. Cuenta con tres centros de producción de derivados.

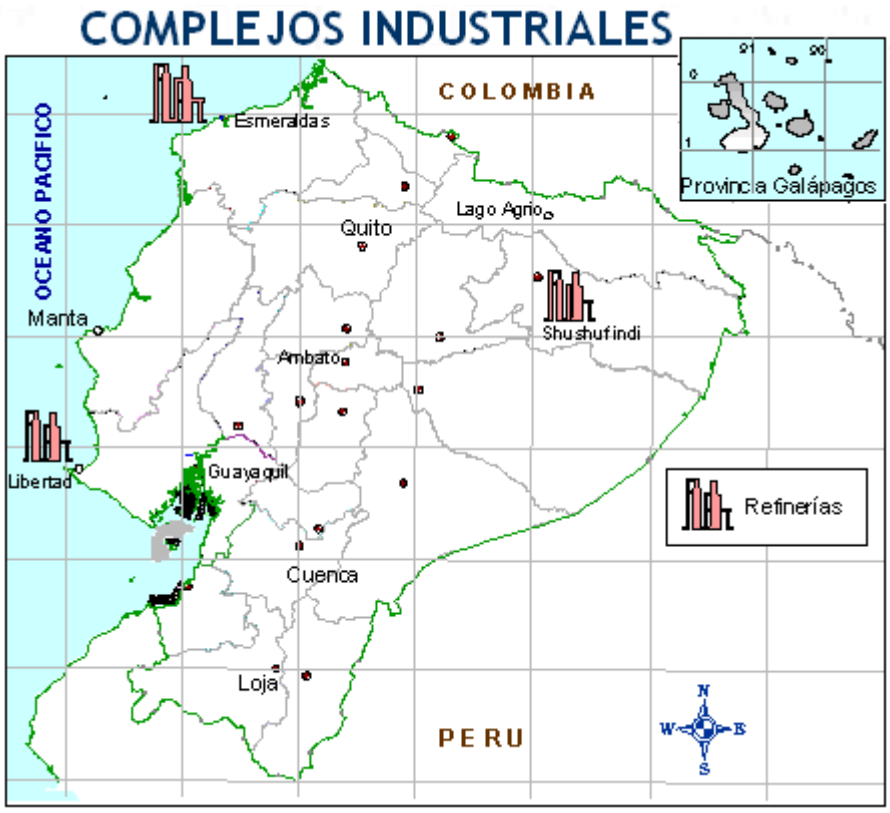
Misión: La misión de ñPETROINDUSTRIALò es la industrialización, incluida la refinación de hidrocarburos en el territorio ecuatoriano obteniendo derivados de calidad, para producir oportunamente los combustibles que requiere el mercado nacional y con las mejores normas de calidad, procurando la mayor eficiencia en la gestión empresarial y preservando el equilibrio ecológico para lo cual deberá prevenir y controlar la contaminación ambiental.

OBJETIVOS:

- Industrializar los hidrocarburos con la mayor eficiencia empresarial, previniendo la contaminación ambiental.
- Procesar los crudos que se obtienen principalmente el los campos de la Amazonía.
- Abastecer la demanda de combustibles del país.

4.3.1 Estructura de Petroindustrial

ñPETROINDUSTRIALò cuenta con tres centros de producción de derivados: Refinería Estatal Esmeraldas REE, Refinería La Libertad y Complejo Industrial Shushufindi; los mismos que se encuentran ubicados en Esmeraldas, La Libertad y Shushufindi como muestra el mapa siguiente.



˘ La Refinería Estatal Esmeraldas, está ubicada en la parte noroccidental, en la costa del Océano Pacífico, junto a la ciudad de Esmeraldas. En los tanques de almacenamiento se

recibe el petróleo de crudo de los campos de explotación del oriente ecuatoriano, parte del petróleo es refinado y el resto se exporta por el puerto de Esmeraldas. La planta está en capacidad de producir gasolinas sin plomo y de cumplir lo estipulado en la "Ley de Regulación de la Producción de la Comercialización de Combustibles en el Ecuador", expedida en octubre de 1995, en donde se prohíbe la utilización de tetraetilo de plomo en la preparación de las gasolinas.

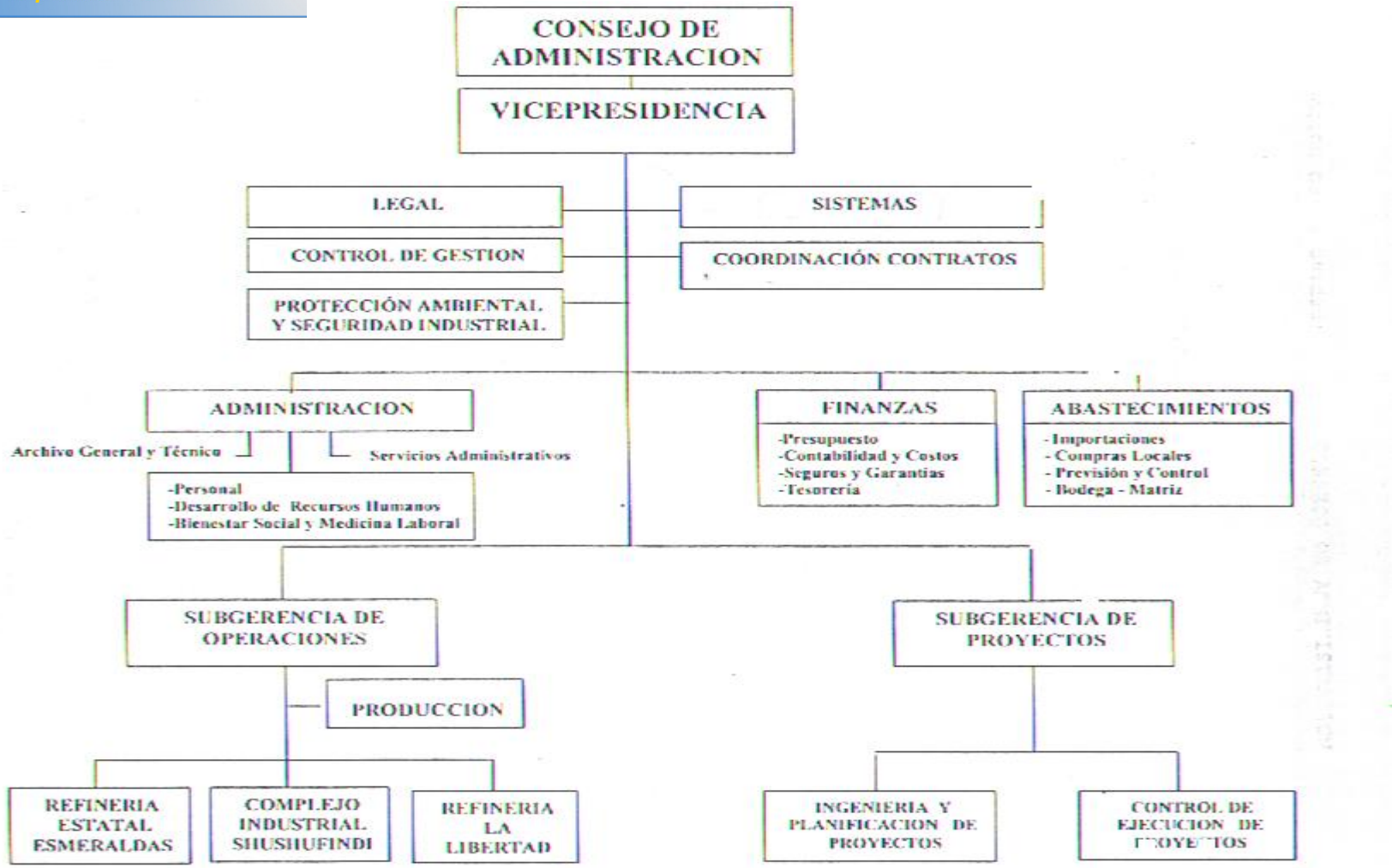
- La Refinería La Libertad, está diseñada para procesar petróleo crudo extraído del Oriente Ecuatoriano y produce los siguientes derivados: LPG, Gasolina, Diesel, Jet Fuel, Fuel Oil y Solventes. La Refinería La Libertad cuenta con dos Terminales Marítimos: Cautivo y La Libertad.

- El Complejo Industrial Shushufindi, está conformado por: refinería Amazonas y planta de gas Shushufindi.
  - Refinería Amazonas, proyecto industrial que se dio por la creciente demanda interna de combustible y la presencia de empresas internacionales contratadas para las actividades de exploración y explotación petrolera en la región amazónica. Dispone de dos plantas de destilación de donde se obtienen los siguientes productos: GLP, nafta bases,

kerosene, jet fuel, diesel 2 y crudo reducido.

- Planta de Gas Shushufindi, es el principal campo de producción de petróleo del país de donde se extrae, además gas natural asociado. El gas producido se transporta a través del poliducto Shushufindi - Quito, de donde se lo distribuye para su consumo como combustible doméstico o industrial.
- PLANTA DE GAS DE SECOYA, es una planta para tratamiento del gas y aprovechar la capacidad instalada de la planta de Shushufindi e incrementa la producción 80 T/d de GLP.

AMA ESTRUCTURAL DE PETROINDUSTRIAL MATRIZ



Las oficinas centrales de Petroindustrial se encuentran ubicadas en la ciudad de Quito, desde estas oficinas se administra los distritos descritos anteriormente desde la subgerencia de Operaciones como muestra el organigrama de la página anterior.

4.4 ÁREA DE TECNOLOGÍA DE PETROINDUSTRIAL

En ñPETROINDUSTRIALò el área de tecnologías de la información se denomina Unidad de Sistemas. Se encuentra ubicada físicamente en el segundo piso del edificio matriz en Quito.

La Unidad de Sistemas: ñEs la Unidad Administrativa a la que le corresponde apoyar a la empresa en todo lo referente a tecnología Informática para apoyar la gestión técnica y administrativa de la filialò

A la Unidad de Sistemas le corresponde:

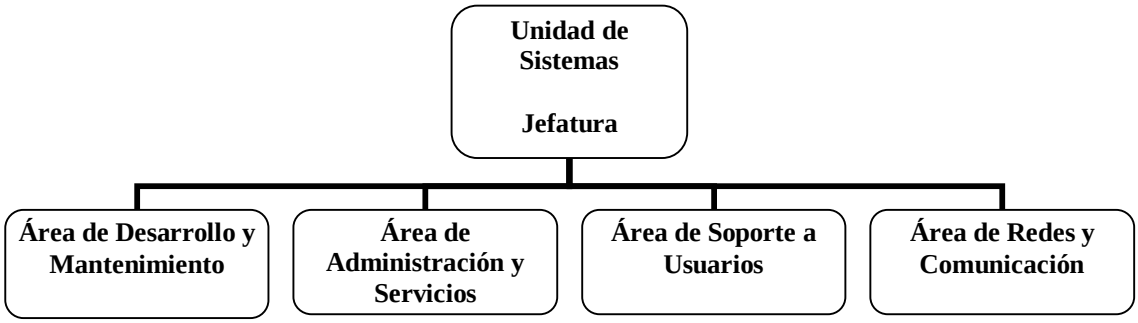
- Implementar soluciones informáticas especificas para ñPETROINDUSTRIAL.ò
- Realizar el desarrollo, implantación y mantenimiento de sistemas y aplicaciones informáticas específicas y corporativas.
- Administrar los recursos informáticos de Hardware y Software de la Filial.
- Coordinar la obtención del servicio del sistema de telecomunicaciones de ñPETROECUADORò para las 4 unidades Operativas de la Filial.
- Brindar soporte técnico a los funcionarios de todas las áreas de la empresa sobre el funcionamiento y utilización del software y hardware computacional.

En cada uno de los distritos existe dentro de su estructura organizacional una Unidad de Sistemas las mismas que están a nivel asesor de las Superintendencias de las Refinerías. Las Unidades de Sistemas de los distritos tienen una relación de dependencia de la Unidad de Sistemas Matriz en la coordinación de proyectos y la planificación informática.

La estructura funcional interna de la Unidad de Sistemas Matriz de PETROINDUSTRIAL es la siguiente:

- Área de Desarrollo y Mantenimiento, esta área orienta sus trabajo al desarrollo de nuevas aplicaciones y requerimientos planteados por la administración de la empresa.
- Área de Administración y Servicios, área encargada de administrar los recursos que están bajo los servidores de dominio de Petroindustrial.
- Área de Soporte a Usuarios, es la encargada de atender los requerimientos diarios y garantizar la utilización de los recursos tecnológicos a los usuarios.
- Área de Redes y Comunicación, se encarga de administrar el servidor IBM y mantener las comunicaciones con los distritos de Petroindustrial y con Petroecuador.

Estructura funcional de la Unidad de Sistemas



El Hardware que actualmente dispone PIN se describe en el cuadro siguiente (sólo incluye computadores o estaciones de trabajo):

Distribución de equipos disponibles en Petroindustrial

DISTRITO	Servidores		Estaciones de trabajo
	IBM AS	Windows 2000	
Refinería Estatal Esmeraldas	1 (9406820)	6	161
Refinería La Libertad	1 (9406820	3	87
Complejo Industrial Shushufindi	1 (9406270)	4	50
Petroindustrial Matriz	4 (DOS 9404-602 DOS 9406810)	5	139
TOTALES->	7	18	437

Petroindustrial tiene como política de estandarización la utilización del Sistema Operativo Windows para el uso de microcomputadores y para los servidores de servicios de red, así también se ha definido el uso de herramientas compatibles con este sistema operativo como: Microsoft Office, Microsoft Visual Basic, Microsoft SQL Server 2000, etc.

4.4.1. Aplicaciones Relevantes

En Petroindustrial existen implementadas muchas aplicaciones que facilitan y apoyan a los usuarios en el desempeño de sus funciones. La mayoría de éstas aplicaciones han sido diseñadas por la Unidad de Sistemas tomando en cuenta los requerimientos específicos de la empresa. A continuación se detallan algunos sistemas relevantes que se manejan en Petroindustrial Matriz y sus distritos:

- *Control de Plantas*, este sistema programa y registra la producción, existencias, movimientos, análisis de laboratorio, consumo de químicos y operatividad de las plantas; emite balances y reportes consolidados o por distritos. Esta aplicación fue desarrollada en AS/SET, existe una versión para cada distrito y matriz.
- *Sistema Financiero Contable*, maneja los procesos contables y financieros, desde el ingreso de transacciones diarias hasta la generación de informes de gestión de la empresa, dispone de información histórica en línea de cada uno de los distritos.
- *Costos y Presupuestos*, controla los presupuestos operativos y de inversiones de la empresa, permite disponer de información en línea de valores predeterminados y reales de todas las Unidades Operativas de PETROINDUSTRIAL.
- *Activos Fijos (UNICLASS*), mantiene el historial en detalle de los archivos fijos de la empresa y su gestión contable (depreciación, revalorización, altas y bajas). Este sistema está instalado en cada una de las Unidades Operativas de PETROINDUSTRIAL.
- *Recursos Humanos*, gestiona la información del personal de la empresa, permite la emisión de roles de pago, control de asistencia y manejo de vacaciones.
- *Control de Contratos y Bienes*, esta aplicación maneja los datos de proveedores calificados de acuerdo con los requerimientos de la empresa y permite el registro, control y seguimiento de contratos.
- *Administración de Materiales y Equipos*, administra y controla el inventario de productos, procesamiento y seguimiento de la gestión de compras, administración del mantenimiento

preventivo y correctivo de las plantas e historia técnica de equipos.

- *Control de Asistencia*, mantiene un registro de las entradas y salidas del personal para efectuar un control preciso de asistencia y generar reportes e información para aplicación de Recursos Humanos.
- *Administración Electrónica de Documentos*, esta aplicación permite la digitalización, archivo, búsqueda y seguimiento de diferentes documentos que son de importancia para la empresa.
- *Distribute Control System DCS,* el Sistemas de Control Distribuido es un sistema especializado que permite la operación de las refinerías, a través de esta aplicación los operadores operan toda la instrumentación de cada una de las plantas.
- *Plant Information System PI,* esta aplicación permite almacenar la información histórica de la producción de las plantas.
- *Balances Másicos,* en base a la información histórica de los datos de operación de las plantas y con datos de los laboratorios el sistema permite la emisión de balances de operación.

4.5 RED DE PETROINDUSTRIAL

En el año de 1998 Petroindustrial incursiona en el ambiente de redes mediante la implementación de la red local de la Matriz que se constituyó en el proyecto piloto de la Red Integral de Información de Petroindustrial (RIIPIN) de lo que hoy es la red WAN de Petroindustrial. En el año 2001 a través de proyecto

RIIPIN II se crean en las Refinerías de la Filial las redes locales de Esmeraldas, Complejo Industrial Shushufindi y La Libertad y se las integra en la Red WAN de Petroindustrial.

Con este propósito se instala en cada Unidad Operativa un servidor que administre localmente los recursos disponibles y se establece el personal responsable de ejecutar tareas de operación y administración. Los servidores locales se configuraron bajo la plataforma de Microsoft Windows 2000 Server y cuentan con Microsoft Exchange 2000, SQL Server y SMS.

La red WAN de Petroindustrial presta a sus funcionarios los servicios de correo electrónico, navegación en Internet y el acceso a Sistemas Cliente/Servidor.

Los beneficios que esta tecnología presta a la Empresa conllevan también riesgos y uno de ellos es contar con las herramientas y lineamientos claramente definidos que permitan asegurar efectivamente la información y los recursos disponibles a través de la red.

Petroindustrial cuenta en la actualidad con una red distribuida en cuatro localidades dentro de un mismo dominio ríz del bosque petroindustria.com.ec De este dominio se desprenden a las localidades 4 subdominios:

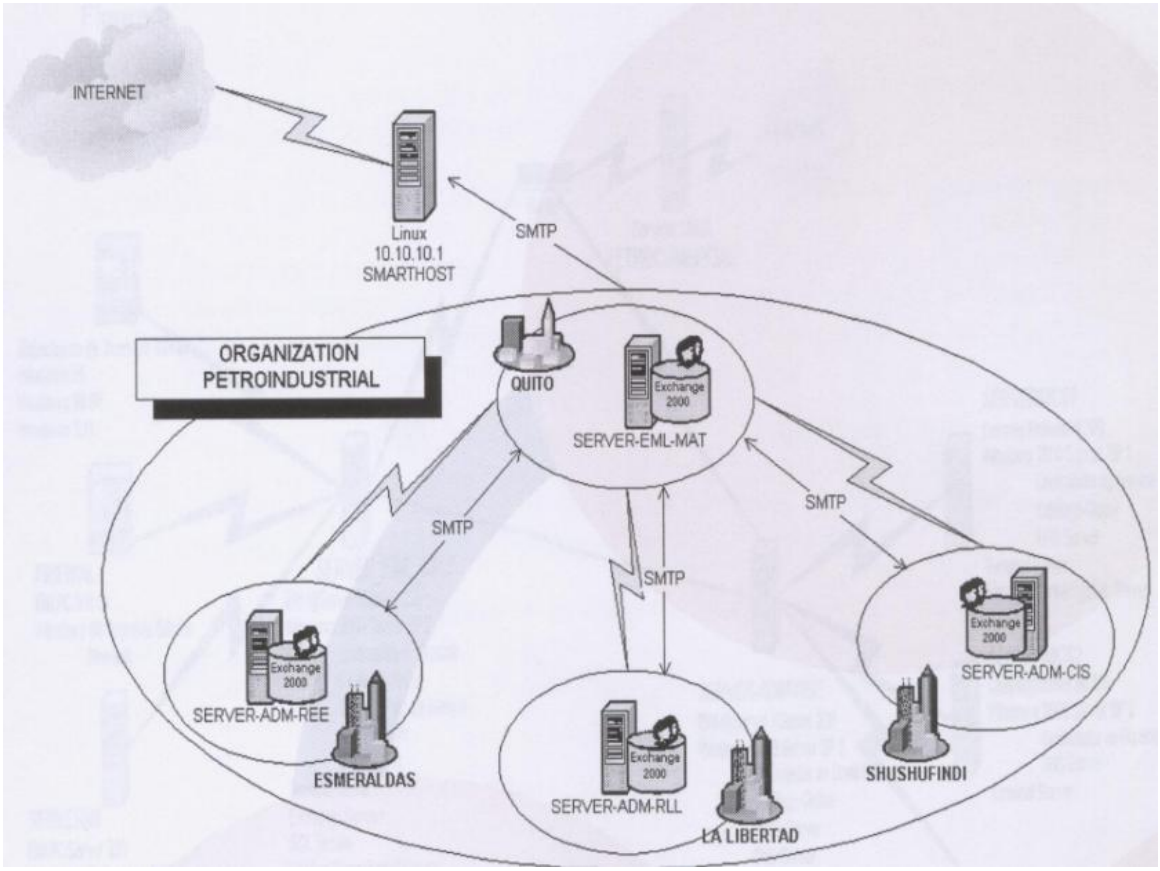
- PIN_MAT, ubicado en la oficina Matriz. Los equipos de que enlazan a la red con Petroecuador y con los diferentes distritos se encuentran ubicados en el segundo piso de la oficina Matriz de Petroindustrial, en esta área están los servidores de red: Server_eml_mat, Server_adm_mat y Server_mail_mat, estos servidores que realizan las funciones de controladores del dominio PIN_MAT, catálogo global, DNS, Exchange Server,

administrador de impresoras, servidores de aplicaciones. Bajo el Server_eml_mat se realiza la replicación el Active Directory entre los sites automáticamente.

- PIN-REE dominio ubicado en la Refinería Estatal Esmeraldas. El departamento de sistemas se encuentra ubicado en la planta baja del edificio administrativo, en está área se encuentra acondicionado un centro de cómputo en el cual han sido ubicados físicamente los servidores de red: Server_eml_ree y Server_mcs1_ree; estos están configurados como hijos del servidor de la oficina matriz (Server_eml_mat) y forma el Dominio PIN-REE.
- PIN_RLL este dominio pertenece a la Refinería La Libertad, dispone de dos servidores de red: Server_eml_rll y Server_mail_rll; el primero está configurado como hijo del servidor de la oficina matriz (Server_eml_mat) y el segundo actúa como servidor alterno.
- PIN_CIS dominio ubicado en el Complejo Industrial Shushufindi, dispone de un solo servidor Server_eml_cis, el mismo que es hijo del servidor de la oficina matriz (Server_eml_mat).

4.5.2. Configuracion Internet y Correo Electrónico

La conexión de Internet se realiza por medio del servidor de Petrocomercial, lo que implica que el tráfico es atendido y controlado por la conexión Petrocomercial según se muestra en la siguiente figura:



Los servidores de mensajería utilizan MS Exchange 2000 para el invío y recepción de mensajes tanto internos como externos. El nombre de la organización para MS Exchange es Petroindustrial, y el nombre de los sitios es igual al nombre de la localidad en la que se encuentra el servidor.

Los sitio MS Exchange están conectados por medio de conectores de sitios (Site Connectors), el mismo que se utiliza para la replicación del directorios y de la mensajería interna.

Para la mensajería externa se utiliza el protocolo SMTP, todo el tráfico se realiza por este protocolo, los sitios envían al servidor de Matriz y este rutea el tráfico al servidor Linux de Petrocomercial para la entrega de mensajes, la misma ruta es seguida para la recepción.

4.6 POLITICAS DE SEGURIDAD DE RED

La implementación en Petroindustrial de nuevas herramientas informáticas, por el auge de las tecnologías Internet/Intranet, ha provocado la aparición de nuevas necesidades. Los beneficios atribuibles a las nuevas tecnologías son muchos, pero también los riesgos: la pérdida de imagen, la pérdida de información, la suplantación de usuarios y el espionaje.

El implementar políticas de seguridad es una necesidad y un requerimiento para disminuir múltiples factores de riesgo como el acceso desautorizado o inadvertido a recursos de la red así como minimizar el soporte técnico.

La Unidad de Sistemas de la Matriz de Petroindustrial ha definido parámetros generales que permiten a los usuarios de las redes locales asegurar los servicios que cada Controlador de dominio presta a sus funcionarios para lo cual se han configurado Políticas de RED enfocadas a:

- Establecer reglas de seguridad que permitan al personal que administra las redes locales de la red WAN de Petroindustrial, minimizar los riesgos tanto a nivel físico como por manipulación no autorizada de los recursos de la red.
- Minimizar el tiempo invertido en administración y soporte a usuarios finales
- Optimizar el uso de recursos integrados a la red, aplicando accesos y autorizaciones específicos que permitan compartirlos de manera segura.
- Explotar las características disponibles en Windows 2000 Server, que permitan configurar las estrategias de seguridad requeridas.

Las políticas de red que la Unidad de Sistemas ha implementado hasta el momento tratan de establecer un nivel de seguridad de red básico como:

- Definir la utilización de herramientas que ofrece Windows 2000 Server, por tener una mayor compatibilidad y en general para lograr un correcto funcionamiento de la red.
- Creación de cuentas personales de usuarios que permitan autenticarlos y a la vez definir su accionar dentro de la red, incluye la definición de autorizaciones por recurso compartido y por usuario. Las cuentas personales incluyen a personal de PIN y los contratados.
- Establecer un servidor de impresoras de red que facilita el trabajo diario del usuario, compartir bajo autorización y alta disponibilidad.
- Generación de backups de seguridad de los servidores.
- Bloqueo de consolas de acceso a servidores y definición de claves de conocimiento restringido.
- Creación de áreas restringidas donde se ubican los servidores, el acceso a esta área está restringida al ingreso exclusivo de

los administradores y operadores, está prohibido el acceso a personal no autorizado.

- Establecer en cada distrito un Servidor Replica (same parents), lo que permite disponer un nivel alto de disponibilidad para autentificación o tolerancia a fallos y balanceo de carga .
- Establecer un estándar en la creación de cuentas de usuarios, las mismas que han sido creadas bajo el siguiente esquema: ABApellido donde A es la inicial del primer nombre del usuario y en el caso de ser necesario se utilizará B que representa la inicial del segundo nombre y Apellido que corresponde al primer apellido del usuario. Ej. Nguzman.
- Establecer un estándar de creación de Unidades Organizaciones que permitan administrar de mejor manera las cuentas y recursos de cada departamento, para facilita la aplicación de políticas de seguridad. Se usa el siguiente estándar: DDDNombreUO donde DDD corresponde a las siglas empleadas por el Distrito (Ej. MAT de Matriz) y NombreUO corresponde al nombre de la Unidad Organizacional. Ej. matSistemas.
- Establecer en los servidores cuentas de administradores y de operadores
- Deshabilitar el cambio de nombre de la cuenta de invitados (guests), además se deshabilita las opciones con invitados y los accesos que se instala por omisión Everyone.
- Deshabilitar el cambio de nombre de la cuenta del administrator.
- Establecer políticas de pasword como:
  - Exige el cambio a los 30 días, y comunica su cambio faltando 5 días.
  - No puede repetirse las últimos 4 cambios de paswords.
  - La longitud del pasword es mínimo 6 caracteres.

- Al ingresar mal un pasword por 5 veces seguidas la cuenta se deshabilita y el único que puede activarle nuevamente es el administrador de la red.
- Las cuentas de empleados que se separan de la institución no se las borra, estas quedan deshabilitadas.

– Establecer políticas de escritorio para los usuarios por Unidad Organizacional, se han activado las siguientes:
  - Desactivación de la opción ejecutar
  - Establecer un fondo predefinido de la empresa por Unidad Organizacional, el fondo de pantalla permite identificar visualmente a que Unidad pertenece.
  - Desactivar todas las opciones del panel de control.
  - Obligar la autentificación con el dominio correspondiente a cada distrito o el dominio Matriz.
– Calendarización de la replicación del Active Directory entre los sites de los diferentes distritos, se ha establecido el siguiente horario de ejecución: una replicación a las 12:00 a.m. y otra a las 18:00 p.m. de lunes a domingo. Además se han establecido puentes de replicación alternos que permitan completar el proceso con éxito en cado de problemas con un distrito.
– Definir el canal de comunicación, con el propósito de optimizar el uso del ancho de banda en se emplea el protocolo SMTP como conector entre sites ya que los controladores de cada dominio son MS Exchange Server y tienen configurado este protocolo.
– Actualización permanentemente los Services Packs que genera Microsoft para el Sistema Operativo Windows 2000 Server.
– Se ha establecido una bitácora de operación de los servidores y su mantenimiento. En ella se documentarán las actividades relevantes ejecutadas sobre ellos y las aplicaciones instaladas.

- Existe personal de seguridad que vigila el acceso de personas extrañas a la Institución.

A nivel de las estaciones de la red se cuenta con los siguientes procesos de prevención y protección:

- Protección contra virus, mediante el monitoreo diario de los discos de todos los equipos enlazados a la red a través del software Symantec Antivirus.
- Mediante el servicio corporativo Petroecuador ofrece a sus Filiales un filtro de seguridad y control de correo electrónico y navegación en Internet.
- Los equipos tienen un mantenimiento continuo por parte de personal calificado.
- Se ha establecido que dentro de la configuración del entorno de red se eliminen todos los protocolos y servicios diferentes a los estándares de comunicación que son: Protocolo TCP y Servicio de Clientes para red Windows. Esta configuración de las tarjetas de red deberá ser revisada y aplicada para todos los dispositivos conectados a la red local; esto permite que se inunde en el tráfico de la red con información basura.
- En caso de fuego, se cuenta con un sistema contra incendios, extinguidores ubicados en sitios estratégicos. El sistema contra incendios es tipo GAS CARBONICO (CO2).
- Se ha definido políticas locales que permitan únicamente ingresar al equipo local con la cuenta de administración del equipo (cuenta que maneja la Unidad de Sistemas) o con la o las cuentas de usuario que tengan permiso de acceso al equipo.

Es importante mencionar que en la instalación de todos los equipos disponen de una alimentación eléctrica en la que se ha eliminado las interferencias electromagnéticas y de radio frecuencia,

es decir, los ruidos eléctricos que interfieren en el funcionamiento de los componentes electrónicos y ponen en peligro la integridad de los datos que almacenan. Todas los toma corrientes que suministren energía eléctrica a los computadores de los usuarios y servidores del centro de cómputo están aterrizados e integrados al UPS central.

4.7 ANALISIS DE RIESGOS

Durante el tiempo de operación de la red WAN de Petroindustrial se han identificado distintos factores de riesgo que pueden desencadenar situaciones críticas en su funcionamiento, de ahí la importancia de identificar estos riesgos, para tomar correctivos y prevenir repercusiones de gran escala. Los factores de riegos mas relevantes que se han identificado son:

Factor de Riesgo	Nivel de Riesgo
Falta de enlace de comunicaciones (via microonda)	Alta
Falla del servidor local y/o componentes activos de la red	Bajo
Ataques por virus y de intrusos en la red WWW	Alta
Contaminación de virus en los equipos de la red	Alta
Fuego	Bajo
Robo común	bajo
Fallas en los equipos, que dañen archivos	Medio
Equivocaciones, que dañen archivos	Bajo
Terremotos o fenómenos naturales, que destruyen equipos y archivos	Bajo
Accesos no autorizados, filtrándose datos no autorizados	Alto
Accesos remontos no autorizados	Medio
Instalación de software no licenciado	Alta

La ocurrencia de estos riegos dentro de la red WAN de Petroindustrial generaría la suspensión total o parcial del servicio de correo electrónico, navegación en internet, el normal funcionamiento de las aplicaciones que operan localmente y/o que son utilizadas en forma remota desde la Matriz.

Todo esto puede incidir en el funcionamiento del servidor, ya que si el problema persiste, el equipo generaría logs y alarmas

permanentes que degradadaría su perfomance, como es el caso de contaminación por virus, donde existe el riesgo de inundar la red con tráfico innecesario y maligno que de ejecutarse en los equipos integrados a la red, conllevaría a una saturación de los servidores.

La red que dispone Petroindustrial ofrece a los funcionarios de las distintas áreas de la Empresa diferentes servicios que constituyen herramientas importantes para la ejecución de su trabajo como:

- Consulta y gestión de coordinación para adquisición de repuestos utilizando los servicios de Internet y/o correo electrónico.
- Obtención de precios y especificaciones técnicas de repuestos o herramientas, entre otras.
- Consulta de información para la toma de decisiones en el área de Producción.
- Actualización tecnológica vía Internet en las diversas especialidades del profesional de la Empresa.

El grado de automatización de la Empresa es del 90%, lo que implica que existe una gran cantidad de actividades que los funcionarios cumplen utilizando los equipos de computación, la red LAN y WAN que dispone la empresa. Si únicamente consideráramos la principal actividad de la Empresa que es la industrialización de hidrocarburos, los efectos de no contar con las herramientas tecnológicas, afectaría en el momento de adquirir los insumos, la programación de la producción, el mantenimiento de las plantas, etc. Por estas razones, es indispensable y justificable las inversiones que permitan adquirir nuevas herramientas que provean, una infraestructura segura y faciliten la administración de la red en general.

4.8 LA PROBLEMÁTICA DE SEGURIDAD

A lo largo de los últimos años los problemas de seguridad que se vienen observando en la empresa tiene su origen en la falta de definiciones estructurales y tecnológicas como:

- La estructura de la organización no define las funciones ni responsabilidades relativas a seguridad de la información, lo que ha ocasionado que Petroindustrial no cuente con una política de Seguridad de la información.
- No existen canales de comunicación predefinidos para tratar incidentes de seguridad en la información, predomina los canales de tipo informal lo que no permite:
  - Un seguimiento adecuado a las causas y solución a problema de seguridad.
  - Analizar e implementar mecanismos preventivos de seguridad a futuros problemas.
- No existe un registro y seguimiento de estos eventos de seguridad por lo que no se puede mostrar estadísticamente, ni evaluar estos tipos de riesgos que se están dando en Petroindustrial. Estos incidentes pueden interrumpir los servicios, inutilizar los sistemas, suprimir o robar información.
- No se han priorizado proyectos dedicados a la seguridad de la información, y cuando existen suelen dedicarse a la seguridad física (puertas, alarmas, dispositivos contra incendios, etc.).
- Como consecuencia de la falta de definición de funciones en temas de seguridad, no existe un responsable que analice y evalúe continuamente los riesgos latentes de la organización, evaluación que permitiría ejecutar medidas que garanticen la operación normal de las actividades de la Empresa.
- Las Unidades de Sistemas de Petroindustrial no tienen una estructura que permita el análisis de problemas de una forma

integral y sobre todo para la planificación y priorización de los proyectos de seguridad que satisfagan necesidades de todas las Unidades de Petroindustrial, lo que a dificulta:

- Involucrar y comprometer a todas las Unidades de Sistemas en proyectos de seguridad.
- Falta de optimización de recursos y apoyo.
- No se ha centralizado, auditado y difundido las normas y procedimientos de los sistemas y procedimientos informáticos.

– Asignación indiscriminada de actividades, en cada una de las Unidades de Sistemas existe personal que con el curso del tiempo a tomado responsabilidades de acuerdo a los requerimientos cronológicos que se han ido dando sin plantear una subestructura que contemple políticas de seguridad a la información que se maneja y que puede dar origen a:

- Manipulación inadecuado de datos, programas y aplicaciones
- Dependencia del personal
- Mala distribución de trabajo que no permite establecer puntos de control y aumenta los niveles riesgos sobre la información.
- Disponer de políticas de manejo y documentación para la administración y operación de los sistemas.

– Mala asignación de responsabilidades de servidores, existe varios servidores que están bajo la administración de diferentes áreas de la Unidad de Sistemas lo que ocasiona que no exista:

- Estandarización en políticas y procesos de administración de usuarios.
- Estandarización en políticas y procesos de backups
- Capacidad de manejar una política integrada de seguridad.

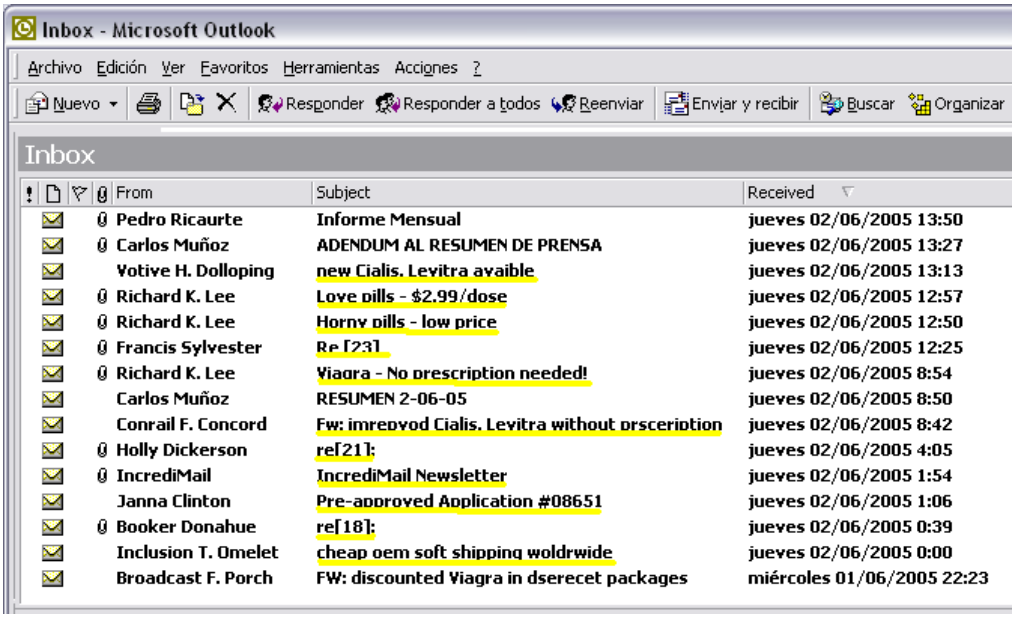
- actualmente la estructura de la Unidad de Sistemas en su funcionamiento interno tiene 4 áreas: Desarrollo y Mantenimiento, Administración y Servicios, Soporte a Usuarios, y Redes y Comunicación, este esquema de trabajo no se ha consolidado totalmente y además no permite un entorno adecuado para establecer políticas de seguridad. En el área de Administración y servicios se lleva el mantenimiento y soporte de la Aplicación de Administración Electrónica de Documentos, lo que obliga a no priorizar temas de administración de servicios.
- Existen aplicaciones que están a cargo de un profesional y el hace: mantenimiento, soporte, actualización y operación.
- No se impulsado y concretado planes de contingencias que garanticen la operatividad de los sistemas de información.

4.9 LA PROBLEMÁTICA DE LA RED

En el entorno de red existente en Petroindustrial Matriz identifica los siguientes aspectos:

- No existen herramientas implementadas que permitan un monitoreo y registro para evaluar:
  - Intentos de accesos no autorizados.
  - Conocer el rendimiento de la red.
  - Saturaciones indebidas por abuso y mal uso de los recursos de la red.
- No se han priorizado pruebas e intentos de intrusión forzada par auditoria y verificar la seguridad de la red.
- La seguridad sobre la red no es manejada como una política de la Unidad de Sistemas, sino como un aporte del responsable de las comunicaciones y de los administradores de los servidores.

- No se ha discriminado y justificado a los funcionarios el acceso a la extranet y al Internet. Actividades no productivas, tales como juegos del Internet, chats, intercambio de música y navegación y descarga de contenido inadecuado, produce el consumo ingente de valiosos recursos de red y de productividad de los funcionarios. Las Unidades de Sistemas de Petroindustrial por muchas ocasiones han detectado el acceso al contenido inapropiado, de esto no se ha hecho un seguimiento y no se han investigado ni implementado correctivos.
- No existe un de Firewall o Proxy de propiedad de Petroindustrial para conectarse directamente con el mundo exterior(Internet), actualmente se realiza a través de los equipos de comunicación de Petroecuador, situación que no Permite a Petroindustrial:
  - Monitorear el tráfico, accesos e incidentes generados por funcionarios de Petroindustrial
  - Disponer filtros adecuados en el perímetro de la red Lan de Petroindustrial Matriz.
- No se ha definido responsabilidad para dirigir los eventos de seguridad. Desde hace varios meses el 70% del correo electrónico corresponde a spam. En el gráfico siguiente muestra que en el buzón de entrada de la cuenta nguzman de 14 mensajes recibidos, 11(subrayados) corresponden a spams, situación que ocasiona múltiples problemas: congestión en la red, consumo de espacio en los buzones, riesgo en la información, etc



CAPITULO V

PROPUESTA

5.1. JUSTIFICACION Y FUNDAMENTACION

El análisis realizado evidencia importantes debilidades en el esquema de la seguridad de la información de Petroindustrial, es urgente realizar acciones preventivas y correctivas que ayuden a mitigar los efectos negativos que pueden derivarse de estas debilidades identificadas.

Las recomendaciones se enfocan a dos tipos de acciones, las urgentes y las necesarias. Dentro del esquema de las urgentes se detallarán acciones que deben implementarse inmediatamente para asegurar un mínimo necesario de seguridad. Las recomendaciones necesarias son las recomendaciones que por su naturaleza o gestión, deberán implementarse en una segunda fase no menos urgente pero generadas bajo una estructura que trabaje en forma planificada, continua y sobre todo que intervengan representantes de los diferentes distritos de Petroindustrial y de la oficina matriz.

Considerando que el presente trabajo se basa en la premisa: ñLa aplicación ordenada de controles y estándares administrativos, operativos y tecnológicos para asegurar la información de Petroindustrial minimizan el riesgo de pérdida, accesos no deseados errores y daños voluntarios e involuntarios a la informaciónò y que en base a esta premisa se ha planteado el objetivo: ñidentificar factores críticos que están afectando a la seguridad del perímetro de petroindustrialò, la propuesta abarca 2 dimensiones: de gestión y técnica.

- Propuesta de Gestión, los complejos entornos tecnológicos y administrativos que maneja en la actualidad Petroindustrial, requiere se desarrolle acciones para mantener la seguridad del la información. La propuesta de gestión que se detalla en este capítulo contempla una reestructuración de la Unidad de Sistemas, la creación de un Comité de Seguridad de la Información que gestione la seguridad de la información de Petroindustrial, recomienda un procedimiento de creación de políticas organizacionales y plantea un conjunto de políticas organizacionales prioritarias, así como un modelo de gestión que permita un trabajo continuo a través del cual se vayan solucionando y elevando el nivel de seguridad de la información de Petroindustrial.
- Propuesta Técnica, dado que los requerimientos de seguridad planteados por la empresa se enmarcaron en el perímetro de la red de Petroindustrial Matriz la misma plantea una alternativa prioritaria a ser adoptada y pautas para llevar a cabo un rediseño de la estructura de seguridad perimetral.

5.2. OBJETIVOS

OBJETIVO GENERAL

Establecer mejoras estructurales organizacionales que permita garantizar la seguridad de la información e identificar un diseños factible técnico que mejore la seguridad del perímetro de la Red de Petroindustrial Matriz.

OBJETIVOS ESPECIFICOS

- Presentar una propuesta factible aplicable de organización estructural dentro de Petroindustrial para que maneje todo lo

relacionado con la seguridad de la información, la misma que analice, evalúe y aplique correctivos de forma continua respecto de la seguridad de la información y describir una metodología con la cual se posicione este organismo en Petroindustrial.

- Presentar una propuesta factible aplicable de organización estructural dentro de la Unidad de Sistemas Matriz, la misma que permita garantizar un manejo adecuado y seguro de la información de Petroindustrial.
- Establecer políticas organizacionales emergentes, las mismas que permitan solucionar de forma inmediata deficiencias en la seguridad de la información.
- Presentar una propuesta tecnológica que permita disponer a Petroindustrial Matriz una red con un alto nivel de seguridad.
- Establecer políticas técnicas-organizacionales emergentes, que permitan solucionar de forma inmediata deficiencias en el manejo de la información dentro de la Unidad de Sistemas.

5.3. UBICACIÓN DE LA APLICACIÓN DEL PROYECTO

El estudio de la propuesta se enfocó en la oficina matriz de Petroindustrial, y dado que desde aquí se aplica los lineamiento institucionales, administrativos y operacionales, existe algunas recomendaciones en la que participan funcionarios de los 3 distritos; pero en sí la aplicación de políticas y cambios estructurales organizacionales y técnicos, está enfocado a ser desarrollado en la Matriz-Quito de Petroindustrial.

5.4. PROPUESTA DE GESTION

Los administradores de seguridad tienen que decidir el tiempo, dinero y esfuerzo que hay que invertir para desarrollar las directivas y controles de seguridad apropiados. Cada organización debe analizar sus necesidades específicas y determinar sus requisitos y limitaciones en cuanto a recursos y programación. Cada entorno informático y directiva organizativa es distinta, lo que hace que cada servicio y cada estrategia de seguridad sean únicos.

Petroindustrial no ha definido a nivel organizacional políticas de seguridad de la información, si consideramos que un gran porcentaje de la información está automatizada, dichas políticas deberían estar ligadas a las tecnologías existentes en la empresa. Para establecer un conjunto eficaz de directivas y controles de seguridad se requiere de un análisis para determinar puntos vulnerables que existen en los sistemas de información de la empresa; análisis que debe ser realizado y mantenido por un equipo de trabajo que desarrolle estrategias de seguridad y canalice proyectos en función de las prioridades de la empresa. Esta propuesta propone la creación de un Comité de Seguridad de la Información, considerando este nombre, ya que la información es el recurso más valioso que tiene la empresa y vital para su operación.

Por lo que se ha mencionado es una estrategia importante la creación del Comité de Seguridad de la Información, grupo de ejecutivos que darían los lineamientos encaminados a mantener la información con altos niveles de confidencialidad, integridad y disponibilidad. Paralelamente a este comité ejecutivo, es necesario que exista en la empresa especialistas dentro del área de

tecnología que investiguen y desarrollen temas de seguridad; razón por la cual Petroindustrial debe transformar o rediseñar la Unidad de Sistemas Matriz para que desarrolle también actividades en temas de seguridad. Se requiere de especialistas que enfrenten el complejo mundo informático, analice, investigue, asesore, de soporte y que apoye directamente en el desarrollo de proyectos y tareas de seguridad.

5.4.1 Nueva Estructura de la Unidad de Sistemas

Como se explicó y detalló en el capítulo 4, actualmente la estructura de la Unidad de Sistemas en su funcionamiento interno tiene 4 áreas: Desarrollo y Mantenimiento, Administración y Servicios, Soporte a Usuarios, y Redes y Comunicación, estructura que crea varias situación que se presta a que exista una falta de seguridad de la información ya que:

- Las áreas de Administración y Servicios, y la de Redes y Comunicación, tienen a su cargo diferentes servidores que dan diferentes servicios a los usuarios de la empresa y que implica:
  - Administración de servicios implementados en cada uno de los servidores.
  - Administración de recursos
  - Administración de usuarios
  - Definición, configuración e implementación de políticas de seguridad
  - Definición de procedimientos de backups

Al estar separados los servidores, no se estandarizan las políticas y procedimientos comunes, así como su documentación.

- Los avances tecnológicos no permite que la seguridad se la enfoque en forma separada, la seguridad hay que analizarla en

forma integrada considerando todos los elementos, por ejemplo, desde una aplicación que no está desarrollada en los equipos IBM que dispone la empresa, se puede acceder a las bases de datos; por lo que el administrador de servicios debe tener el esquema y el conocimiento de cada una de las herramientas para de esta forma evaluar las vulnerabilidades de la información. Además cuando se hace referencia a servicios como por ejemplo el correo electrónico implica deferentes componentes tanto para su funcionalidad como para establecer una política de seguridad.

- Es difícil desarrollar y mantener esquemas de rutas de acceso y controles de conexiones de entrada y salida de los sistemas y servicios que manejan información de Petroindustrial.
- Al hablar de que una unidad es responsable de la operatividad de los servicios, debe estar bajo el control de esta unidad todos los elementos para supervisar, monitorear, controlar y administrar dichos servicios. La Unidad de Administración de Servicios actualmente tiene varios servicios como: disponibilidad de las funciones de red (compartición de archivos, impresoras), servicio de correo electrónico, servicio de web, etc. Todos los servicios están relacionados con las comunicaciones, permisos, enlaces, protocolos, etc. En muchos casos el área de Administración y Servicios no ha podido solucionar problemas porque no está a su alcance.
- El Área de Administración y Servicios se enfoca a la administración de los servicios existentes en los servidores bajo Windows 2000 Server y las políticas de seguridad están enfocadas únicamente en este entorno, esta limitación no permite desarrollar ni enfocar políticas en forma integral.
- El Área de Redes y Comunicaciones de igual forma tiene enmarcado su campo de acción por lo que de igual forma no se

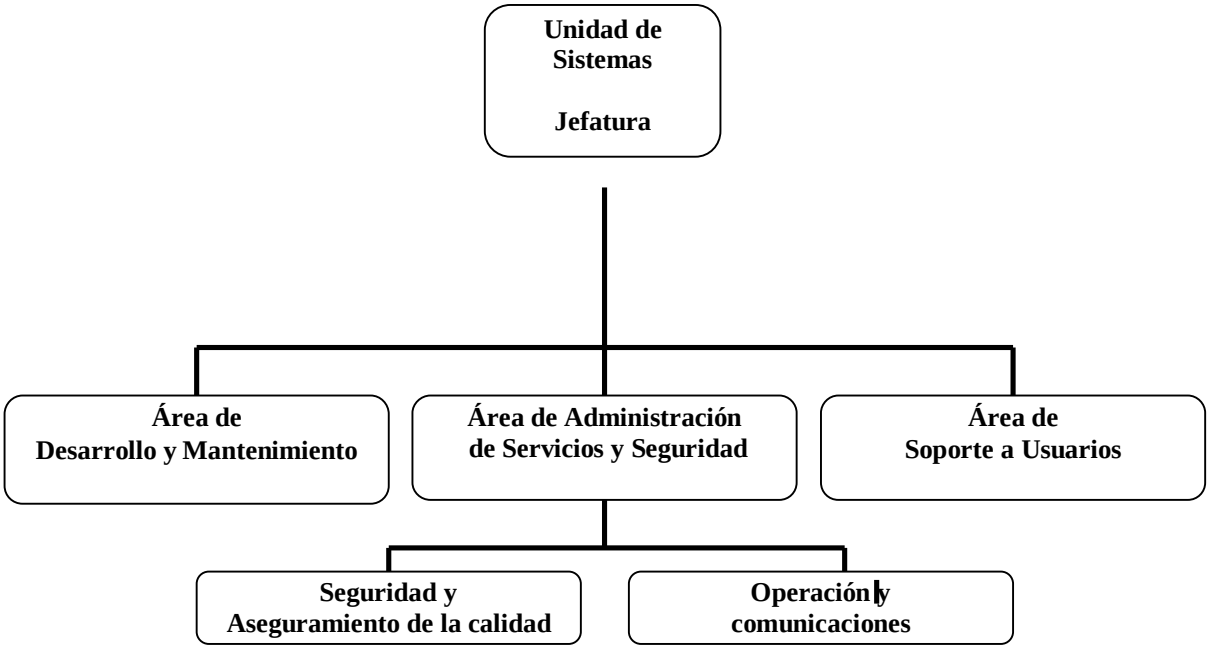
establecen políticas en forma centralizada y con un enfoque integral.

Por lo expuesto se recomienda que las áreas de Administración y Servicios, y el Área de Redes y Comunicaciones, formen una unidad la que podría llamarse Administración de Servicios y Seguridad, no se hace referencia a las comunicaciones y red ya que son elementos implícitos para la operatividad de los Servicios, esta fusión permitiría:

- Exista profesionales que se especialicen en todos los servicios existentes en la empresa en forma íntegra, que tengan conocimientos que permitan un mejor soporte, asesoramiento, control y toma de decisiones.
- Administración centralizada que permita la canalizar de mejor forma la solución a problemas de inoperatividad.
- Manejo de políticas de seguridad en forma integral.
- El área de Servicios y Seguridad, tendría a cargo todo lo que respecta a la operatividad de los servicios de los usuarios, al referirnos a servicios implica: correo electrónico, Internet, sistemas de usuario, red de impresoras, etc. Todos estos servicios dan el ambiente de **operación** necesario para mantener la seguridad interna de la información existente en las aplicaciones desarrolladas y mantenidas por el área de Desarrollo y Mantenimiento.

De lo expresado la propuesta en forma de estructura organigrama la Unidad de Sistemas debería estar estructurada de la siguiente forma:

Propuesta a la Estructura funcional de la



En el organigrama presentado es importante destacar que dentro del Área de Administración de Servicios y Seguridad se incluye 3 responsabilidades importantes: Seguridad y Aseguramiento de la calidad, Operación, y Comunicaciones.

- Seguridad y Aseguramiento de la calidad, que implica:
  - Desarrollo e implementación de estándares de seguridad.
  - Monitoreo del cumplimiento de estándares de seguridad.
    - Políticas y procedimientos de seguridad
    - Documentación y estándares de Sistemas
    - Documentación y estándares de BDD
    - Manuales técnicos de usuario e instalación
    - Manuales de errores comunes y contingencias
  - Apoyo y orientación en los nuevos proyectos de desarrollo y seguridad

- Investigación y actualización permanente de nuevas tendencias y tecnologías
- Administración de claves y accesos:

ˇ Operación, se encarga de la administración de los servicios y sistemas en producción, el alcance de sus funciones es:

- Recepción e instalación de sistemas en producción
- Monitoreo de servidores y servicios habilitados
- Ejecución procesos de backup
- Ejecución de procesos de recuperación
- Mantenimiento preventivo de servidores

ˇ Comunicaciones.

- Monitoreo de enlaces y comunicaciones
- Mantenimiento preventivo y correctivos de equipos de comunicaciones.
- Monitoreo de balanceo de carga de los equipos
- Optimización de uso de canales de comunicación

La mayoría de las empresas consideran como prioridad estratégica el mejorar la seguridad de la red en toda la organización, prioridad que requiere que alguien investigue, profundice en temas de seguridad y desarrolle habilidades avanzadas necesarias en área de seguridad, habilidades que permitirán analizar, diseñar, implemente y asesorar continuamente.

Petroindustrial dispone de 4 Unidades de Sistemas, 3 en los distritos y una ubicado en las oficinas de la Matriz; personal que resulta insuficiente para atender las necesidades informáticas de la empresa por lo que en todos los distritos existe personal misceláneo contratado. Pese a esta realidad la empresa debe asignar una persona que esté enfocada a realizar trabajos y

proyectos de seguridad de información, profesional cuyo trabajo serviría el que ejecuta los proyectos definidos por el Comité de Seguridad de Información y se recomienda pertenezca al área de Administración de Servicios y Seguridad.

5.4.2 Perfil del Coordinador del Área de Administración de Servicios y Seguridad

Es importante considerar que al hablar de servicios implica todo un conjunto de elementos que se requiere para que un servicio que se encuentra a disposición de Petroindustrial esté disponible, por ejemplo el servicio de correo electrónico requiere que: la aplicación Exchange Server esté levantada, que la red interna esté funcionando, que la comunicación con el mundo externo esté activa. Y además que todo esté funcionando adecuadamente bajo un esquema de seguridad.

El personal de tecnología informática en la actualidad tiene que enfrentar grandes desafíos, ya que cada vez intervienen nuevos y complejos elementos sobre los que debe administrar, supervisar, monitorear los servicios, asegurar la información y los equipos. El coordinador del Área de Servicio y Seguridad debe ser un profesional que tenga conocimientos y experiencia en equipos de comunicaciones, redes, protocolos y seguridades. Dado los continuos avances de la tecnología tanto en hardware como en Software el coordinador de esta área debe gustarle la investigación e impulsar la misma en su área. A continuación se detalla el perfil que debe tener el Coordinador del Área de Administración de Servicios y Seguridad:

- Profesional que tenga estudios superiores en Computación o Comunicaciones.

- Preferible con formación de postgrado en alguna área de comunicación, seguridad o administración Informática.
- Persona creativa, investigadora y con capacidad para participar activamente en el desarrollo y la innovación de tecnología. Con visión amplia, capacidad de trabajo en equipo y para interactuar con profesionales de distintas disciplinas.
- Experiencia en equipos de comunicaciones mínimo de 1 año
- Experiencia en redes mínimo 3 años.
- Experiencia en servicios de red como: correo electrónico, monitoreo de la seguridad y administración de usuarios.
- Capacidad de evaluar, investigar y solucionar sucesos de seguridad.
- Habilidad para reconocer las vulnerabilidades y bloquear los intentos de aprovechar dichas vulnerabilidades.
- Habilidad para evaluar de las amenazas de los componentes integrales de los servicios que se encuentran en la red de Petroindustrial.
- Habilidad desarrollar mecanismos de protección de los recursos valiosos, las redes y los sistemas de información, así como para implementar protecciones robustas contra los hackers, virus y otras amenazas en línea.
- Habilidad de liderar y desarrollar proyectos de investigación, realizar el seguimiento y control de los mismos.

5.4.3 Estructura Organizacional de la Seguridad

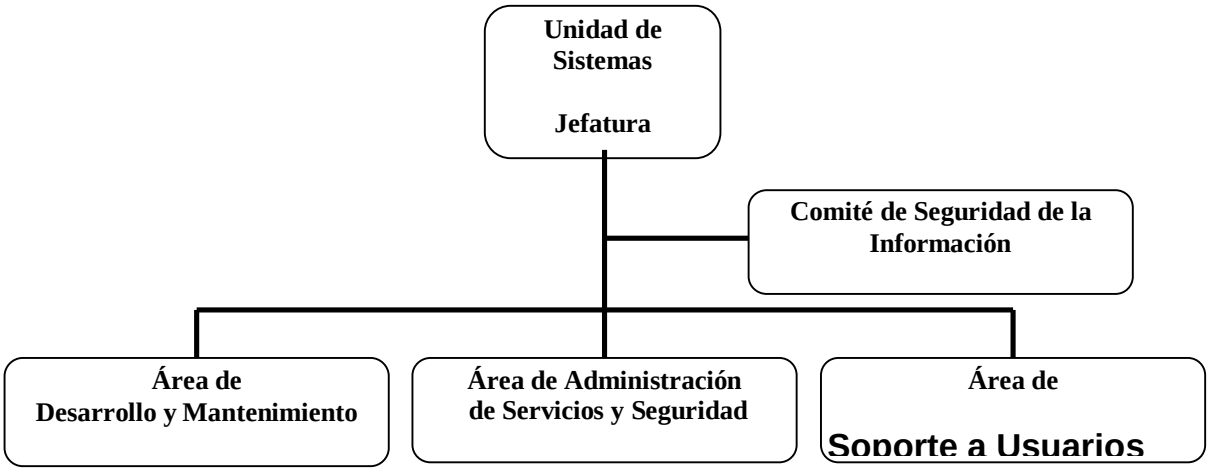
En los capítulos I se analizó el actual panorama de amenazas a los que están expuestos los sistemas de información, amenazas que generan una mayor presión a las áreas de tecnología de las empresas, la cual debe realizar acciones y estrategias para corregirlas y prevenirlas; por esta razón se requiere que dentro de la estructura de Petroindustrial esté definido un equipo de trabajo que continuamente esté analizando, investigando, evaluando, diseñando, implementando y difundiendo, temas de seguridad de información en la empresa; equipo que tenga una visión amplia de la empresa, que conozca el entorno y los elementos sobre los cuales opera la información. Considerando la estructura de Petroindustrial, la misma que está formada por 3 distritos y las oficina Matriz, es necesario que el equipo de trabajo esté compuesto con personal de cada uno de estos puntos. Considero conveniente que se crea un Comité de Seguridad de Información, el que tenga como enfoque primordial la seguridad de la información, que establezca líneas de acción sobre los acontecimientos que pasan y que puedan afectar a los sistemas de información. Este comité deberá tener los siguientes objetivos:

- Gestionar la seguridad de la información en todo Petroindustrial.
- Mantener la seguridad de acceso operacional de la información y de los activos que se relacionan con los sistemas de información.
- Preservar la seguridad de la información con el mundo externo.

Comité de Seguridad de Información dentro de la estructura organizacional debería estar a nivel asesor de la Vicepresidencia de Petroindustrial e inmersa en el campo tecnológico, es decir

bajo la coordinación de la Unidad de Sistemas Matriz de Petroindustrial como muestra el organigrama siguiente:

Propuesta a la Estructura funcional de la



El Comité de Seguridad de Información dentro de la estructura organizacional, debe establecer un marco de trabajo de gestión para iniciar y controlar el proceso de seguridad de la información dentro de la organización; para ello es necesario establecer un foro de gestión de seguridad de la información, foro que se convierta en un ente coordinador de todos los aspectos relativos a la implementación de controles para la seguridad de la información y que:

- Analice los riesgos, prevenga daños o robos de los activos de información y evite la interrupción de las actividades del negocio.
- Establezca procedimientos y responsabilidades para el manejo eficiente y ordenado de incidentes de seguridad.
- Defina y delimite roles y responsabilidades respecto a la seguridad de la información.

- Establezca procedimientos de autorización y adopción de seguridades en el procesamiento de información.
- Promueva la cooperación entre distritos para aplicar políticas de seguridad de información.

Es recomendable que Petroindustrial cree un Comité de Seguridad de la Información que esté bajo la coordinación del Jefe de Sistemas de la Unidad de Sistemas Matriz y que el mismo esté conformado con los Jefes de Sistemas de cada uno de los Distritos de Petroindustrial. La creación de este comité permitiría priorizar actividades de seguridad y viabilizar acciones correctivas y preventivas encaminadas a garantizar la seguridad de la información en todo el sistema Petroindustrial.

5.4.4 Comité de Seguridad de la Información

La necesidad de precautelar la gestión de información para que la misma sea confiable y sirva de base para un buen desenvolvimiento de la empresa, torna imperante definir una arquitectura estratégica de Seguridad de Información, la misma que debe cubrir las expectativas de seguridad de Petroindustrial tanto interna como externa de acuerdo a:

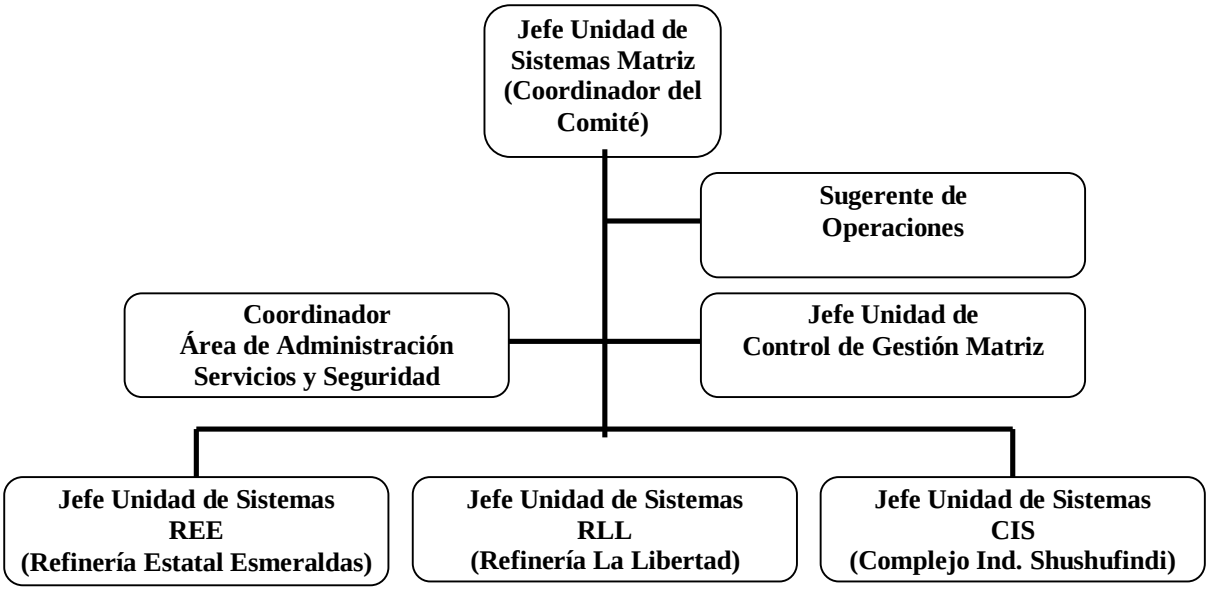
- Las estrategias, políticas y necesidades definidas por la alta dirección de Petroindustrial
- Las políticas y estándares internacionales de Seguridad de Información.

Es por eso que los integrantes del comité deben comprender:

- Jefe de la Unidad de Sistemas, el mismo que actuará como coordinador del comité.

- Subgerente de operaciones, el mismo que permitirá alinear y priorizar los objetivos del comité a los objetivos de Petroindustrial.
- Los jefes de las Unidades de Sistemas de cada Distrito y de la Matriz de Petroindustrial, ya que conocen la realidad de los procesos de información automatizados, su estructuración, así como de las necesidades de cada sitio.
- Jefe de la Unidad de Control de Gestión Matriz, quien conoce y define políticas a los procesos de la organización.
- Coordinador del Área de Servicios y Seguridad, como profesional especialista de seguridad

Propuesta a la Estructura del Comité de Seguridad de la Información



Crear el Comité de Seguridad de la Información, en el cual participe funcionarios de los descritos y en coordinación con el Jefe de la Unidad de Sistemas Matriz permitirá que ellos tengan las siguientes funciones:

- Elaborar el plan de Seguridad tecnológica que se encuentre en línea con las necesidades de Petroindustrial.
- Identificar componentes críticos en la seguridad de la información y sus posibles riesgos, valorar dichos riesgos, e implementar medidas para su prevención.
- Definir proyectos estratégicos que permitan alcanzar óptima y eficazmente los objetivos del Plan de Seguridad Informática, optimizar el manejo de recursos en estos proyectos priorizando el alcance de sus resultados.
- Coordinar el desarrollo de políticas y procedimientos para la definición y administración de Seguridad.
- Gestionar por el cumplimiento de las políticas que emita Riesgo y las recomendaciones que de otras unidades de control de Petroindustrial
- generar políticas para evitar riesgos, a través de lineamientos a ser acatados por todos los funcionarios de Petroindustrial.
- Dar atención a los procesos de la Organización, ayudarlo a su rol e importancia dentro del proceso de Seguridad.
- Monitorear requerimientos de seguridad recibidos y atendidos, analizar la calidad de los resultados.
- Resolver problemas de seguridad o tomar decisiones inmediatas y si es posible estándar para ser implementadas en la oficina Matriz y en todos los distritos, siempre que éstos se encuentren dentro de su ámbito de acción de acuerdo a las políticas y procedimientos institucionales y de Seguridad establecidos.
- Anualmente elaborar y justificar presupuestos de seguridad de acuerdo al plan estratégico definido por el Comité de Seguridad de Información para ser presentado a la Vicepresidencia de Petroindustrial.

- Exigir tanto en la etapa de aprobación de proyectos, como en la recepción de proyectos de automatización, requerimientos y controles de seguridad, los mismos que deben ser acordados y definidos en los contratos formales con terceros.
- Promover la investigación y capacitación permanente del personal informático para robustecer los Sistemas de Información.

Actualmente existe una mayor toma de conciencia sobre los parámetros, estándares y marcos de referencia que se han desarrollado para que las empresas desarrollen programas sólidos de seguridad de la información. La reglamentación más conocida ISO 17799 para la seguridad de los sistemas y redes de información que contienen puntos de referencia de las mejores prácticas para la seguridad, guía que ha sido revisada y aplicada por muchas empresa, por lo que es recomendable que el Comité de Seguridad de la Información aplique esta norma para garantizar la seguridad integral del entorno de Petroindustrial, estas directrices de seguridad representan una base de seguridad para que la empresas desarrollen su políticas de seguridad a su estrategia empresarial, enfocando su trabajo al:

- Descubrimiento, diagnóstico y priorización de medidas de control de vulnerabilidades, estableciendo un método para medir los riesgos de amenazas y ataques internos y externos.
- Mitigación de vulnerabilidades, para lo cual se debe desarrollar procesos y flujo de trabajo para mejora la seguridad integral del entorno y minimizar riesgos.
- Monitoreo eficaz para mantener la seguridad, ya que las amenazas cambian con el tiempo. Se deben monitorear las nuevas vulnerabilidades, las fallas en el cumplimiento de las

políticas de configuración de la seguridad y las fallas en los procesos.

- Análisis de las reglamentaciones, ya que el panorama cambiante de las amenazas no es la única fuerza que está afectando a la seguridad de la información, las regulaciones sobre las que opera Petroindustrial también pueden cambiar y el incumplimiento puede ocasionar sanciones y pérdidas económicas.
- Concienciar la seguridad para facilitar el cumplimiento y la administración de temas de seguridad, administrar mejor las amenazas a la información y sobre todo crear una cultura corporativa en la que los funcionarios participen activamente en la protección de la información contra los ataques, acceso no autorizado y fraude.

5.4.4.1. Coordinador del Comité de Seguridad de Información

Dentro de la propuesta plantead el Coordinador del Comité de Seguridad de la Información debe ser la persona que se relacione directamente con la Vicepresidencia de Petroindustrial del cual recibirá recomendaciones sobre la seguridad en función de la visión de la empresa, además se relacionará con todas las Unidades Operativas para hacer seguimiento, recomendaciones y soluciones en aspectos de seguridad. Este Comité tendría las siguientes funciones:

- Presentar a la Vicepresidencia el plan de Seguridad Informática.
- Liderar y coordinar las reuniones del Comité de Seguridad de Información. Dichas reuniones se recomiendan se realicen trimestralmente, para el análisis de nuevas necesidades, seguimiento y definición de correctivos de seguridad.

- Gestionar y controlar presupuestos de seguridad de acuerdo al plan estratégico definido por el Comité de Seguridad de Información.
- Documentar y mantener actualizadas las estrategias de Seguridad
- Hacer seguimiento a compromisos y proyectos, para garantizar el cumplimiento de acuerdos establecidos.
- Gestionar el cumplimiento y la implementación de políticas y procedimientos de Seguridad.
- Exige Promueve a todos los funcionarios y en especial los profesionales del área de informática, la concienciación de la necesidad de proteger la información, activos importante de Petroindustrial.

5.4.4.2. Coordinador del Área de Servicios y Seguridad

Considerar la inseguridad informática como parte del ejercicio de seguridad informática de Petroindustrial, sugiere la capacidad de la organización para cuestionarse sobre la situación real de la seguridad para evaluar el nivel de dificultad que tendrían los atacantes para ingresar y vulnerar los medios de protección. Mientras más se conoce la inseguridad informática más se comprenden las acciones y resultados de la seguridad. En este sentido, la detección de posibles problemas de seguridad generaría valor, seríamos capaces de reconocer y actuar en situaciones inesperadas, nuestra capacidad de análisis y control aumentaría.

El tema de la seguridad informática es una disciplina del conocimiento, que nos recuerda que existen procesos, muchas veces ocultos a nuestro pensamiento, que pondrán a prueba la realidad de los sistemas y sus propiedades, razón por la cual debe

existir en la empresa un área donde se investigue, desarrolle e implemente mecanismos de seguridad. El coordinador del Área de Servicios y Seguridades dentro del Comité de Seguridad de la Información tiene las siguientes funciones:

- Investigar y ampliar los conocimientos de técnicas utilizadas a nivel mundial que vulneran la confidencialidad, integridad y disponibilidad de los sistemas informáticos.,
- Investigar estrategias necesarias para garantizar la seguridad de los activos informáticos de la empresa
- Asesorar en aspectos de seguridad al Comité de Seguridad de Información.
- Aplicar metodologías actualizadas que conduzcan a la práctica de una cultura de seguridad informática.
- Investigar, diseñar y proponer estrategias de seguridad informática al Comité de Seguridad de Información
- Participar en el desarrollo e implementación del Plan de Seguridad Informática.
- Mantener un adecuado esquema de seguridad en todos los componentes tecnológicos de la organización.
- Desarrollar políticas de prevención contra posibles riesgos que afecten los servicios tecnológicos, y a la integridad y confiabilidad de la información.
- Velar por el cumplimiento de políticas, normas y procedimientos establecidos
- Dar seguimiento a compromisos y proyectos, para garantizar el cumplimiento de acuerdos establecidos en el Comité de Seguridad de la Información.
- Identificar las necesidades de Seguridad sobre herramientas y productos tecnológicos.

- Promover la investigación en temas de seguridad en su área, y difundir a la organización.

5.4.4.3. Subgerente de Operaciones

En el momento económico que estamos viviendo, donde continuamente cambian las reglas del juego, es necesario que la empresa se esfuerce por acercar la tecnología al desarrollo de Petroindustrial. Sin embargo, conseguir asociar estas dos áreas no es una tarea fácil ya que se tienen que producir muchos cambios en ámbitos como la estrategia, la cultura, la organización o la forma de llevar a cabo los procesos.

El alineamiento adecuado entre las estrategias corporativas con las tecnológicas es un factor que, en muchos casos, determina el éxito empresarial. Petroindustrial podría obtener mayor valor de sus inversiones tecnológicas si su planificación tecnológica lo realiza como una parte integrada dentro del desarrollo de la empresa. Por esta razón el contar con el Subgerente de Operaciones de Petroindustrial como parte del Comité de Seguridad de la Información, es vital, ya que con ello se lograría:

- Alinear las estrategias de seguridad con las de la empresa.
- Recomendar proyectos de seguridad de acuerdo a las prioridades de Petroindustrial.
- Identificación de componentes críticos de seguridad para la organización, valoración de su riesgo y canalización de medidas preventivas
- Analizar e Identificar amenazas y vulnerabilidades de Petroindustrial respecto a la seguridad.
- Difundir políticas y fomentar una cultura de seguridad.

- Analizar la seguridad de las conexiones con proveedores o entidades externas a Petroindustrial.

5.4.4.4. Apoyo del Área de Administración de Servicios y Seguridad

La propuesta planteada propone el Área de Administración de Servicios y Seguridad como partícipe ejecutor y controlador de la seguridad de la información de Petroindustrial y que sería responsable de:

- Administrar Usuarios y perfiles de Servicios:
  - Administrar claves de acceso a la red
  - Administrar claves de acceso a software y bases de datos
- Administrar sistemas de control de acceso a las áreas de tecnología
- Validar el uso de estándares de seguridad en aplicativos y certificar
  las aplicaciones que se instalarán en producción
- Monitorear el cumplimiento de normas, políticas internas y procedimientos de seguridad
- Apoyo a las estrategias de seguridad
- Participar en la elaboración plan de contingencia
- Aplicar normativas de seguridad ISO 17799
- Supervisar el buen Funcionamiento de los Servicios de la Red y las aplicaciones instaladas en los servidores.
- Asegurar oportunidad y disponibilidad en el uso de la Red de Petroindustrial.
- Realizar continuas evaluaciones de la carga y el buen Funcionamiento de todos los equipos y elementos de la Red.

- Supervisar la ejecución de servicios por parte de terceros con la finalidad de garantizar los niveles de seguridad.
- Validar que las políticas y procedimientos de Seguridad se encuentren actualizados.
- Administrar las comunicaciones de Petroindustial con los distritos y con Petroecuador.
- Participar y dar soporte de seguridad en los proyectos tecnológicos a implementarse en Petroindustrial.
- Administrar de forma integral todos los componentes de seguridad
- Investigar temas de seguridad para proponer y coordinar la implantación de iniciativas que mejoren la seguridad de la información.
- Velar por el cumplimiento de las normas de seguridad física de la infraestructura tecnológica.
- Responsable de hacer recomendaciones al Comité de Seguridad de la Información, justificar, documentar e impulsar la emisión de políticas cuando se identifique algún riesgo tecnológico.
- Realizar el seguimiento del cumplimiento de las políticas emitidas por el Comité de Seguridad de la Información.
- Evaluar la Seguridad Tecnológica, riesgos de componentes críticos
- Apoyar y llevar a cabo proyectos de Seguridad tecnológica.
- Velar por la seguridad física en el centro de cómputo, para precautelar por integridad y confiabilidad de los datos, respaldos, restauración de servidores.
- Monitoreo del correo electrónico y comunicaciones, monitoreo de sistemas de seguridad: antivirus, firewall, y detección de intrusos.

- Actualizar parches de seguridad , incorporar el software y hardware necesario para protección de los activos informáticos de la organización

5.4.4.5. Esquema de Desarrollo de la Política de Seguridad

En este momento sería inadecuado el planteamiento de políticas detalladas y de alcance organizacional enfocadas a la seguridad de la información fundamentalmente porque:

- Es necesario que la organización primero cree el Comité de Seguridad de la Información, con la autoridad y el alcance necesario para su implementación.
- El comité debe definir dentro de un gran contexto las necesidades, actualmente Petroindustrial tiene muchas falencias dentro de su esquema en el manejo de las seguridades de la información por lo que el comité debe priorizar las urgencias y requerimientos actuales.
- Para que exista el compromiso en la implementación de estas políticas estas deben nacer de los integrantes del comité y estos, con el convencimiento de la necesidad y la bondad de estas políticas liderar su implementación en cada uno de los Distritos su implementación.
- Porque los miembros del comité conocen las debilidades y necesidades institucionales de petroindustrial y las políticas deben ajustarse a estas.

A continuación se proponen una secuencia de acciones que debe seguir para lograr establecer la base de información organizacional para el análisis de riesgos y la elaboración de políticas de seguridad de la información en Petroindustrial:

- *Aprobación y creación del Comité de Seguridad de la Información*, en este punto se debe concienciar a la alta gerencia la necesidad de crear este comité, plantear su organización e incluso puede darse la sugerencia de nuevos miembros, lo importante en este punto es que se considere un grupo viable que permita el alcance de los objetivos establecidos para el comité. Es necesario que se considere varios acercamientos antes de que el Jefe del Área de Sistemas realice la presentación de la propuesta. Este paso debe culminar con la oficialización por parte del Vicepresidente de Petroindustrial de la creación del Comité de Seguridad de la Información
- *Conformación del Comité de Seguridad de la Información,* se organizará una reunión taller con los integrantes del comité la misma que incluya la siguiente agenda de trabajo:
  - Conferencia de las amenazas de la información (se puede tomar como referencia el primer capítulo de este trabajo)
  - Conferencia de la seguridad de la información (se puede tomas como referencia segundo capítulo)
  - Taller para analizar riesgos de la información, identificando los que son prioritarios para el desenvolvimiento de las actividades de Petroindustrial.
  - Explicar hoja de recolección de datos para el análisis de riesgos. La hoja de trabajo propongo contenga:
    - Distrito
    - Año/mes
    - Una matriz que contenga

      Nombre del Sistema o Servicio

      Unidad Responsable

      # Usuarios que utilizan la aplicación (pude ser todos)

Nivel de Importancia de la aplicación o servicio

Muy importante

Importante

Medio

Poco importante

Muy poco importante

Impacto económico a la falta

Ninguno

Bajo

Medio

Alto

Nombre de soporte técnico

Ubicación de la aplicación (equipo)

Custodio de la aplicación

Custodio de los datos

Nivel de seguridad (0 ninguna, 1 baja, 2 media, 3 alta)

Observaciones

- *Levantamiento de información*, los Jefes de las Unidades de Sistemas ejecutarán este levantamiento de información considerando todas las aplicaciones que están bajo su unidad y los servicios que presta la unidad tecnológica como: correo electrónico, mail, etc.

  Es importante mencionar que este levantamiento de información también deben realizarlo los demás miembros del comité, enfocando los servicios y sistemas que no estén bajo el control de la unidad tecnológica y alineando los importantes para poder ejecutar los objetivos de la empresa.

  Con este primer levantamiento de información se obtendrá la base fundamental para analizar riesgos, amenazas y priorizar

acciones encaminadas elevar el nivel de seguridad de la información en Petroindustrial.

- *Consolidación y pre-análisis de la información* una vez realizado el paso anterior y antes de que se reúna nuevamente el Comité, la información levantada será consolidada por el especialista de seguridad de la Unidad de Sistemas Matriz, el mismo que realizará cuatros e informe previo el análisis del comité. Posteriormente se realizará un taller para analizar los riesgos y los impactos para Petroindustrial.

Los pasos que debe seguir el Comité de Seguridad de la Información para desarrollar la política de Petroindustrial tomando en cuenta la información obtenida son:

- *Identifique y evalúe los activos:* Qué activos deben protegerse y cómo protegerlos de forma que permitan la garantizar la integridad, confidencialidad y disponibilidad de la información de Petroindustrial.

- *Identificación de las amenazas:* en este punto el Comité deberá definir: ¿Cuáles son las causas de los potenciales problemas de seguridad?, se considera la posibilidad de violaciones a la seguridad y el impacto que tendrían si ocurrieran. Se identifican dos tipos de amenazas: externas y internas:

  - *Amenazas externas:* Se originan fuera de Petroindustrial, pueden ser: virus, gusanos, caballos de Troya, intentos de ataques de los hackers, retaliaciones de ex-empleados o espionaje.

  - *Amenazas internas:* Son las amenazas que provienen del interior de la empresa y que pueden ser muy costosas

porque el infractor tiene mayor acceso y perspicacia para saber donde reside la información sensible e importante.

- *Evaluación de riesgos:* éste paso es uno de los componentes más desafiantes del desarrollo de una política de seguridad. Debe estimarse la probabilidad de que ocurran ciertos sucesos y determinar cuáles tiene el potencial para causar mayor daño a la organización. El costo puede ser más que monetario, se debe asignar un valor a la pérdida de datos, la privacidad, responsabilidad legal, atención pública indeseada, la pérdida de confianza de inversionistas y los costos asociados con las soluciones por las violaciones a la seguridad. Como resultado de este punto se debe obtener un listado de prioridades sobre las cuales hay que trabajar.

- *Asignación de tiempos y responsabilidades:* se debe identificar claramente las acciones y/o mecanismos a seguir todo esto se hará constar en el acta de reunión de trabajo.

- *Establecer políticas de seguridad:* si es necesario se establecerán políticas que permitan llevar a cabo las estrategias de seguridad definidas.

- *Implementar y difundir políticas en toda la organización:* La política que se escoja debe establecer claramente las responsabilidades en cuanto a la seguridad, difundida adecuadamente y documentada.

5.4.4.6. Políticas Prioritarias Organizacionales

Como se comentó el plantear políticas organizacionales respecto a la seguridad de la información es inadecuado, ya que esto requiere un proceso que no incluye este proyecto. La presente propuesta plantea varias políticas que deberían implementarse de forma urgente en Petroindustrial Matriz, ya que son prioritarias para mantener la seguridad de la información en el sistema Petroindustrial:

- La definición de políticas, estrategias, procedimientos y demás relativos a seguridades de la información deberán ser administradas a través del Comité de Seguridad de la Información.

- El Comité de Seguridad de la Información presentar la planificación anual de las reuniones de trabajo para llevar a cabo la gestión de la seguridad de información de Petroindustrial.

- La investigación, análisis, asesoramiento ejecución de procedimientos y demás relativos a seguridades tecnológicas deberán ser administradas por el área de Administración y Seguridades de la Unidad de Sistemas Matriz..

- Las definiciones políticas y procedimientos dictados por el Comité de Seguridad de la Información son de aplicación obligatoria para el desarrollo de sistemas y para las áreas usuarias de Petroindustrial.

- El Comité de sistemas deberá elaborar un plan estratégico para ir ajustar los esquemas de seguridad tomando en cuenta las normas ISO 17799 la misma que se detalla en el capítulo 2.

- La seguridad de la integridad de la información, por su mismo manejo requiere que los datos y aplicaciones en producción debe ser manejado de forma independiente de la información de pruebas y desarrollo; así mismo la actualización de la data de producción debe ser absoluta responsabilidad del área de Administración de Servicios y Seguridad de la Unidad de Sistemas Matriz.

- Cualquier sistema que se desarrolle en el futuro a través de empresas externas tienen que ajustarse a las políticas de seguridad de la información establecidas en Petroindustrial.

- Se debe estandarizar y documentar las políticas de administración de usuarios.

- La data de las bases de datos solo podrá ser alterada con autorización por la aprobación por escrito del dueño de la data (Jefe del área usuaria) y el Jefe de la Unidad de Sistemas.

- Las diferentes áreas de la Unidad de Sistemas Matriz deberán detallar un registro de eventos que influyen en la seguridad de la información como:

  En el área de Desarrollo y Mantenimiento: se debe registrar las solicitudes de mantenimiento a los programas en producción y nuevos requerimientos que detalle:

  - fecha
  - Unidad
  - Usuario
  - Requerimiento
  - Solución
  - Fecha de atención
  - Observación

En el área de Soporte a Usuarios, debe mantener un registro de eventos de seguridad que detalle:

- fecha
- Unidad
- Usuario
- Evento
- Acción tomada
- Fecha de atención
- Observación

Administración de Servicios y Seguridad

- Bitácora de backup
- Registro de administración de claves (cambios, eliminación, bajas, etc)
- Registro de actividades realizadas en los servidores: aplicación de actualizaciones, implementación de nuevos software, etc.
- Mantener datos estadísticos del rendimiento de las comunicaciones.

5.4.4.7. Sistema de Gestión de los Sistemas de Información

En el mundo informático en general, y en la Seguridad Informática en particular, se han aplicado y desarrollado habitualmente soluciones técnicas y de infraestructura antes que de gestión a los requerimientos organizacionales y que en pocas veces se han involucrados a los usuarios de información. La norma ISO 17799, puntualiza la necesidad de implementar en las empresas un Sistema de Gestión de los Sistemas de Información a través del modelo PHVA (Planificar, Hacer, Verificar, Actuar).

El equipo que forme el Comité de Seguridad de la Información, debe ser el motor de la cultura de la Seguridad tecnológica de Petroindustrial, la misma que debe ser llevada a

cabo a través de la aplicación de un Sistema de Gestión de los Sistemas de Información, que permita una evaluación continua de riesgos y el incremento de los niveles de seguridad, el modelo PHVA, a continuación se describe y enfoca su utilización al Comité de Seguridad de la Información:

Fuente: De La Norma ISO 17799

- *Planificar*, es importante que los funcionarios que gestionen la seguridad de la información en petroindustrial definan y se responsabilicen por su planificación, se cree las políticas y espacios necesarios para mantener esta actividad es base para desarrollar una cultura de seguridad de la información. En la propuesta se ha identificado varios actores de la planificación:

    - Comité de la Seguridad de la Información, es recomendable que cuando se conforme el comité se defina como una política prioritaria el establecer un esquema de reuniones de trabajo anuales, se sugiere que sean trimestralmente para una continua identificación y evaluación de riesgos y la definición de acciones preventivas y correctivas. No es recomendable un tiempo

mayor ya que no se podría llevar a cabo un monitoreo adecuado.

- Jefe de Sistemas como coordinador del comité, será la responsable de impulsar y coordinar la ejecución e la agenda de trabajo y demás detalles orientados a obtener óptimos resultados.

- Área de Administración de Servicios y Seguridad, será el apoyo directo en la ejecución de los proyectos de seguridad de la información de finidos por el Comité, además llevará a cabo un plan de tareas técnicas del área orientadas a investigar, diseñar e implementar controles de seguridad para crear un entorno de seguridad sobre el que opere la información.

- *Hacer*, se centra inicialmente en el desarrollo e implementación de un plan efectivo para mitigar los riesgos y corregir las vulnerabilidades. Durante esta fase. Es necesario que exista canales de información (correo electrónico) y seguimiento de los coordinadores para incrementar la concienciación y conocimiento del personal.

- *Verificar*, tan importante como la planificación es la verificación en seguridad, por lo que es necesario que dentro de la planificación se considere siempre la verificación de controles por cada uno de los gestores de la seguridad de la información.

- *Actuar*, es necesario que cuando se identifique un incidente que se relacione con la seguridad de la información, y que amerite ser definido acciones por el Comité, exista la posibilidad de realizar reuniones de trabajo extraordinarias, que permitan realizar correctivos inmediatos.

5.5. PROPUESTA TECNICA

A menudo, la seguridad es un componente que no es excesivamente vigilado cuando se diseña una red. Un plan serio debe dedicarse a proteger y asegurar los datos valiosos y la propiedad intelectual. La mayoría de las pérdidas ocurren debido a una falta de seguridad.

Cada vez más, las principales publicaciones de noticias están subrayando las intrusiones en la seguridad de red. Esto se debe a dos importantes razones. Primera, las personas y los grupos que asaltan los sistemas de seguridad de red corporativos revelan sus intrusiones en foros públicos, además, a medida que las empresas dependen cada vez más de sus conexiones de acceso público para la continuidad de sus operaciones, las irrupciones en estos entornos implican daños económicos y sociales de consideraciones importantes.

La seguridad tiene que incluirse en el diseño de la red, más aún si se dispone de acceso a Internet. En los últimos tiempos no se ha hecho suficiente hincapié en la seguridad durante la fase de diseño de las redes, pese a que se pueden obtener grados de seguridad más altos implantando las seguridades desde el principio.

La propuesta técnica que se detalla a continuación considera políticas prioritarias tecnológicas, necesarias que debe adoptar la Unidad de Sistemas para garantizar la seguridad de la información que es manejada bajo la tecnología a su cargo, se define el diseño que necesita Petroindustrial Matriz implementar para mantener un nivel de seguridad en el perímetro de su Red.

5.5.1. Políticas Prioritarias Tecnológicas

La identificación de los datos sensibles y/o críticos es vital para una organización, de ello depende el normal funcionamiento de la operatividad de empresa. El avance que ha tenido Petroindustrial en el área tecnológica, en la actualidad le permite que un porcentaje alto de la información se almacene y manejen a través de los sistemas y herramientas informáticas. El área de Administración de Servicios y Seguridad planteada en la presente propuesta tendría la responsabilidad de la operatividad de todos los elementos físicos, de software y de procedimiento, necesarios para garantizar la:

- Confidencialidad, protección contra la divulgación no autorizada. Por ejemplo información de sueldos del personal o información definida como confidencial.

- Integridad. Establecer controles que eviten modificaciones no autorizadas, imprevistas o accidentales.

- Disponibilidad, implementar mecanismos para que los servicios estén siempre disponibles.

Para garantizar las características mencionadas de la información es necesario que la Unidad de Sistemas adopte las siguientes políticas enfocadas a la tecnología que maneja:

- *Aseguramiento de Componentes de Datos*, buscar garantizar a través de mecanismos adecuados la información del sistema de información esté siempre disponible (disponibilidad), que se mantenga íntegra (integridad), y que solo se permita el acceso a personas autorizadas (confidencialidad).
- *Aseguramiento de Componentes de Software*, buscar optimizar los sistemas operativos y las aplicaciones que trabajan en el

sistema de información, de manera que sean configurados de manera segura y solo permitan su utilización dentro de parámetros preestablecidos y aceptados, que funcionen de manera continua y estable (disponibilidad), que ofrezcan un servicio con un nivel de calidad aceptable, que no permitan su utilización por personas no autorizadas, y que permitan establecer las responsabilidad de uso.

- *Aseguramiento de Componentes de Hardware*, buscar optimizar los componentes de hardware de los sistemas de información (equipos de cómputo, periféricos, medios de almacenamiento removibles, etc.), de manera que sean configurados de manera segura y solo permitan su utilización dentro de parámetros de funcionamiento predefinidos, que funcionen de manera continua y estable, que ofrezcan un servicio con un nivel de calidad aceptable, que no permitan su utilización por personas no autorizadas.
- *Aseguramiento de Componentes de Interconectividad*, buscar optimizar el componente de comunicaciones del sistema de información (cableado, dispositivos de interconexión ï hubs, switches, routers, etc.-, antenas, etc.), de manera que los canales funcionen de manera continua y estable se pueda establecer la identidad de los participantes, los datos transmitidos puedan ser accesados únicamente por personas autorizadas, los datos no puedan ser modificados durante su transmisión y se pueda establecer el origen de toda comunicación.
- *Aseguramiento de Infraestructura Física*, buscar optimizar el entorno físico de las instalaciones, en las cuales opera el sistema de información de Petroindustrial, de manera que estas provean niveles de seguridad adecuados.

- *Utilización de Estándares*, es importante que los encargados de la seguridad se familiaricen con los estándares recomendados para la seguridad y los cuales pueden ser adoptados como:
  - Análisis de riesgos ISO/IEC 17799, NIST SP 800-30, NIST SP 800-6
  - Análisis de requerimientos y establecimiento de políticas de seguridad informática ISO/IEC 17799, CSC-STD-001-83, ISO 15408, NIST SP 800-55, NIST SP 800-42, NIST SP 800-26, NIST SP 800-18, NIST SP 800-16
  - Aseguramiento de Componentes de Datos ISO/IEC 17799, IEEE P1363, NIST SP 800-36, NIST SP 800-21, NIST SP 800-14, NIST SP 800-12
  - Aseguramiento de Componentes de Software ISO/IEC 17799, NIST FIPS 73, NIST SP 800-44, NIST SP 800-41, NIST SP 800-36, NIST SP 800-14, NIST SP 800-5
  - Aseguramiento de Componentes de Hardware ISO/IEC 17799, NSA/CSS Manual 130-2, NACSIM 5000, NIST SP 800-36, NIST SP 800-14
  - Aseguramiento de Componente Humano ISO/IEC 17799, NSA Security Guidelines Handbook, NIST SP 800-50, NIST SP 800-36, NIST SP 800-16, NIST SP 800-14, NSTISSI 4011, NSTISSD 500, NSTISSI 4013, NSTISSI 4014, NSTISSI 4015, CSC-STD-002-85
  - Aseguramiento de Componentes de Interconectividad ISO/IEC 17799, IEEE P1363, NIST SP 800-45, NIST SP 800-47, NIST SP 800-41, NIST SP 800-36, NIST SP 800-25, NIST SP 800-21, NIST SP 800-14, NIST SP 800- 13
  - Aseguramiento de Infraestructura Física ISO/IEC 17799, DoD 5220.22-M, NSA Security Guidelines Handbook,

NSTISSI 7000, NIST SP 800-36, NIST SP 800-14, NIST SP 800-12

- Administración de la seguridad informática ISO/IEC 17799, ISO/IEC DTR 13335, ISO/IEC DIS 14980, NIST SP 800-64, NIST SP 800-61, NIST SP 800-50, NIST SP 800-55, NIST SP 800-42, NIST SP 800- 40, NIST SP 800-36, NIST SP 800-35, NIST SP 800-34, NIST SP 800-18, NIST SP 800-16, NIST SP 800-6, NIST SP 800-5

Todos los estándares se pueden obtener de manera gratuita de sitios Web en la Internet, excepto los estándares de la ISO/IEC que sólo pueden ser bajados al comprarlos en el sitio Web de la ISO.

- *Cultura Investigativa*, el proceso de diseñar un sistema de seguridad muchas veces encamina a cerrar las posibles vías de ataque, lo cual hace imprescindible un profundo conocimiento acerca de las debilidades que los atacantes aprovechan, y del modo en que lo hacen. Para que Petroindustrial, y particularmente la Unidad de Sistemas ejecute unana gestión eficaz de la seguridad de la información requiere de mucha investigación, por lo que se debe establecer como política que a través del coordinador del área de Administración y Seguridad investigue y difunda semanalmente temas de tecnología que son necesarios se conozcan la información respecto a las últimas vulnerabilidades de los sistemas y los mecanismos para protegerse o corregirlo.

5.5.2. Identificación de Componentes Críticos

La información es un activo intangible y de mucho valor para la organización, razón por lo la cual es necesario identificar todos los elementos tecnológicos críticos que posee Petroindustrial Matriz y sobre los cuales la Unidad de Sistemas debe tomar en cuenta para desarrollar medidas de seguridad:

Seguridad de la red de datos interna:

- Elementos de cómputo:
  - Red Servidores de Usuarios y Dominios
  - Servidores Bases de Datos
  - Servidores Correo Electrónico
  - Servidores de Aplicaciones
  - Servidores de Impresión
  - Servidores de otros servicios (DNS, FTP..)
  - UPS
- Red de Datos:
  - Protocolos
  - Red de Datos física
  - Dispositivos Ruteadores / Switches (Enlaces WAN , LAN)
  - Topologías: Internet y WAN
  - Estaciones de trabajo (pc´s, notebooks)
- Aplicaciones y Servicios
  - Distribuidas
  - Centralizadas
- Datos
  - Almacenamiento
  - Recuperación
- Procedimientos
  - Instalación
  - Operación
  - Administración
  - Recuperación

Seguridad de la red de datos externa:

- Proceso de identificación de vulnerabilidades
- Ingenieria Social.
- Pruebas de passwords.
- Detección de conexiones externas.
- Obtención de rangos de direcciones en Internet.
- Detección de protocolos.

- Scanning de puertos TCP, UDP.
- Intentos de acceso vía Internet.
- Análisis de la seguridad de las conexiones con proveedores o entidades externas a la Organización.
- Ataques de denegación de servicio.

Seguridades en el Área de Sistemas:

- Seguridad física en el centro de cómputo
- Integridad y confiabilidad de los datos, respaldos, restauración.
- Cumplimiento de normas en el manejo de programas
- Revisión del esquema de seguridades en nuevas aplicaciones.
- Monitoreo y seguimiento permanente del cumplimiento de las normas, políticas y procedimientos de seguridad.
- Monitoreo del correo electrónico y comunicaciones.
- Monitoreo de sistemas de seguridad: antivirus, y detección de intrusos.
- Incorporar el software y hardware necesario para protección de activos informáticos de la organización
- Nivel de seguridad establecido en los equipos críticos
- Cumplimiento de las políticas emitidas
- Generación de métricas y reportes.

5.5.3. Seguridad Perimetral

La red de Petroindustrial desde el punto de vista de la empresa, cumple varios objetivos que son necesarios identificarlos para evaluar el nivel de seguridad apropiada que requiere se implemente en la empresa. Se ha identificado los siguientes objetivos que persigue la empresa con la red de Petroindustrial:

- Mejorar la eficacia de la empresa reduciendo los costos asociados a la administración y operación de la refinación de petróleo que realiza Petroindustrial.
- Apoyo para mejorar la agilidad y reducción de costos en los procesos de comunicación y coordinación entre los Distritos y

Matriz, existe un nivel alto de comunicación a través de correo electrónico.

- Apoyo para mejorar la agilidad y reducción de costos en los procesos de comunicación con proveedores y publicación de ofertas, las mismas que se realizan a través de correo electrónico y publicación en página web de Petrocomercial.
- Permitir a los funcionarios tener acceso a datos y servicios internos asegura dos (correo electrónico, servicios de impresión, aplicaciones desarrolladas para trabajar en red)
- Proporcionar a sus funcionarios acceso a Internet y a la red de los Distritos de Petroindustrial como herramienta que permitan acelerar y controlar la ejecución de trabajos.
- Petroindustrial, no Proporcionar acceso público a la información relacionada con la empresa, se realiza a través del servidor Web de Petroecuador, pero se quiere a futuro que Petroindustrial disponga de su propio servidor Web.

El servicio de correo electrónico e internet por las actividades de operación que mantiene la empresa principalmente en los distrito donde existen turnos de trabajos, se requiere que el servicio esté activo 24 horas al día, 7 días a la semana. Por lo que el perímetro de la red de Petroindustrial requiere de un esquema de seguridad.

Es necesario centrarnos en el perímetro de la red para diseñar un acceso seguro a la intranet o entre dominios de intranet. Todos los servidores, independientemente de su propósito, necesitan seguridad local y la construcción de la topología proporcionan los fundamentos necesarios para diseñar una seguridad. El firewall se considera un componente esencial para cumplir los requisitos de acceso seguro a la red dentro del diseño.

El implementar un firewall en el perímetro de la red de Petroindustrial permitiría implementar medidas fundamentales en el perímetro de la Red de Petroindustrial Matriz como:

- *Reducción y control servicios TCP/IP*

  Habitualmente los sistemas Operativos vienen configurados de fábrica con una serie de servicios TCP/IP activados, que en la gran mayoría de los casos nunca se utilizan, o en otros casos, pueden servir como puerta de acceso relativamente fácil a posibles intrusos.

- *Monitorización de tráfico sospechoso*

  Permite tener una idea bastante aproximada del nivel de carga de la red en los distintos periodos del día. Esta monitorización del tráfico permite detectar tanto averías en el caso de ausencia de tráfico, como actividades sospechosas.

- *Escaneos periódicos del perímetro*

  Detecta programas denominados *escaneadores que* se dedican metódicamente a probar uno por uno todos estos sistemas, intentando penetrarlos

- *Permite implementar políticas de acceso*

  Una de las tareas importantes que realizan el *firewall*, es permitir o denegar determinados servicios en función de los distintos usuarios y su ubicación como:

  - Usuarios internos con permiso de salida para servicios restringidos como FTP y Telnet.
  - usuarios internos con permiso de salida para servicios no restringidos como el Correo electrónico.

- Usuarios externos con permiso de entrada desde el exterior, este caso es menos habitual y además es más sensible a la hora de vigilarse. Suele tratarse cuando se requiere acceder a consultar el correo electrónico. También se ha dado en Petroindustrial cuando por parte de terceras empresas para dar servicios de tele-mantenimiento a software.
- Es de dominio público que Internet no es un canal seguro, se torna en un problema más sensible cuando la información a transmitir se trata de nombres de usuarios y sus passwords correspondientes, esto porque en Petroindustrial se puede consultar el correo electrónico de los usuarios desde el internet.

˘ *Política de gestión de Bases de Datos públicas*

Permitiría crear el ambiente para desarrollar unos de los requerimientos de Petroindustrial, publicar cierta información de operación de la Refinería tanto para uso de los ciudadanos como de los funcionarios de la empresa.

El diseño de firewall se centra en el perímetro de la red para proporcionar un acceso seguro a la intranet. Al implementar la seguridad en los perímetros de red, si no se realiza adecuadamente, la arquitectura y las directivas que se aplican a cada dispositivo pueden tener un efecto negativo, ya que el rendimiento es un delicado equilibrio entre suficiente seguridad y firewall, y el acceso a los datos, cuantas más capas de seguridad se apliquen, más lento será el rendimiento, ya que cuanto más largo sea el listado de filtros, más tiempo se necesitará para examinar cada paquete. El rendimiento variará en función del número de filtros que se utilicen, hasta qué capa del paquete sea necesario examinar.

5.3.3.4. Plataforma de Firewall

Existen diferentes plataformas de firewalls en el mercado, esta propuesta Plantea que petroindustrial adquiera un **equipo firewall** por las siguientes razones:

- En un entorno corporativo como es el caso de Petroindustrial, existen cientos muchas máquinas que necesitan protección en una red, el **firewall basado en host** no proporciona una administración centralizada y no ofrece escalabilidad. Las empresas están estandarizando e implementando firewall basados en host para que los usuarios finales los utilicen en la red de su casa.
- Un **Firewall de red basados en host,** es un método de implantación del software de firewall sobre un sistema operativo. Petroindustrial tiene sus red bajo un Windows 2000 Server, Microsoft también dispone de un software firewall ISA Microsoft Internet Security, debido a que Windows se ha caracterizado por tener muchos vacíos, de ahí su requerimiento de que tenga continuos upgrade, y por ser aplicaciones más comerciales son más propensos a tener una mayor vulnerabilidad. Por otro lado la puesta planteada plantea un equipo con una solución integrada y con funciones que no dispone los firewall de red basados en hos. Y Adicionalmente si es al comparar con el equipo firewall requiere de menos soporte técnico punto importante que hay que tomar en cuenta debido a la carga de trabajo de la Unidad de Sistemas.
- **Firewall basados en enrutadores,** normalmente los enrutadores se utilizan como la primera capa de protección en una arquitectura de seguridad general y, a veces, se utilizan en lugar de un firewall, especialmente en las redes pequeñas. Esto sólo se debe a motivos económicos, lo que implica que no cumple con el nivel de seguridad que requiere Petroindustrial.

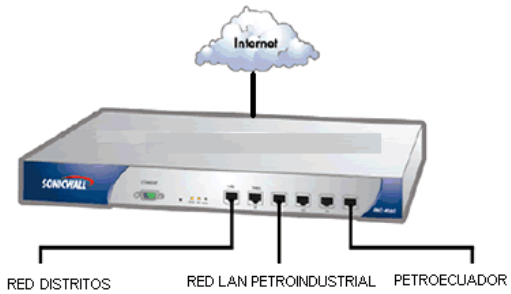
Firewalls, Servidores VPN e IDSs utilizados independientemente fallan, por lo que las empresas se veían en la necesidad de incorporar otros elementos como: antivirus de pasarela, filtros antispam, IDS, etc. Razón por la cual los proveedores de equipos de seguridad han sacado al mercado equipo más poderoso y multifuncionales, que permiten dar mayor seguridad a las redes como por ejemplo FORTINET 1000 que se especifica en el capítulo 3.

5.3.3.5. Diseño

En el diseño de firewall que se especifica gráficamente en la página siguiente se establece diferentes niveles de seguridad y acceso. En la zona desmilitarizada (DMZ, Demilitarized Zone) que permite el tráfico de Internet dentro o fuera de la intranet mientras se mantiene la seguridad de la intranet, mejoran la seguridad evitando que la intranet esté expuesta a Internet.

En el gráfico de red de Petroindustrial incluye un equipos de gestión integrada de seguridad del que están interconectando 3 segmentos:

- Red de Petroecuador
- Red de Distritos
- Red LAN de Petroindustrial



Esta configuración permitiría filtrar toda la información que viene de cada uno de los distrito y del Sistema Petroecuador, así reducirías los peligros del mundo respecto a la red LAN de Petroindustrial.

Es recomendable que una segunda etapa para aprovechar los puertos que tenga el equipo se utilice otro segmento únicamente para los servidores con esto cualquier información que esté en el tráfico de la red LAN también estaría siendo monitoriada.

La red LAN de Petroindustrial está configurada con redes virtuales VLAN, que permite mejorar la seguridad proporcionando un mecanismo para el filtrado del tráfico de red entre segmentos. Desde la perspectiva de la seguridad, mediante VLAN, un grupo de servidores que necesitan acceso externo a una Intranet pueden pertenecer a la misma VLAN y enrutarse a un firewall específico sin estar físicamente conectados al firewall. El firewall puede participar en varias VLAN, y sólo las VLAN que necesitan características de firewall estarán dirigidas hacia el servicio de firewall. Los servidores que no necesiten acceso externo podrán excluirse de las VLAN de acceso externo.

Utilizando VLAN para agrupar servidores y firewall, se puede controlar mejor los servidores que tienen acceso a firewall específicos, Para que un puerto pueda tener acceso a una VLAN, un administrador debe iniciar la sesión en el conmutador con privilegios administrativos, activar el puerto y, a continuación, agregar el puerto a la VLAN apropiada.

5.3.3.6. Características del Equipo de Gestión Integrada de Seguridad.

El equipo que debe implementar Petroindustrial para asegura la red debe ofrecer simultáneamente todos los servicios que están ofreciendo los equipos de gestión integrada, los mismos que ofrecen varios servicios, o que permitir configurar alguna combinaciones; dado que el equipo a adquirir será usado como una

plataforma de seguridad de defensa en profundidad contra ataques el equipo debe incluir:

- Firewall con filtrado de contenido utilizando DPI Deep Packet Inspec , filtrado de contenido, procesamiento de contenido de red a velocidad gigabit.
- Firewalls Antivirus
- Anti Spam
- Router
- VPN (Virtual Private Netware)
- DHCP
- IPS
- WEB FILTER
- Gestión centralizada de dispositivos
- Gestión centralizada de logs y reportes.
- Software cliente VPN IPsec, firewall de PC, antivirus e IPS de puesto de trabajo.
- Software y equipo debe contar con certificaciones en: Firewall, Antivirus, IPsec VPN.
- Consola de administración que permite visualizar registros, alertas e informes centralizados y escalables, incluyendo la generación de informes estándar y personalizados.
- Consola de administración que permita configuración de políticas en múltiples monitoreos, prevención y detección de intrusos.
- Disponibilidad de portal de información actualizado ñal minutoò que proporciona todos los datos sobre nuevos virus y vulnerabilidades.
- Disponibilidad a través de Internet de expertos en seguridad dedicados a la investigación de nuevas amenazas y el

desarrollo de firmas que permitan a los dispositivos actualizarse para que detecten y prevengan nuevos ataques.

- Disponga una red de servidores de distribución de alta disponibilidad, que proporcionan actualizaciones automáticas e inmediatas a los firewall antivirus.

- Alta disponibilidad y balanceo de carga para alcanzar un tiempo de actividad máximo.
- Permita el manejo de las aplicaciones en tiempo real como voz sobre IP, descargas de aplicaciones web, que requieren un procesamiento totalmente seguro en tiempo real.
- Incluya Switch de 6 puertos para lograr mayor flexibilidad en el diseño de topologías En el diseño que se presenta en el siguiente punto están considerados 3 segmentos de Red, en el mercado hay de 3, 6, y 12; y no se debe adquirir con 3 ya que se podría abrir un segmento adicional a futuro. Incluyendo puertos en Gigabit Ethernet.

En el mercado existe algunas marcar de equipos que cumplen estas características, en el capítulo 3 se detalla algunos de estos. Es importante mencionar que Petroecuador tiene instalado desde aproximadamente 2 años FORTINET 1000, el cual ha dado buenos resultados.

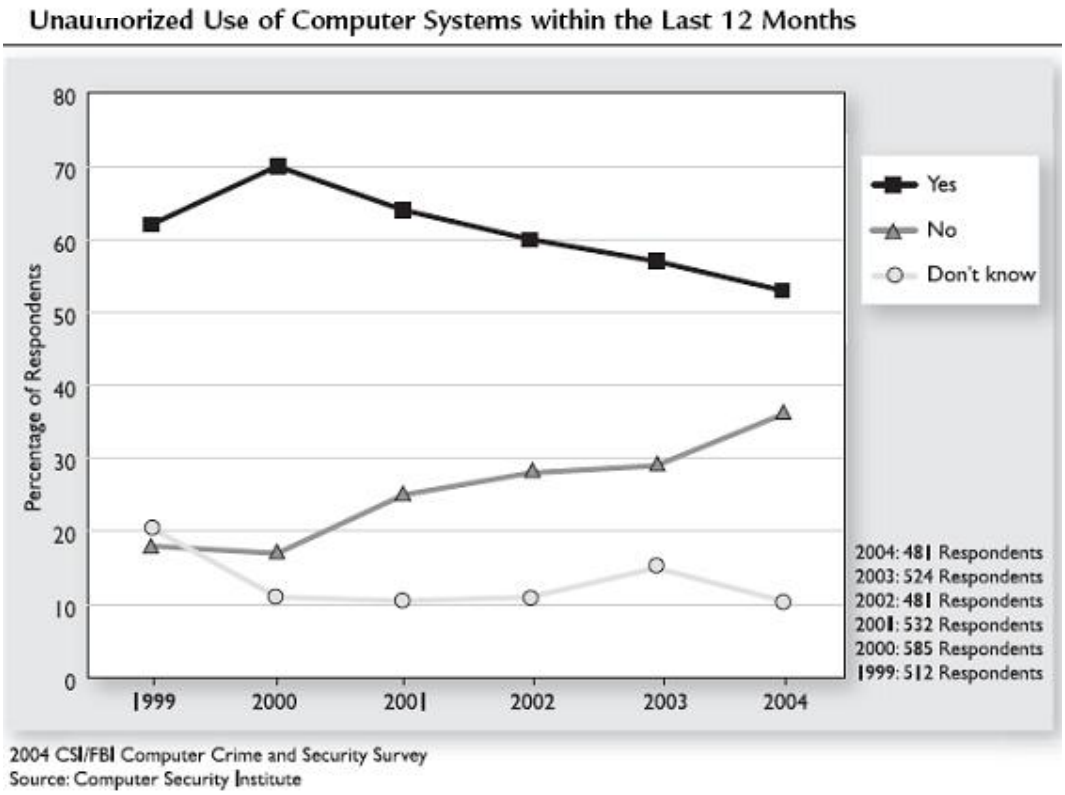
5.6. EVALUACION DE RIESGO Y JUSTIFICACIÓN DEL DESARROLLO DE LA PROPUESTA

Como se ha detallado en este trabajo, Petroindustrial a través de su red tecnológica se expone a eventos internos y externos que pueden afectar la información que fluye dentro de estos recursos tecnológicos, debido principalmente a la carencia de una estructura formal que administre los riesgos existentes en base a la realidad

institucional, no se cuenta con información o registros de eventos que permita sustentar y evaluar dichos riesgos.

El Ecuador no cuenta con estadísticas que permita medir el costo que significa para el país la vulneración de las seguridades, pérdidas de información, robos, sabotajes y tiempo perdido para las organizaciones, tampoco Petroindustrial como ente gubernamental autónomo, cuenta con mediciones que permitan evaluar estos costos, por lo que se ha tomado como referencia la última información disponible del CSI Instituto de Seguridad de la Información, ente gubernamental de los Estados Unidos en su informe 2004 CSI/FBI Computer crime an security survey, de donde se ha extractado importante información con la finalidad de dimensionar los riesgos a los que está expuesta la red de Petroindustrial, pues nuestra realidad tecnológica, dadas las condiciones actuales, no puede calificarse diferente respecto a la accesibilidad y vulnerabilidad, pero si definitivamente menos protegida.

Un primer análisis nos aproxima a la alarmante realidad de los accesos no autorizados, de 481 empresas norteamericanas encuestadas, un 52% reporta haber identificado accesos no autorizados en el último año, mientras un 10% confiesa no conocer si fue víctima de estos eventos indeseables.



Es importante tomar en cuenta que el gráfico muestra una tendencia a la baja en cuanto a intentos de ataque, pero esto se debe a que cada vez más las empresas están implementando tecnología de seguridad. Para el caso de Petroindustrial considerando que es una empresa del estado que tiene información clave de una de las actividades productivas del país, que actualmente constituye sobre la cual existen muchos intereses económicos y políticos; la probabilidad que tenga ataque es igual de alta comparado con los datos estadísticos planteados.

El cuadro siguiente analiza si los accesos no autorizados fueron generados desde dentro de la organización o desde fuera de ella, existe un porcentaje alto en el desconocimiento de dichos ataques. El que no existan herramientas que no detectan intrusos

no asevera que no exista peligro de los mismos, de igual forma para Petroindustrial, la no existencia de registro de eventos de accesos indebidos, no es una razón para que la empresa esté fuera de estos datos estadísticos.

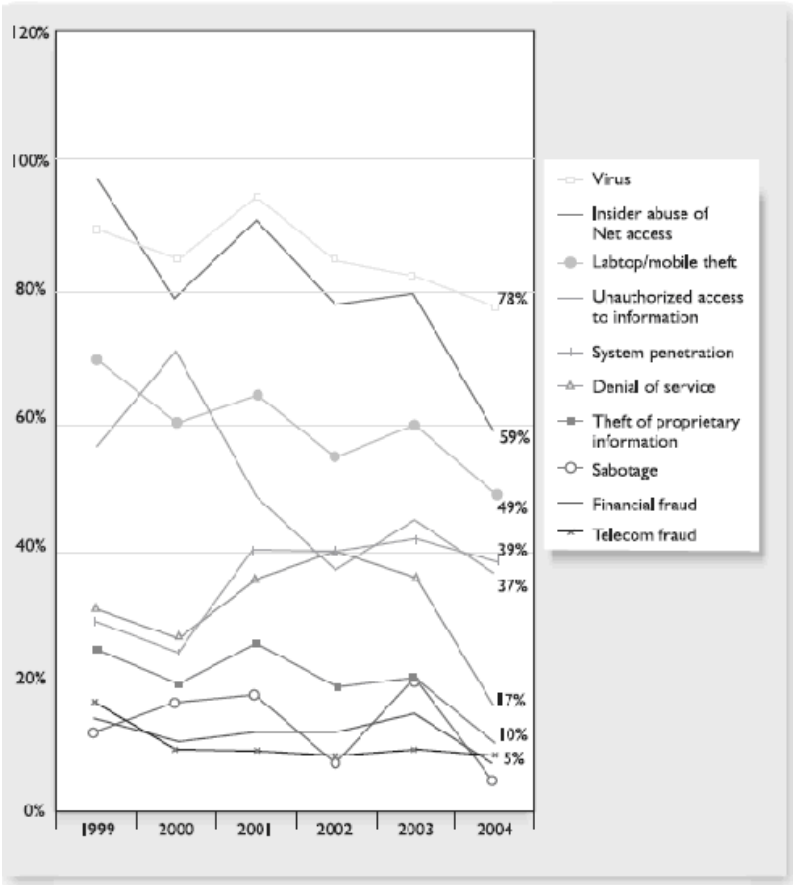
How Many Incidents? From Outside? From Inside?

How Many Incidents? by percentage	1 – 5	6 – 10	>10	Don't Know
2004	47%	20%	12%	22%
2003	38%	20%	16%	26%
2002	42%	20%	15%	23%
2001	33%	24%	11%	31%
2000	33%	23%	13%	31%
1999	34%	22%	14%	29%
How Many Incidents From the Outside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	9%	9%	30%
2003	46%	10%	13%	31%
2002	49%	14%	9%	27%
2001	41%	14%	7%	39%
2000	39%	11%	8%	42%
1999	43%	8%	9%	39%
How Many Incidents From the Inside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

Las estadísticas muestran un balance entre los accesos no autorizados generados desde dentro de la institución y los de fuera de ella. Para nuestro caso asumimos que la realidad será similar, más aún si se considera que la inestabilidad política y las implicaciones legales de los actos de las ñcuotas políticasò de Petroindustrial, podrían buscar sustento en la manipulación de información propia de la institución.

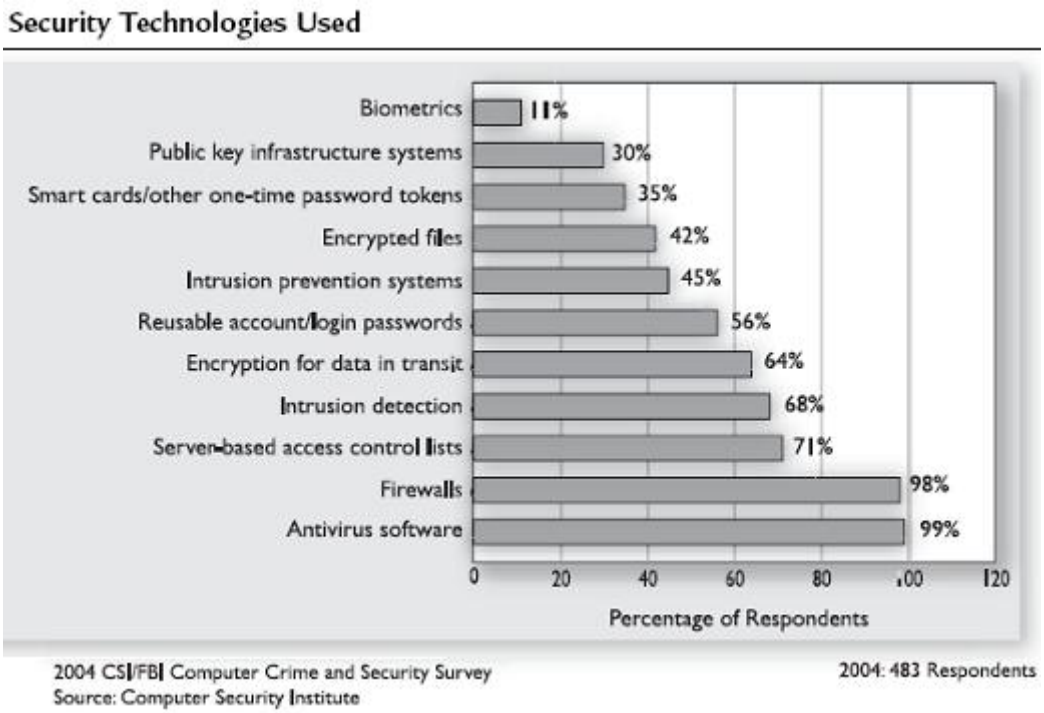
Los virus informáticos siguen estando a la cabeza como los principales problemas a enfrentar dentro de los esquemas de seguridad de las organizaciones, pero es muy importante notar que el abuso del personal interno de los accesos de la red, está en un segundo lugar y con seguridad, debido a los efectos de mal uso de Internet por estos, es la causa de la infección por virus. Escalofriantes montos de pérdidas por diferentes tipos de ataque se producen continuamente en el mundo. En el país los montos proporcionales deben mantenerse aunque no tenemos herramientas para calcularlos sabemos que son muy importantes y justifican plenamente la estructuración de esquemas de seguridad, acordes a nuestra realidad, que minimicen su impacto.

Types of Attacks or Misuse Detected in the Last 12 Months
(by percent)



2004 CSI/FBI Computer Crime and Security Survey 2004: 481 Respondents
Source: Computer Security Institute

Un interesante aporte adicional del CSI muestra en el cuadro siguiente que los sistemas de protección más usados son los equipos de seguridad como firewall e IDS; información que permite una orientación de por donde se debe priorizar los esfuerzos institucionales.



Un complemento importante es identificar las percepciones que los expertos tienen respecto a la eficiencia de los controles, ubicando como un factor importante a las políticas de seguridad.

Los elementos analizados nos dan una perspectiva del problema implícito en las seguridades, nuestra evaluación para Petroindustrial tiene que realizarse más en términos cualitativos pues carecemos de la información adecuada para cuantificar el impacto efectivo.

Para tener elementos de evaluación respecto a la seguridad de la información que se maneja en Petroindustrial y en particular en la Unidad de Sistemas, desde el punto de vista de la percepción que tienen las personas técnicas de acuerdo a su experiencia y labor que realizan se realizó una encuesta. Para ello se ha diseñado la matriz adjunta en los anexos, la misma que permitió evaluar la percepción del riesgo al que está expuesto Petroindustrial y la percepción de la efectividad de las seguridades implementadas. Los resultado que se presentan gráficamente a continuación reflejan las percepciones respecto de las vulnerabilidades de Petroindustrial en relación a Seguridades informáticas, situación que tiene un nivel que amerita y justifica llevar a cabo proyectos que permitan mejorar los niveles de seguridad de Petroindustrial Matriz.

5.7. CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES:

1. El esquema de seguridad de información que emplea Petroindustrial actualmente es débil, lo que pone en riesgo la confidencialidad, oportunidad y disponibilidad de la información en la empresa.
2. Petroindustrial no dispone de una estructura administrativa que soporte o tenga por funciones específicas el manejo de la seguridad de la información, lo que ocasiona la dilución de las responsabilidades parciales y un debilitamiento de los controles necesarios para mantener un buen nivel de seguridad de la información.
3. No existe una clara identificación de los responsables de las seguridades informáticas dentro de la Unidad de Sistemas Matriz de Petroindustrial, afectando a la planificación de seguridad en la empresa, por las falencias que esto ocasiona en la asignación de responsabilidades.
4. No existe el seguimiento de eventos que implican problemas de seguridad en Petroindustrial, por lo que estos se vuelven recurrentes y no logran soluciones eficientes.
5. No existe a nivel de usuarios la percepción de riesgos que implica la ausencia de un esquema fuerte de seguridad de la información de Petroindustrial, lo que deriva en una sintomatología de una falta de cultura de seguridad.
6. No existe disponibilidad de herramientas tecnológicas que permitan medir cuantitativamente la realidad de los ataques

que sufre la red de Petroindustrial, por lo cual medir la cuantificación monetaria y sus implicaciones no es factible en Petroindustrial.

7. Los especialistas del área informática evalúan el nivel de riesgo en seguridad de la información de la empresa en grado crítico, lo que afecta a la imagen y servicio profesional de la Unidad de Sistemas.
8. No existe un esquema procedimental claro para el manejo de la seguridad de la información en la Unidad de Sistemas Matriz, lo que genera un entorno vulnerable en el manejo de la información.
9. Petroindustrial no dispone de una herramienta tecnológica que le permita protegerse en el perímetro de la red de Petroindustrial Matriz, lo que no facilita la identificación de intrusos y monitoreo de spams y configuración de acceso s permitidos.

RECOMENDACIONES:

Las conclusiones mencionadas evidencian importantes debilidades en el esquema de seguridad de la información de Petroindustrial, es urgente realizar acciones preventivas y correctivas que ayuden a mitigar los efectos perniciosos que pueden derivarse de estas debilidades, para ello se recomienda atacar dos frentes simultáneamente: el frente administrativo-organizativo y el frente tecnológico

Las recomendaciones se enfocan a dos tipos de acciones, las urgentes y las necesarias. Dentro del esquema de las **urgentes** se detallarán acciones que deben implementarse inmediatamente para asegurar un mínimo necesario de seguridad. Las

recomendaciones **necesarias** son las recomendaciones que por su naturaleza o gestión, deberán implementarse en una segunda fase no menos urgente bajo la gestión del Comité de Seguridad de Información de Petroindustrial.

Recomendaciones Urgentes.-

1. Que la Vicepresidencia de Petroindustrial debe crear en su estructura organizacional un Comité de Seguridad de la Información, conformado:
    a. Con cada uno de los responsables de las Unidades de Sistemas de los Distritos,
    b. Jefe de la Unidad de Sistemas Matriz,
    c. Coordinador del Área de Administración de Servicios y Seguridad,
    d. El Jefe Control de Gestión, y
    e. El Subgerente de Operaciones.

    Esta creación deberá realizarse de manera urgente a fin de que, Petroindustrial cuente con una estructura que le permita continuamente medir los riesgos internos y externos respecto a la seguridad de la información y el desarrollo de medidas correctivas y preventivas que permitan elevar el nivel de seguridad de la empresa.
2. Que la Vicepresidencia de Petroindustrial debe disponer que el coordinador del Comité de Seguridad de la Información sea el Jefe de la Unidad de Sistemas Matriz en el momento que se cree el Comité de Seguridad de la Información, a fin de garantizar la coordinación adecuada y desarrollo de proyectos de seguridad de la información, ya que en la propuesta contempla una reestructuración de esta Unidad con un enfoque de apoyo a la seguridad de la información y

directamente al Comité. Con lo que se elevará el nivel de la seguridad de la información de la empresa.

3. Que la Vicepresidencia de Petroindustrial disponga que las funciones de los miembros del Comité de Seguridad de la Información sean las que se detallan en la presente propuesta una vez creado el Comité, a fin de dar impulso, responsabilizar y formalizar sus funciones

4. Que el Comité de Seguridad de Información aplique las metodologías presentadas:

    a. Esquema de Desarrollo de la Política de Seguridad, y

    b. Sistema de Gestión de los Sistemas de Información.

Las mismas que se deben aplicar en el desarrollo de sus actividades, a fin de que sea el ente que guíe y regule la seguridad de la información de toda la filial de Petroindustrial.

5. Que la Vicepresidencia de Petroindustrial en coordinación con el Comité de Seguridad de la Información autorice e impulse la implementación las Políticas Prioritarias Organizacionales detalladas en esta propuesta, como acción inmediata para fundamentar, sustentar y formalizar las acciones del Comité de Seguridad de la Información.

6. Que el Jefe de la Unidad de Sistemas Matriz aplique las recomendaciones de reestructuración del trabajo de la Unidad de Sistemas planteadas en esta propuesta, de manera urgente, a fin de que la Unidad de Sistemas Matriz trabaje bajo un esquema que le permita garantizar el manejo de la información de la empresa.

7. Que el Jefe de la Unidad de Sistemas Matriz aplique las políticas técnicas presentadas en la propuesta de manera

inmediata, para que se regulen y normen los estándares básicos que apoyen el desarrollo adecuado del manejo de la información bajo la nueva estructura.

Estas recomendaciones deben implementarse inmediatamente a fin de viabilizar la conformación, depuración e implementación de las políticas, procedimientos, controles y demás eventos necesarios que demande la estructuración de un esquema ordenado y efectivo de Seguridades de Información para Petroindustrial.

Recomendaciones Necesarias.-

Las recomendaciones necesarias son las que Petroindustrial con el soporte de la nueva estructura organizacional desarrolle las siguientes recomendaciones:

1. Que el Jefe de la Unidad de Sistemas Matriz tramite la adquisición del equipo con su correspondiente software de seguridad con las características planteadas en la presente propuesta a corto plazo, a fin de asegurar la red perimetral de Petroindustrial y disponer de herramientas que permitan medir los ataques y configurar restricciones.

2. Que el Jefe de la Unidad de Sistemas Matriz desarrolle e implemente procedimientos y estándares formales a corto plazo, a fin de que apoyen a mantener la confidencialidad, integridad y disponibilidad de la información en los siguientes campos:

- Procedimientos de recepción formal de requerimientos, reclamos y errores, respecto al manejo de la información.
- Estructura y procedimiento formal para manejo y solución de eventos reportados de seguridad.
- Estandarización de la administración y manejo de claves.
- Estandarización de la documentación de los sistemas automatizados.
- Desarrollo e implementación de un plan de contingencias que administre eventos indeseables en equipos de comunicaciones y servidores.

3. Que el Comité de Seguridad de la Información en coordinación con el Jefe de la Unidad de Sistemas Matriz apliquen la norma para el desarrollo de políticas de seguridad empresarial, ISO 17799 a corto plazo, a fin de ejecutar lineamientos para la seguridad de los sistemas y redes de información que garanticen la seguridad integral del entorno sobre el que se maneja la información de Petroindustrial.
4. Que el Comité de Seguridad de la Información en coordinación con el Jefe de la Unidad de Sistemas Matriz desarrollen un plan de difusión de las políticas y procedimientos que aseguren la información de Petroindustrial a mediano plazo, a fin de concienciar sobre los riesgos derivados de la falta de seguridades y la importancia de los nuevos esquemas a implementarse, e involucrar a toda la organización en el proceso de elevar el nivel de seguridad sobre la información.

BIBLIOGRAFIA

1. **Libros:**

MC GRAW HILL, (2002). FIREWALLS MANUAL DE REFERENCIA

2. **Internet:**

Apuntes sobre la inversión y gestión de la seguridad informática
http://www.virusprot.com/Art49.html

Apuntes sobre la inversión y gestión de la seguridad informática
http://www.belt.es/expertos/experto.asp?id=2340

Gobierno de Colombia ï Políticas de Seguridad Informática
www.dnp.gov.co/archivos/documentos/
DIFP_Presupuesto/seguridad.pdf

DPI. Deep Packet Inspection. Inspección profunda de paquetes
http://www.sahw.com/wp/archivos/2005/01/24/dpi_deep_packet_inspection_inspeccion_profunda_de_paquetes/

Microsoft TechNet - Windows
www.microsoft.com/spain/technet/
recursos/wxpsp2/mejoras/default.mspx

Security
www.**symantec**.com

Servicios de Seguridad de Windows Server 2003
http://www.microsoft.com/spain/servidores/windowsserver2003/technologies/networking/ipsec/default.aspx
http://www.microsoft.com/spain/servidores/windowsserver2003/technologies/security/default.aspx

AUTORIZACION DE PUBLICACION

Autorizo al Instituto de Altos Estudios Nacionales la publicación de esta Tesis, de su bibliografía y anexos, como artículos de la Revista o como artículos para lectura seleccionada.

Quito, 15 de Julio del 2005

_____

ING. NANCY GUZMAN G.