Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

"SEGURIDAD DE LA INFORMACION FUNDAMENTADAS EN LA NORMA ISO 27001, IMPLEMENTACION PRACTICA SOBRE EL CONTROL DE ACCESO A DOS SERVIDORES LINUX DE LA EMPRESA MUNICIPAL DE ASEO DE CUENCA EMAC."

Trabajo de graduación previo a la obtención del título de Ingeniero de Sistemas

Autores: Tania Karina Vélez Vanegas

Director: Ing. Oswaldo Merchán

Cuenca, Ecuador
2007

DEDICATORIA

A Mauricio Andrés, se que estas junto al Señor, tu recuerdo me acompaña en los momentos felices de mi vida.

Tu mamá

AGRADECIMIENTO

A Daniel de Jesús, conocido por todos, como “Cuqui”, gracias por tu tiempo, gracias por acompañarme en algunas largas horas de trabajo y/o estudio, haciendo travesuras a mi lado, siempre recordándome que tengo por quien tratar de ser mejor.

Tu mamá

Las ideas, hechos y contenidos de esta tesis son de exclusiva responsabilidad del autor

.....

Tania Vélez Vanegas

INTRODUCCION

La seguridad informática consiste en el conjunto de controles que tienen la finalidad de mantener la confidencialidad, integridad y confiabilidad de la información electrónica; así como resguardar los activos tecnológicos de una organización. Dicha seguridad comprende aspectos relacionados con políticas, estándares, buenas prácticas, controles, valoración de riesgos, capacitación y otros elementos necesarios para la adecuada administración de los recursos tecnológicos y de la información que se maneja por esos medios.

En ese sentido, la seguridad informática salvaguarda los activos contra daños, destrucción, uso no autorizado o robo; mantiene la integridad de los datos, permitiendo que la información electrónica sea oportuna, precisa, confiable y completa; ayuda a alcanzar las metas institucionales y permite el uso eficiente de los recursos tecnológicos destinados para el procesamiento de la información.

En la actualidad las empresas son conscientes de la gran importancia que tiene para el desarrollo de sus actividades proteger de forma adecuada la información que poseen y especialmente aquella que les sirve para realizar correctamente su actividad.

Debido esta necesidad 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.

Igualmente, se han desarrollado Normas de Estandarización a nivel internacional para la certificación de Sistemas de Gestión de la Seguridad de la Información (ISO 27001, ISO/IEC 17799), que permitirán a la empresa, no sólo garantizar que ante eventuales riesgos presentes o futuros tiene implantado un Sistema de Gestión de la Seguridad para la protección de su Información, sino ofrecer una imagen de calidad y solidez a su mercado.

RESUMEN

Este documento abarca aspectos como:

- Controles de la seguridad informática, necesarios para mantener la confidencialidad, integridad y confiabilidad de la información electrónica; así como resguardar los activos tecnológicos de una organización.

- Proceso de la seguridad informática basada en la norma ISO 27001, el cual identifica los pasos que se deben seguir para establecer las mejores prácticas para este fin.

- Funciones del personal de seguridad informática, de conformidad con el estándares ISO 27001, que coadyuvan a la identificación de las labores a cargo del personal respectivo.

- Controles a implementarse en linux con el fin de prevenir ataques y actividades maliciosas.

- Respuestas a incidentes de seguridad y seguimiento de las actividades maliciosas

ABSTRACT

This document includes aspects like:

- Controls of security informatic, necessary to maintain the confidentiality, integrity and trustworthiness of the information; as well as to protect the technological of an organization.

- Process of the computer science security based on the norm ISO 27001, which identifies the steps that are due to follow to establish the best practices for this aim.

- Functions of the personnel of security informatic, in accordance with the standards ISO 27001, that help to the identification of the workings in charge of the respective personnel.

- Controls to implement itself in linux with the purpose of preventing attacks and malicious activities.

- Answers to security incidents and pursuit of the malicious activities

CAPITULO I

En esta parte se definen aspectos generales sobre la seguridad de la información, y los tipos de controles básicos que podrían existir en una organización.

1. Seguridad Informática

La Seguridad Informática es una necesidad creciente en todas las organizaciones; hoy en día conforme se brindan servicios tanto a través de Internet, como de Intranet y Extranets, se abren oportunidades para que personas con cierto nivel de conocimiento o con ningún nivel de conocimiento pero con poderosas herramientas puedan no solo hacer colapsar los sistemas sino también robar uno de los activos más valiosos de las organizaciones: **La Información**

Un concepto global de seguridad informática sería aquel definido como el conjunto de procedimientos y actuaciones encaminados a conseguir la garantía de funcionamiento del sistema de información, obteniendo eficacia, entendida como el cumplimiento de la finalidad para el que estaba establecido, manteniendo la integridad, entendida como la inalterabilidad del sistema por agente externo al mismo, y alertando la detección de actividad ajena, entendida como el control de la interacción de elementos externos al propio sistema.

Los criterios implantados por la política de seguridad deben seguirse siempre, desde que el sistema es simple o sencillo hasta cuando su crecimiento lo transforma en uno complejo, la responsabilidad de implantación de la política de seguridad afecta a todos los usuarios del sistema de información, tanto los normales como los privilegiados, donde habría que englobar a administradores de sistemas, administradores de bases de datos y responsables de comunicaciones.

1.1 Controles de seguridad existentes en la EMAC

1.1.1 Controles Físicos

El control físico es la implementación de medidas de seguridad usada para prevenir o detener el acceso no autorizado a material confidencial, existen diversos mecanismos de controles físicos tales como:

- Cámaras de circuito cerrado
- Sistemas de alarmas térmicos o de movimiento
- Guardias de seguridad
- Biométrica (huellas digitales, voz, etc)

El único control físico de acceso a los bienes tangibles e intangibles de la EMAC es el contar con el servicio de guardianía privada ininterrumpidamente durante todo el año.

1.1.2 Controles Técnicos

Los controles técnicos utilizan la tecnología como una base para controlar el acceso y uso de datos en la estructura física de la EMAC; así como, sobre la red. Los controles técnicos son mucho más extensos en su ámbito e incluyen tecnologías tales como:

- Encriptación:
- Tarjetas inteligentes
- Autenticación a nivel de la red
- Listas de control de acceso (ACLs)
- Software de auditoría de integridad de archivos

Encriptación:

Esta tecnología es utilizada en el sistema de Banda Ancha Inalámbrica CANOPY, instalado actualmente en la EMAC, el mismo que provee conectividad entre las diferentes oficinas de la EMAC, esto es Relleno Sanitario, Planta de Operación y Areas Verdes.

Estos equipos ofrecen encriptación DES (Data Encryption Standard) ,una de las formas de encriptación más robustas que existen hoy en el mercado basado en un sistema monoalfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones. Inicialmente el texto en claro a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

- **Autenticación a nivel de la red**

Autenticación básica (la contraseña se envía como texto no cifrado): Este tipo de autentificación únicamente requiere un login y una contraseña, por lo tanto proporciona nivel bajo de seguridad, las credenciales se envían como texto sin cifrar a través de la red, es fácil de ser visto por analizadores de protocolo. En la EMAC se utiliza este mecanismo únicamente para conceder acceso a información con poca o ninguna necesidad de privacidad sobre todo información existente en la página web que contiene información sobre la facturación de los clientes especiales y biopeligrosos catastrados en la EMAC.

- **Listas de control de acceso**

Las ACLs pueden dividirse fundamentalmente en dos clases.

Una ACL *estándar* consiste exclusivamente en las entradas de tipo *owner* (propietario), *owning group* (grupo propietario) y *other* (otros) y coincide con los bits de permisos tradicionales para archivos y directorios.

Una ACL *extendida* (*extended*) contiene además una entrada *mask* (máscara) y puede incluir varias entradas del tipo *named user* (usuario identificado por el nombre) y *named group* (grupo identificado por el nombre).

1.1.3 Controles Administrativos

Los controles administrativos definen los factores humanos de la seguridad. Incluye todos los niveles del personal dentro de la organización y determina cuáles usuarios tienen acceso a qué recursos e información usando medios tales como:

- . Entrenamiento y conocimiento
- . Planes de recuperación y preparación para desastres
- . Estrategias de selección de personal y separación

Estos controles se encuentran en desarrollo en la EMAC puesto que forman parte de la norma IS0 9001, que se encuentra en proceso de implementación.

1.2 **CONCLUSIONES**

Si bien existen muchos métodos para establecer controles que garanticen la integridad de la información, el acceso a recursos, los mismos en la EMAC deberían implementarse, difundirse y monitorearse periódicamete

CAPITULO II

Para poder diseñar e implementar estrategias de seguridad y respuestas a incidentes, se debe tener conocer sobre los tipos de ataques, vulnerabilidades y amenazas más comunes que un atacante puede explotar para comprometer los sistemas.

2. Ataques, vulnerabilidades y amenazas a la seguridad de los servidores y la red.

2.1 Arquitecturas inseguras

Una red mal configurada es un punto de entrada para usuarios no autorizados. Al dejar una red local abierta, se vuelve vulnerable a la Internet y altamente insegura, puede que no ocurra nada durante un cierto tiempo, pero *eventualmente* alguien intentará aprovecharse de la oportunidad.

2.2 Redes de difusión

Los administradores de sistemas a menudo fallan al darse cuenta de la importancia del hardware de la red en sus esquemas de seguridad. El hardware simple, tal como concentradores y enrutadores a menudo se basan en broadcast; es decir, cada vez que un nodo transmite datos a través de la red a un nodo recipiente, el concentrador o enrutador hace una difusión de los paquetes de datos hasta que el nodo recipiente recibe y procesa los datos. Este método es el más vulnerable para hacer engaños de direcciones (spoofing) al protocolo de resolución de direcciones (*arp*) o control de acceso a la media (*MAC*) tanto por intrusos externos como por usuarios no autorizados.

2.3. Servidores centralizados

Otra falla potencial de redes es el uso de computación centralizada. Una forma común de reducir costos para muchos negocios, es el de consolidar todos los servicios a una sola máquina poderosa, esto puede ser conveniente porque es fácil de manejar y cuesta considerablemente menos que una configuración de múltiples servidores. Sin embargo, un servidor centralizado introduce un punto único de falla en la red. Si el servidor central está comprometido, puede dejar la red totalmente inútil o peor aún, sensible a la manipulación o robo de datos. En estas situaciones un servidor central se convierte en una puerta abierta, permitiendo el acceso a la red completa.

2.4. Servicios inutilizados y puertos abiertos

Una instalación completa de un servidor de red contiene aproximadamente más de mil aplicaciones y bibliotecas de paquetes. Es muy común entre los administradores de sistemas realizar una instalación del sistema operativo sin prestar atención a qué programas están siendo realmente instalados. Esto puede ser problemático puesto que se pueden instalar servicios innecesarios, configurados con sus valores por defecto y, posiblemente activados por defecto. Esto puede causar que servicios no deseados, tales como Telnet, DHCP, o DNS, se ejecuten en un servidor o estación de trabajo sin que el administrador se entere, lo cual en consecuencia puede causar tráfico indeseado al servidor, o peor aún dejar abierto un agujero de seguridad.

2.5. Servicios sin sus parches

La mayoría de las aplicaciones de servidores incluidas en la instalación por defecto, son piezas de software robustas y sólidas que ya han sido probadas. Estas han sido usadas en ambientes de producción por varios años y su código ha sido refinado en detalle y muchos de los errores han sido encontrados y reparados. Sin embargo, no hay tal cosa como un software sin errores y siempre hay espacio para mejorar o refinarlo. Más aún, el nuevo software usualmente no es probado tan rigurosamente como uno se esperaría, debido a su reciente llegada al ambiente de producción o porque quizás no es tan popular como otras aplicaciones de servidores.

Los desarrolladores y administradores de sistemas a menudo encuentran fallas (bugs) en las aplicaciones de servidores y publican la información de la falla en sitios webs de seguimiento de errores y seguridad, aún cuando éstos mecanismos constituyen una forma efectiva de alertar a los usuarios sobre vulnerabilidades de seguridad, depende de los administradores de sistemas el aplicar los parches de sistemas a tiempo. Esto es particularmente cierto puesto que los crackers tienen acceso a las mismas fuentes e intentarán utilizar esta información para violar sistemas que no hayan sido emparchados. Una buena administración de sistemas requiere vigilancia, seguimiento constante de errores y un mantenimiento de sistemas apropiado para asegurar un ambiente computacional seguro.

2.6. Administración desatendida

Una de las amenazas más grandes a la seguridad de los servidores son los administradores distraídos, la causa primaria de la vulnerabilidad de seguridad de los sistemas es asignar personal poco entrenado para mantener la seguridad y no proporcionar ni el entrenamiento ni el tiempo para permitir que ejecuten su trabajo

Esto aplica tanto a los administradores nuevos como a aquellos demasiado confiados o poco motivados. Algunos administradores fallan en emparchar sus servidores y estaciones de trabajo, mientras que otros fallan en leer los mensajes del registro de eventos del kernel del sistema o tráfico de la red o los logs del sistema.

2.7. Contraseñas inseguras

El administrador de sistemas deberá cambiar sus contraseñas inmediátamente luego de la instalación y de forma periódica. Si un administrador de bases de datos no cambia las contraseñas, hasta un cracker sin mucha experiencia puede utilizar una contraseña conocida por todo el mundo para ganar acceso con privilegios administrativos a la bases de datos. Estos son sólo unos ejemplos de como una administración descuidada puede llevar a servidores comprometidos.

2.8. Servicios intrínsecamente inseguros

Aún hasta la organización más atenta y vigilante puede ser victima de vulnerabilidades si los servicios de red que seleccionen son intrínsecamente

inseguros. Por ejemplo, hay muchos servicios desarrollados bajo la suposición de que serían usados en una red confiable; sin embargo, esta supuesto falla tan pronto como el servicio se vuelve disponible sobre la Internet . la cual es por sí misma insegura. Una categoría de servicios de red inseguros son aquellos que requieren nombres y contraseñas de usuario sin encriptar para la autenticación.Telnet y FTP son dos de estos servicios. Un software para espiar paquetes que esté monitoreando el tráfico entre un usuario remoto y tal servicio, puede fácilmente robarse los nombres de usuario y contraseña.

Tales servicios pueden también ser presa fácil de lo que en términos de seguridad se conoce como un ataque de *hombre en el medio*. En este tipo de ataque, un pirata redirige el tráfico de la red a que apunte a su máquina en vez del servidor destino. Una vez que alguien abre una sesión remota con el servidor, la máquina del atacante actua como un conductor invisible, quedándose tranquilamente capturando la información entre el servicio remoto y el usuario inocente. De esta forma un pirata puede reunir contraseñas administrativas y datos sin que el servidor o el usuario se den cuenta.

Otro categoría de servicios inseguros incluye sistemas de archivos de red y servicios de información tales como NFS o NIS, los cuales son desarrollados específicamente para uso de LAN pero son, desafortunadamente, extendidos para para los usuarios remotos. NFS por defecto, no tiene ningún tipo de autenticación o mecanismos de seguridad configurado para prevenir que un pirata monte un directorio compartido NFS y a partir de allí accesar cualquier cosa dentro de el. NIS también, tiene información vital que debe ser conocida por cada computador de la red, incluyendo contraseñas y permisos de archivos, dentro de una base de datos de texto plano ACSII o DBM (derivado de ASCII).

Un cracker que gana acceso a esta base de datos puede tener acceso a todas las cuentas de usuarios en la red, incluyendo la cuenta del administrador.

CAPITULO III

Este capítulo es un resumen de la literatura obtenida tanto del internet como de medios impresos, referente a los controles que forman parte la Norma ISO 27001, con el fin de adquirir conocimientos, metodologías y herramientas de implementación y control de medidas de seguridad de la información de acuerdo con estándares internacionales

3. Principios fundamentales de la norma ISO 27001

Las redes informáticas las organizaciones, y en consecuencia, la información almacenada en ellas, se están viendo afectadas por amenazas de seguridad, ataques y fraudes informáticos, problemas de sabotajes, virus informáticos así como otro tipo de imprevistos y catástrofes mayores, que muchas veces suponen un gran obstáculo para la continuidad del negocio cuando no se tienen previstas medidas que permitan la recuperación o reparación de la información afectada, es decir, un buen Sistema de Gestión de Seguridad de la Información.

Para la implantación de un Sistema de Gestión de la Seguridad de la Información eficaz en las empresas, es imprescindible la interrelación de varios factores: las tecnologías de la información, la seguridad de las instalaciones, la formación e información del personal y los procesos de negocio.

Igualmente, se han desarrollado Normas de Estandarización a nivel internacional para la certificación de Sistemas de Gestión de la Seguridad de la Información (ISO 27001, ISO/IEC 17799), que permitirán a la empresa, no sólo garantizar que ante eventuales riesgos presentes o futuros tiene implantado un Sistema de Gestión de la Seguridad para la protección de su Información, sino ofrecer una imagen de calidad y solidez a su mercado.

La norma ISO 27001 se basa en los siguientes controles fundamentales:

3.1 Política de seguridad

La Política de Seguridad, se divide en dos partes

- Política de seguridad (Nivel político o estratégico de la organización): Es la mayor línea rectora, la alta dirección. Define las grandes líneas a seguir y el nivel de compromiso de la dirección con ellas.

- Plan de Seguridad (Nivel de planeamiento o táctico): Define el "Cómo". Es decir, baja a un nivel más de detalle, para dar inicio al conjunto de acciones o líneas rectoras que se deberán cumplir.

La política es el marco estratégico de la Organización, es el más alto nivel. El análisis de riesgo y el grado de exposición determinan el impacto que puede producir los distintos niveles de clasificación de la información que se posee. Una vez determinado estos conceptos, se pasa al Cómo que es el Plan de Seguridad que se implementará de acuerdo a la necesidad de las organizaciones.

3.2 Organización de la Información

Abarca los siguientes controles

- Organización Interna: Compromiso de la Dirección, coordinaciones, responsabilidades, autorizaciones, acuerdos de confidencialidad, contactos con autoridades y grupos de interés en temas de seguridad, revisiones independientes.

- Organización externa: Riesgos relacionados con terceros, gobierno de la seguridad respecto a clientes y socios de negocio.

Lo más importante a destacar de este grupo son dos cosas fundamentales que abarcan a ambos subgrupos:

- Organizar y Mantener actualizada la cadena de contactos (internos y externos), con el mayor detalle posible (Personas, responsabilidades, activos, necesidades, acuerdos, riesgos, etc).

3.3 Administración y Seguridad de los recursos humanos

En este aspecto se debe tener en cuenta lo siguiente:

- **Antes del empleo:** Responsabilidades y roles, verificaciones curriculares, términos y condiciones de empleo.

- **Durante el empleo:** Administración de responsabilidades, preparación, educación y entrenamiento en seguridad de la información, medidas disciplinarias.
- Finalización de responsabilidades, devolución de recursos.
- Finalización o cambio de empleo o revocación de derechos.

Se debe partir por la redacción de la documentación necesaria para la contratación de personal y la revocación de sus contratos. En la misma deberá quedar bien claro las acciones a seguir para los diferentes perfiles de la organización, basados en la responsabilidad de manejo de información que tenga ese puesto. Tanto la contratación el cese de un puesto, es una actividad conjunta de estas dos áreas, y cada paso deberá ser coordinado, según la documentación confeccionada, para que no se pueda pasar por alto ningún detalle, pues son justamente estas pequeñas omisiones de las que luego resulta el haber quedado con alta dependencia técnica de personas cuyo perfil es peligroso, o que al tiempo de haberse ido, mantiene accesos o permisos que no se debieran.

Se debe contar con un “Plan de Formación” y debe ser una actividad periódica y tratada como cualquier otra actividad de importancia de la organización, debería plantear lo siguiente:

- Meta a la que se desea llegar.
- Determinación de los diferentes perfiles de conocimiento.
- Forma de acceder al conocimiento.
- Objetivos de la formación.
- Metodología a seguir.
- Planificación y asignación de recursos.
- Confección del plan de formación.
- Implementación del plan.
- Medición de resultados.

- Mejoramiento contínuo.

3.4. Seguridad física y del entorno

Se encuentra subdividido en:

- Áreas de seguridad: Abarca la seguridad física y perimetral, control físico de entradas, seguridad de locales edificios y recursos, protección contra amenazas externas y del entorno, el trabajo en áreas e seguridad, accesos públicos, áreas de entrega y carga.

- Seguridad de elementos: Ubicación y protección de equipos, elementos de soporte a los equipos, seguridad en el cableado, mantenimiento de equipos, seguridad en el equipamiento fuera de la organización, seguridad en la redistribución o reutilización de equipamiento, borrado de información y/o software.

Aplicación: Todo tipo de aplicaciones.

Transporte: Control de puertos UDP y TCP.

Red: Medidas a nivel protocolo IP e ICMP, túneles de nivel 3.

Enlace: Medidas de segmentación a nivel direccionamiento MAC, tablas estáticas y fijas en switchs, control de ataques ARP, control de broadcast y multicast a nivel enlace, en el caso WiFi: verificación y control de enlace y puntos de acceso, 802.X (Varios), empleo de túneles de nivel 2, etc.

Físico: Instalaciones, locales, seguridad perimetral, CPDs, gabinetes de comunicaciones, control de acceso físico, conductos de comunicaciones, cables, fibras ópticas, radio enlaces, centrales telefónicas. En el caso físico, es conveniente también separar todas ellas, por lo menos en los siguientes documentos:

Documentación de control de accesos y seguridad perimetral general, áreas de acceso y entrega de materiales y documentación, zonas públicas, internas y restringidas, responsabilidades y obligaciones del personal de seguridad física.

Documentación de CPDs: Parámetros de diseño estándar de un CPD,

medidas de protección y alarmas contra incendios/humo, caídas de tensión, inundaciones, control de climatización (Refrigeración y ventilación), sistemas vigilancia y control de accesos, limpieza, etc.

Documentación y planos de instalaciones, canales de comunicaciones, cableado, enlaces de radio, ópticos u otros, antenas, certificación de los mismos, etc.

Empleo correcto del material informático y de comunicaciones a nivel físico: Se debe desarrollar aquí cuales son las medidas de seguridad física que se debe tener en cuenta sobre los mismos (Ubicación, acceso al mismo, tensión eléctrica, conexiones físicas y hardware permitido y prohibido, manipulación de elementos, etc.) . No se incluye aquí lo referido a seguridad lógica.

Seguridad física en el almacenamiento y transporte de material informático y de comunicaciones: Zonas y medidas de almacenamiento, metodología a seguir para el ingreso y egreso de este material, consideraciones particulares para el transporte del mismo (dentro y fuera de al organización), personal autorizado a recibir, entregar o sacar material, medidas de control. No se incluye aquí lo referido a resguardo y recuperación de información que es motivo de otro tipo de procedimientos y normativa.

Documentación de baja, redistribución o recalificación de elementos: Procedimientos y conjunto de medidas a seguir ante cualquier cambio en el estado de un elemento de Hardware (Reubicación, cambio de rol, venta, alquiler, baja, destrucción, compartición con terceros, incorporación de nuevos módulos, etc.).

3.5 Control de accesos

Este es el grupo de control más extenso y hace hincapié en documentar todos los procedimientos, manteniéndolos disponibles a todos los usuarios que los necesiten, segregando adecuadamente los servicios y las responsabilidades para evitar uso inadecuado de los mismos.

Este apartado consta de los siguientes puntos a considerar:

3.5.1 Administración de las comunicaciones y operaciones:

Esta tarea en todas las actividades de seguridad, se suele realizar por medio de lo que se denomina Procedimientos Operativos Normales o Procedimientos Operativos de Seguridad, y en definitiva consiste en la realización de documentos breves y ágiles, que dejen por sentado la secuencia de pasos o tareas a llevar a cabo para una determinada función. Cuanto mayor sea el nivel de desagregación de esta función, más breve será cada PON y a su vez más sencillo y comprensible. Luego de trabajar algún tiempo en esta actividad, se llegará a comprender que la mayoría de las actividades relacionadas con seguridad, son fácilmente descriptibles, pues suelen ser una secuencia de pasos bastante “mecanizables”, y allí radica la importancia de estos procedimientos. La enorme ventaja que ofrece poseer todo procedimentado es:

•Identificar con absoluta claridad los responsables y sus funciones.

•Evitar la “imprescindibilidad” de ciertos administradores.

•Evitar ambigüedades el procedimientos.

•Detectar “zonas grises” o ausencias procedimentales (futuras brechas de seguridad).

3.5.2. Administración de prestación de servicios de terceras partes:

Se refiere fundamentalmente, como su nombre lo indica, a los casos en los cuales se encuentran tercerizadas determinadas tareas o servicios del propio sistema informático.

Los controles están centrados en tres aspectos fundamentales de esta actividad:

•Documentar adecuadamente los servicios que se están prestando (acuerdos, obligaciones, responsabilidades, confidencialidad, operación, mantenimiento, etc.).

•Medidas a adoptar para la revisión, monitorización y auditoría de los mismos
•Documentación adecuada que permita regularizar y mantener un eficiente control de cambios en estos servicios.

3.5.3. Planificación y aceptación de sistemas:

El objetivo es realizar una adecuada metodología para que al entrar en producción cualquier sistema, se pueda minimizar el riesgo de fallos.

De acuerdo a la magnitud de la empresa y al impacto del sistema a considerar, siempre es una muy buena medida la realización de maquetas. Estas maquetas deberían “acercarse” todo lo posible al entorno en producción, para que sus pruebas de funcionamiento sean lo más veraces posibles, simulando ambientes de trabajo lo más parecidos al futuro de ese sistema (Hardware y Software, red, carga de operaciones y transacciones, etc.), cuanto mejor calidad y tiempo se dedique a estas maquetas, menor será la probabilidad de fallos posteriores, es una relación inversamente proporcional que se cumple en la inmensa mayoría de los casos.

Los aspectos claves de este control son el diseño, planificación, prueba y adecuación de un sistema por un lado; y el segundo, es desarrollar detallados criterios de aceptación de nuevos sistemas, actualizaciones y versiones que deban ser implantados. Este último aspecto será un documento muy “vivo”, que se realimentará constantemente en virtud de las modificaciones, pruebas, incorporaciones y avances tecnológicos, por lo tanto se deberá confeccionar de forma flexible y abierto a permanentes cambios y modificaciones.

3.5.4. Protección contra código móvil y maligno:

El objetivo de este apartado es la protección de la integridad del software y la información almacenada en los sistemas.

El código móvil es aquel que se transfiere de un equipo a otro para ser ejecutado en el destino final, este empleo es muy común en las arquitecturas cliente-servidor, y se está haciendo más común en las arquitecturas “víctima-gusano”, por supuesto con un empleo no tan deseado.

En cuanto al código malicioso, a esta altura no es necesario ahondar en ningún detalle al respecto, pues “quien esté libre de virus y troyanos que tire la primera piedra”.El estándar hace referencia al conjunto de medidas comunes que ya suelen ser aplicadas en la mayoría de las empresas, es decir, detección, prevención y recuperación de la información ante cualquier tipo de virus. Tal vez lo más importante aquí y suele ser el punto débil de la gran mayoría es la preparación y la existencia de procedimientos (Lo que implica practicarlos).

La gran mayoría de las empresas confían su seguridad antivirus en la mera aplicación de un determinado producto y nada más, pero olvidan preparar al personal de administradores y usuarios en cómo proceder ante virus; y, por supuesto, tampoco realizan procedimientos de recuperación y verificación del buen funcionamiento de lo documentado.

3.5.5. Resguardo:

El objetivo de esta apartado conceptualmente es muy similar al anterior, comprende un solo control que remarca la necesidad de las copias de respaldo y recuperación. Siguiendo la misma insistencia del párrafo precedente, de nada sirve realizar copias de respaldo y recuperación, sino se prepara al personal e implementan las mismas con prácticas y procedimientos

3.5.6. Administración de la seguridad de redes:

Los dos controles que conforman este apartado hacen hincapié en la necesidad de administrar y controlar lo que sucede en nuestra red, es decir, implementar todas las medidas posibles para evitar amenazas, manteniendo la seguridad de los sistemas y aplicaciones a través del conocimiento de la información que circula por ella. Se deben implementar controles técnicos, que evalúen permanentemente los servicios que la red ofrece, tanto propios como tercerizados.

3.5.7. Manejo de medios:

En esta traducción, como “medio” debe entenderse todo elemento capaz de almacenar información (discos, cintas, papeles, etc. tanto fijos como removibles).Por lo tanto el objetivo de este grupo es, a través de sus cuatro controles, prevenir la difusión, modificación, borrado o destrucción de cualquiera de ellos o lo que en ellos se guarda.

3.5.8. Intercambios de información:

Este grupo contempla el conjunto de medidas a considerar para cualquier tipo de intercambio de información, tanto en línea como fuera de ella, y para movimientos internos o externos de la organización.

•Políticas, procedimientos y controles para el intercambio de información para tipo y medio de comunicación a emplear.

•Acuerdos, funciones, obligaciones, responsabilidades y sanciones de todas las partes intervinientes.

•Medidas de protección física de la información en tránsito.

•Consideraciones para los casos de mensajería electrónica

•Medidas particulares a implementar para los intercambios de información de negocio, en especial con otras empresas.

En el caso de que se trate de una empresa que sea la prestadora de -Servicios de comercio electrónico: La prestación de servicios de comercio electrónico por parte de una empresa exige el cumplimiento de varios detalles desde el punto de vista de la seguridad:

•Metodologías seguras de pago.

•Confidencialidad e integridad de la transacción.

•Mecanismos de no repudio.

•Garantías de transacción.

•Conformidades legales.

Para el cumplimiento de lo expuesto es que este grupo presenta, un conjunto de medidas a considerar referidas al control de información que circula a través de redes públicas para evitar actividades fraudulentas, difusión, modificación o mal uso de la misma. Medidas tendientes a evitar transacciones incompletas, duplicaciones o réplicas de las mismas, y por último mecanismos que aseguren la integridad de la totalidad de la información disponible.

3.5.9. Monitorización:

Este apartado tiene como objetivo la detección de actividades no autorizadas en la red y reúne los siguientes aspectos:

•Auditar Logs que registren actividad, excepciones y eventos de seguridad.

•Realizar revisiones periódicas y procedimientos de monitorización del uso de los sistemas.

•Implementación de robustas medidas de protección de los Logs de información de seguridad. Se debe considerar que una de las primeras enseñanzas que recibe cualquier aprendiz de intruso, es a borrar sus huellas para poder seguir operando sin ser descubierto el mayor tiempo posible. Por esta razón, es una de las principales tareas de seguridad, la de proteger todo indicio o prueba de actividad sospechosa. En casos de máxima seguridad, se llega hasta el extremo de tener

una impresora en línea, que va registrando sobre papel en tiempo real, cada uno de los logs que se configuran como críticos, pues es uno de los pocos medios que no puede ser borrado remotamente una vez detectada la actividad.

•La actividad de los administradores y operadores de sistemas, también debe ser monitorizada, pues es una de las mejores formas de tomar conocimiento de actividad sospechosa, tanto si la hace un administrador propio de la empresa (con o sin mala intención) o si es uno que se hace pasar por uno de ellos. Hay que destacar que una vez que se posee acceso a una cuenta de administración, se tiene control total de esa máquina y en la mayoría de los casos, ya está la puerta abierta para el resto de la infraestructura, es decir, se emplea es máquina como puente o máquina de salto hacia las demás.

•Así como es vital, ser estricto con el control de Logs, lo es también el saber lo antes posible, si cualquiera de ellos está fallando, pues esa debe ser la segunda lección de un aprendiz de intruso. Es decir, lograr que se dejen de generar eventos de seguridad por cada paso que da. Por lo tanto, es necesario implementar un sistema de alarmas quemonitorice el normal funcionamiento de los sistemas de generación de eventos de seguridad y/o Logs.

3.5.10. Sincronización de tiempos:

Hoy en día el protocolo NTP (Network Time Protocol) está tan difundido y fácilmente aplicable que es un desperdicio no usarlo. Se debe implementar una buena estrategia de estratos, tal cual lo propone este protocolo, y sincronizar toda la infraestructura de servidores, tanto si se depende de ellos para el funcionamiento de los servicios de la empresa, como si no. Pues cuando llega la hora de investigar, monitorizar o seguir cualquier actividad sospechosa es fundamental tener una secuencia cronológica lógica que permita moverse pro todos los sistemas de forma coherente.

De acuerdo a la actividad de la empresa, se deberá ser más o menos estrictos con la precisión del reloj del máximo estrato (hacia el exterior) el cual puede soportar mayor flexibilidad en los casos que no sea vital su exactitud con las jerarquías internacionales y luego el resto de las máquinas dependerán de este. Pero lo que no debe suceder y así lo exige esta norma, es la presencia de servidores que no estén sincronizados.

3.5.11. Autenticación

No se debe confundir la actividad de control de accesos con autenticación, esta última tiene por misión identificar que verdaderamente “sea, quien dice ser”.El control de acceso es posterior a la autenticación y debe regular que el usuario autenticado, acceda únicamente a los recursos sobre los cuales tenga derecho y a ningún otro, es decir que tiene dos tareas derivadas:

•Encauzar (o enjaular) al usuario debidamente.

•Verificar el desvío de cualquier acceso, fuera de lo correcto.

El control de acceso es una de las actividades más importantes de la arquitectura de seguridad de un sistema. Al igual que sucede en el mundo de la seguridad física, cualquiera que ha tenido que acceder a una caja de seguridad bancaria.

3.5.12. Requerimientos para el control de accesos:

Debe existir una Política de Control de accesos documentada, periódicamente revisada y basada en los niveles de seguridad que determine el nivel de riesgo de cada activo.

3.5.13. Administración de accesos de usuarios:

Prevenir el uso no autorizado, exige llevar un procedimiento de registro y revocación de usuarios, una adecuada administración de los privilegios y de las contraseñas de cada uno de ellos, realizando periódicas revisiones a intervalos regulares, empleando para todo ello procedimientos formalizados dentro de la organización.

3.5.14. Responsabilidades de usuarios:

Todo usuario dentro de la organización debe tener documentadas sus obligaciones dentro de la seguridad de la información de la empresa.

Independientemente de su jerarquía, siempre tendrá alguna responsabilidad a partir del momento que tenga acceso a la información. Evidentemente existirán diferentes grados de responsabilidad, y proporcionalmente a ello, las obligaciones derivadas de estas funciones, de este ítem se derivan tres actividades.

•Identificar niveles y responsabilidades.
•Documentarlas correctamente.

•Difundirlas y verificar su adecuada comprensión.

Para estas actividades propone tres controles, orientados a que los usuarios deberán aplicar un correcto uso de las contraseñas, ser conscientes del equipamiento desatendido (por lugar, horario, lapsos de tiempo, etc.) y de las medidas fundamentales de cuidado y protección de la información en sus escritorios, medios removibles y pantallas.

3.5.15. Control de acceso a redes:

Todos los servicios de red deben ser susceptibles de medidas de control de acceso; en este grupo se busca prevenir cualquier acceso no autorizado a los mismos.

Como primer medida establece que debe existir una política de uso de los servicios de red para que los usuarios, solo puedan acceder a los servicios específicamente autorizados. Luego se centra en el control de los accesos remotos a la organización, sobre los cuales deben existir medidas apropiadas de autenticación.

Un punto sobre el que merece la pena detenerse es sobre la identificación de equipamiento y de puertos de acceso. Este aspecto es una de las principales medidas de control de seguridad.

En la actualidad se poseen todas las herramientas necesarias para identificar con enorme certeza las direcciones, puertos y equipos que pueden o no ser considerados como seguros para acceder a las diferentes zonas de la empresa. Tanto desde una red externa como desde segmentos de la propia organización.

En los controles de este grupo se menciona medidas automáticas, segmentación, diagnóstico y control equipamiento, direcciones y de puertos, control de conexiones y rutas de red.Para toda esta actividad se deben implementar: IDSs, IPSs, FWs con control de estados, honey pots, listas de control de acceso, certificados digitales, protocolos seguros, túneles, etc…Es decir, existen hoy en día muchas herramientas para implementar estos controles de la mejor forma y eficientemente, por ello, tal vez este sea uno de los grupos que más exigencia técnica tiene dentro de este estándar.

3.5.16. Control de acceso a sistemas operativos:

Presupone uno de los mejores puntos de escalada para una intrusión; de hecho son los primeros pasos de esta actividad, denominados “Fingerprintig y footprinting”, pues una vez identificados los sistemas operativos, versiones y parches, se

comienza por el más débil y con solo conseguir un acceso de usuario, se puede ir escalando en privilegios hasta llegar a encontrar el de ”root”, con lo cual ya no hay más que hablar.

La gran ventaja que posee un administrador, es que las actividades sobre un sistema operativo son mínimas, poco frecuentes sus cambios, y desde ya que no comunes a nivel usuario del sistema, por lo tanto si se saben emplear las medidas adecuadas, se puede identificar rápidamente cuando la actividad es sospechosa, y en definitiva es lo que se propone en este control: Seguridad en la validación de usuarios del sistema operativo, empleo de identificadores únicos de usuarios, correcta administración de contraseñas, control y limitación de tiempos en las sesiones y por último verificaciones de empleo de utilidades de los sistemas operativos que permitan realizar acciones “interesantes”.

3.5.17. Control de acceso a información y aplicaciones:

Están dirigidos a prevenir el acceso no autorizado a la información mantenida en las aplicaciones. Propone redactar, dentro de la política de seguridad, las definiciones adecuadas para el control de acceso a las aplicaciones y a su vez el aislamiento de los sistemas sensibles del resto de la infraestructura.

Este último proceder es muy común en sistemas críticos (Salas de terapia intensiva, centrales nucleares, servidores primarios de claves, sistemas de aeropuertos, militares, etc.), los cuales no pueden ser accedidos de ninguna forma vía red, sino únicamente estando físicamente en ese lugar.Por lo tanto si se posee alguna aplicación que entre dentro de estas consideraciones, debe ser evaluada la necesidad de mantenerla o no en red con el resto de la infraestructura.

-Movilidad y teletrabajo:Esta nueva estructura laboral, se está haciendo cotidiana en las organizaciones y presenta una serie de problemas desde el punto de vista de la seguridad:

•Accesos desde un ordenador de la empresa, personal o público.
•Posibilidades de instalar o no, medidas de hardware/software seguro en el ordenador remoto.

•Canales de comunicaciones por los cuales se accede (red publica, privada, GPRS, UMTS, WiFi, Túnel, etc.).

•Contratos que se posean sobre estos canales.

•Personal que accede:propio, tercerizado, o ajeno.

•Lugar remoto: fijo o variable.

•Aplicaciones e información a la que accede.

•Nivel de profundidad en las zonas de red a los que debe acceder.

•Volumen y tipo de información que envía y recibe.

•Nivel de riesgo que se debe asumir en cada acceso.

La norma no entra en mayores detalles, pero de los dos controles que propone se puede identificar que la solución a esto es adoptar una serie de procedimientos que permitan evaluar, implementar y controlar adecuadamente estos aspectos en el caso de poseer accesos desde ordenadores móviles y/o teletrabajo.

3.5.18. Procesamiento correcto en aplicaciones:

Su misión es el correcto tratamiento de la información en las aplicaciones de la empresa.Para ello las medidas a adoptar son, validación en la entrada de datos, la implementación de controles internos en el procesamiento de al información para verificar o detectar cualquier corrupción de la información a través de los procesos, tanto por error como intencionalmente, la adopción de medidas par asegurar y proteger los mensajes de integridad de las aplicaciones.Y por último la validación en la salida de datos, para asegurar que los datos procesados, y su posterior tratamiento o almacenamiento, sea apropiado a los requerimientos de esa aplicación.

3.5.19. Controles criptográficos:

En este caso, a través de dos controles, lo que propone es desarrollar una adecuada política de empleo de estos controles criptográficos y administrar las calves que se emplean de forma consciente con el fin de garantizar la integridad, confidencialidad y autenticidad de la información.

El tema de claves criptográficas, como se ha podido apreciar hasta ahora, es un denominador común de toda actividad de seguridad, por lo tanto más aún cuando lo que se pretende es implementar un completo SGSI, por lo tanto es conveniente y muy recomendable dedicarle la atención que evidentemente merece, para lo cual una muy buena medida es desarrollar un documento que cubra todos los temas sobre los cuales los procesos criptográficos participarán de alguna forma y desde el

mismo referenciar a todos los controles de la norma en los cuales se hace uso de claves. Este documento “rector” de la actividad criptográfica, evitará constantes redundancias y sobre todo inconsistencias en la aplicación de claves.

3.5.20. Seguridad en los sistemas de archivos:

La Seguridad en los sistemas de archivos, independientemente que existan sistemas operativos más robustos que otros en sus técnicas de archivos y directorios, es una de las actividades sobre las que se debe hacer un esfuerzo técnico adicional, pues en general existen muchas herramientas para robustecerlos, pero no suelen usarse.

Es cierto que los sistemas de archivos no son un tema muy estático, pues una vez que un sistema entra en producción suelen hacerse muchas modificaciones sobre los mismos, por esto último principalmente es que una actividad que denota seriedad profesional, es la identificación de ¿Cuáles son los directorios o archivos que no deben cambiar y cuáles sí?.

Suele ser el mejor indicador de una actividad anómala, si se ha planteado bien el interrogante anteriormente propuesto. Si se logra identificar estos niveles de “estaticidad y cambio” y se colocan los controles y auditorías periódicas y adecuadas sobre los mismos, este será una de las alarmasde la que más haremos uso a futuro en cualquier etapa de un incidente de seguridad, y por supuesto será la mejor herramienta para restaurar un sistema a su situación inicial mediante control de software operacional, test de esos datos y controlar el acceso al código fuente.

3.5.21. Seguridad en el desarrollo y soporte a procesos: Los aspectos calve de este grupo son:

•Desarrollar un procedimiento de control de cambios.

•Realización de revisiones técnicas a las aplicaciones luego de realizar cualquier cambio, teniendo especial atención a las aplicaciones críticas.

•Documentar claramente las restricciones que se deben considerar en los cambios de paquetes de software.

•Implementación de medidas tendientes a evitar fugas de información.
•Supervisión y monitorización de desarrollos de software externalizado.

3.6. Adquisición de sistemas de información desarrollo y mantenimiento.

En este control se debe considera lo siguiente:

3.6.1. Requerimientos de seguridad de los sistemas de información:

Plantea la necesidad de realizar un análisis de los requerimientos que deben exigirse a los sistemas de información, desde el punto de vista de la seguridad para cumplir con las necesidades del negocio de cada empresa en particular, para poder garantizar que la seguridad sea una parte integral de los sistemas.

3.7 Administración de los incidentes de seguridad

Todo lo relativo a incidentes de seguridad queda resumido a dos formas de proceder:

- Proteger y proceder.
- Seguir y perseguir.

Lo que trata de poner de manifiesto es que ante un incidente, quien no posea la capacidad suficiente solo puede “Proceder y proteger”, es decir cerrar, apagar, desconectar, pero al volver sus sistemas al régimen de trabajo normal el problema tarde o temprano volverá pues no se erradicaron sus causas.

En definitiva, es esto lo que trata de dejar claro este punto de la norma a través de los cinco controles que agrupa, y subdivide en:

3.7.1. Reportes de eventos de seguridad de la información y debilidades.

Como su nombre lo indica, este apartado define el desarrollo de una metodología eficiente , monitorización y seguimiento de reportes, los cuales deben reflejar, tanto para la generación eventos de seguridad como debilidades de los sistemas.Estas metodologías deben ser ágiles, por lo tanto se presupone el empleo de herramientas automatizadas que lo hagan. En estos momentos se poseen muchas de ellas.

En concreto para que estos controles puedan funcionar de manera eficiente, lo mejor es implantar herramientas de detección de vulnerabilidades, ajustarlas a la

organización, para saber con total certeza dónde se es débil y donde no, y a través de estas desarrollar un mecanismo simple de difusión de las mismas a los responsables de su administración y solución.

3.7.2. Administración de incidentes de seguridad de la información y mejoras.

La siguiente tarea es disponer de una metodología de administración de incidentes, lo cual no es nada más que un procedimiento que describa claramente: pasos, acciones, responsabilidades, funciones y medidas concretas.

Todo esto no es eficaz si no se realiza la preparación adecuada, por lo tanto es necesario difundirlo, practicarlo y simularlo, es decir generar incidentes que no hagan peligrar los elementos en producción, tanto sobre maquetas como en planta y poner a prueba todos los eslabones de la metodología.

La preparación, en los casos defensivos hace principalmente esto, es decir analizar las posibles metodologías que puede aplicar un enemigo y practicar su contramedida, esto es el entrenamiento militar y a su vez son los denominados “ejercicios militares” en el terreno o en mesas de arena, que no son otra cosa que simulaciones sobre qué sucedería si reacciono de una forma u otra.

3.7.3. Aspectos de seguridad de la información en la continuidad del negocio.

Este aspecto tiene como objetivo contemplar todas las medidas tendientes a que los sistemas no hagan sufrir interrupciones sobre la actividad que realiza la empresa. Hoy en día los sistemas informáticos son uno de los pilares fundamentales de toda empresa, independientemente de la actividad que realice, ya se puede afirmar que no existe ninguna que no tenga un cierto grado de dependencia con estas tecnologías.

Cualquier anomalía de sus sistemas repercute en la actividad de la empresa y esta anomalía debería minimizarse al máximo. Lo primero que considera este aspecto es que la seguridad de la información se encuentre incluida en la administración de la continuidad de negocio, esto que tal vez parezca muy intangible o impreciso, no es nada más que considerar los puntos o hitos en los cuales debe incluirse “controles” de seguridad dentro de los procesos de la empresa

.Es decir, si una empresa conoce bien su actividad, debe ser capaz de redactar su metodología de trabajo a través de flujos o procesos. En cada una de las líneas que unen este grafo, se debe considerar la seguridad, y verificar si esta influye o no en esta secuencia, si influye es un hito de seguridad y debe ser considerado, evaluado e implementado el control correspondiente. Este punto que se presentó unos renglones arriba como intangible, puedo asegurar que debe ser el más importante de esta norma, y es el que desencadenará absolutamente todos los controles de seguridad de la empresa, pues si un control no está relacionado con los procesos de la empresa, no tiene mayor sentido y, peor aún, si no se conocen con exactitud los procesos de la empresa, es muy difícil asegurar los sistemas de la misma.

Una vez detectada y analizada la inclusión de hitos o controles de seguridad en los procesos de la empresa, el segundo paso es evaluar los riesgos que impone este para la interrupción del negocio de la organización, de ese riesgo se derivará un impacto, cuyas consecuencias se deberá determinar cómo asumir.

Las medidas o determinaciones que se adopten para solucionar, minimizar, mejorar o asumir esos riesgos deberán expresarse por medio de planes de continuidad de negocio (o planes de contingencia), los cuales tienen el objetivo de mantener y restaurar el nivel operacional de la empresa, por medio de un conjunto de medidas que reflejen la forma de proceder y/o escalar ante la ocurrencia de cualquiera de los efectos que produciría un fallo en esos hitos.

3.8 Marco Legal

Este grupo cubre uno de los aspectos más débiles que en estos momentos posee la norma, pues la aplicación de la misma en cada país, debe estar de acuerdo a las bases y regulaciones legales del mismo.

3.8.1. Cumplimiento de requerimientos legales.

Lo primero a considerar aquí es la identificación de la legislación aplicable a la empresa, definiendo explícitamente y documentando todo lo que guarde relación con estos aspectos.

Otro componente de este primer grupo es lo relacionado con los derechos de propiedad intelectual y las regulaciones, referentes al empleo de software legal, su

concienciación y difusión.

Todos los registros que guarden algún tipo de información clasificada desde el punto de vista legal, deben ser protegidos para evitar pérdidas, alteraciones y un aspecto muy importante:“divulgación inadecuada”, en particular, y esto ya es una regulación generalizada en todos los Países, los registros de carácter personal y de ello lo más importante es lo que se puede considerar como datos íntimos en el caso de tener necesidad de almacenarlos, como pueden ser enfermedades, discapacidades, orientación religiosa, sexual, política, etc.

Para todos estos registros, se deben implementar todos los procedimientos necesarios, para prevenir su procesamiento incorrecto, pues se pueden haber considerado todos los aspectos legales en su guarda y custodia, pero al momento de ser procesados, quedan expuestos (memorias temporales, permanencia exterior, o transmisión insegura, etc.), o sus resultados, quedan fuera del perímetro o las evaluaciones de seguridad que fueron realizadas sobre los registros. Por lo tanto, para todo registro deberá ser identificado, analizado, implementado y documentado, todos los aspectos legales que le aplican, durante el almacenamiento y también en todo momento en que sea requerido para su procesamiento (incluyendo aquí sus desplazamientos).

3.8.2. Cumplimiento de políticas de seguridad, estándares y técnicas de buenas prácticas.

La norma trata de hacer hincapié en el control del cumplimiento de estas medidas, pues de nada sirve tener todo en regla con los aspectos legales, si luego el personal involucrado no da cumplimiento alas medidas y en definitiva, la implementación falla. Para evitar estas debilidades y los graves problemas que pueden ocasionar, es que se debe asegurar que todos estos procedimientos se cumplan y verificar periódicamente que las regulaciones estén vigentes, sean aplicables y estén de acuerdo con toda la organización.

3.8.3. Consideraciones sobre auditorías de sistemas de información.

Las auditorías de los sistemas de información son imprescindibles, las dos grandes consideraciones son realizarla de forma externa o interna. Cuando se contrata este servicio a través de empresas externas, los resultados son mejores, pues son su

especialidad detectar los aciertos y errores, la parte negativa es que por los recursos económicos que implica, no pueden ser todo lo periódicas que se desean. Por otro lado, las auditorías internas, no poseen tal vez tanta“expertiz”, pero por realizarse con recursos propios, ofrecen la posibilidad de realizarlas con mayor periodicidad e inclusive realizarlas aleatoriamente lo cual suele ser muy efectivo.El aspecto fundamentalde una auditoría interna es que no puede estar involucrado el personal responsable de lo que se audita, es decir, no se puede ser “Juez y parte”.

3.8.4. Herramientas de Auditoría

Este es un tema de vital interés desde varios aspectos:
•Una herramienta de auditoría de seguridad instalada, puede servir para el lado bueno o el “oscuro” de la organización. Por lo tanto, las mismas deberán ser tratadas con todas las precauciones (Inventariadas, identificadas, controladas en su acceso, monitorizadas, desinstaladas, etc.).Pues si un usuario no autorizado, accede a ellas, se le está sirviendo la red en bandeja de plata.

•El empleo de una herramienta de auditoría de seguridad debe ser perfectamente regulado, en cuanto a su alcance, profundidad, potencialidad, horario, fechas, ventanas de tiempo de operación, objetivo, resultados deseados, etc. Pues al igual que en el punto anterior, no puede dejarse librado al azar su uso correcto, caso contrario se puede disparar todo un procedimiento de incidencias, o caerse una infraestructura, etc.

•Se debe coordinar con cada sistema a auditar qué es exactamente lo que se va a hacer sobre este y cuales son los derechos y obligaciones que se poseen en el uso de esa herramienta sobre cada sistema en particular, pues no tiene porqué ser el mismo para todos.

•Se debe regular contractualmente, en los casos de auditorías externas cuáles son los derechos, obligaciones y responsabilidades en el empleo de las mismas, incluyendo claramente las indemnizaciones por daños y perjuicios que pueden ocasionar en su empleo incorrecto.

3.8.5 Conclusiones:

Es necesario adquirir conocimientos, metodologías y herramientas de implementación y control de medidas de seguridad de la información de acuerdo con estándares internacionales uno de ellos es la Norma ISO 27001.

CAPITULO IV

Todo sistema se convierte en un objetivo para ataques. Por esta razón, es de suma importancia para todo administrador de sistemas fortalecer el sistema informático y bloquear servicios innecesarios

4. Configuración de Seguridades referentes al control de acceso en Red Hat Enterprise Linux en la Empresa Municipal de Aseo de Cuenca –EMAC-

4.1 Evaluación de la seguridad actual

La seguridad de la información se basa en tres aspectos fundamentales:

Confidencialidad: La información confidencial sólo debería estar disponible a un conjunto de individuos predefinido. Las transmisiones no autorizadas y el uso de información debería ser restringido.

Integridad: La información no debería ser alterada en formas que la hagan incompleta o incorrecta. Los usuarios no autorizados deberían ser restringidos de la habilidad de modificar o destruir información confidencial.

Disponibilidad: La información debería estar disponible para los usuarios autorizados en cualquier momento que estos la requieran. La disponibilidad es una garantía de que la información pueda ser obtenida con la frecuencia acordada y en el momento previsto.

4.1.1 Seguridad de la estación de trabajo

Al evaluar la seguridad de las estaciones de trabajo con el sistema operativo linux se ha considerado lo siguiente:

Seguridad de la contraseña: Las contraseñas utilizan combinación de letras mayúsculas, minúsculas y números y no son obvias.

Controles administrativos: Se ha verificado que personas tienen acceso una cuenta en el sistema y cuales son sus privilegios.

Servicios de red disponibles: Se ha verificado que servicios se están ejecutando y si es que son necesarios

Cortafuegos: Se ha verificado la existencia de un firewall que proteja el acceso a los servidores.

Herramientas de comunicación: Se ha verificado como se accede de forma remota al servidor, y las herramientas utilizadas y para qué

4.1.2 Seguridad del BIOS y del gestor de arranque

La seguridad del BIOS y el gestor de arranque, puede prevenir que usuarios no autorizados que tengan acceso físico a los sistemas, arranquen desde medios removibles u obtengan acceso como root.

4.1.3 Contraseñas del BIOS

Se ha verificado que el BIOS este protegido con contraseñas con el fin de prevenir cambios en las configuraciones que pudieran permitir a un intruso acceder a los sistemas desde un diskette o CD-ROM, esto permitiría entrar en modo de rescate o monousuario, lo que a su vez les permite plantar programas dañinos en el sistema o copiar datos confidenciales.

Existe está funcionalidad activada, y cualquier usuario esta forzado a introducir una contraseña antes de que el BIOS lanze el gestor de arranque.

4.2 Gestión de acceso de usuarios

4.21. Seguridad en las contraseñas

Las contraseñas son el método principal que Red Hat Enterprise Linux utiliza para

verificar la identidad de los usuarios. Por esta razón la seguridad de las contraseñas es de suma importancia para la protección del usuario, la estación de trabajo y la red.

Para propósitos de seguridad, el programa de instalación configura el sistema para usar el Message-Digest Algorithm (MD5) y contraseñas shadow. Lo recomendable es no cambiar estas configuraciones, el sistema MD5 no limita las contraseñas a ocho caracteres.

4.2.2 Recomendaciones para contraseñas robustas

Cuando se crea una contraseña segura, es una buena idea seguir las siguientes pautas:

- No utilizar solamente palabras o números
- No utilizar palabras reconocibles (nombres propios)
- No utilizar palabras comunes en idiomas extranjeros .
- No utilizar terminología de hackers .
- No utilizar información personal
- No utilizar palabras invertidas
- No escribir su contraseña en papel
- No utilizar la misma contraseña para todas las máquinas

4.2.3. Creación de cuentas de usuario

Cuando existe un número significativo de usuarios dentro de una organización, los administradores de sistemas tienen dos opciones básicas para forzar el uso de buenas contraseñas.

- Asignar contraseñas a los usuarios
- Dejar que creen sus propias contraseñas dándoles directrices para su creación

En estos dos casos se debería forzar la creación de contraseñas robustas y forzar el cambio periódico de las mismas. La razón de esto es que si un usuario es forzado a cambiar su contraseña de forma periódica si ésta ha sido descifrada por un craker sólo le será útil por un tiempo.

4.2.4. Controles administrativos

Cuando se otorga privilegios para que algunos usuarios puedan llevar a acabo algunas tareas como root o adquiriendo privilegios a través de sudo o su, se debería tener muy en cuenta qué usuarios a pesar de tener estos privilegios pueden realizar actividades tales como reinicio o montaje de una unidad removible. El dar acceso a algunos usuarios con privilegios de root podría traer las siguientes consecuencias:

- Mala configuración de las máquinas . Se podrían configurar las máquinas de forma errónea y/o abrir agujeros de seguridad sin saberlo.

- Habilitar servicios inseguros . Se podría activar servicios inseguros como FTP o Telnet,

El administrador debería asegurar aún más que las conexiones como root sean limitadas mediante los siguientes métodos.

Cambiar el shell de root: Modificando el archivo /etc/passwd y cambiando el shell de /bin/bash a /sbin/nologin, este método impide el acceso al shell de root y registra el intento, además no se podrá acceder como root a aplicaciones como login, su , ssh, scp, sftp.

Deshabilitar el acceso como root a traves de consola tty: Un archivo /etc/securetty previene la conexión como root a través de consola o red, no permite el acceso como root mediante login, gdm, kdm, xdm.

Deshabilitar conexiones root SSH. Se tiene que modificar el archivo /etc/ssh/sshd_config y cambiar el parámetro PermitRootLogin a no, previene el acceso a través del conjunto de herramientas OpenSSH, prohibe el acceso mediante ssh, scp, sftp.

4.3 Responsabilidades de los usuarios

Se ha sugerido se incluya dentro Manual de Políticas Administrativas y de Control Interno de la EMAC, lo siguiente referente a la responsabilidad de los usuarios en

el uso de los sistemas de información.

- Los usuarios tendrán máximo cuidado en la manipulación y el uso de los equipos informáticos y de toda la infraestructura complementaria. Evitarán realizar cualquier acción, que de forma voluntaria o no, pueda dañar la integridad física de la instalación (destrozos, sustracción, traslados no autorizados, etc.)
- Las cuentas de usuarios en los sistemas informáticos de la EMAC son personales e intransferibles y de uso en el ámbito estrictamente laboral o de investigación relacionada con la gestión administrativa y operativa de la Empresa.
- Los Usuarios, bajo su estricta responsabilidad harán uso de los medios y servicios de comunicación electrónicos, de telecomunicaciones e Internet, y entenderán y seguirán los procedimientos establecidos para el buen uso, mantenimiento y conservación de las tecnologías de información.
- Los administradores de los sistemas y bases de datos deberán prever políticas de administración de claves de acceso y perfiles de usuarios,
- Los Usuarios en todo momento serán responsables del uso de sus claves,
- Los respaldos previamente a su almacenamiento y resguardo, deberán de ser analizados a fin de verificar que no contengan virus, gusanos o códigos maliciosos informáticos.

4.4 Configuración de acceso remoto y local a la red

/etc/passwd

El archivo de contraseñas es uno de los más crítico en Linux, contiene el mapa de nombres de usuarios, identificaciones de usuarios y la ID del grupo primario al que pertenece esa persona. También puede contener el archivo real, aunque es más seguro utilizar contraseñas con shadow para mantener las contraseñas en /etc/shadow. Este archivo debe ser legible por todo el mundo, o si no comandos tan simples como ls dejarían de funcionar correctamente. El campo GECOS puede contener datos tales como el nombre real, el número de teléfono y otro tipo de cosas parecidas en cuanto al usuario, su directorio personal, que es el directorio en que se coloca al usuario por defecto si hace un login interactivo, y el shell de login

tiene que ser un shell interactivo (como bash), y estar listado en /etc/shells para que el usuario pueda hacer login. El formato es:

nombreusuario:contraseña_cifrada:UID:GID:campo_GECOS:direct_personal:login_shell

Las contraseñas se guardan utilizando un hash (MD5). Las contraseñas no pueden obtenerse a partir de la forma cifrada, sin embargo, se puede tratar de encontrar una contraseña utilizando fuerza bruta para pasar por el hash cadenas de texto y compararlas, hasta conseguir una contraseña.

/etc/shadow

El archivo de shadow alberga pares de nombres de usuario y contraseñas, así como información contable, como la fecha de expiración, y otros campos especiales. Se ha asegurado en la EMAC que el archivo sea solo de lectura y que sólo sea accedido por el root.

/etc/groups

El archivo de grupos contiene toda la información de pertenencia a grupos, y opcionalmente elementos como la contraseña del grupo. El formato es:

nombregrupo:contraseña_cifrada:GID:miembro1,miembro2,miembro3

Un grupo puede no contener miembros, sólo un miembro o múltiples miembros, y la contraseña es opcional.

/etc/gshadow

Similar al archivo shadow de contraseñas, este fichero contiene los grupos, contraseñas y miembros.

/etc/login.defs

Este archivo permite definir algunos valores por defecto para diferentes programas como useradd y expiración de contraseñas. Tiende a variar ligeramente entre

distribuciones e incluso entre versiones, pero suele estar bien comentado y tiende a contener los valores por defecto.

/etc/shells

El fichero de shells contiene una lista de shells válidos, si el shell por defecto de un usuario no aparece listado aquí, quizás no pueda hacer login interactivamente. Mira la sección sobre Telnetd para más información.

/etc/securetty

Este archivo contiene una lista de tty's desde los que el root puede hacer un login. Los tty's de la consola suelen ir de /dev/tty1 a /dev/tty6. Los puertos serie son /dev/ttyS0 y superiores por lo general. Si quieres permitirle al root hacer login vía red entonces añade /dev/ttyp1 y superiores. Generalmente, sólo se debería permitir conectar al root desde /dev/tty1, y es aconsejable deshabilitar la cuenta de root, sin embargo antes de hacer esto, se debería asegurarse de permitir al root acceder a comandos.

4.5 Configuración de control de acceso al sistema operativo

Hay varios archivos de configuración importantes, que controlan qué servicios ejecuta Linux.

4.5.1 inetd.conf

Frecuentemente, los servicios son llevados a cabo por los llamados demonios. Un demonio es un programa que abre un determinado puerto, y espera a recibir peticiones de conexión. Si se recibe una petición de conexión, lanza un proceso hijo que aceptará la conexión, mientras el padre continua escuchando a la espera de más peticiones. Este concepto tiene el inconveniente de que por cada servicio ofrecido, se necesita ejecutar un demonio que escuche las conexiones a un puerto, lo que generalmente significa un desperdicio de recursos de sistema como, por ejemplo, de espacio de intercambio.

Mediante inetd.conf se inician los servicios, generalmente aquellos que no necesitan ejecutarse de continuo, o que están basados en sesiones (como telnet o

ftpd).

Para algunos servicios como DNS que sirven a muchas conexiones rápidas, la sobrecarga de arrancar servicios cada pocos segundos sería mayor que tenerlo constantemente ejecutándose. De igual forma ocurre con servicios como DNS y el correo, donde el tiempo es crítico, no así el caso de una sesión ftp en donde unos segundos de retraso no afectan el sistema.

Cada vez que se hagan cambios a inetd.con, hay que reiniciar inetd para hacer efectivos los cambios, killall –1 inetd lo reiniciará correctamente.

Se aconseja desabilitar tantos servicios de inetd.conf como sea posible, por lo general los que se suelen usar son ftp, pop e imap. Se debería reemplazar telnet por el SSH. El acceso a programas arrancados por inetd se puede controlar con facilidad mediante el uso de TCP_WRAPPERS.

4.5.2. TCP_WRAPPERS

Usar TCP_WRAPPERS hace que el asegurar servidores contra intrusiones externas sea bastante más simple TCP_WRAPPERS se controla desde dos ficheros:

/etc/hosts.allow
/etc/hosts.deny

Primero se comprueba hosts.allow, y las reglas se comprueban desde la primera a la última. Si no puede encontrar ninguna regla que te corresponda en hosts.allow, entonces va a comprobar hosts.deny en busca de una regla que la entrada. De nuevo comprueba las reglas de hosts.deny desde la primera a la última, y la primera regla que encuentre que te deniega acceso significa que no te deja entrar. Si tampoco encuentra una regla denegando la la entrada, entonces por defecto deja entrar. Si se va a utilizar una política por defecto no optimista en cuanto a seguridad debería ser:

ALL: 0.0.0.0/0.0.0.0

Significa que todos los servicios y todos los lugares se encuentran bloqueados. Por

ejemplo se podría denegar el acceso por defecto por ejemplo a telnet y permitir el acceso a ftp de la siguiente forma

en hosts.allow: in.ftpd: 0.0.0.0/0.0.0.0
Permitir acceso desde cualquier parte del mundo

en hosts.deny: in.telnetd: 0.0.0.0/0.0.0.0
Denegar acceso a telnetd desde cualquier parte

Si se deja activado un servicio que no debería figurar en inetd.conf y no se tiene una política de denegación por defecto, se pueden tener problemas. Es más seguro tener reglas de denegación por defecto para el cortafuegos y TCP_WRAPPERS, de modo que si se olvida algo por accidente, por defecto no tendrá acceso. Si se instala algo para lo cual necesitan tener acceso los usuarios y se olvida poner reglas, enseguida se quejarán y se podrá rectificar el problema rápidamente. Fallar por precaución y denegar accidentalmente algo es más seguro que dejarlo abierto.

4.5.3. TCP Wrappers y el mejoramiento de la conexión

Si ciertos tipos de conexión son de mayor preocupación que otros, se puede subir el nivel de conexión para ese servicio a través de la opción severity. Por ejemplo, se asume que cualquiera que esté intentando conectarse al puerto 23, en un servidor FTP, es un maleante informático. Para resaltar esto, coloque una bandera emerg en los archivos de registro en vez de la bandera por defecto, info, y niegue la conexión.

Para hacer esto, coloque la línea siguiente en /etc/hosts.deny: in.telnetd : ALL : severity emerg

Esto usará la facilidad de conexión por defecto authpriv, pero subirá el nivel de prioridad del valor por defecto de info a emerg, lo cual coloca los mensajes de conexión directamente a la consola.

4.5.4. Protección de Portmap

El servicio portmap es un demonio de asignación de puertos dinámico para servicios RPC, tales como NIS y NFS. Tiene mecanismos de autenticación débiles

y la habilidad de asignar un amplio rango de puertos para los servicios que controla. Por estas razones, es difícil de asegurar.

Para restringir más aún el acceso al servicio portmap, es una buena idea añadir reglas de IPTables al servidor para así limitar el acceso a redes específicas.

Abajo se muestran dos ejemplos de comandos IPTables que permiten conexiones TCP al servicio portmap (escuchando en el puerto 111) desde la red 192.168.0/24 y desde la máquina local (la cual es necesaria para el servicio sgi_fam, utilizado por Nautilus). Todos los demás paquetes son descartados.

```
iptables -A INPUT -p tcp -s! 192.168.0.0/24 --dport 111 -j DROP
iptables -A INPUT -p tcp -s 127.0.0.1 --dport 111 -j ACCEPT
iptables -A INPUT -p udp -s! 192.168.0.0/24 --dport 111 -j DROP
```

4.5.4. Protección de NIS

NIS viene de *Network Information Service*, o servicio de información de redes. Es un servicio RPC llamado ypserv el cual es usado en conjunto con portmap y otros servicios relacionados, para distribuir mapas de nombres de usuarios, contraseñas y otra información confidencial a cualquier computador que se encuentre dentro de su dominio.

Un servidor NIS esta compuesto de varias aplicaciones. Ellas incluyen las siguientes:

. /usr/sbin/rpc.yppasswdd. También llamado el servicio yppasswdd, este demonio permite a los usuarios cambiar sus contraseñas NIS.

. /usr/sbin/rpc.ypxfrd. También llamado ypxfrd, es el demonio responsable de las transferencias de mapas NIS sobre la red.

. /usr/sbin/yppush . Esta aplicación propaga las bases de datos NIS modi_cadas a múltiples servidores NIS.

. /usr/sbin/ypserv. Este es el demonio del servidor NIS.

NIS es más bien inseguro para los estándares de hoy día. No tiene mecanismos de autenticación y pasa toda la información sobre la red sin encriptación, incluyendo las contraseñas. Como consecuencia, se debe tener extremo cuidado cuando se configure una red que utilice NIS. Para complicar la situación aún más, la configuración por defecto de NIS es insegura en si

4.5.5. Utilizar un nombre de dominio NIS y de host de tipo contraseña

Cualquier máquina dentro de un dominio NIS puede usar comandos para extraer información desde el servidor sin necesidad de autenticación, siempre y cuando el usuario conozca el nombre DNS y del dominio del servidor NIS.

Por ejemplo, si alguien conecta una portátil a la red o irrumpe en la red desde afuera y logra simular una dirección IP interna, el comando siguiente revelará el mapa /etc/passwd:

ypcat –d $ NIS_domain%-h$DNS_hostname%passwd

4.5.6. Asignar puertos estáticos y uso de reglas IPTables

A todos los servidores relacionados con NIS se les pueden asignar puertos específicos excepto por rpc.yppasswdd. El demonio que permite a los usuarios cambiar sus contraseñas de conexión. Asignar puertos a los otros dos demonios de servidores NIS, rpc.ypxfrd y ypserv, permite crear reglas de cortafuegos para proteger aún más los demonios del servidor NIS contra los intrusos.

Para hacer esto, se añade las líneas siguientes a /etc/sysconfig/network:

YPSERV_ARGS="-p 834"
YPXFRD_ARGS="-p 835"

Las siguientes reglas IPTables se pueden emitir para imponer a cual red el servidor escuchará para estos puertos:

iptables -A INPUT -p ALL -s! 192.168.0.0/24 --dport 834 -j DROP
iptables -A INPUT -p ALL -s! 192.168.0.0/24 --dport 835 -j DROP

4.5.7. TCP-IP y seguridad de redes

Los ataques más comunes son los ataques de negación de servicio, ya que son los más fáciles de ejecutar y los más difíciles de impedir, seguidos del sniffing de paquetes, escaneo de puertos y otras actividades relacionadas.

Los nombres de hosts no apuntan siempre a la dirección IP correcta, y las direcciones IP's no siempre se pueden resolver al nombre de host adecuado.

En lo posible no se debe utilizar autentificación basada en nombres de hosts, puesto que el envenenamiento de cachés DNS es algo relativamente sencillo, confiar la autentificación en una dirección IP reduce el problema al spoofing, lo cual es algo más seguro, pero de ningún modo completamente seguro. No existen mecanismos extendidos para verificar quién envió los datos y quién los está recibiendo, excepto mediante el uso de sesiones o cifrado a nivel IP. Se puede empezar por denegar los datos entrantes que dicen originarse desde la red interna, puesto que estos datos son evidentemente falsos, para evitar que los usuarios, u otros que hayan irrumpido en tu red puedan lanzar ataques falsificados, se deberían bloquear todos los datos salientes que no provengan de nuestra dirección IP. Si todo en Internet tuviera filtros salientes es decir, restringir todo el tráfico saliente a aquel que se originase desde las direcciones IP internas, los ataques mediante spoofing serían imposibles, y a la vez sería mucho más fácil tracear el origen de los atacantes. También se deberían bloquear las redes reservadas (127.*, 10.*,etc.).

4.6. Configuración de acceso a aplicaciones e información y servicios de red.

Primero se ha ejecutado los comandos ps y netstat ps dice qué servicios se está nejecutando y con netstat se podrá conocer el estado de los puertos cuales están abiertos y escuchando.

4.6.1. Salida de PS

El programa ps nos muestra el estado de procesos (información disponible en /proc). Las opciones más comúnmente utilizadas son
"ps -xau",

```
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0 0 1668 560 ? S Feb-06 0:00 init [5]
root 2 0 0 0 0 ? S Feb-06 0:00 [migration/0]
root 3 0 0 0 0 ? SN Feb-06 0:00 [ksoftirqd/0]
root 4 0 0 0 0 ? S< Feb-06 0:00 [events/0]
root 5 0 0 0 0 ? S< Feb-06 0:00 [khelper]
root 6 0 0 0 0 ? S< Feb-06 0:00 [kblockd/0]
root 7 0 0 0 0 ? S Feb-06 0:00 [khubd]
root 44 0 0 0 0 ? S Feb-06 0:00 [pdflush]
root 45 0 0 0 0 ? S Feb-06 0:02 [pdflush]
root 47 0 0 0 0 ? S< Feb-06 0:00 [aio/0]
root 46 0 0 0 0 ? S Feb-06 0:00 [kswapd0]
root 120 0 0 0 0 ? S Feb-06 0:00 [kseriod]
root 191 0 0 0 0 ? S Feb-06 0:00 [scsi_eh_0]
root 202 0 0 0 0 ? S Feb-06 0:00 [scsi_eh_1]
root 207 0 0 0 0 ? S Feb-06 0:04 [kjournald]
root 1112 0 0 2576 452 ? S<s Feb-06 0:00 udevd
root 1549 0 0 0 0 ? S Feb-06 0:00 [kjournald]
root 1550 0 0 0 0 ? S Feb-06 0:01 [kjournald]
root 1551 0 0 0 0 ? S Feb-06 0:07 [kjournald]
root 1931 0 0 2460 588 ? Ss Feb-06 0:02 syslogd -m 0
root 1935 0 0 3324 484 ? Ss Feb-06 0:01 klogd -x
rpc 1947 0 0 3280 572 ? Ss Feb-06 0:00 portmap
root 1993 0 0 2732 576 ? S Feb-06 0:00 /usr/sbin/smartd
root 2003 0 0 4476 1016 ? Ss Feb-06 0:01 /usr/sbin/dovecot
root 2014 0 0 7560 1764 ? S Feb-06 0:04 dovecot-auth
dove cot 201 0 0 4312 1460 ? S Feb-06 0:01 imap-login
dove cot 201 0 0 4532 1460 ? S Feb-06 0:01 imap-login
dove cot 201 0 0 5088 1460 ? S Feb-06 0:01 imap-login
name d 206 0 0.1 37820 3636 ? Ssl Feb-06 0:00 /usr/sbin/named -u named -t /var/named/chroot
root 2073 0 0 5452 1652 ? Ss Feb-06 0:02 /usr/sbin/sshd
root 2091 0 0 2308 828 ? Ss Feb-06 0:00 xinetd -stayalive -pidfile /var/run/xinetd.pid
clam av 210 0 2.4 76184 5133 2 ? Ss Feb-06 0:48 /usr/sbin/clamd
clam av 211 0 0 5852 1440 ? Ss Feb-06 0:00 /usr/bin/freshclam -d -p /var/run/clamav/freshclam.pid
root 2138 0 0.1 8072 3096 ? Ss Feb-06 0:01 sendmail: accepting connections
smm p 214 0 0.1 7188 2596 ? Ss Feb-06 0:00 sendmail: Queue runner@00:15:00 for /var/spool/clientmqueue
root 2147 0 0.1 7124 2688 ? Ss Feb-06 0:00 sendmail: Queue runner@00:15:00 for /var/spool/mqueue
root 2165 0 0.9 25812 1978 8 ? Ss Feb-06 0:00 MailScanner: starting child
root 2178 0 0 3032 544 ? Ss Feb-06 0:00 gpm -m /dev/input/mice -t imps2
root 2199 0 0 4624 812 ? Ss Feb-06 0:00 crond
xfs 2251 0 0 4820 1608 ? Ss Feb-06 0:00 xfs -droppriv -daemon
root 2261 0 0.1 11044 2444 ? Ss Feb-06 0:00 smbd -D
root 2265 0 0 8740 2048 ? Ss Feb-06 2:19 nmbd -D
root 2274 0 0.1 11044 2392 ? S Feb-06 0:00 smbd -D
daem on 228 0 0 3404 648 ? Ss Feb-06 0:00 /usr/sbin/atd
dbus 2304 0 0 2764 1216 ? Ss Feb-06 0:00 dbus-daemon-1 --system
root 2315 0 0 5476 556 ? Ss Feb-06 0:33 rhnsd --interval 240
root 2325 0 0 2924 1044 ? Ss Feb-06 0:00 cups-config-daemon
root 2336 0 0.2 7536 5852 ? Ss Feb-06 0:07 hald
root 2575 0 0.3 10780 6924 ? Ss Feb-06 0:00 /usr/bin/perl /usr/libexec/webmin/miniserv.pl /etc/webmin/miniserv.conf
root 2585 0 0 1772 408 tty1 Ss+ Feb-06 0:00 /sbin/mingetty tty1
root 2610 0 0 2876 408 tty2 Ss+ Feb-06 0:00 /sbin/mingetty tty2
root 2611 0 0 3212 408 tty3 Ss+ Feb-06 0:00 /sbin/mingetty tty3
root 2693 0 0 1568 408 tty4 Ss+ Feb-06 0:00 /sbin/mingetty tty4
root 2710 0 0 1824 404 tty5 Ss+ Feb-06 0:00 /sbin/mingetty tty5
root 2727 0 0 1932 408 tty6 Ss+ Feb-06 0:00 /sbin/mingetty tty6
root 2776 0 0.1 12160 2332 ? Ss Feb-06 0:00 /usr/bin/gdm-binary -nodaemon
root 3057 0 0.1 12792 2892 ? S Feb-06 0:00 /usr/bin/gdm-binary -nodaemon
root 3062 0 0.4 11512 8820 ? S Feb-06 0:01 /usr/X11R6/bin/X :0 -audit 0 -auth /var/gdm/:0.Xauth -nolisten tcp vt7
gdm 3162 0 0.5 21984 1194 4 ? Ss Feb-06 0:00 /usr/bin/gdmgreeter
root 8766 0 0.4 19176 1016 8 ? Ss Feb-06 0:00 /usr/sbin/httpd
dove cot 151 0 0 4116 1452 ? S Feb-07 0:01 pop3-login
dove cot 151 0 0 4904 1456 ? S Feb-07 0:01 pop3-login
dove cot 151 0 0 5428 1452 ? S Feb-07 0:01 pop3-login
dove cot 151 0 0 4264 1452 ? S Feb-07 0:01 pop3-login
dove cot 151 0 0 5492 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4668 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 3620 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 5444 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4584 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4420 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4340 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4208 1456 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 5140 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 3780 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 5280 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4724 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 4172 1452 ? S Feb-07 0:01 pop3-login
dove cot 152 0 0 3572 1452 ? S Feb-07 0:01 pop3-login
root 10155 0 0.1 7544 2288 ? Ss Feb-09 0:00 squid -sY -f /etc/squid/squid.conf
squi d 1015 0 1.8 20548 4 375 08 ? Sl Feb-09 1:03 (squid) -sY -f /etc/squid/squid.conf
squi d 1015 0 0 2628 272 ? Ss Feb-09 0:00 (unlinkd)
root 26982 0 0.1 9436 2332 ? Ss Feb-11 0:00 cupsd
apac he 270 0 0.5 19312 1048 0 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.4 19176 1034 4 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.5 19720 1084 8 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.5 19720 1085 2 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.5 19448 1056 0 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.5 19312 1054 0 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.5 19720 1084 8 ? S Feb-11 0:00 /usr/sbin/httpd
apac he 270 0 0.5 19312 1040 8 ? S Feb-11 0:00 /usr/sbin/httpd
root 16536 0 1.8 43380 3780 4 ? S 13:29 0:01 MailScanner: waiting for messages
root 16929 0 1.7 42848 3728 8 ? S 14:28 0:00 MailScanner: waiting for messages
root 16982 0 1.8 43944 3848 4 ? S 14:49 0:01 MailScanner: waiting for messages
root 17342 0 1.9 45516 4001 6 ? S 15:13 0:01 MailScanner: waiting for messages
root 17829 0 0.1 9376 3816 ? S 16:16 0:00 sendmail: server 255.32.4.122.broad.jn.sd.dynamic.163data.com.cn [122.4.32.255] (may be forged) cmd read
root 17997 0 0.1 7888 2216 ? Ss 16:49 0:00 sshd: root@pts/1
root 17999 0 0 5340 1544 pts/1 Ss 16:49 0:00 =bash
root 18164 0.3 1.7 42604 3697 2 ? S 17:00 0:00 MailScanner: waiting for messages
root 18165 0 0 5180 1068 ? S 17:01 0:00 crond
root 18166 0 0 2532 912 ? Ss 17:01 0:00 /bin/bash /usr/bin/run-parts /etc/cron.hourly
root 18184 0 0 3292 892 ? S 17:01 0:00 /bin/bash /etc/cron.hourly/update_virus_scanners
root 18195 0 0 3852 556 ? S 17:01 0:00 awk -v progname=/etc/cron.hourly/update_virus_scanners progname {????? print progname ":\n"????? progname="";???? }???? { print; }
root 18197 0 0 3876 1160 ? S 17:01 0:00 perl -e sleep int(rand(600));
root 18205 0 0.1 11656 3344 ? S 17:03 0:00 smbd -D
root 18223 0 0 2864 776 pts/1 R+ 17:04 0:00 ps -xau
```

4.6.2 Salida de NETSTAT

Sirve para sacar listados de conexiones activas y en que puertos. Salida con Netstat –an.

```
Activ  e Inter   net con  nections (servers and      established)
Proto  Recv-Q  Send-Q  Local Address           Foreign Address         State
tcp            0      0 0.0.0.0:139           0.0.0.0:*               LISTEN
tcp            0      0 0.0.0.0:3310          0.0.0.0:*               LISTEN
tcp            0      0 0.0.0.0:111           0.0.0.0:*               LISTEN
tcp            0      0 192.168.0.1:8080      0.0.0.0:*               LISTEN
tcp            0      0 0.0.0.0:10000         0.0.0.0:*               LISTEN
tcp            0      0 192.168.0.1:53        0.0.0.0:*               LISTEN
tcp            0      0 200.55.228.162:53     0.0.0.0:*               LISTEN
tcp            0      0 127.0.0.1:53          0.0.0.0:*               LISTEN
tcp            0      0 127.0.0.1:631         0.0.0.0:*               LISTEN
tcp            0      0 0.0.0.0:25            0.0.0.0:*               LISTEN
tcp            0      0 127.0.0.1:953         0.0.0.0:*               LISTEN
tcp            0      0 0.0.0.0:445           0.0.0.0:*               LISTEN
tcp            0      0 200.55.228.162:52890  200.41.112.124:80       TIME_WAIT
tcp            0      0 200.55.228.162:52906  64.233.161.99:80        ESTABLISHED
tcp            0      0 200.55.228.162:52898  207.46.8.124:80         ESTABLISHED
tcp            0      0 200.55.228.162:52903  207.46.8.124:80         ESTABLISHED
tcp            0      0 200.55.228.162:52896  207.46.216.62:80        TIME_WAIT
tcp            0      0 200.55.228.162:52891  208.172.96.250:80       TIME_WAIT
tcp            0      0 200.55.228.162:52902  207.68.178.12:80        ESTABLISHED
tcp            0      0 200.55.228.162:52739  208.101.61.164:80       TIME_WAIT
tcp            0      0 200.55.228.162:52740  208.101.61.164:80       TIME_WAIT
tcp            0      0 200.55.228.162:52897  64.4.32.7:80            TIME_WAIT
tcp            0      0 200.55.228.162:25     200.93.222.229:40306    ESTABLISHED
tcp            0      0 200.55.228.162:52892  65.54.179.248:80        TIME_WAIT
tcp            0      0 200.55.228.162:52886  200.55.228.163:80       TIME_WAIT
tcp            0      0 200.55.228.162:52885  200.55.228.163:80       TIME_WAIT
tcp            0      0 200.55.228.162:52893  66.228.115.152:80       TIME_WAIT
tcp            0      0 200.55.228.162:52894  208.174.87.30:80        TIME_WAIT
tcp            0      0 200.55.228.162:52895  208.174.87.30:80        TIME_WAIT
tcp            0      0 :::110                :::*                    LISTEN
tcp            0      0 :::143                :::*                    LISTEN
tcp            0      0 :::80                 :::*                    LISTEN
tcp            0      0 :::22                 :::*                    LISTEN
tcp            0      0 :::443                :::*                    LISTEN
tcp            0     52 ::ffff:200.55.228.16  2:22    ::ffff:192.168.5.6 ESTABLISHED
tcp            0      0 ::ffff:200.55.228.16  2:22    ::ffff:192.168.5.6 ESTABLISHED
udp            0      0 0.0.0.0:32768         0.0.0.0:*
udp            0      0 192.168.0.1:137       0.0.0.0:*
udp            0      0 200.55.228.162:137    0.0.0.0:*
udp            0      0 0.0.0.0:137           0.0.0.0:*
udp            0      0 192.168.0.1:138       0.0.0.0:*
udp            0      0 200.55.228.162:138    0.0.0.0:*
udp            0      0 0.0.0.0:138           0.0.0.0:*
udp            0      0 0.0.0.0:10000         0.0.0.0:*
udp            0      0 192.168.0.1:53        0.0.0.0:*
udp            0      0 200.55.228.162:53     0.0.0.0:*
udp            0      0 127.0.0.1:53          0.0.0.0:*
udp            0      0 0.0.0.0:3130          0.0.0.0:*
udp            0      0 0.0.0.0:53072         0.0.0.0:*
udp            0      0 0.0.0.0:111           0.0.0.0:*
udp            0      0 0.0.0.0:631           0.0.0.0:*
udp            0      0 :::32769              :::*
Activ  e UNIX  domain  sockets (servers and      established)
Proto  RefCnt  Flags   Type       Stat          e      I-Node Path
unix       2  [ ]     DGRAM                    5775   @/var/run/hal/hotplug_socket
unix       2  [ ACC ]  STREAM     LISTENING     4721   /var/rugin/default
unix       2  [ ACC ]  STREAM     LISTENING     5592   /var/rum_bus_socket
unix       2  [ ]     DGRAM                    2884   @udevd
unix       2  [ ACC ]  STREAM     LISTENING     5325   /dev/gpmctl
unix      46  [ ]     DGRAM                    4562   /dev/log
unix       2  [ ACC ]  STREAM     LISTENING     5484   /tmp/.                100
unix       2  [ ACC ]  STREAM     LISTENING     7224   /tmp/.gdm_socket
unix       2  [ ACC ]  STREAM     LISTENING     7289   /tmp/.X11-unix/X0
unix       2  [ ]     DGRAM                    657406
unix       2  [ ]     DGRAM                    652982
unix       2  [ ]     DGRAM                    641472
unix       2  [ ]     DGRAM                    635448
unix       2  [ ]     DGRAM                    634328
unix       3  [ ]     STREAM     CONNECTED     515635 /var/rum_bus_socket
unix       3  [ ]     STREAM     CONNECTED     515634
unix       2  [ ]     DGRAM                    515597
unix       2  [ ]     DGRAM                    388128
unix       2  [ ]     DGRAM                    388126
unix       3  [ ]     STREAM     CONNECTED     113119 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113118
unix       3  [ ]     STREAM     CONNECTED     113117 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113116
unix       3  [ ]     STREAM     CONNECTED     113115 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113114
unix       3  [ ]     STREAM     CONNECTED     113113 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113112
unix       2  [ ]     DGRAM                    113106
unix       3  [ ]     STREAM     CONNECTED     113105
unix       3  [ ]     STREAM     CONNECTED     113104
unix       2  [ ]     DGRAM                    113101
unix       3  [ ]     STREAM     CONNECTED     113100
unix       3  [ ]     STREAM     CONNECTED     113099
unix       2  [ ]     DGRAM                    113096
unix       3  [ ]     STREAM     CONNECTED     113095
unix       3  [ ]     STREAM     CONNECTED     113094
unix       2  [ ]     DGRAM                    113091
unix       3  [ ]     STREAM     CONNECTED     113090
unix       3  [ ]     STREAM     CONNECTED     113089
unix       3  [ ]     STREAM     CONNECTED     113068 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113057
unix       2  [ ]     DGRAM                    113054
unix       3  [ ]     STREAM     CONNECTED     113053
unix       3  [ ]     STREAM     CONNECTED     113052
unix       3  [ ]     STREAM     CONNECTED     113067 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113051
unix       2  [ ]     DGRAM                    113048
unix       3  [ ]     STREAM     CONNECTED     113047
unix       3  [ ]     STREAM     CONNECTED     113046
unix       3  [ ]     STREAM     CONNECTED     113066 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113045
unix       2  [ ]     DGRAM                    113042
unix       3  [ ]     STREAM     CONNECTED     113041
unix       3  [ ]     STREAM     CONNECTED     113040
unix       3  [ ]     STREAM     CONNECTED     113065 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113039
unix       2  [ ]     DGRAM                    113036
unix       3  [ ]     STREAM     CONNECTED     113035
unix       3  [ ]     STREAM     CONNECTED     113034
unix       3  [ ]     STREAM     CONNECTED     113015 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113014
unix       2  [ ]     DGRAM                    113011
unix       3  [ ]     STREAM     CONNECTED     113010 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113009
unix       2  [ ]     DGRAM                    113006
unix       3  [ ]     STREAM     CONNECTED     113005 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     113004
unix       2  [ ]     DGRAM                    113001
unix       3  [ ]     STREAM     CONNECTED     112991
unix       3  [ ]     STREAM     CONNECTED     112990
unix       3  [ ]     STREAM     CONNECTED     112989
unix       3  [ ]     STREAM     CONNECTED     112988
unix       3  [ ]     STREAM     CONNECTED     112985
unix       3  [ ]     STREAM     CONNECTED     112984
unix       3  [ ]     STREAM     CONNECTED     112939 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112929
unix       2  [ ]     DGRAM                    112926
unix       3  [ ]     STREAM     CONNECTED     112925
unix       3  [ ]     STREAM     CONNECTED     112924
unix       3  [ ]     STREAM     CONNECTED     112938 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112923
unix       2  [ ]     DGRAM                    112920
unix       3  [ ]     STREAM     CONNECTED     112919
unix       3  [ ]     STREAM     CONNECTED     112918
unix       3  [ ]     STREAM     CONNECTED     112267 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112266
unix       3  [ ]     STREAM     CONNECTED     112263 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112262
unix       3  [ ]     STREAM     CONNECTED     112259 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112258
unix       2  [ ]     DGRAM                    112252
unix       3  [ ]     STREAM     CONNECTED     112251
unix       3  [ ]     STREAM     CONNECTED     112250
unix       2  [ ]     DGRAM                    112249
unix       3  [ ]     STREAM     CONNECTED     112248
unix       3  [ ]     STREAM     CONNECTED     112247
unix       3  [ ]     STREAM     CONNECTED     112257 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112246
unix       2  [ ]     DGRAM                    112243
unix       3  [ ]     STREAM     CONNECTED     112242
unix       3  [ ]     STREAM     CONNECTED     112241
unix       3  [ ]     STREAM     CONNECTED     112256 /var/run/default
unix       3  [ ]     STREAM     CONNECTED     112240
unix       2  [ ]     DGRAM                    112237
unix       3  [ ]     STREAM     CONNECTED     112236
unix       3  [ ]     STREAM     CONNECTED     112235
unix       2  [ ]     DGRAM                    112232
unix       3  [ ]     STREAM     CONNECTED     112231
unix       3  [ ]     STREAM     CONNECTED     112230
unix       2  [ ]     DGRAM                    7607
unix       3  [ ]     STREAM     CONNECTED     7527   /tmp/.X11-unix/X0
unix       3  [ ]     STREAM     CONNECTED     7526
unix       3  [ ]     STREAM     CONNECTED     7520   /tmp/.X11-unix/X0
unix       3  [ ]     STREAM     CONNECTED     7519
unix       3  [ ]     STREAM     CONNECTED     7499   /tmp/                 100
unix       3  [ ]     STREAM     CONNECTED     7498
unix       3  [ ]     STREAM     CONNECTED     7503   /tmp/.X11-unix/X0
unix       3  [ ]     STREAM     CONNECTED     7339
unix       2  [ ]     DGRAM                    6187
unix       2  [ ]     DGRAM                    6181
unix       3  [ ]     STREAM     CONNECTED     5774   /var/run/m_bus_socket
unix       3  [ ]     STREAM     CONNECTED     5773
unix       3  [ ]     STREAM     CONNECTED     5628   /var/run/m_bus_socket
unix       3  [ ]     STREAM     CONNECTED     5627
unix       2  [ ]     DGRAM                    5617
unix       3  [ ]     STREAM     CONNECTED     5595
unix       3  [ ]     STREAM     CONNECTED     5594
unix       2  [ ]     DGRAM                    5500
unix       2  [ ]     DGRAM                    5377
unix       2  [ ]     DGRAM                    5324
unix       2  [ ]     DGRAM                    5176
unix       2  [ ]     DGRAM                    5163
unix       2  [ ]     DGRAM                    5152
unix       2  [ ]     DGRAM                    5000
unix       2  [ ]     DGRAM                    4943
unix       2  [ ]     DGRAM                    4761
unix       3  [ ]     STREAM     CONNECTED     4765   /var/run/default
unix       3  [ ]     STREAM     CONNECTED     4754
unix       3  [ ]     STREAM     CONNECTED     4764   /var/run/default
unix       3  [ ]     STREAM     CONNECTED     4751
unix       3  [ ]     STREAM     CONNECTED     4763   /var/run/default
unix       3  [ ]     STREAM     CONNECTED     4748
unix       2  [ ]     DGRAM                    4740
unix       2  [ ]     DGRAM                    4739
unix       2  [ ]     DGRAM                    4738
unix       3  [ ]     STREAM     CONNECTED     4730
unix       3  [ ]     STREAM     CONNECTED     4729
unix       3  [ ]     STREAM     CONNECTED     4728
unix       3  [ ]     STREAM     CONNECTED     4727
unix       3  [ ]     STREAM     CONNECTED     4726
unix       3  [ ]     STREAM     CONNECTED     4725
unix       3  [ ]     STREAM     CONNECTED     4724
unix       3  [ ]     STREAM     CONNECTED     4723
unix       2  [ ]     DGRAM                    4704
unix       2  [ ]     DGRAM                    4570
```

En la salida numérica se puede observar el número que corresponde al servicio activo. Los campos que nos interesan son el primero, el tipo de servicio, el cuarto campo, que es la dirección IP de la interfaz y el puerto, la dirección externa (si no es 0.0.0.0.* significa que alguien le está hablando activamente), y el estado del puerto.

La línea en la que el puerto es 80, corresponde a un cliente remoto hablando con el servidor de Web. Cuando se ve el servidor www escuchando en 0.0.0.0:80 que significa, todos los interfaces, puerto 80, seguidos del servidor DNS ejecutándose en las 3 interfaces, un servidor samba (139), un servidor de correo (25) etc.

También se observan conexiones ssh desde la dirección 192.168.5.6, y conexiones utilizando el servicio de mail.

4.6.3. Salida de lsof

lsof es un comando cuya idea es similar a la de ps, excepto en que muestra qué ficheros/etc están abiertos, lo cual puede incluir sockets de red. Salida lsof | less.

COMMAND	PID	USER	FD	TYPE	DEVICE	SIZE	NODE	NAME
squid	10155	root	cwd	DIR	8,3	4096	1077447	/usr/libexec/webmin/squid
squid	10155	root	rtd	DIR	8,3	4096	2	/
squid	10155	root	txt	REG	8,3	632080	562255	/usr/sbin/squid
squid	10155	root	mem	REG	8,3	82944	568258	/usr/lib/libgssapi_krb5.so.2.2
squid	10155	root	mem	REG	8,3	79576	131591	/lib/libresolv-2.3.4.so
squid	10155	root	mem	REG	8,3	63528	560888	/usr/lib/libz.so.1.2.1.2
squid	10155	root	mem	REG	8,3	47851	131584	/lib/tls/librt-2.3.4.so
squid	10155	root	mem	REG	8,3	94480	131577	/lib/tls/libpthread-2.3.4.so
squid	10155	root	mem	REG	8,3	95320	131583	/lib/libnsl-2.3.4.so
squid	10155	root	mem	REG	8,3	179139	131580	/lib/tls/libm-2.3.4.so
squid	10155	root	mem	REG	8,3	45868	130354	/lib/libnss_files-2.3.4.so
squid	10155	root	mem	REG	8,3	7004	130401	/lib/libcom_err.so.2.1
squid	10155	root	mem	REG	8,3	15384	131579	/lib/libdl-2.3.4.so
squid	10155	root	mem	REG	8,3	933408	131592	/lib/libcrypto.so.0.9.7a
squid	10155	root	mem	REG	8,3	102447	131575	/lib/ld-2.3.4.so
squid	10155	root	mem	REG	8,3	136016	568256	/usr/lib/libk5crypto.so.3.0
squid	10155	root	mem	REG	8,3	27231	131588	/lib/libcrypt-2.3.4.so
squid	10155	root	mem	REG	8,3	213600	131593	/lib/libssl.so.0.9.7a
squid	10155	root	mem	REG	8,3	1454835	131576	/lib/tls/libc-2.3.4.so
squid	10155	root	mem	REG	8,3	415188	568257	/usr/lib/libkrb5.so.3.2
squid	10155	root	0u	CHR	1,3		1598	/dev/null
squid	10155	root	1u	CHR	1,3		1598	/dev/null
squid	10155	root	2u	CHR	1,3		1598	/dev/null
squid	10155	root	3u	unix	0xe8e00780		388128	socket

Este ejemplo muestra que se tiene ejecutándose a Squid, se muestra tambien que existe una conexión abierta con www.emac.gov.ec.

4.6.4. Protección del Servidor Apache http

El Servidor Apache HTTP es uno de los servicios más estables y seguros que se entregan con Red Hat Enterprise Linux. Hay una cantidad impresionante de opciones y técnicas disponibles para asegurar el Servidor Apache HTTP. demasiadas para verlas en profundidad.

A continuación se detalla una lista con las opciones de configuración que los administradores deberían tener mucho cuidado cuando las usen.

FollowSymLinks: Esta directiva está activada por defecto, por lo tanto tenga cuidado al crear enlaces simbólicos al documento raíz del servidor Web. Por ejemplo, es una mala idea proporcionar un enlace simbólico a /.

Indexes: Esta directiva está activada por defecto, pero puede que no sea recomendable. Si no desea que los usuarios hojeen los archivos en el servidor, es mejor que elimine esta directiva.

UserDir: UserDir está desactivada por defecto porque puede confirmar la presencia de una cuenta de usuario en el sistema. Si desea activar la navegación del directorio del usuario en el servidor, utilice las directivas siguientes:

UserDir enabled
UserDir disabled root

Estas directivas activan la navegación del directorio del usuario para todos los directorios de usuarios excepto /root. Si desea añadir usuarios a la lista de cuentas deshabilitadas, añada una lista de usuarios delimitada por espacios en la línea UserDir disabled.

IncludesNoExec: Por defecto, el servidor contiene módulos que no pueden ejecutar comandos. No se recomienda modificar esta configuración a menos que tenga la necesidad real de hacerlo, puesto que potencialmente habilita a que un atacante pueda ejecutar comandos en el sistema.

Asegurar directorios ejecutables: Asegúrese de que solamente asigna permisos de escritura al usuario root para cualquier directorio que contenga scripts o CGIs. Esto se puede lograr mediante llos siguientes comandos:

chown root
directory_name
+ chmod 755
directory_name
+

4.6.5. Protección de FTP

El *Protocolo de transferencia de archivos* o *FTP*, es un protocolo de TCP antiguo diseñado para transferir archivos sobre la red. Debido a que todas las transacciones con el servidor no son encriptadas, incluyendo la autenticación de usuarios, se considera un protocolo inseguro y debería ser configurado cuidadosamente.

Red Hat Enterprise Linux proporciona tres servidores FTP.

.gssftpd. Un demonio FTP kerberizado basado en xinetd que no pasa información de autenticación sobre la red.

. **Red Hat Content Accelerator** (tux) . Un servidor Web con espacio kernel que posee capacidades de FTP.

.vsftpd. Una implementación de servicio FTP independiente y orientado a la seguridad.

Antes de suministrar un nombre de usuario y contraseña, a todos los usuarios se les presenta una pancarta de saludo. Por defecto, esta pancarta incluye información relacionada con la versión, lo que es útil para los maleantes informáticos que estén intentando averiguar las debilidades del sistema. Para cambiar la pancarta de bienvenida para vsftpd, añada la directiva siguiente a /etc/vsftpd/vsftpd.conf:

ftpd_banner= <mensaje de bienvenida>

4.6.6 Protección de Sendmail

Sendmail es un Agente de transporte de correos (MTA) que utiliza el protocolo de transporte de correos simple (Simple Mail Transport Protocol, SMTP) para entregar mensajes electrónicos entre otros MTA y a los clientes de correo o agentes de entrega. Aún cuando muchos MTAs son capaces de encriptar el tráfico entre unos y otros, la mayoría no lo hacen, por tanto el envío de correos electrónicos sobre redes públicas es considerado una forma insegura de comunicación.

Se recomienda que cualquiera que esté planeando implementar un servidor Sendmail, tenga en cuenta los siguientes problemas

4.6.6.1. Limitar los Ataques de Rechazo de Servicio (DoS)

Debido a la naturaleza del correo electrónico, un atacante determinado puede inundar fácilmente el servidor con correos y de esta manera causar un rechazo de servicio. Se puede limitar la efectividad de tales ataques mediante la colocación de límites a las siguientes directrices en /etc/mail/sendmail.mc.

. confCONNECTION_RATE_THROTTLE . El número de conexiones que el servidor puede recibir por segundo. Por defecto, Sendmail no limita el número de conexiones. Si se establece un límite y este es alcanzado, las conexiones siguientes son retrasadas.

. confMAX_DAEMON_CHILDREN. El máximo número de procesos hijo que se pueden producir por el servidor. Por defecto, Sendmail no asigna un límite al número de procesos hijos. Si se coloca un límite y este es alcanzado, las conexiones siguientes son retrasadas.

. confMIN_FREE_BLOCKS. El número mínimo de bloques libres que debe haber disponible para que el servidor acepte correos. Por defecto es 100 bloques.

. confMAX_HEADERS_LENGTH . El tamaño máximo aceptable (en bytes) para la cabecera de un mensaje.

. confMAX_MESSAGE_SIZE. El tamaño máximo aceptable (en bytes) para cualquier mensaje.

Para ayudar a prevenir explotaciones del usuario local en el servidor Sendmail, es mejor para los usuarios de correo electrónico solamente accedan al servidor Sendmail usando un programa de correo. No deberían permitirse las cuentas shell en el servidor de correo y todos los usuarios shell en el archivo /etc/passwd deberían ser colocados a /sbin/nologin.

4.6.6.2. Verificar cuáles puertos están escuchando: Una vez que haya configurado los servicios en la red, es importante poner atención sobre cuáles puertos están escuchando en realidad en las interfaces de red del sistema. Cualquier puerto abierto puede ser una evidencia de una intrusión.

Existen dos soluciones básicas para listar cuales puertos están escuchando en la red. La solución menos confiable es consultar la pila de la red tipeando comandos tales como netstat -an o lsof

-i. Este método es menos confiable puesto que estos programas no conectan a la máquina desde la red, sino más bien verifican qué está ejecutándose en el sistema.

Por esta razón, estas aplicaciones son objetivos frecuentes de atacantes para reemplazarlas. De esta forma, los crackers intentan cubrir sus rastros si abren puertos no autorizados.

Una forma más confiable de verificar qué puertos están escuchando en la red es usar un escaner de puertos tal como nmap.

El comando siguiente ejecutado desde la consola, determina cuáles puertos están escuchando por conexiones TCP desde la red:

Starting nmap 3.70 (http://www.insecure.org/nmap/) at 2007-02-13 16:27 ECT
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1647 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
111/tcp open rpcbind
139/tcp open netbios-ssn
143/tcp open imap
443/tcp open https
445/tcp open microsoft-ds
631/tcp open ipp
953/tcp open rndc
10000/tcp open snet-sensor-mgmt
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7)
Uptime 7.320 days (since Tue Feb 6 08:47:05 2007)
Nmap run completed -- 1 IP address (1 host up) scanned in 2.245 seconds

Para verificar si el puerto está asociado con la lista oficial de servicios conocidos, se utiliza el siguiente comando:

cat /etc/services | grep (número del servicio)

Este comando no devuelve ninguna salida. Esto indica que aunque el puerto está en el rango reservado (es decir del 0 al 1023) y requiere acceso root para ser abierto, no está asociado con un servicio conocido.

El comando lsof revela información similar puesto que es capaz de enlazar puertos abiertos a servicios:

lsof -i | grep 631

[root@mail ~]# lsof -i |grep 631
cupsd 26982 root 0u IPv4 515631 TCP localhost.localdomain:ipp (LISTEN)
squid 27226 squid 17u IPv4 763182 TCP mail.emac.gov.ec:webcache->192.168.6.1:1519 (ESTABLISHED)

Estas herramientas pueden revelar mucha información sobre el estado de los servicios ejecutándose en la máquina. Estas herramientas son flexibles y pueden proporcionar gran cantidad de información sobre los servicios de red y la

configuración. Se recomienda la revisión de las páginas man para lsof, netstat, nmap, y services.

4.6.7. Cortafuegos

Las implementaciones de seguridad estándar usualmente emplean alguna forma de mecanismo dedicado para controlar los privilegios de acceso y restringir los recursos de la red a los usuarios autorizados, identificables y localizables. Red Hat Enterprise Linux incluye muchas herramientas poderosas para asistir a los administradores con los problemas de control de acceso al nivel de la red.

4.6.7.1 Descripción general de iptables

El poder y flexibilidad de Netfilter es implementado a través de la interfaz de iptables. Esta herramienta de línea de comandos es similar en sintaxis a su predecesor, ipchains; sin embargo, iptables utiliza el subsistema Netfilter para mejorar la conexión de la red, inspección y procesamiento; mientras que ipchains usa conjuntos de reglas intrincados para filtrar rutas de fuentes

El primer paso en el uso de iptables es iniciar el servicio iptables. Esto se puede llevar a cabo con el comando:

Los servicios ip6tables deberían ser desactivados para utilizar el servicio iptables con los siguientes comandos:

service iptables start
service ip6tables stop
chkconfig ip6tables off

Para hacer que iptables se inicie por defecto cada vez que se arranca el sistema, debe cambiar el estado del nivel de ejecución en el servicio usando chkconfig.

chkconfig --level 345 iptables on

La sintaxis de iptables está separada en niveles. El nivel principal es la *cadena*. Una cadena específica el estado en el cual se puede manipular un paquete. El uso es como se muestra a continuación:

iptables -A *chain* -j *target*

La -A anexa una regla al final de un conjunto de reglas existente. La *chain* es el nombre de la cadena para una regla. Las tres cadenas embebidas de iptables(esto es, las cadenas que afectan cada paquete que atraviesa la red) son INPUT, OUTPUT, y FORWARD. Estas cadenas son permanentes y no se pueden borrar.
Las nuevas cadenas (también conocidas como cadenas definidas por el usuario) se pueden crear usando la opción -N. Es útil crear una nueva cadena para la personalización granulada o para crear reglas más elaboradas.

4.6.7.2. Políticas básicas del Cortafuegos

Establecer algunas políticas básicas desde el comienzo pueden servir como una base para la construcción de reglas más detalladas definidas por el usuario. iptables utiliza políticas (-P) para crear reglas por defecto. Los administradores orientados a la seguridad usualmente eligen descartar todos los paquetes como una política y solamente permiten paquetes específicos basados en el caso. Las
reglas siguientes bloquean todo los paquetes entrantes y salientes en una puerta de enlace de red.

iptables -P INPUT DROP
iptables -P OUTPUT DROP

Adicionalmente, se recomienda que cualquier *paquete redirigido* . el tráfico de la red que se debe enrutar desde el cortafuegos a su nodo destino . también se niegue, para restringir a los clientes internos de una exposición inadvertida a la Internet. Para hacer esto, utilice la regla siguiente:

iptables -P FORWARD DROP

Después de configurar las cadenas de políticas, puede crear las nuevas reglas para su red y requerimientos de seguridad particulares. Las secciones siguientes resaltan algunas reglas que puede implementar en el curso de la construcción de su cortafuegos iptables.

4.6.7.3. Filtros comunes de iptables

El mantener a los atacantes remotos fuera de la LAN es un aspecto importante de la seguridad de la red, o quizás el *más* importante. La integridad de una LAN

debería ser protegida de usuarios remotos maliciosos a través del uso de reglas del cortafuegos rigurosas. Sin embargo, con una política por defecto configurada para bloquear todos los paquetes entrantes, salientes y redirigidos, es imposible para el cortafuegos/puerta de enlace y los usuarios internos de la LAN comunicarse entre ellos o con recursos externos. Para permitir a los usuarios realizar funciones relacionadas a la red y utilizar las aplicaciones de la red, los administradores deben abrir ciertos puertos para la comunicación.

Por ejemplo, para permitir el acceso al puerto 80 *en el cortafuegos*, añada la siguiente regla:

```
iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
```

Esto permite la navegación web normal desde los sitios web que se comunican a través del puerto 80. Para permitir el acceso a sitios web seguros (tales como https://www.example.com/), se debe abrir el puerto 443 también.

```
iptables -A INPUT -p tcp -m tcp --sport 443 -j ACCEPT
iptables -A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
```

Hay muchas veces en que se requiere el acceso remoto a la LAN desde fuera de la LAN. Se puede utilizar un servicio seguro, tal como SSH, para encriptar conexiones remotas a los servicios LAN. Se puede configurar iptables para aceptar conexiones desde clientes SSH remotos.

```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p udp --sport 22 -j ACCEPT
```

4.6.7.4. Reglas FORWARD y NAT

La mayoría de las organizaciones se les asigna un número limitado de direcciones IP públicas enrutables desde sus ISP. Debido a esta limitación en la asignación, los administradores deben buscar formas creativas de compartir el acceso a los servicios de Internet sin otorgar las limitadas direcciones IP públicas a todos los nodos en la LAN. El uso de direcciones IP privadas es la forma común de permitir a

todos los nodos en una LAN acceder apropiadamente a los servicios de redes internos y externos. Los enrutadores en las puntas de la red (tales como cortafuegos), pueden recibir las transmisiones entrantes desde la Internet y enrutar los paquetes al nodo objetivo en la LAN; al mismo tiempo los cortafuegos/puertas de enlace pueden enrutar peticiones salientes desde un nodo LAN al servicio Internet remoto. Este reenvío del tráfico de la red se puede volver peligroso a veces, especialmente con la disponibilidad de herramientas modernas para violar redes que pueden engañar direcciones IP *internas* y hacer que la máquina remota del atacante actúe como un nodo en su propia LAN. Para prevenir esto, iptables proporciona políticas de enrutamiento y reenvío que se pueden implementar para prevenir el uso inadecuado de los recursos de la red.

La política FORWARD permite al administrador controlar donde se enviaran los paquetes dentro de una LAN. Por ejemplo, para permitir el reenvío a la LAN completa (asumiendo que el cortafuegos/puerta de enlace tiene una dirección IP interna en eth1), se pueden configurar las reglas siguientes:

```
iptables -A FORWARD -i eth1 -j ACCEPT
iptables -A FORWARD -o eth1 -j ACCEPT
```

Esta regla dá a los sistemas detrás del cortafuegos/puerta de enlace acceso a la red interna. La puerta de enlace enruta los paquetes desde un nodo de la LAN hasta su nodo destino, pasando todos los paquetes a través del dispositivo eth1.

Por defecto, la política IPv4 en los kernels Red Hat Enterprise Linux desactivan el soporte para el reenvío IP, lo cual previene que las cajas ejecutando Red Hat Enterprise Linux funcionen como enrutadores de bordes de la red dedicados. Para activar el reenvío IP, ejecute el comando siguiente:

```
sysctl -w net.ipv4.ip_forward=1
```

Si este comando se ejecuta a través del indicador de comandos, entonces este valor no se recuerda luego de un reinicio. Puede configurar el reenvío de forma permanente modificando el archivo

```
/etc/sysctl.conf
```

Modificar línea siguiente, reemplazando 0 con 1:

net.ipv4.ip_forward = 0

Activar el cambio al archivo sysctl.conf:
sysctl -p /etc/sysctl.conf
El aceptar paquetes reenviados a través del dispositivo interno IP interno del cortafuegos permite a los nodos LAN comunicarse entre ellos; sin embargo, no se les permite comunicarse externamente (por ejemplo, a la Internet). Para permitir a los nodos de la LAN que tengan una dirección IP privada comunicarse con redes públicas externas, configure el cortafuegos para el *enmascaramiento IP*, lo cual coloca máscaras en las peticiones desde los nodos LAN con la dirección IP del dispositivo externo del cortafuegos (en este caso, eth0):

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

La regla utiliza la tabla de coincidencias de paquetes NAT (-t nat) y específica la cadena incorporada de POSTROUTING para NAT (-A POSTROUTING) en el dispositivo de red externo del cortafuegos (-o eth0). POSTROUTING permite la alteración de los paquetes a medida que dejan el dispositivo externo del cortafuegos. Se específica el objetivo de -j MASQUERADE para enmascarar la dirección IP privada de un nodo con la dirección IP del cortafuegos/puerta de enlace.
Si tiene un servidor en su red interna que desea colocar disponible de forma externa, puede utilizar el objetivo -j DNAT de la cadena PREROUTING en NAT para especificar una dirección IP destino y un puerto donde se pueden reenviar los paquetes entrantes solicitando una conexión a su servicio interno. Por ejemplo, si desea reenviar las peticiones HTTP entrantes a su sistema servidor ServidorApache HTTP dedicado en 200.55.228.162, ejecutar el comando siguiente

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT \
--to 200.55.228.162:80

Esta regla especifica que la tabla NAT utiliza la cadena incorporada PREROUTING para reenviar las peticiones HTTP entrantes exclusivamente a la dirección IP listada 200.55.228.162

Si tiene una política por defecto de DROP en su cadena FORWARD, debe anexar una regla para permitir el reenvío de peticiones HTTP entrantes para que sea posible el enrutamiento NAT. Para lograr esto, ejecute el comando siguiente:

iptables -A FORWARD -i eth0 -p tcp --dport 80 -d 200.55.228.162 -j ACCEPT
Esta regla permite el reenvio de peticiones HTTP entrantes desde el cortafuegos a su servidor Servidor Apache HTTP destino detrás del cortafuegos.

4.6.7.5. Seguimiento de conexiones

Iptables incluye un módulo que permite a los administradores inspeccionar y restringir conexiones a servicios disponibles en una red interna conocido como *seguimiento de conexiones*. El seguimiento de conexiones almacena las conexiones en una tabla, lo que permite a los administradores otorgar o negar acceso basado en los siguientes estados de conexiones:

. NEW. Un paquete solicitando una nueva conexión, tal como una petición HTTP.
. ESTABLISHED. Un paquete que es parte de una conexión existente.
. RELATED. Un paquete que está solicitando una nueva conexión pero que es parte de una conexión existente, tal como las conexiones FTP pasivas donde el puerto de conexión es 20, pero el puerto de transferencia puede ser cualquiera desocupado más allá del puerto 1024.
. INVALID . Un paquete que no forma parte de ninguna conexión en la tabla de seguimiento de conexiones.
Puede utilizar la funcionalidad de vigilancia continua de seguimiento de conexiones de iptables con un protocolo de red, aún si el protocolo mismo es sin supervisión (tal como UDP). El ejemplo siguiente muestra una regla que utiliza el seguimiento de conexiones para reenviar solamente paquetes que esten asociados con una conexión establecida:

iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ALLOW

CAPITULO V

Esta parte proporciona una vista general de la teoría y práctica de evaluaciones de seguridad.

Con el tiempo suficiente y los recursos un intruso puede violar casi cualquier sistema todos los procedimientos de seguridad y la tecnología disponible actualmente no pueden garantizar que los sistemas estén seguros de un ataque.

Sin embargo, el éxito de cada una de estas tecnologías depende de un número de variables, como la experiencia del personal responsable de la configuración, supervisión y mantenimiento de las tecnologías, la habilidad de remendar y actualizar servicios y kernels rápida y eficientemente, la responsabilidad de mantener vigilancia constante sobre la red.

5. Evaluación de la seguridad

5.1 Respuesta a incidentes de seguridad.

En el evento de que la seguridad de un sistema haya sido comprometida, se requiere una *respuesta rápida a incidentes*. Es la responsabilidad del equipo de seguridad responder rápida y efectivamente a los problemas.

Una respuesta a incidentes es una reacción acelerada a un problema. Con respecto a la seguridad de la información incidente es la violación de la seguridad. La respuesta depende de cómo el equipo de seguridad reaccione, qué acciones toman para reducir los daños y cuándo reestablecen los recursos, todo esto mientras intentan garantizar la integridad de los datos.

Toda empresa depende de la tecnología y de los sistemas de computación. Si hay un problema, existe una potencial pérdida de tiempo y de recursos, por lo que es muy importante contar con un *plan de respuestas a incidentes*, soportarlo a lo largo de la Empresa y probarlo regularmente. Un buen plan de respuestas a incidentes puede minimizar los efectos de una violación.

El aspecto positivo de entender la inevitabilidad de una violación a los sistemas es que permite al equipo de seguridad desarrollar un curso de acciones para minimizar los daños potenciales. Combinando un curso de acciones con la experiencia le permite al equipo responder a condiciones adversas de una manera formal y oportuna. El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata para detener o minimizar el incidente
- Investigación del incidente
- Restauración de los recursos afectados
- Reporte del incidente a los canales apropiados

Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

Un plan de respuesta a incidentes tiene un número de requerimientos, que incluye:

. Un e*quipo de respuesta a emergencias:* El *Equipo de respuestas a emergencias de computación* debe estar preparado para actuar rápidamente en el evento de una catástrofe computacional. El concepto de personal adecuado va mucho más allá de la experiencia técnica e incluye logísticas tales como ubicación, disponibilidad y el deseo de poner a la organización más allá de la vida personal cuando surge una emergencia.

Una emergencia nunca es planeada, puede ocurrir en cualquier momento y todos los miembros del equipo deben estar dispuestos a aceptar la responsabilidad que les es requerida para responder a una emergencia a cualquier hora.

Los administradores de sistemas proporcionarán el conocimiento y la experiencia de los recursos del sistema, incluyendo respaldo de los datos, hardware de respaldo disponible para ser usado; asi como, proporcionarán su conocimiento de protocolos de redes y la habilidad de redirigir el tráfico de la red.

El personal encargado de la seguridad de la información es útil para hacer un seguimiento detallado de los problemas de seguridad así como también llevar a cabo análisis *port-mortem* de los sistemas en peligro.

Se debe también tener en cuenta que si sólo una persona tiene la llave a la seguridad e integridad de los datos, entonces la empresa completa estará desamparada si la persona está ausente.

. Una estrategia legal revisada y aprobada: Otros aspectos importantes a considerar en una respuesta a incidentes son los aspectos legales.

Los planes de seguridad deberían ser desarrollados con miembros del equipo de asesoría jurídica. De la misma forma en que cada compañía debería tener su propia política de seguridad corporativa, cada compañía tiene su forma particular de manejar incidentes desde la perspectiva legal.

Se deben también tener en cuenta ciertos aspectos importantes como:

- Soporte financiero
- Soporte ejecutivo de alto nivel
- Recursos físicos, tal como almacenamiento redundante, sistemas de replica y servicios de respaldo

5.2. Implementación de un Plan de respuestas a incidentes

Una vez creado un plan de acción, este debe ser aceptado e implementado activamente. Cualquier aspecto del plan que sea cuestionado durante la implementación activa lo más seguro es que resulte en un tiempo de respuesta pobre y tiempo fuera de servicio en el evento de una violación. Aquí es donde los ejercicios prácticos son invalorables. La implementación del plan debería ser acordada entre todas las partes relacionadas y ejecutada con seguridad, a menos que se llame la atención con respecto a algo antes de que el plan sea colocado en producción.

Si se detecta una violación mientras el equipo encargado está presente para una respuesta rápida, las acciones potenciales pueden variar. El equipo puede decidir

sacar las conexiones de red, desconectar los sistemas afectados, reparar la violación y luego reconectar rápidamente sin mayor complicación. El equipo puede también observar a los autores y hacer un seguimiento de sus acciones. El equipo puede inclusive redirigir a los autores a un *pote de miel* . un sistema o segmento de la red conteniendo intencionalmente datos falsos . usado para poder seguir la pista de la incursión de forma segura y sin interrupciones a los recursos de producción.
La respuesta a incidentes debe ir acompañada con recolección de información siempre que esto sea posible. Los procesos en ejecución, conexiones de red, archivos, directorios y mucho más debería ser auditado activamente en tiempo real. Puede ser muy útil tener una toma instantánea de los recursos de producción al hacer un seguimiento de servicios o procesos maliciosos.

El personal encargado de la seguridad del sistema debe estar entrenado con el fin de detectar cualquier anomalía en el sistema, deben conocer que procesos deben estarse ejecutando y verificar si hay algún proceso ajeno, mediante top o ps. Los administradores de la red estan conscientes de cómo se vé el tráfico normal de la red cuando se ejecuta snort o tcpdump. Estos miembros del equipo deberían conocer sus sistemas y ser capaces de notar una anomalía más rápido que cualquier otra persona que no esté familiarizadacon la infraestructura.

5.3. Detección de eventos de seguridad

Investigar una violación de sistemas es como investigar la escena de un crimen. Se debe reunir la evidencia, seguir cualquier pista extraña y hacer un inventario de las pérdidas y daños. Un análisis de un sistema en peligro se puede llevar a cabo mientras el ataque está ocurriendo o después del ataque.

Aún cuando es imprudente contar y confiar en cualquier archivo de registro de un sistema atacado, existen otras utilidades forenses para asistirlo en su análisis. El propósito y características de estas utilidades varían, pero normalmente crean copias imágenes de la media, correlacionan eventos y procesos, muestran información del sistema de bajo nivel y recuperan datos borrados siempre que sea posible.

Es también una buena idea registrar todas las acciones de investigación ejecutadas en un sistema comprometido, usando el comando script y guardar el archivo de registro en un lugar diferente al disco duro del sistema atacado.

5.3.1 Recopilación de una imagen de la evidencia

Es recomendable hacer dos copias de una imagen de bits una para análisis e investigación y otra para ser almacenada con la evidencia original para cualquier procedimiento legal.

Se puede utilizar el comando dd que es parte del paquete coreutils en Red Hat Enterprise Linux para crear una imagen monolítica de un sistema explotado como evidencia en una investigación o para comparar con copias confiables.

Si existe un sólo disco duro en un sistema del cual se desea hacer una imagen, se debe conectar esa unidad como un esclavo a su sistema y luego utilice el comando dd para crear el archivo imagen, como se muestra a continuación:

dd if=/dev/hdd bs=1k conv=noerror,sync of=/home/evidence/image1

Este comando crea un archivo único llamado image1 usando un tamaño de bloque de 1k para velocidad. Las opciones conv=noerror,sync obligan a dd a continuar leyendo y descargando datos aún si se encuentran sectores dañados en la unidad sospechosa. Ahora si es posible estudiar el archivo de imagen resultante o hasta intentar recuperar archivos borrados.

5.3.2. Recopilación de información luego de la violación

Red Hat Enterprise Linux es una plataforma excelente para realizar análisis de violaciones de seguridad, pues incluye muchas utilidades para restauración y respuesta luego de una violación.

5.3.3 Comandos útiles para auditoría:

En el siguiente cuadro se detalla algunos de los comandos para auditoría y administración de archivos con ejemplos; los mismos que pueden ser usados para identificar archivos y sus atributos (tales como permisos y fechas de acceso) para que así pueda reunir evidencia adicional de items de análisis.

Estas herramientas, cuando se combinan con sistemas de detección de intrusos, cortafuegos, servicios reforzados y otras medidas de seguridad, lo pueden ayudar a reducir los daños potenciales cuando ocurre un ataque.

COMANDO	FUNCION	EJEMPLO
dd	Crea una copia de imagen de bits (o *descarga del disco*) de los archivos y particiones. Combinado con una verificación md5sums de cada imagen, los administradores pueden comparar una imagen de la partición antes de la violación con una imagen del sistema ya violentado para verificar si las sumas coinciden.	dd if=/bin/ls of=ls.dd|md5sum ls.dd >ls-sum.txt
grep	Encuentra información de texto útil dentro de archivos y directorios así como también revela permisos, cambios de script, atributos de archivos y más. Se usa comúnmente como un comando entubado con otro comando tal como ls, ps o ifconfig.	ps auxw |grep /bin
strings	Imprime las cadenas de caracteres imprimibles en un archivo. Es muy utilizado para auditoría de archivos ejecutables tales como comandos mail a direcciones desconocidas o el registro a archivos de registro que no son estándar	strings /bin/ps |grep 'mail'
file	Determina las características de archivos basados en formato,codificación, bibliotecas que enlaza (si hay alguna) y el tipo de archivo (binario, de texto, etc). Es muy útil para determinar si un archivo ejecutable tal como /bin/ls ha sido modificado usando bibliotecas estáticas, las cuales son una señal segura de que un ejecutable ha sido reemplazado con otro instalado por un usuario malicioso.	file /bin/ls
find	Busca en directorios por archivos particulares. Es una herramienta útil para revisar la estructura de directorios por palabras clave, fecha y hora de acceso, permisos, etc. Esto puede ser de gran ayuda a los administradores que realizan auditorías generales de sistemas de directorios o archivos particulares.	find -atime +12 -name *log* -perm u+rw
stat	Despliega información varia sobre un archivo, incluyendo la última vez que este fue accesado, permisos, configuraciones del bit de UID y GID, etc. Es muy útil para verificar cuando fue la última vez que un ejecutable de un sistema violado fue modificado o usado	stat /bin/netstat
md5sum	Calcula la suma de verificación de 128 bit usando el algoritmo tipo hash md5. Puede usar el comando para crear un archivo de texto que liste todos los archivos ejecutables cruciales que son a menudo modificados o reemplazados durante un ataque de seguridad. Redirige las sumas a un archivo para crear una base de datos simple de sumas de verificación y luego copia el archivo a una media de sólo lectura tal como un CD-ROM.	md5sum /usr/bin/gdm>>md5sum.txt

5.3.4 Restauración y recuperación de recursos

Mientras la respuesta a incidentes está en progreso, el equipo encargado debería estar investigando al mismo tiempo que trabajando en función de la recuperación

de los datos y el sistema. Depende del tipo de daño que ha provocado para el proceso de recuperación. Tener sistemas redundantes o respaldos de datos fuera de línea, es invalorable durante estos momentos.

Para recuperar sistemas, el equipo de respuestas debe colocar en funcionamiento cualquier sistema caído o aplicaciones, tales como servidores de autenticación, servidores de bases de datos y cualquier otro recurso de producción.

Se recomienda tener hardware de respaldo de producción listo para ser usado, tales como discos duros extra, servidores de respuesto en caliente, y otros similares. Los sistemas ya listos deberían tener todo el software de producción cargado y listo para uso inmediato. Quizás sólo los datos más recientes e importantes necesitarán ser importados. Estos sistemas ya hechos deberían ser mantenidos aislados del resto de la red. Si un ataque ocurre y los sistemas de respaldo son parte de la red, entonces se frusta el propósito de tener un sistema de respaldo.

La recuperación de un sistema puede ser un proceso tedioso. En muchas ocasiones hay dos cursos de acción a partir de los cuales escoger. Los administradores pueden llevar a cabo una reinstalación limpia del sistema operativo en cada sistema afectado seguido de la restauración de todos los datos y aplicaciones. Alternativamente, los administradores pueden remendar el sistema de la vulnerabilidad y volverlo a poner en producción.

5.3.5. Reinstalación del sistema

Al realizar una reinstalación limpia se asegura que el sistema afectado estará limpio de cualquier troyano, puertas traseras o procesos maliciosos. La reinstalación también asegura que cualquier dato esté limpio de cualquier modificación maliciosa. La desventaja de una reinstalación total del sistema es el tiempo que implica reconstruir los sistemas desde el principio. Sin embargo, si hay disponible un sistema de respaldo en caliente donde la única acción a tomar es descargar los datos más recientes, entonces el tiempo fuera de servicio es reducido en gran medida.

5.3.6 Emparchar el sistema

El emparchado del sistema afectado es un curso de acción más peligroso y debería ser tomado con gran precaución. El riesgo con reparar un sistema en vez de llevar a cabo una reinstalación, es determinar si el sistema se ha limpiado lo suficiente de huecos, troyanos y datos dañados.

CAPITULO VI

6. Conclusiones Generales

Luego de realizado este trabajo se ha concluido lo siguiente:

- La seguridad ha dejado de ser un problema exclusivo de las áreas informáticas, de una organización en particular, y se ha convertido en una estrategias que abarca todas las áreas de las empresas con el fin de enfrentar de forma coordinada y cooperativa las amenazas y vulnerabilidades que se derivan del uso de las tecnologías.

- Día a día aparecen nuevos y complejos tipos de incidentes y/o amenazas, y aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las personas. En consecuencia, se requieren efectivas acciones de concienciación, capacitación y difusión de mejores prácticas de los usuarios a todo nivel.

- Con todo lo anterior, cuando menos, ciertas medidas de seguridad informática pueden darse por adoptadas. Nunca se puede creer que la seguridad perfecta existe pues siempre se estará expuesto a algún tipo de amenaza, pero lo importante es estar preparados para adoptar medidas preventivas y políticas de seguridad que impidan o minimicen una hecatombe.

- Es necesario adquirir conocimientos, metodologías y herramientas de implementación y control de medidas de seguridad de la información de acuerdo con estándares internacionales uno de ellos es la Norma ISO 27001

CAPITULO VII

7- Recomendaciones

Los programas de seguridad más eficaces son aquellos que cuentan con una participación activa desde dentro de la organización. Fuentes externas pueden proporcionar conocimientos y experiencia específica. No obstante, el programa de seguridad en sí debe ser dirigido y gestionado internamente.

La EMAC debe empezar por reconocer la importancia de la seguridad a alto nivel y asignar recursos adecuados para implementar los procedimientos con eficacia.

La Seguridad de la Información comienza a través de la planificación y apoyo de la alta Gerencia. El primer paso de este apoyo consiste en incluir la seguridad en los objetivos de un Plan Estratégico Institucional. Esto asegurará que los esfuerzos integrados de las personas responsables de la seguridad en la organización se canalicen hacia una objetivo común que sea realista, factible y apoyado adecuadamente por toda la estructura organizativa.

GLOSARIO

ISO 27001: Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual serán certificados por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última

Confidencialidad: Información accesible sólo a aquellas personas autorizadas a tener acceso.

Integridad: Exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: Acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

Recurso : Cualquier cosa que tenga valor para la organización

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas

Eventos de seguridad de la información: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

Incidente de seguridad: uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información

TCP/IP: (*Transmission Control Protocol/Internet Protocol*) Protocolo de control de transmisiones/protocolo Internet. Protocolos de comunicaciones desarrollados bajo contrato del Departamento de Defensa de los Estados Unidos para intercomunicar sistemas diferentes. Es un estándar UNIX de hecho, pero está respaldado por sistemas operativos de micro a mainframe. Es utilizado por muchas corporaciones y casi todas las universidades y entidades federales.

Telnet: Protocolo de emulación de terminales usado con frecuencia en Internet. Permite al usuario tener acceso a un programa y ejecutarlo desde un terminal o computador remote. Fue desarrollado originalmente por ARPAnet y es parte del protocolo de comunicación TCP/IP.

Proxy: Proxy Server, Servidor Proxy. También se le conoce como Proxy; es una aplicación que opera como barrera de fuego al interrumpir la conexión entre el emisor y el receptor. Toda la información de entrada es enviada a un puerto diferente, cerrando el camino directo entre dos redes, previniendo así que un intruso (hacker) pueda obtener direcciones internas y detalles acerca de una red privada.

Demonio: Es como un programa que permanece en segundo plano ejecutándose continuamente para dar algún tipo de servicio.

Host: En general, un host es un nodo de red, es decir, algo que es capaz de recibir y enviar algún tipo de mensajes en la red. Normalmente será un ordenador, pero puede ser también un terminal X o una impresora de red.

HTTP HiperText Transfer Protocol: Protocolo para Transferencia de HiperTexto. Es el protocolo que se utiliza para transmitir documentos de la WWW a los programas de usuario conocidos como navegadores.

BIBLIOGRAFIA

Iso Internacional Estándar Organization http://www.iso.org ,30/12/2006, 11h00 am

Normas de Seguridad Informática <http://iso27001.es>, 4/01/2007, 12h00

ICONTEC <www.icontec.com>, 3,4,5,6/01/2007,
http://sgsi-iso27001.blogspot.com/

http://www.tb-security.com/prens_artic.htm

RED HAT LINUX <http://www.redes-linux.com/manuales.php?catId=Correo%20(Servidor)> 5,6,7,8/02/2006

Red Hat Linux <https://www.redhat.com/apps/support> 7,8,9/02/2006

INDICE

CAPITULO IV

Configuración de Seguridades referentes al control de acceso en Red Hat Enterprise Linux en la Empresa Municipal de Aseo de Cuenca –EMAC-

CAPITULO V
Evaluación de la seguridad

CAPITULO VI

CAPITULO VII