

INDICE

<u>1</u>	<u>CRIPTOGRAFIA</u>	<u>1</u>
1.1	INTRODUCCIÓN A LA CRIPTOGRAFÍA	1
1.2	CRIPTOGRAFIA SIMETRICA VS. CLAVE PÚBLICA.	1
1.3	CONTROL DE ACCESO, AUTENTIFICACIÓN Y AUTORIZACION.	2
1.4	GESTION DE CLAVES	4
1.5	PKI. INFRAESTRUCTURAS DE CLAVE PÚBLICA	7
<u>2</u>	<u>SEGURIDAD EN NODOS Y REDES</u>	<u>8</u>
2.1	SEGURIDAD EN ENTORNOS WINDOWS	8
2.1.1	GESTIÓN DE USUARIOS	9
2.1.2	SERVICIOS DE DIRECTORIO	12
2.1.3	SISTEMA DE ARCHIVOS	13
2.1.4	SEGURIDAD DE SERVIDORES WEB	15
2.2	SEGURIDAD EN REDES WI-FI	16
<u>3</u>	<u>SEGURIDAD PERIMETRAL</u>	<u>20</u>
3.1	CORTAFUEGOS	20
3.1.1	TEORÍA SOBRE LOS CORTAFUEGOS	21
3.1.2	IPTABLES	24
3.2	REDES PRIVADAS VIRTUALES	32
3.2.1	INTRODUCCIÓN A LAS VPNs	34
3.2.2	LINUX (IPCop)	39
<u>4</u>	<u>AUDITORIA DE SEGURIDAD</u>	<u>43</u>
4.1	TÉCNICAS DE AUDITORÍA	44
4.2	TIPOS DE AUDITORÍA	45
4.3	FASES DE LA AUDITORÍA	47
4.4	INFORME DE AUDITORÍA	47

5	ANÁLISIS DE VULNERABILIDADES Y BITÁCORAS (LOGS)	50
5.1	ANÁLISIS DE VULNERABILIDADES	50
5.1.1	TIPOS DE VULNERABILIDADES	52
5.1.2	HERRAMIENTAS DE ANÁLISIS	53
5.1.3	GESTIÓN DE VULNERABILIDADES	54
5.2	ANÁLISIS DE BITÁCORAS	57
5.2.1	BITÁCORAS DE WEB, CORTAFUEGOS, ROUTERS, CORREO.	58
		60
5.2.2	FORMATOS	61
5.2.3	CENTRALIZACIÓN DE BITÁCORAS	61
5.2.4	HERRAMIENTAS PARA ANÁLISIS	62
6	MANEJO DE INCIDENTES DE SEGURIDAD	64
6.1	GESTIÓN DE INCIDENTES	64
6.2	GRUPOS DE RESPUESTA A INCIDENTES	65
6.3	DETECCIÓN Y ANÁLISIS	67
6.4	ELIMINACIÓN Y RECUPERACIÓN DEL INCIDENTE	71
6.5	INFORME DE INCIDENTES	73

1 CRIPTOGRAFIA

1.1 INTRODUCCIÓN A LA CRIPTOGRAFÍA

La criptografía actualmente se encarga del estudio de los algoritmos, protocolos y sistemas que se utilizan para dotar de seguridad a las comunicaciones, a la información y a las entidades que se comunican. El objetivo de la criptografía es diseñar, implementar, implantar, y hacer uso de sistemas criptográficos para dotar de alguna forma de seguridad. Por tanto el tipo de propiedades de las que se ocupa la criptografía son por ejemplo:

Confidencialidad. Es decir garantiza que la información está accesible únicamente a personal autorizado. Para conseguirlo utiliza códigos y técnicas de cifrado.

Integridad. Es decir garantiza la corrección y completitud de la información. Para conseguirlo puede usar por ejemplo funciones hash criptográficas MDC, protocolos de compromiso de bit, o protocolos de notaría electrónica.

No repudio. Es decir proporcionar protección frente a que alguna de las entidades implicadas en la comunicación, pueda negar haber participado en toda o parte de la comunicación. Para conseguirlo se puede usar por ejemplo firma digital. En algunos contextos lo que se intenta es justo lo contrario: Poder negar que se ha intervenido en la comunicación. Por ejemplo cuando se usa un servicio de mensajería instantánea y no queremos que se pueda demostrar esa comunicación. Para ello se usan técnicas como el cifrado negable.

Autenticación. Es decir proporciona mecanismos que permiten verificar la identidad del comunicante. Para conseguirlo puede usar por ejemplo función hash criptográfica MAC o protocolo de conocimiento cero.

Un sistema criptográfico es seguro respecto a una tarea si un adversario con capacidades especiales no puede romper esa seguridad, es decir, el atacante no puede realizar esa tarea específica.

1.2 CRIPTOGRAFIA SIMETRICA VS. CLAVE PÚBLICA.

La criptografía simétrica es un método en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican deben ponerse de acuerdo de antemano sobre la clave a utilizar. Una vez que ambos tienen esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Algunos ejemplos de algoritmos simétricos son DES, 3DES, RC5, AES, Blowfish e IDEA.

La criptografía asimétrica es el método que usa un par de claves para el envío de mensajes. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja

de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Algunos algoritmos y tecnologías de clave asimétrica son: Diffie-Hellman, RSA, DSA, ElGamal, criptografía de curva elíptica, Merkle-Hellman

1.3 CONTROL DE ACCESO, AUTENTIFICACIÓN Y AUTORIZACION.

Autenticación:

WEP proporciona dos tipos de autenticación: un sistema abierto, en el que todos los usuarios tienen permiso para acceder a la WLAN, y una autenticación mediante clave compartida, que controla el acceso a la WLAN y evita accesos no autorizados a la red. De los dos niveles, la autenticación mediante clave compartida es el modo seguro. En él se utiliza una clave secreta compartida entre todas las estaciones y puntos de acceso del sistema WLAN. Cuando una estación trata de conectarse con un punto de acceso, éste replica con un texto aleatorio, que constituye el desafío (challenge). La estación debe utilizar la copia de su clave secreta compartida para cifrar el texto de desafío y devolverlo al punto de acceso, con el fin de autenticarse. El punto de acceso descifra la respuesta utilizando la misma clave compartida y compara con el texto de desafío enviado anteriormente. Si los dos textos son idénticos, el punto de acceso envía un mensaje de confirmación a la estación y la acepta dentro de la red. Si la estación no dispone de una clave, o si envía una respuesta incorrecta, el punto de acceso la rechaza, evitando que la estación acceda a la red.

La autenticación mediante clave compartida funciona sólo si está habilitado el cifrado WEP. Si no está habilitado, el sistema revertirá de manera predeterminada al modo de sistema abierto (inseguro), permitiendo en la práctica que cualquier estación que esté situada dentro del rango de cobertura de un punto de acceso pueda conectarse a la red. Esto crea una ventana para que un intruso penetre en el sistema, después de lo cual podrá enviar, recibir, alterar o falsificar mensajes. Es bueno asegurarse de que WEP está habilitado siempre que se requiera un mecanismo de autenticación seguro. Incluso, aunque esté habilitada la autenticación mediante clave compartida, todas las estaciones inalámbricas de un sistema WLAN pueden tener la misma clave compartida, dependiendo de cómo se haya instalado el sistema. En tales redes, no es posible realizar una autenticación individualizada; todos los usuarios, incluyendo los no autorizados, que dispongan de la clave compartida podrán acceder a la red. Esta debilidad puede tener como resultado accesos no autorizados, especialmente si el sistema incluye un gran número de usuarios. Cuantos más usuarios haya, mayor será la probabilidad de que la clave compartida pueda caer en manos inadecuadas.

Control de acceso a red (del inglés NAC) es un enfoque de la seguridad en redes de computadoras que intenta unificar la tecnología de seguridad en los equipos finales (tales como antivirus, prevención de intrusión en hosts, informes de vulnerabilidades), usuario o sistema de autenticación y reforzar la seguridad de la red.

Autenticación de red

Debido a la posibilidad de escuchar los paquetes que circulan por la red, es importante que no se transmitan passwords sin encriptar por ella. Pero el hecho de enviar las contraseñas encriptados plantea el problema de la comunicación de las claves. Uno de los servicios que usan autenticación de red es el de RPC. Algunas aplicaciones que usan este servicio son Admintool y NIS+[Sun90b]. Las modalidades de autenticación que se pueden usar en Solaris 2 son:

AUTH_NONE	Sin autenticación
AUTH_SYS	Identificación basada en el NetID
AUTH_DES	Usa autenticación DES
AUTH_KERB	Autenticación <i>Kerberos</i>

Las características de seguridad que incluyen cada una de ellas son las siguientes:

Autenticación DES. Usa el estándar de encriptación DES y criptografía de llave pública para llevar a cabo la autenticación de usuarios y sistemas. En el sistema de criptografía de llave pública el cliente y el servidor obtienen una clave común denominada de conversación. El servidor deduce la clave conversación combinando la clave pública del cliente con su clave privada y viceversa. El cliente establece sus claves públicas y privadas usando el comando keylogin, como root. Un usuario, normalmente, lo lleva a cabo de forma transparente cada vez que accede al sistema.

Autenticación Kerberos. Este sistema de autenticación fue desarrollado por el MIT dentro del proyecto Athena. Usa autenticación DES para encriptar unas etiquetas que se asignan cuando se accede al sistema. Duran un cierto periodo de tiempo, por defecto 8 horas. La clave debe mostrarse cada vez que el usuario accede a ficheros.

Autorización.

La autorización de acceso a una red se concede o se deniega según las directivas de red y las propiedades de marcado de las cuentas de usuario de Active Directory® que se configuran en el Servidor de directivas de redes (NPS).

Las directivas de red permiten conceder o denegar el acceso a la red a usuarios y equipos pertenecientes a grupos de Windows, mientras que la configuración del permiso de acceso a la red definido en las propiedades de marcado de cada cuenta de usuario en los Servicios de dominio de Active Directory (AD DS) permite conceder o denegar el acceso a la red para usuarios individuales. Además, AD DS permite designar la concesión del permiso de acceso a la red en función de la configuración de la directiva de red.

Cuando diseñe el esquema de autorización, debe determinar si decide administrar la autorización por usuario o por grupo.

Autorización por usuario

Si administra la autorización por usuario, defina el permiso de acceso a la red para la cuenta de usuario o equipo en Conceder acceso o Denegar acceso y, si lo desea, cree diversas directivas de red según los diferentes tipos de conexión.

Por ejemplo, es posible que desee crear una directiva de red para conexiones de red privada virtual (VPN) y una directiva de red diferente para conexiones inalámbricas.

La administración de una autorización por usuario se recomienda sólo cuando tiene un número reducido de cuentas de usuario o equipo para administrar.

Si administra la autorización por usuario, el proceso básico que usa NPS para autorizar una solicitud de conexión es el siguiente:

- Si NPS encuentra que la solicitud de conexión se ajusta a todas las condiciones de la directiva de red, comprueba la configuración del permiso de acceso a la red de la cuenta de usuario.
- Si la configuración del permiso de acceso a la red de la cuenta de usuario está definida para conceder acceso, NPS aplica la configuración de la conexión de la cuenta de usuario y la directiva de red a la conexión, que se concede.
- Si la configuración del permiso de acceso a la red de la cuenta de usuario está definida para denegar el acceso, NPS rechaza la solicitud de conexión.
- Si la solicitud de conexión no se ajusta a todas las condiciones de la primera directiva de red, NPS procesa la directiva de red siguiente.
- Si la solicitud de conexión no se ajusta a todas las condiciones de ninguna directiva de red, NPS rechaza la solicitud de conexión.

1.4 GESTION DE CLAVES

Abarca la generación, distribución, almacenamiento, tiempo de vida, destrucción y aplicación de las claves de acuerdo con una política de seguridad.

Generación de claves

La seguridad de un algoritmo descansa en la clave. Un criptosistema que haga uso de claves criptográficamente débiles será él mismo débil. Algunos aspectos a considerar que se presentan a la hora de la elección de las claves son:

Espacio de claves reducido

Cuando existen restricciones en el número de bits de la clave, o bien en la clase de bytes permitidos (caracteres ASCII, caracteres alfanuméricos, imprimibles, etc.), los ataques de fuerza bruta con hardware especializado o proceso en paralelo pueden desbaratar en un tiempo razonable estos sistemas.

Elección pobre de la clave

Cuando los usuarios eligen sus claves, la elección suele ser muy pobre en general (por ejemplo, el propio nombre o el de la mujer), haciéndolas muy débiles para un ataque de fuerza bruta que primero pruebe las claves más obvias (ataque de diccionario).

Claves aleatorias

Claves buenas son las cadenas de bits aleatorios generadas por medio de algún proceso automático (como una fuente aleatoria fiable o un generador pseudo-aleatorio criptográficamente seguro), de forma que si la clave consta de 64 bits, las 264 claves posibles sean igualmente probables. En el caso de los criptosistemas de clave pública, el proceso se complica, ya que a menudo las claves deben verificar ciertas propiedades matemáticas (ser primos dos veces seguros, residuos cuadráticos, etc.).

Distribución de claves

Sin duda alguna, el problema central de todo sistema de gestión de claves lo constituyen los procedimientos de distribución de éstas. Esta distribución debe efectuarse previamente a la comunicación. Los requisitos específicos en cuanto a seguridad de esta distribución dependerán de para qué y cómo van a ser utilizadas las claves. Así pues, será necesario garantizar la identidad de su origen, su integridad y, en el caso de claves secretas, su confidencialidad.

Las consideraciones más importantes para un sistema de gestión de claves son el tipo de ataques que lo amenazan y la arquitectura del sistema. Normalmente, es necesario que la distribución de claves se lleve a cabo sobre la misma red de comunicación donde se está transmitiendo la información a proteger. Esta distribución es automática y la transferencia suele iniciarse con la petición de clave por parte de una entidad a un Centro de Distribución de Claves (intercambio centralizado) o a la otra entidad involucrada en la comunicación (intercambio directo). La alternativa es una distribución manual (mediante el empleo de correos seguros, por ejemplo), independiente del canal de comunicación. Esta última alternativa implica un alto coste económico y un tiempo relativamente largo para llevarse a cabo, lo que la hace descartable en la mayoría de las situaciones. La distribución segura de claves sobre canal inseguro requiere protección criptográfica y, por tanto, la presencia de otras claves, conformando una jerarquía de claves. En cierto punto se requerirá protección no criptográfica de algunas claves (llamadas maestras), usadas para intercambiar con los usuarios de forma segura las claves que usarán en su(s) futura(s) comunicación(es). Entre las técnicas y ejemplos no criptográficos podemos citar seguridad física y confianza.

La distribución de claves se lleva siempre a cabo mediante protocolos, es decir, secuencias de pasos de comunicación (transferencia de mensajes) y pasos de computación. Muchas de las propiedades de estos protocolos dependen de la estructura de los mensajes intercambiados y no de los algoritmos criptográficos subyacentes. Por ello, las debilidades de estos protocolos provienen normalmente de errores cometidos en los niveles más altos del diseño.

Las claves criptográficas temporales usadas durante la comunicación, llamadas claves de sesión, deben ser generadas de forma aleatoria. Para protegerlas será necesaria seguridad física o cifrado mediante claves maestras, mientras que para evitar que sean modificadas deberá utilizarse seguridad física o autenticación. La autenticación hace uso de parámetros como time-stamps y contadores para protegerse también contra la reactivación con antiguas claves.

Almacenamiento de claves

En sistemas con un solo usuario, la solución más sencilla pasa por ser su retención en la memoria del usuario. Una solución más sofisticada y que desde luego funcionará mejor para claves largas, consiste en almacenarlas en una tarjeta de banda magnética, en una llave de plástico con un chip ROM (ROM key) o en una tarjeta inteligente, de manera que el usuario no tenga más que insertar el dispositivo empleado en alguna ranura a tal efecto para introducir su clave.

Otra manera de almacenar claves difíciles de recordar es en forma encriptada mediante una clave fácil de recordar, como por ejemplo almacenar en disco la clave privada RSA cifrada mediante una clave DES.

Tiempo de vida de claves

Una clave nunca debería usarse por tiempo indefinido. Debe tener una fecha de caducidad, por las siguientes razones:

- Cuanto más tiempo se usa una clave, aumenta la probabilidad de que se comprometa (la pérdida de una clave por medios no criptoanalíticos se denomina compromiso).
- Cuanto más tiempo se usa una clave, mayor será el daño si la clave se compromete, ya que toda la información protegida con esa clave queda al descubierto.
- Cuanto más tiempo se usa una clave, mayor será la tentación de alguien para intentar desbaratarla.
- En general es más fácil realizar criptoanálisis con mucho texto cifrado con la misma clave.

Para protocolos orientados a conexión, una elección obvia es usar la misma clave de sesión durante la duración de la comunicación, siendo descartada al finalizar la comunicación y nunca reutilizada. Si la conexión lógica posee una vida muy larga, sería prudente en este caso cambiar la clave de sesión periódicamente, por ejemplo cada vez que el número de secuencia de la PDU completa un ciclo.

Para protocolos no orientados a conexión, no existe un inicio o fin de sesión explícitos. Por lo tanto, no resulta tan obvio con qué frecuencia debería cambiarse la clave. Con el fin de no recargar la información de control ni retrasar la transacción, una estrategia válida sería usar una clave de sesión durante un cierto período o para un cierto número de transacciones.

Las claves maestras no necesitan ser reemplazadas tan frecuentemente, ya que se usan ocasionalmente para el intercambio de claves. En cualquier caso, no hay que olvidar que si una clave maestra se

compromete, la pérdida potencial es enorme, de hecho, todas las comunicaciones cifradas con claves intercambiadas con esa clave maestra.

En el caso del cifrado de grandes ficheros de datos, una solución económica y segura, mejor que andar descifrando y volviendo a cifrar los ficheros con una nueva clave todos los días, sería cifrar cada fichero con una única clave y después cifrar todas las claves con una clave maestra, que deberá ser almacenada en un lugar de alta seguridad, ya que su pérdida o compromiso echaría a perder la confidencialidad de todos los ficheros.

Destrucción de claves

Las claves caducadas deben ser destruidas con la mayor seguridad, de modo que no caigan en manos de un adversario, puesto que con ellas podría leer los mensajes antiguos. En el caso de haber sido escritas en papel, éste deberá ser debidamente destruido; si habían sido grabadas en una EEPROM, deberá sobrescribirse múltiples veces, y si se encontraba en EPROM, PROM o tarjeta de banda magnética, deberán ser hechas añicos (muy pequeñitos, a poder ser). En función del dispositivo empleado, deberá buscarse la forma de que se vuelvan irrecuperables.

1.5 PKI. INFRAESTRUCTURAS DE CLAVE PÚBLICA

Es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia y a veces confusa, al uso de algoritmos de clave pública en comunicaciones electrónicas. Este último significado es incorrecto, ya que no se requieren métodos específicos de PKI para usar algoritmos de clave pública.

2 SEGURIDAD EN NODOS Y REDES

2.1 Seguridad en entornos Windows

Al Instalar un Sistema Operativo Windows por defecto les pide activar las Actualizaciones Automáticas [Siendo el Caso de que el S.O no sea legal la mayoría de usuarios las desactivan]

Esto es un grave error ya que un Sistema sin actualizar es un blanco fácil para intrusiones informáticas;

¿Porque? Porque si un sistema no está actualizado con sus Parches, Cualquier virus o cualquier otro programa indeseado que se aprovecha de una Vulnerabilidad de este S.O tomara el control total del mismo.

¿En que nos puede afectar si llegan a infectarnos? Pues en mucho ya que eso compromete su seguridad en la red y en el equipo, cualquier dato o información que en este se encuentra podrá estar a la disposición de la persona que maneja el Virus o Troyano.

¿Cómo puedo saber si estoy infectado? Actualmente hay muchas maneras de saberlo Windows tiene herramientas que ayudan a saber eso.

Algunas de esas herramientas son:

- Administrador de Tareas.
- MsConfig.
- Consola de comandos (CMD).

También se pueden usar herramientas que no vienen con el S.O y que en la mayoría de los casos son mas sofisticadas.

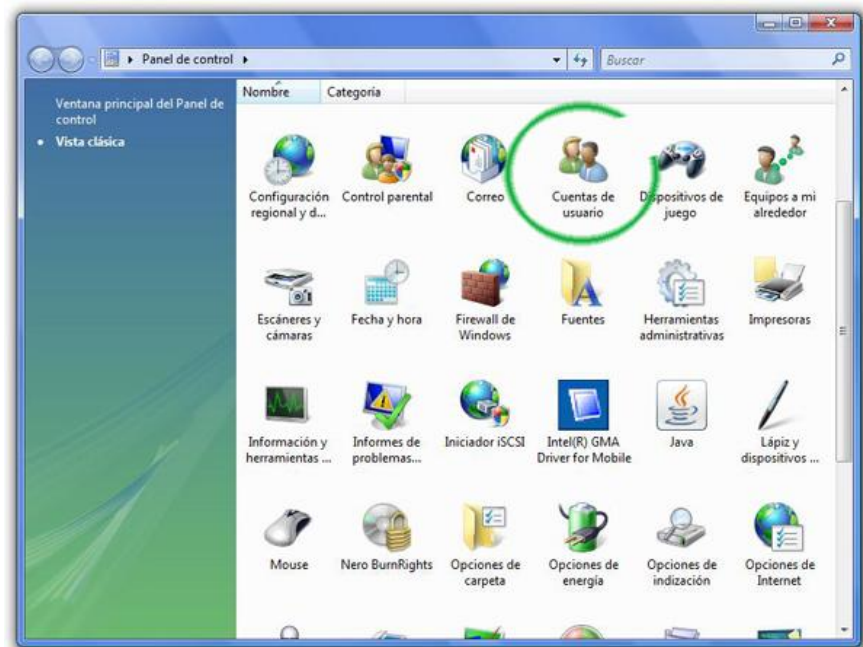
Alguna de estas son los " Sniffer " que sirven para ver todo el tráfico de la RED

¿Que recomendaciones nos harías? Principalmente les recomendaría si no tienen un Windows Original y pueden adquirirlo háganlo. sino en la RED hay muchos activadores y no me refiero a programas que saltan la activación o la borran. Sino a loader que instalan certificados OEM y deja " legal " el Equipo y que pueda bajar todas las actualizaciones.

2.1.1 Gestión de usuarios

Gestión de usuarios en Windows XP

La gestión de usuarios en Windows XP es un proceso realmente sencillo. Todas las opciones necesarias las encontraremos en la opción `Cuentas de Usuario`, dentro de nuestro `Panel de Control`.



Desde esta ventana es desde donde realizaremos toda la gestión de usuarios de Windows XP. A continuación vamos a hacer nuestro Windows XP un poco más seguro, siguiendo unos sencillos pasos.

Desactivar la cuenta de invitado

Lo primero que debemos hacer es desactivar la cuenta de invitado, pues no queremos que nadie más que los usuarios registrados accedan a nuestro ordenador. Para eso pulsamos sobre el icono de la cuenta de invitado, y entre las opciones que nos aparecen seleccionamos `desactivar cuenta de invitado`.

Creando una nueva cuenta de administrador

A continuación vamos a crear una cuenta de administrador con la que llevar a cabo todas las tareas propias como instalar/desinstalar programas. Tan sencillo como esto.

Pulsamos sobre la opción `Crear una cuenta nueva`.

En la siguiente pantalla introducimos el nombre que deseamos darle a la nueva cuenta.

Tras poner el nombre, Windows nos pregunta el tipo de cuenta que queremos crear, Administrador o Limitada. Elegimos la primera y finalizamos.

Limitar los permisos de nuestra cuenta

El siguiente paso será limitar los permisos de nuestra cuenta de usuario, la cual si usábamos la configuración por defecto de Windows XP, tendría permisos de administrador.

Pulsamos sobre el icono de nuestra cuenta.

Seleccionamos la opción `Cambiar el tipo de cuenta`.

Pasamos de cuenta de administrador a cuenta limitada y cerramos. No so preocupéis por las advertencias de compatibilidad con programas antiguos, pues la mayoría de programas actuales trabajan perfectamente con distintos usuarios.

Estableciendo contraseñas

Todavía debemos ponerle una contraseña a nuestra cuenta de administrador, pues de lo contrario ¿para que querríamos tener separadas las cuentas, cuando cualquiera podría acceder libremente a los privilegios del admin. Para eso nada más fácil que pulsar sobre el icono de la nueva cuenta de administrador, y en la ventana siguiente seleccionar `Establecer contraseña`.

Establecer una para vuestra cuenta limitada dependerá de vosotros mismos. En general, si el ordenador lo utilizáis sólo vosotros, no es necesario proteger esta cuenta, aunque mucho mejor prevenir que curar. Si compartes el ordenador con otras personas, es más que recomendable utilizar una contraseña. También es recomendable crear una cuenta por persona, de forma que cada usuario del sistema tenga su propio directorio privado donde guardar sus documentos, sólo accesible por él mismo y el administrador. Una ventaja más de utilizar esta gestión de usuarios.

Cambiar la forma en la que los usuarios inician la sesión

Ya tenemos nuestros usuarios creados y, para concluir solo nos faltan unos detalles que, si bien no son necesarios, simplificarán la forma en la que utilizaremos el sistema. Para ello, desde la ventana principal de gestión de usuarios, seleccionaremos la opción `Cambiar la forma en la que los usuarios inician o cierran la sesión`.

Desde ahí podremos acceder a otras dos opciones, `Usar pantalla de bienvenida` y `Usar cambio rápido de usuario`. La primera nos presentará una pantalla con los iconos de nuestras cuentas al encender el sistema, mientras la segunda permite que cambiemos de usuario sin cerrar sesión en la cuenta en la que nos encontremos (realmente útil).

Con esto, hemos concluido nuestra tarea de gestión de usuarios en Windows XP. ¿A que no ha sido nada complicado? El siguiente punto lo dedicaré a contar un poco como manejarnos con nuestras recién creadas cuentas.

Trabajando con nuestra nueva cuenta limitada

Para comenzar a trabajar con nuestra recién creada cuenta limitada tan solo tenemos que ir al menú inicio, y seleccionar la opción `Cerrar Sesión`. Si todo ha salido bien, Windows nos debería presentar nuestra nueva pantalla de bienvenida, con tantos iconos como cuentas de usuarios hayamos creado. Pulsamos sobre nuestra cuenta limitada, introducimos la contraseña si fuera necesario, y en unos segundos estaremos dentro.

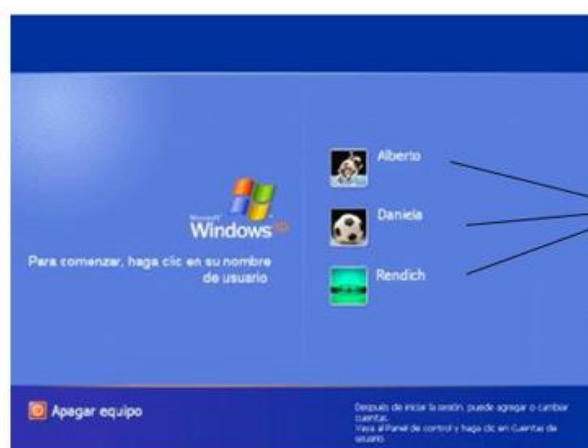
A primera vista no debéis notar ninguna diferencia, pero hay unas cuantas importantes. Para empezar podéis probar a instalar algún programa, para ver como el sistema os tira para atrás durante la instalación, para recordaros que no tenéis permisos de administrador. Luego podéis abrir el explorador de archivos, ir a vuestro disco duro, y localizar la carpeta `Documents and Settings`. Allí es donde se guarda la carpeta privada de cada usuario. Intentad entrar a la del administrador y veréis como no os lo permite.

Ahora vamos a probar el cambio rápido de usuario para intentar lo mismo desde la cuenta de administrador. Para ello vamos seleccionamos nuevamente `Cerrar Sesión`, nos aparecerá una ventana con dos opciones, `Cambiar de usuario` o `Cerrar Sesión`. Seleccionamos la primera, y nos transportan a la pantalla de bienvenida. Desde ahí seleccionamos la cuenta de administrador, repetimos las pruebas, y vemos que tenemos permiso para cualquier cosa.

La ventaja del cambio rápido de usuario sobre cerrar sesión es que no se cierran los programas que tuviéramos abiertos al cambiar de cuenta. De esa forma es mucho más cómodo realizar las tareas administrativas. Ahora bien, ¿es necesario abrir la cuenta de administrador cada vez que necesitemos instalar un programa? Ni siquiera.

Para instalar un programa desde nuestra cuenta limitada podemos seleccionar el ejecutable, y pulsar el botón derecho de nuestro ratón. Entre las opciones disponibles, veremos una nueva denominada `Ejecutar como`, que nos permitirá ejecutar un programa como un usuario distinto al de nuestra cuenta.

Seleccionamos
El



Iconos de
cuentas de
quienes utilizan
el ordenador

ejecutar como
siguiente

usuario, introducimos los datos de nuestro administrador, y el programa será instalado como si lo estuviera haciendo el administrador.

2.1.2 Servicios de directorio

Un servicio de directorio es un servicio de red que nos identifica todos y cada uno de los recursos que la misma nos ofrece y los hace disponibles para usuarios y aplicaciones. Es un servicio muy importante que nos proporciona una vía de información sobre el nombre, descripción, localización, acceso, gestión y seguridad sobre dichos recursos.

Así cuando un usuario busque un recurso en la red, será el servicio de directorio el que identificará el recurso y le dé la información al usuario.

En Windows Server 2003 el servicio de directorio se llama **Active Directory**, conocido como AD, que además de las funcionalidades conocidas de un servicio de directorio añade otras muy interesantes y beneficiosas, como:

- su integración con el Servidor de Nombres de Dominio (DNS), al usarlo para su estructura jerárquica.
- su organización en secciones capaces de albergar un gran número de objetos. Como resultado puede expandirse al mismo ritmo que crece la organización.
- su facilidad de administración centralizada, donde permite a los administradores a distribuir escritorios, servicios de red o aplicaciones desde un lugar central, mientras se usa un interfaz de administración estable. También ofrece el control centralizado de accesos a los recursos de la red.
- su facilidad de delegar la administración dentro de su estructura jerárquica a aquellos segmentos específicos de la jerarquía que se quiera.

Los componentes de la estructura de AD son los siguientes:

1. **Dominio** (*Domain*). La unidad central o núcleo de la estructura del Directorio Activo es el dominio. Una colección de equipos, definido por un administrador, que comparte la base de datos de directorio común. Un dominio tiene un nombre único y provee acceso a las cuentas de usuario y grupos mantenidos por el administrador del dominio.
2. **Unidad Organizativa** (*Organizational Unit, OU*). Una Unidad organizativa es un tipo de contenedor de objetos que se utiliza para organizarlos dentro del dominio. Puede contener objetos como cuentas de usuario, de grupos, equipos, impresoras, y otras OU's.
3. **Bosque** (*Forest*). Un bosque se compone de uno o más dominios, los cuales comparten una configuración común, esquema y Catálogo Global.
4. **Árbol** (*Tree*). El árbol consiste en dominios de un bosque que comparten un espacio de nombres DNS contiguo.

2.1.3 Sistema de archivos

Los sistemas de archivo estructuran la información guardada en una [unidad de almacenamiento](#) (normalmente un [disco duro](#) de una [computadora](#)), que luego será representada ya sea textual o gráficamente utilizando un [gestor de archivos](#). La mayoría de los [sistemas operativos](#) manejan su propio sistema de archivos.

Lo habitual es utilizar dispositivos de almacenamiento de datos que permiten el acceso a los datos como una cadena de bloques de un mismo tamaño, a veces llamados sectores, usualmente de 512 [bytes](#) de longitud (También denominados clústers). El [software](#) del sistema de archivos es responsable de la organización de estos sectores en archivos y directorios y mantiene un registro de qué sectores pertenecen a qué archivos y cuáles no han sido utilizados. En la práctica, un sistema de archivos también puede ser utilizado para acceder a datos generados dinámicamente, como los recibidos a través de una conexión de [red](#) (sin la intervención de un dispositivo de almacenamiento).

Los sistemas de archivos tradicionales proveen métodos para crear, mover, renombrar y eliminar tanto archivos como directorios, pero carecen de métodos para crear, por ejemplo, enlaces adicionales a un directorio o archivo ([enlace duro](#) en Unix) o renombrar enlaces padres (". ." en Unix).

El acceso seguro a sistemas de archivos básicos puede estar basado en los esquemas de [lista de control de acceso](#) o capacidades. Las listas de control de acceso hace décadas que demostraron ser inseguras, por lo que los sistemas operativos experimentales utilizan el acceso por capacidades. Los sistemas operativos comerciales aún funcionan con listas de control de acceso.

Rutas y nombre de archivos

La estructura de directorios suele ser jerárquica, ramificada o "en árbol", aunque en algún caso podría ser plana. En algunos sistemas de archivos los nombres de archivos son estructurados, con sintaxis especiales para [extensiones de archivos](#) y números de versión. En otros, los nombres de archivos son simplemente cadenas de texto y los [metadatos](#) de cada archivo son alojados separadamente.

En los sistemas de archivos jerárquicos, usualmente, se declara la ubicación precisa de un archivo con una cadena de texto llamada "[ruta](#)" —o *path* en inglés—. La nomenclatura para rutas varía ligeramente de sistema en sistema, pero mantienen por lo general una misma estructura. Una ruta viene dada por una sucesión de nombres de directorios y subdirectorios, ordenados jerárquicamente de izquierda a derecha y separados por algún carácter especial que suele ser una diagonal ('/') o diagonal invertida (\) y puede terminar en el nombre de un archivo presente en la última rama de directorios especificada.

Ejemplo de 'ruta' en un sistema Unix

Así, por ejemplo, en un sistema tipo Unix como [GNU/Linux](#), la ruta para la canción llamada "La canción.ogg" del usuario "álvaro" sería algo como

/home/Álvaro/Mi música/La canción.[ogg](#)

donde:

- '/' representa el directorio **raíz** donde está montado todo el sistema de archivos.
- '**home/álvaro/Mi música/**' es la ruta del archivo.
- '**La canción.ogg**' es el *nombre* del archivo.

que se establece como único.

Ejemplo de 'ruta' en un sistema Windows

Un ejemplo análogo en un sistema de archivos de [Windows](#) (específicamente en [Windows XP](#)) se vería como:

C:\Documents and Settings\Álvaro\Mis Documentos\Mi Música\canción.mp3

donde:

- '**C:**' es la unidad de almacenamiento en la que se encuentra el archivo.
- '**\Documents and Settings\Álvaro\Mis Documentos\Mi Música**' es la ruta del archivo.
- '**canción**' es el *nombre* del archivo.
- '**.mp3**' es la [extensión del archivo](#), este elemento, parte del nombre, es especialmente relevante en los sistemas [Microsoft Windows](#), ya que sirve para identificar qué tipo de archivo es y la aplicación que está asociada con el archivo en cuestión, es decir, con qué programa se puede editar o reproducir el archivo. Para la mayoría de los sistemas operativos modernos la extensión del archivo es un complemento burocrático solo útil para la observación del usuario, ya que los entornos de administración de archivos y aplicaciones varias, analizan la información contenida en el principio del interior del archivo (MIME headers) para determinar su función o asociación, la cual normalmente esta catalogada en la tabla [MIME](#) Content-Type en el sistema.

Resumen de características de los sistemas de Archivos

- Seguridad o [permisos](#)
 - [listas de control de acceso](#) (ACLs)
 - UGO (Usuario, Grupo, Otros, o por sus siglas en [inglés](#), *User, Group, Others*)
 - Capacidades granuladas
 - Atributos extendidos (ej.: sólo añadir al archivo pero no modificar, no modificar nunca, etc.)
- Mecanismo para evitar la [fragmentación](#)
- Capacidad de enlaces [simbólicos](#) o [duros](#)
- Integridad del sistema de archivos ([Journaling](#))
- Soporte para archivos dispersos
- Soporte para cuotas de discos
- Soporte de crecimiento del sistema de archivos nativo

Tipo de sistemas de archivos

Sistemas de archivos de disco

Un sistema de archivo de disco está diseñado para el almacenamiento de archivos en una unidad de disco, que puede estar conectada directa o indirectamente a la computadora.

Sistemas de archivos de red

Un sistema de archivos de red es el que accede a sus archivos a través de una [red](#). Dentro de esta clasificación encontramos dos tipos de sistemas de archivos: los sistemas de archivos distribuidos (no proporcionan E/S en paralelo) y los sistemas de archivos paralelos (proporcionan una E/S de datos en paralelo).

Sistemas de archivos de propósito especial

(Special purpose file system). Aquellos tipos de sistemas de archivos que no son ni sistemas de archivos de disco, ni sistemas de archivos de red. Ejemplos: acme (Plan 9), archfs, cdfs, cfs, devfs, udev, ftpfs, lnfs, nntdfs, plumber (Plan 9), procfs, ROMFS, swap, sysfs, TMPFS, wikifs, LUFS, etc.

2.1.4 Seguridad de servidores Web

La seguridad de servidores Web

Las aplicaciones Web, por definición, permiten el acceso de usuarios a recursos centrales, el servidor Web y, a través de éste, a otros como los servidores de base de datos.

Con los conocimientos y la implementación correcta de medidas de seguridad, se pueden proteger los recursos así como proporcionar un entorno seguro donde los usuarios trabajen cómodos con su aplicación.

Una aplicación Web, especialmente una que se despliega en Internet, es un objetivo mucho más atractivo para un atacante que una aplicación autónoma o cliente-servidor típica. Hay varias razones para esto:

- Disponibilidad y accesibilidad: Muchas aplicaciones Web están disponibles para los usuarios públicos en cualquier momento del día o de la noche. Como los servidores Web tienen que permitir el acceso a usuarios públicos y no tienen la protección completa de los cortafuegos típicos de una empresa.
- Familiaridad: La mayoría de los atacantes, incluso los menos sofisticados, conocen las interfaces Web. Un navegador Web es fácil de obtener y es uno de los programas de aplicación más comunes. El protocolo HTTP está bien definido, y existen muchas herramientas de hacking creadas específicamente para ayudar a los atacantes a penetrar y comprometer aplicaciones Web.
- Facilidad: La configuración de un servidor Web, contenedor Web y aplicación Web para uso público es extremadamente compleja. Los atacantes, frecuentemente, pueden aprovechar esta complejidad y explotar deficiencias en la configuración de la aplicación o del sistema.
- Publicidad: El aliciente de algunos atacantes experimentados es la publicidad, la fama, el ego o un simple deseo de probar que pueden hacer algo que pocas otras personas pueden hacer. Desfigurar o comprometer un sitio Web popular tiene mucho más valor desde la perspectiva de las “relaciones públicas” que comprometer una aplicación interna que utilizan unos cuantos empleados corporativos.

2.2 Seguridad en redes Wi-Fi

Asegurar el Punto de Acceso:

1. Cambia la contraseña por defecto.

- Todos los fabricantes establecen un password por defecto de acceso a la administración del Punto de Acceso.

Al usar un fabricante la misma contraseña para todos sus equipos, es fácil o posible que *el observador* la conozca.

[!] *Evita contraseñas como tu fecha de nacimiento, el nombre de tu pareja, etc. Intenta además intercalar letras con números.*

Aumentar la seguridad de los datos transmitidos:

2. Usa encriptación WEP/WPA.

- Activa en el Punto de Acceso la encriptación WEP. Mejor de 128 bits que de 64 bits... cuanto mayor sea el número de bits mejor.

Los Puntos de Acceso más recientes permiten escribir una *frase* a partir de la cual se generan automáticamente las claves. Es importante que en esta frase intercales mayúsculas con minúsculas y números, evites utilizar palabras incluidas en el diccionario y secuencias contiguas en el teclado (como "qwerty", "fghjk" o "12345").

También tendrás que establecer en la configuración WEP la clave que se utilizará de las cuatro generadas (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

Después de configurar el AP tendrás que configurar los accesorios o dispositivos Wi-Fi de tu red. En éstos tendrás que marcar la misma clave WEP (posiblemente puedas utilizar la *frase* anterior) que has establecido para el AP y la misma clave a utilizar (*Key 1*, *Key 2*, *Key 3* o *Key 4*).

- Ya hemos visto que con algunos programas y el suficiente tiempo pueden obtenerse estas claves. En cualquier caso si el observador encuentra una red sin encriptación y otra con encriptación, preferirá "investigar" la primera en vez de la segunda.
- Algunos Puntos de Acceso más recientes soportan también encriptación WPA (Wi-Fi Protected Access), encriptación dinámica y más segura que WEP.

Si activas WPA en el Punto de Acceso, tanto los accesorios y dispositivos WLAN de tu red como tu sistema operativo deben soportarlo (Palm OS por el momento no y para Windows XP es necesario instalar una actualización).

Ocultar tu red Wi-Fi:

3. Cambia el SSID por defecto.

- Suele ser algo del estilo a "default", "wireless", "101", "linksys" o "SSID".

En vez de "MiAP", "APManolo" o el nombre de la empresa es preferible escoger algo menos atractivo para *el observador*, como puede ser "Broken", "Down" o "Desconectado".

Si no llamamos la atención de *el observador* hay menos posibilidades de que éste intente entrar en nuestra red.

4. Desactiva el broadcasting SSID.

- El broadcasting SSID permite que los nuevos equipos que quieran conectarse a la red Wi-Fi identifiquen automáticamente los datos de la red inalámbrica, evitando así la tarea de configuración manual.

Al desactivarlo tendrás que introducir manualmente el SSID en la configuración de cada nuevo equipo que quieras conectar.

[!] Si el observador conoce nuestro SSID (por ejemplo si está publicado en alguna web de acceso libre) no conseguiremos nada con este punto.

Evitar que se conecten:

5. Activa el filtrado de direcciones MAC.

- Activa en el AP el filtrado de direcciones MAC de los dispositivos Wi-Fi que actualmente tengas funcionando. Al activar el filtrado MAC dejarás que sólo los dispositivos con las direcciones MAC especificadas se conecten a tu red Wi-Fi.

[!] Por un lado es posible conocer las direcciones MAC de los equipos que se conectan a la red con tan sólo "escuchar" con el programa adecuado, ya que las direcciones MAC se transmiten "en abierto", sin encriptar, entre el Punto de Acceso y el equipo.

Además, aunque en teoría las direcciones MAC son únicas a cada dispositivo de red y no pueden modificarse, hay comandos o programas que permiten simular temporalmente por software una nueva dirección MAC para una tarjeta de red.

6. Establece el número máximo de dispositivos que pueden conectarse.

- Si el AP lo permite, establece el número máximo de dispositivos que pueden conectarse al mismo tiempo al Punto de Acceso.

7. Desactiva DHCP.

- Desactiva DHCP en el router ADSL y en el AP.

En la configuración de los dispositivos/accesorios Wi-Fi tendrás que introducir a mano la dirección IP, la puerta de enlace, la máscara de subred y el DNS primario y secundario.

[!] Si el observador conoce "el formato" y el rango de IPs que usamos en nuestra red, no habremos conseguido nada con este punto.

Para los más cautelosos:

8. Desconecta el AP cuando no lo uses.

- Desconecta el Punto de Acceso de la alimentación cuando no lo estés usando o no vayas a hacerlo durante una temporada. El AP almacena la configuración y no necesitarás introducirla de nuevo cada vez que lo conectes.

9. Cambia las claves WEP regularmente.

- Por ejemplo semanalmente o cada 2 ó 3 semanas.

Antes decíamos que existen aplicaciones capaces de obtener la clave WEP de nuestra red Wi-Fi analizando los datos transmitidos por la misma. Pueden ser necesarios entre 1 y 4 Gb de datos para romper una clave WEP, dependiendo de la complejidad de las claves.

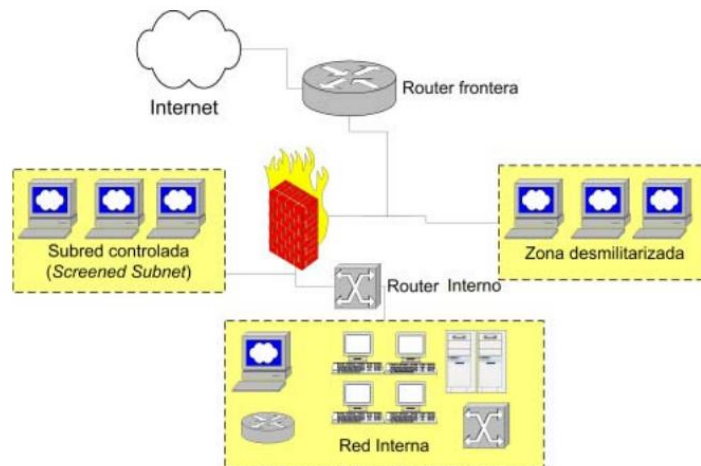
Cuando lleguemos a este caudal de información transmitida es recomendable cambiar las claves.

Recuerda que tendrás que poner la misma clave WEP en el Punto de Acceso y en los dispositivos que se vayan a conectar a éste.

3 Seguridad perimetral

La seguridad informática se encarga de proteger la información, más específicamente, podemos definir que lo logrará preservando su confidencialidad, disponibilidad, integridad, autenticidad.

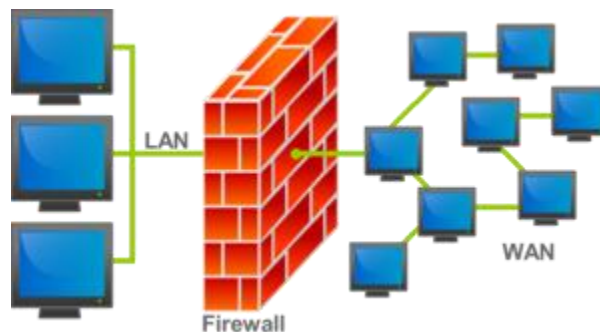
La mayoría de las empresas sufren la problemática de seguridad debido a sus necesidades de acceso y conectividad.



3.1 Cortafuegos

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.



Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets.

Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuego, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada «zona desmilitarizada» o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

3.1.1 Teoría sobre los cortafuegos

Hay diferentes tipos de servidores de seguridad en función de que la comunicación se lleva a cabo, donde se intercepta la comunicación y el Estado que se realiza un seguimiento.

Capa o paquete de filtros de red

Firewalls de capa de red, también llamada filtros de paquetes, operan a un nivel relativamente bajo del TCP/IP protocol stack, no permitiendo que los paquetes pasen a través del firewall a no ser que coincida con el conjunto de reglas establecidas. El administrador del servidor de seguridad puede definir las reglas, o se puede aplicar reglas predeterminadas. El término "filtro de paquetes" se originó en el contexto de BSD sistemas operativos.



Firewalls de capa de red generalmente se dividen en dos subcategorías, con estado y sin estado. Firewalls mantienen contexto sobre las sesiones activas, y el uso que "la información de estado" para acelerar el procesamiento de paquetes. Cualquier conexión de red existente puede ser descrito por varias propiedades, incluyendo direcciones de origen y destino IP, UDP o puertos TCP, y la etapa actual de la vida de la conexión (incluida la iniciación de sesión, toma de contacto, datos de la transferencia o conexión de terminación). Si el paquete no coincide con una conexión existente, se evalúa de acuerdo con el conjunto de reglas para las nuevas conexiones. Si un paquete coincide con una conexión existente con base en la comparación con la tabla de estado del servidor de seguridad, se le permite pasar a su estado natural.

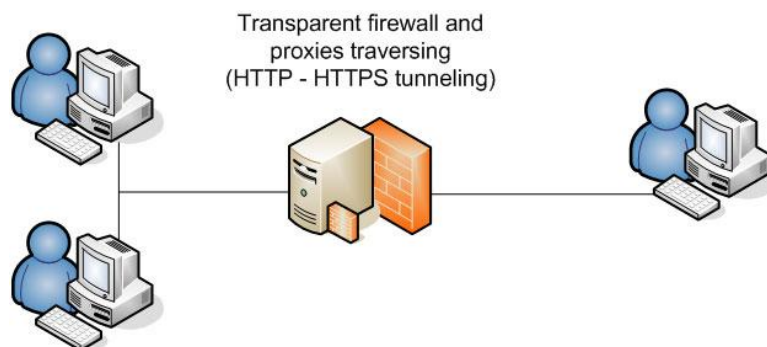
Cortafuegos sin estado requieren menos memoria, y pueden ser más rápido para los filtros simples que requieren menos tiempo para filtrar que mirar una sesión. También pueden ser necesarios para el filtrado de protocolos de red sin estado que no tienen ningún concepto de una sesión. Sin embargo, ellos no pueden tomar decisiones más complejas sobre la base de lo que las comunicaciones entre los hosts etapa han alcanzado.

Firewalls nuevos pueden filtrar el tráfico basado en paquetes de muchos atributos, como fuente de la dirección IP , la fuente de puerto , la dirección IP de destino o puerto, servicio de destino como WWW o FTP . Se pueden filtrar basándose en protocolos, TTL valores, NetBlock de autor, de la fuente, y muchos otros atributos.

Filtros de paquetes se utilizan frecuentemente en varias versiones de Unix son IPFilter (varios), ipfw (FreeBSD / Mac OS X), NPF (NetBSD), PF (OpenBSD, y algunas otras BSD), iptables / ipchains (Linux).

La capa de aplicación

Firewalls de aplicación de capas funcionan en el nivel de aplicación de la pila TCP / IP (es decir, todo el tráfico del navegador, o todos telnet o ftp tráfico), y pueden interceptar todos los paquetes que viajan hacia o desde una aplicación. Bloquean otros paquetes (generalmente soltándolas sin acuse de recibo al remitente).



Al inspeccionar todos los paquetes de contenido inapropiado, firewalls pueden restringir o impedir de plano la difusión de la red gusanos informáticos y troyanos. Los criterios de inspección adicionales pueden agregar latencia adicional para el envío de paquetes a su destino.

Firewalls de aplicaciones funcionan mediante la determinación de si un proceso debe aceptar cualquier conexión determinada. Los cortafuegos de aplicación cumplen su función mediante la conexión en llamadas de socket para filtrar las conexiones entre la capa de aplicación y las capas más bajas del modelo OSI.

Firewalls de aplicación que se enganchan en llamadas de socket también se conocen como filtros de socket. Firewalls de aplicaciones funcionan como un filtro de paquetes, pero los filtros de aplicación se aplican las reglas de filtrado (permitir / bloquear) en función de cada proceso en vez de filtrar las

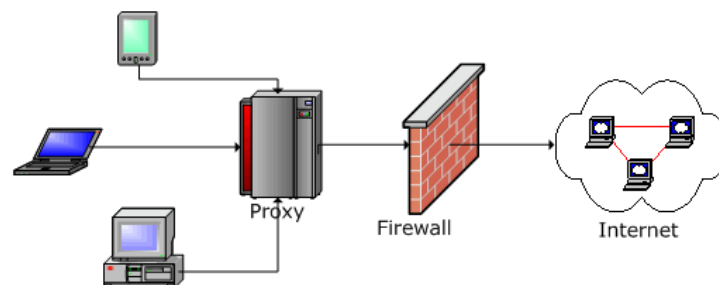
conexiones en una base por puerto. Generalmente, se utilizan avisos para definir reglas para los procesos que aún no han recibido una conexión. Es raro encontrar cortafuegos de aplicación no combinados o usados en conjunto con un filtro de paquetes.

Además, las conexiones de cortafuegos de aplicación más filtros de examinar el proceso de identificación de paquetes de datos en contra de un conjunto de reglas para el proceso local que participan en la transmisión de datos. La medida de la filtración que se produce se define por el conjunto de reglas proporcionado. Dada la variedad de software que existe, cortafuegos de aplicación sólo tienen conjuntos de reglas más complejas para los servicios estándar, tales como servicios de intercambio.

Estos conjuntos de reglas por procesos han limitado la eficacia en el filtrado de cada posible asociación que puede ocurrir con otros procesos. Además, estos conjuntos de reglas por procesos no pueden defenderse contra la modificación del proceso a través de la explotación, como las hazañas de corrupción de memoria. Debido a estas limitaciones, los firewalls de aplicaciones están comenzando a ser sustituida por una nueva generación de firewalls de aplicaciones que se basan en el control de acceso obligatorio (MAC), también conocida como sandboxing, para proteger los servicios vulnerables.

Proxies

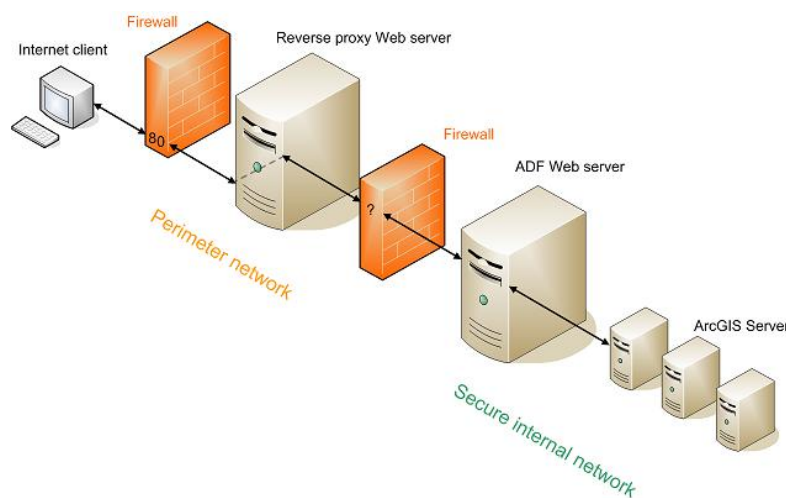
Un servidor proxy (que ejecuta en el hardware dedicado o como software en una máquina de propósito general) puede actuar como un servidor de seguridad por responder a los paquetes de entrada (peticiones de conexión, por ejemplo) en la forma de una aplicación, mientras que el bloqueo de otros paquetes. Un servidor proxy es una pasarela de una red a otra para una aplicación específica de la red, en el sentido de que funciona como un proxy en nombre del usuario de la red.



Los proxies hacen manipulación con un sistema interno de la red externa más difícil y el mal uso de un sistema interno no necesariamente causar un fallo de seguridad explotable desde fuera del servidor de seguridad (siempre y cuando el proxy de aplicación se mantiene intacto y configurado correctamente). Por el contrario, los intrusos pueden secuestrar un sistema de acceso público y lo utilizan como un sustituto para sus propios fines, el proxy se disfraza como el sistema a otros sistemas internos. Si bien el uso de los espacios de direcciones internas aumenta la seguridad, galletas todavía pueden emplear métodos tales como la suplantación de IP para tratar de pasar los paquetes a una red de destino.

Traducción de direcciones de red

Los cortafuegos tienen a menudo la traducción de direcciones de red la funcionalidad (NAT) y los hosts protegidos detrás de un firewall comúnmente tienen direcciones en el "rango de direcciones privadas", como se define en RFC 1918. Usualmente tienen esa funcionalidad para ocultar la verdadera dirección de los ejércitos protegidos. Originalmente, la función NAT se desarrolló para abordar el número limitado de direcciones IPv4 direccionales que pueden ser utilizados o asignados a empresas o particulares, así como reducir la cantidad y por lo tanto el costo de la obtención de suficientes direcciones públicas para todos los equipos de una organización. Ocultar las direcciones de los dispositivos protegidos se ha convertido en una defensa cada vez más importante en contra de reconocimiento de red.



3.1.2 [Iptables](#)

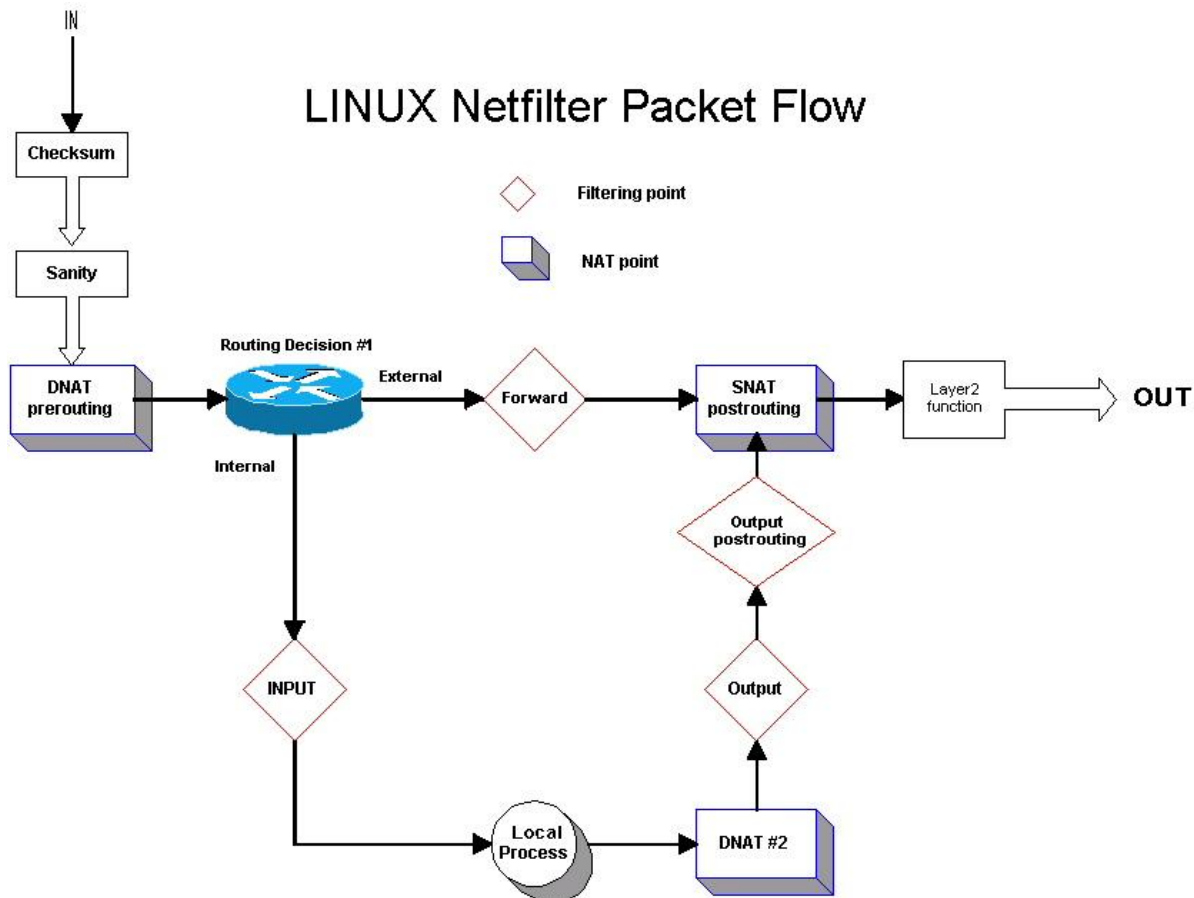
Iptables se utiliza para configurar, mantener e inspeccionar las tablas de IPv4 reglas de filtrado de paquetes en el kernel de Linux. Varias tablas diferentes se pueden definir. Cada tabla contiene una serie de cadenas incorporadas y también puede contener cadenas definidas por el usuario.

Cada cadena es una lista de reglas que pueden coincidir con un conjunto de paquetes. Cada regla especifica qué hacer con un paquete que coincide. Esto se conoce como un 'target', que puede ser un salto a una cadena definida por el usuario en la misma tabla.

Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de paquetes en diferentes estados del procesamiento. Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

El componente más popular construido sobre Netfilter es iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT)

para IPv4 o mantener registros de log. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.



Iptables es el nombre de la herramienta de espacio de usuario mediante la cual el administrador puede definir políticas de filtrado del tráfico que circula por la red. El nombre iptables se utiliza frecuentemente de forma errónea para referirse a toda la infraestructura ofrecida por el proyecto Netfilter. Sin embargo, el proyecto ofrece otros subsistemas independientes de iptables tales como el connection tracking system o sistema de seguimiento de conexiones, que permite encolar paquetes para que sean tratados desde espacio de usuario. Iptables es un software disponible en prácticamente todas las distribuciones de Linux actuales.

Tablas

Actualmente hay cinco mesas independientes (las tablas que están presentes en cualquier momento depende de las opciones de configuración del kernel y los módulos que se presente).

–T, -tabla de la tabla

Esta opción especifica la tabla de concordancia de paquetes que el comando debe operar. Si el núcleo está configurado con la carga automática de módulos, se realiza un intento de cargar el módulo apropiado para esa mesa si no está ya allí.

Las tablas son las siguientes:

Filtro:

Esta es la tabla por defecto (si se pasa la opción no-t). Contiene la cadena integrada ENTRADA (para los paquetes destinados a los sockets locales), FORWARD (para los paquetes encaminados por la máquina), y OUTPUT (para los paquetes generados localmente).

NAT:

Esta tabla se consulta cuando se encuentra un paquete que crea una nueva conexión. Se compone de tres empotrados: PREROUTING (para modificar los paquetes tan pronto como lleguen), OUTPUT (para modificar los paquetes generados localmente antes de encaminarlos) y POSTROUTING (para modificar los paquetes a punto de salir).

Mangle:

Esta tabla se usa para la alteración de paquetes especializados. Hasta el kernel 2.4.17 que tenía dos cadenas incorporadas: PREROUTING (para modificar los paquetes entrantes antes de enrutamiento) y OUTPUT (para modificar los paquetes generados localmente antes de encaminarlos). Desde kernel 2.4.18, otras tres cadenas internas también son compatibles: ENTRADA (para los paquetes que llegan a la máquina), FORWARD (para modificar los paquetes encaminados por la máquina), y POSTROUTING (para modificar los paquetes a punto de salir).

RAW:

Esta tabla se utiliza principalmente para la configuración de las exenciones de seguimiento de conexiones en combinación con el blanco NOTRACK. Se registra en los ganchos de filtrado de red con mayor prioridad y por lo tanto se llama antes de ip_conntrack, o cualquier otra tabla IP. Proporciona la incorporada en las cadenas siguientes: PREROUTING (para los paquetes que llegan a través de cualquier interfaz de red) SALIDA (para los paquetes generados por los procesos locales)

Seguridad:

Esta tabla se usa para el control de las normas obligatorias de redes de acceso (MAC), como las habilitadas por las SECMARK y CONNSECMARK objetivos. Mandatory Access Control se implementa módulos de seguridad de Linux como SELinux. La tabla de seguridad se llama después de la tabla de filtros, permitiendo a cualquier control de acceso discrecional (DAC) reglas en la tabla de filtro entre en vigor antes de las reglas MAC. Esta tabla presenta las siguientes características integradas en las cadenas: ENTRADA (para los paquetes que llegan a la máquina), OUTPUT (para modificar los paquetes generados localmente antes de encaminarlos) y FORWARD (para modificar los paquetes encaminados por la máquina).

Comandos

Estas opciones especifican la acción que desee realizar. Sólo uno de ellos se puede especificar en la línea de comandos a menos que se indique lo contrario a continuación. Para las versiones largas de los nombres de comando y opción, debe utilizar sólo letras suficientes para garantizar que iptables puede diferenciarla de las demás opciones.

–A - append cadena de reglas de especificación

Anexar una o más reglas al final de la cadena seleccionada. Cuando la fuente y / o nombres de destino se resuelven a más de una dirección, se añadirá una regla para cada posible combinación de dirección.

–C - comprobación cadena de reglas de especificación

Compruebe si una regla que coincide la especificación no existe en la cadena seleccionada. Este comando utiliza la misma lógica que -D para encontrar una entrada coincidente, pero no modifica la configuración de iptables existente y utiliza su código de salida para indicar el éxito o el fracaso.

–D - delete cadena de reglas de especificación

–D - delete cadena número de regla

Eliminar una o más reglas de la cadena seleccionada. Hay dos versiones de este comando: la regla se puede especificar como un número en la cadena (empezando por 1 para la primera regla) o una regla de igualar.

–I - insert cadena [número de regla] norma de especificación

Introduzca una o más reglas en la cadena seleccionada como el número de la regla dada. Por lo tanto, si el número de la regla es 1, la regla o reglas se insertan en la cabecera de la cadena. Esta es la opción por defecto si no se especifica ningún número de la regla.

–R - replace cadena número de regla norma de especificación

Reemplazar una regla en la cadena seleccionada. Si el origen y / o nombres de destino se resuelven a múltiples direcciones, el comando fallará. Las reglas se numeran a partir del 1.

`-L - list [cadena]`

Enumere todas las reglas de la cadena seleccionada. Si no se selecciona ninguna cadena, todas las cadenas se enumeran. Como todos los otros comandos iptables, se aplica a la tabla especificada (filtro es el valor predeterminado), por lo que las reglas NAT obtener la lista por

```
Iptables -t nat -n -L
```

Tenga en cuenta que se utiliza a menudo con la `-n` opción, a fin de evitar largas búsquedas de DNS inversas. Es legal para especificar la `Z` (cero) opción, así, en cuyo caso la cadena (s) será automáticamente aparece y pone a cero. El resultado final depende de los otros argumentos dados. Las reglas exactas se suprimen hasta que utilice

```
Iptables -L -v
```

`-S - list-normativa [cadena]`

Imprimir todas las reglas de la cadena seleccionada. Si no se selecciona ninguna cadena, todas las cadenas se imprimen de `iptables-save`. Como todos los otros comandos iptables, se aplica a la tabla especificada (filtro es el valor predeterminado).

`-F - flush [cadena]`

Vaciar la cadena seleccionada (todas las cadenas en la tabla si no se da). Esto es equivalente a borrar todas las reglas una por una.

`-Z - zero [cadena [número de regla]]`

Poner a cero los contadores de paquetes y bytes en todas las cadenas, o sólo la cadena dada, o sólo la regla dada en una cadena. Es legal para especificar el `-L - list` opción (lista), así, para ver los contadores inmediatamente antes de que se borren. (Véase más arriba.)

`-N - nueva cadena de la cadena`

Crear una nueva cadena definida por el usuario con el nombre dado. No debe haber ningún objeto de ese nombre.

`-X - delete-chain [Cadena]`

Eliminar la cadena definida por el usuario opcional especificado. No debe haber referencias a la cadena. Si los hay, debe eliminar o sustituir las normas referidas antes de la cadena se puede eliminar. La cadena debe estar vacío, es decir, no contiene ninguna norma. Si no se da ningún argumento, se intentará eliminar todas las cadenas no incorporado en la tabla.

-P - política de la cadena de destino

Establecer la política de la cadena hasta el destino dado. Consulte la sección OBJETIVOS para los objetivos legales. Sólo las cadenas construidas (no definidos por el usuario) pueden tener políticas, y tampoco incorporado ni las cadenas definidas por el usuario pueden ser objetivos de política.

-E - la cadena de cambiar el nombre nuevo de la cadena antigua de la cadena

Cambiar el nombre de la cadena especificada por el usuario para el nombre de usuario suministrado. Esta es cosmético, y no tiene ningún efecto sobre la estructura de la tabla.

-H

Ayuda. Da una descripción (actualmente breve) de la sintaxis de comandos

Reglas de iptables Ejemplo

La mayor parte de las acciones enumeradas en este artículo están escritos con la suposición de que van a ser ejecutados por el usuario root ejecutando el shell bash o cualquier otro shell moderna. No escriba los comandos en el sistema remoto, ya que se desconecta su acceso.

Para fines de demostración que he usado RHEL 6.x, pero el comando siguiente debería funcionar con cualquier distribución de Linux moderna.

Esto no es un tutorial sobre cómo configurar iptables. Ver tutorial aquí (<http://www.cyberciti.biz/faq/rhel-fedorta-linux-iptables-firewall-configuration-tutorial/>). Se trata de una hoja de trucos rápido a los comandos de iptables comunes.

Visualización del estado del servidor de seguridad

Escriba el siguiente comando como root:

```
Iptables -L -n -v
```

Salida anterior indica que el firewall no está activo. El siguiente ejemplo muestra un firewall activo:

```
Iptables -L -n -v
```

-L: Lista de reglas.

-V: Muestra información detallada. Esta opción hace que el comando list muestra el nombre de la interfaz, las opciones de la regla y las máscaras TOS. Los contadores de bytes y de paquetes también se enumeran, con el sufijo 'K', 'M' o 'G' para 1000, 1000000 y 1000000000 multiplicadores respectivamente.

-N: la dirección IP y el puerto de pantalla en formato numérico. No utilice DNS para resolver nombres. Esto acelerará el listado.

Para inspeccionar firewall con números de línea, escriba:

```
Iptables -L -n -v --line-numbers
```

1.2: para mostrar los datos o las reglas de la cadena de salida, entre:

```
Iptables -L ENTRADA -n -v
```

```
Iptables -L SALIDA -n -v --line-numbers
```

Stop / Start / Restart del Firewall

Si utiliza CentOS / RHEL Fedora Linux, especifique:

```
service iptables dejan
```

```
service iptables start
```

```
service iptables restart
```

Puede usar el comando iptables en sí para detener el servidor de seguridad y eliminar todas las reglas:

```
Iptables-F
```

```
Iptables-X
```

```
Iptables -t nat -F
```

```
Iptables-t nat-X
```

```
Iptables-t mangle-F
```

```
Iptables-t mangle-X
```

```
Iptables-P ENTRADA ACCEPT
```

```
Iptables-P OUTPUT ACCEPT
```

```
Iptables-P FORWARD ACCEPT
```

-F: La eliminación (flushing) todas las reglas.

-X: la cadena Delete.

-T nombre_tabla: Seleccione una tabla (llamada nat o mangle) y eliminar reglas / ras.

-P: Establecer la política por defecto (por ejemplo, DROP, REJECT, o aceptar).

Eliminar las reglas del cortafuego

Para mostrar el número de línea junto con otra información de las reglas existentes, escriba:

```
Iptables -L -n ENTRADA --line-numbers
Iptables -L -n SALIDA --line-numbers
Iptables -L -n SALIDA --line-numbers | less
Iptables -L -n SALIDA --line-numbers | grep 202.54.1.1
```

Usted obtendrá la lista de IP. Mira el número de la izquierda, a continuación, utilizar el número para eliminarlo. Por ejemplo borrar la línea número 4, escriba:

```
Iptables -D INPUT 4
```

O Encontrar fuente IP 202.54.1.1 y eliminar del dominio:

```
iptables -D ENTRADA-s 202.54.1.1-j DROP
```

-D: Eliminar una o más reglas de la cadena seleccionada

Inserte reglas de firewall

Para insertar una o más reglas en la cadena seleccionada como el número de la regla dada utilice la sintaxis siguiente. En primer lugar saber los números de línea, escriba:

```
Iptables -L -n ENTRADA --line-numbers
```

El bloqueo de una dirección IP (IP bloqueadas)

Para bloquear una dirección IP atacantes llamada 1.2.3.4, escriba:

```
Iptables-A INPUT-s 1.2.3.4-j DROP
Iptables-A INPUT-s 192.168.0.0/24-j DROP
```

Para obtener más referencias y ejemplos de iptables ir a este link (<http://www.cyberciti.biz/tips/linux-iptables-examples.html>)

Conclusión:

Este artículo sólo enumera las reglas básicas para los nuevos usuarios de Linux. Puede crear y construir reglas más complejas. Esto requiere una buena comprensión de TCP / IP, tuning kernel Linux a través

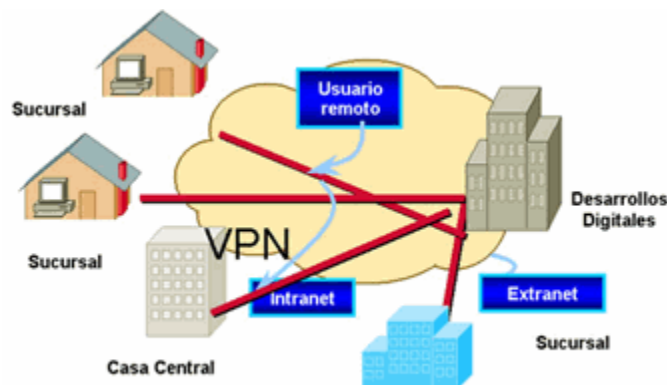
sysctl.conf, y un buen conocimiento de su propia configuración. Manténgase atento a los temas siguientes:

- La inspección de estado de paquetes.
- Usando ayudantes de seguimiento de conexiones.
- Traducción de direcciones de red.
- Capa 2 filtrado.
- Herramientas de prueba de firewall.
- Tratar con VPN, DNS, Web, Proxy, y otros protocolos.

3.2 Redes Privadas Virtuales

Una red privada virtual, RPV, o VPN de las siglas en inglés de Virtual Private Network, es una tecnología de red que permite una extensión segura de la red local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, encriptación o la combinación de ambos métodos.

Las empresas pueden usar redes privadas virtuales para conectar en forma segura oficinas y usuarios remotos a través de accesos a Internet económicos proporcionados por terceros, en vez de costosos enlaces WAN dedicados o enlaces de marcación remota de larga distancia.



Las organizaciones pueden usar redes privadas virtuales para reducir los costos de ancho de banda de redes WAN, y a la vez aumentar las velocidades de conexión a través de conectividad a Internet de alto ancho de banda, tal como DSL, Ethernet o cable.

Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación. Estas tecnologías protegen los datos que pasan por la red privada virtual contra accesos no autorizados. Las empresas pueden aprovechar la infraestructura estilo Internet de la red privada virtual, cuya sencillez de abastecimiento permite agregar rápidamente nuevos sitios o usuarios. También pueden aumentar drásticamente el alcance de la red privada virtual sin expandir significativamente la infraestructura.

Las redes privadas virtuales extienden la seguridad a los usuarios remotos

Las redes VPN SSL y VPN IPsec se han convertido en las principales soluciones de redes privadas virtuales para conectar oficinas remotas, usuarios remotos y partners comerciales, porque:

Proporcionan comunicaciones seguras con derechos de acceso adaptados a usuarios individuales, tales como empleados, contratistas y partners

Aumentan la productividad al ampliar el alcance de las redes y aplicaciones empresariales

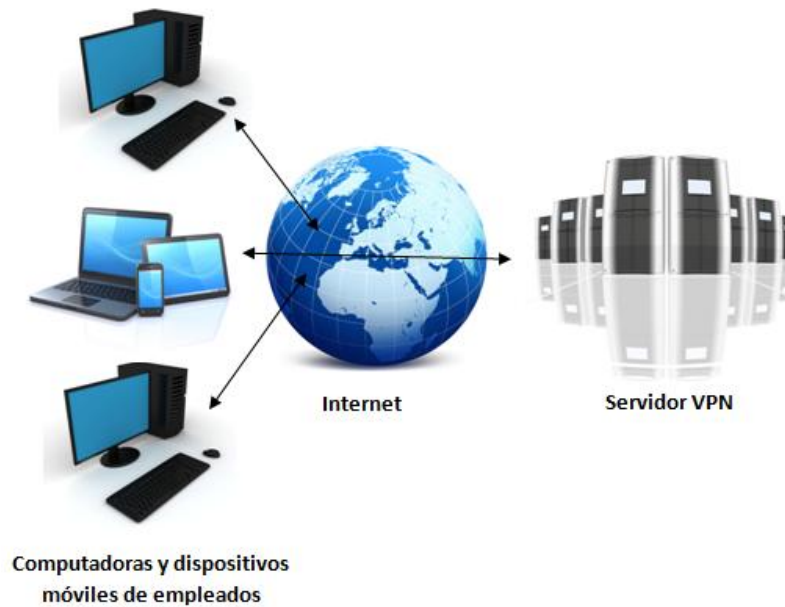
Reducen los costos de comunicación y aumentan la flexibilidad

Los dos tipos de redes virtuales privadas cifradas:

VPN IPsec de sitio a sitio: Esta alternativa a Frame Relay o redes WAN de línea arrendada permite a las empresas extender los recursos de la red a las sucursales, oficinas en el hogar y sitios de los partners comerciales.

VPN de acceso remoto: Esto extiende prácticamente todas las aplicaciones de datos, voz o video a los escritorios remotos, emulando los escritorios de la oficina central. Las redes VPN de acceso remoto pueden desplegarse usando redes VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación.

Ejemplos comunes son la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.



La conexión VPN a través de Internet es técnicamente una unión wide area network (WAN) entre los sitios pero al usuario le parece como si fuera un enlace privado de allí la designación "virtual private network".

3.2.1 Introducción a las VPNs

Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad de toda la comunicación:

Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: de que los datos enviados no han sido alterados. Para ello se utilizan funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

Confidencialidad/Privacidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.

Control de acceso: Se trata de asegurar que los participantes autenticados tiene acceso únicamente a los datos a los que están autorizados.

Auditoria y registro de actividades: Se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.

Calidad del servicio: Se trata de asegurar un buen rendimiento, que no haya una degradación poco aceptable en la velocidad de transmisión.

Requisitos básicos

Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

Cifrado de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que así no puedan ser leídos si son interceptados. Esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor.

Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

Nuevo algoritmo de seguridad SEAL.

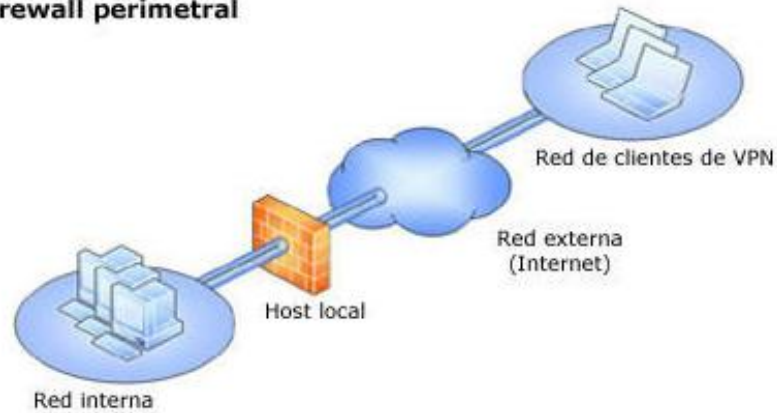
Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

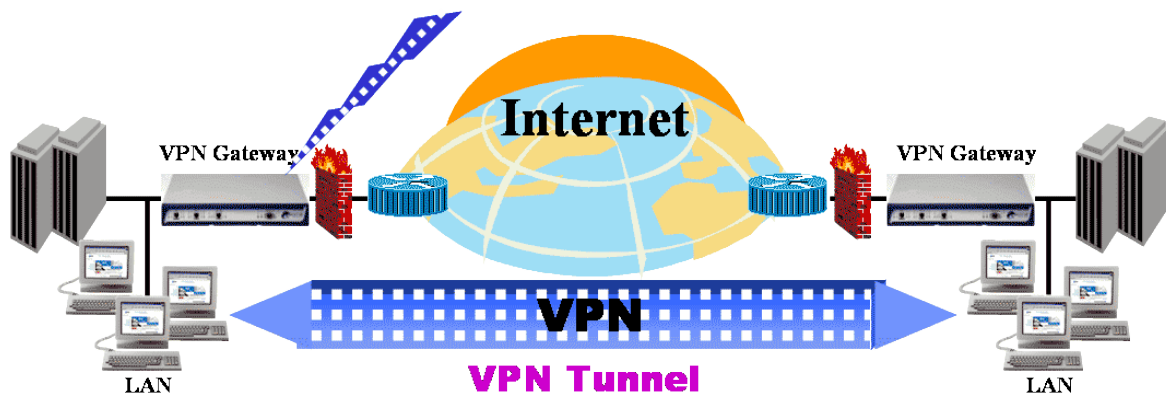
Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

Firewall perimetral



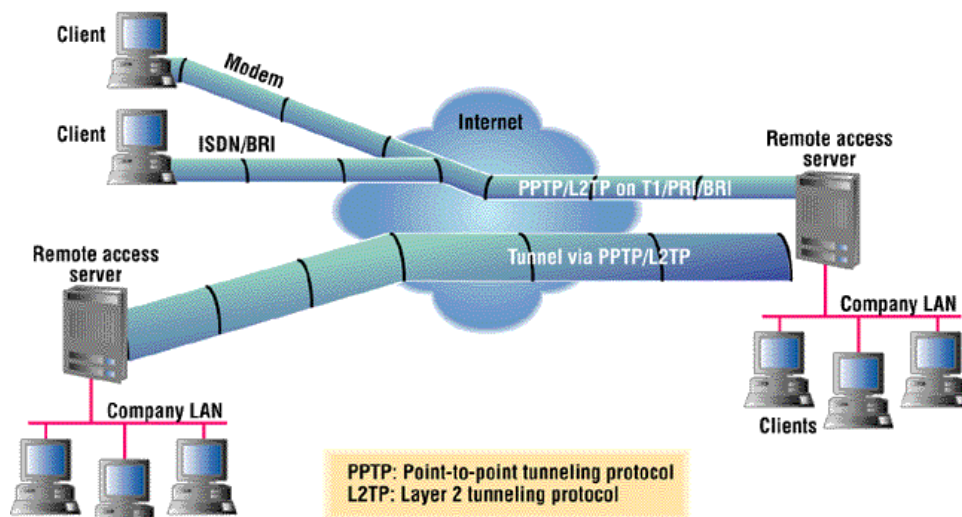
VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.



Tunneling

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU (unidades de datos de protocolo) determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

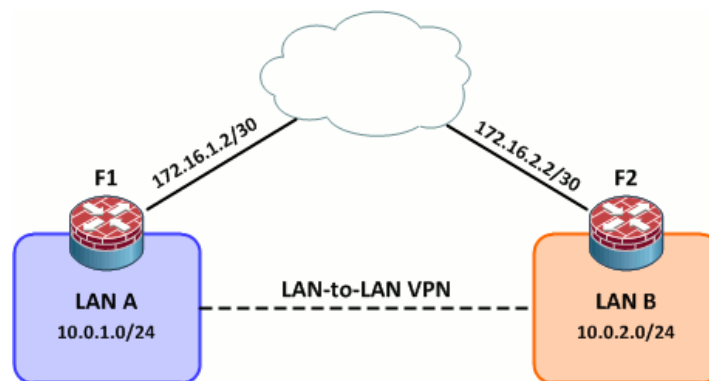


El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP Móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

VPN over LAN

Este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo "acceso remoto" pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).



Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

Otro ejemplo es la conexión a redes Wi-Fi haciendo uso de túneles cifrados IPSec o SSL que además de pasar por los métodos de autenticación tradicionales (WEP, WPA, direcciones MAC, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna o externa.

Tipos de conexión

Conexión de acceso remoto

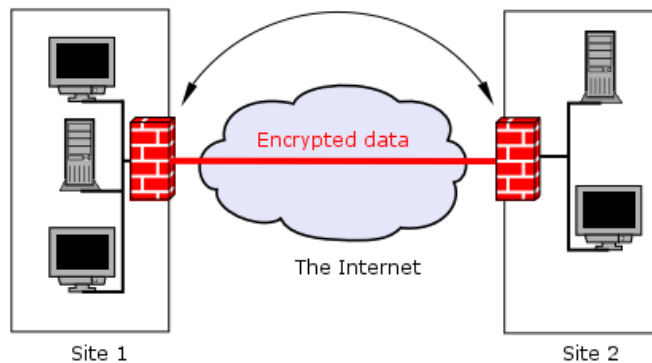
Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada. En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers. El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentifica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

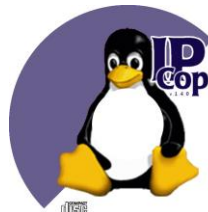
Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet.



El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

3.2.2 [Linux \(IPCop\)](#)

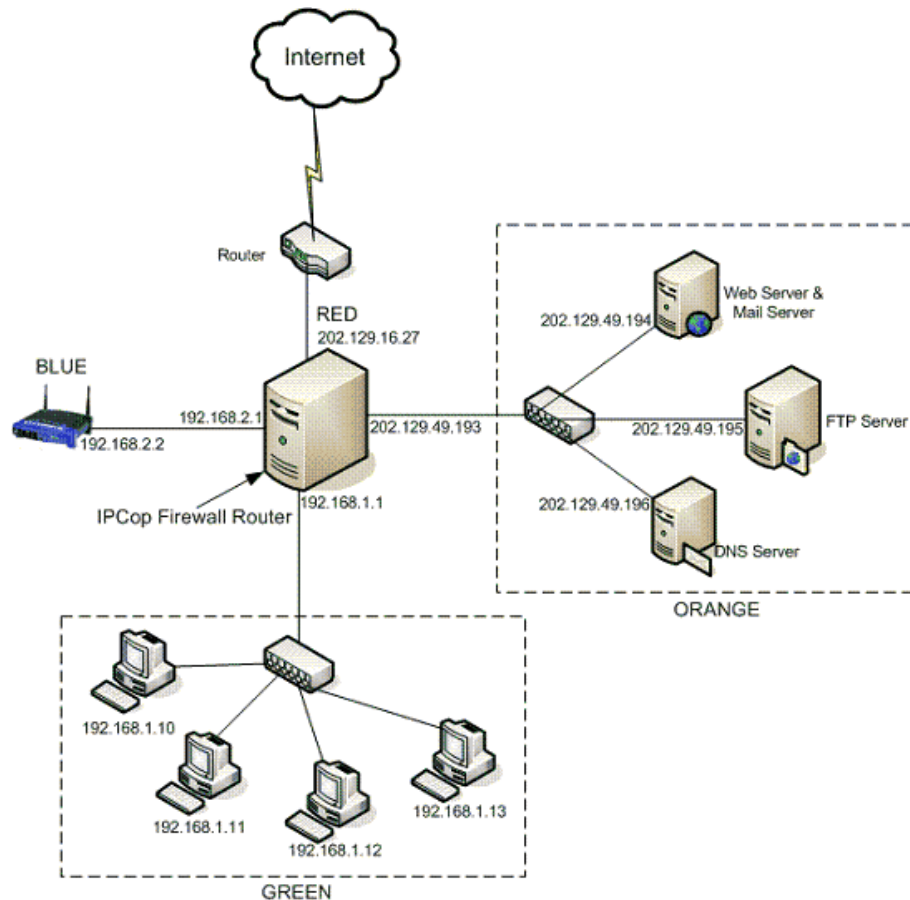
IPCop es una distribución Linux que implementa un cortafuego (o firewall) y proporciona una simple interfaz web de administración basándose en una computadora personal. Originalmente nació como una extensión (fork) de la distribución SmoothWall cuyo desarrollo había estado congelado bastante tiempo.



IPCop tiene como objetivos ser un cortafuegos sencillo, con pocos requerimientos hardware orientado a usuarios domésticos o a pequeñas empresas (SOHO), administrado a través de una interfaz web, con funcionalidades básicas y avanzadas, yendo (a manera de ejemplo) desde el simple filtrado de paquetes hasta la asignación de ancho de banda fijo a cada puesto de trabajo o la configuración de redes virtuales VPN. IPCop se actualiza desde la Interfaz Web de manera muy sencilla, incluyendo actualizaciones del Kernel.

IPCop está capado y solo tiene instaladas las herramientas justas para su función como firewall, limitando el daño que podría hacer un intruso que comprometiera el sistema. Si se desea ampliar la

funcionalidad existen extensiones (addons), comunes con SmoothWall, que permiten instalar todo tipo de utilidades como por ejemplo instalar Nmap para escanear IPs.



La distribución Linux se puede bajar desde el sitio oficial en inglés, consiste de una imagen ISO de menos de 100Mb la cual puede ser grabada en un CD e instalada en cualquier computador que tenga al menos dos interfaces de red.

IPCop se desarrolla, en el tradicional código abierto estilo, por un diverso grupo de desarrollo de difundir a través de Internet en general. CD-ROM de imágenes en el CD de instalación se distribuyen a través de una red de espejos. Páginas web de asistencia se mantienen en Inglés, francés, alemán y holandés. Interfaz de usuario de IPCop está disponible en 35 idiomas.

La versión 1.4.0 fue lanzada en 2004, basado en el LFS distribución y un núcleo 2.4, que ofrece una interfaz de usuario actualizada y una serie de opciones de idiomas adicionales. Esta versión ya no es compatible con las actualizaciones o correcciones de errores.

La rama estable actual es 2.0.X, lanzado en 2011, después de tres años de desarrollo. Hay un nuevo instalador, y una nueva interfaz de usuario, con un número de antiguos complementos incorporados a sí IPCop. Las nuevas características y los cambios se describen aquí.

Aunque no es una parte oficial de IPCop, hay muchos complementos, algunos basados en el servidor add-on, que añaden funcionalidad adicional al IPCop, tales como QoS avanzada, detección de virus de correo electrónico, resumen de tráfico, interfaces extendidas para controlar el poder, y muchos más.

Extensiones (Addons):

Algunas de las extensiones más importantes son:

BOT: (Block Out Traffic) esta extensión nos permite cortar o bloquear todo el tráfico de salida de IPCop ya que en un principio este firewall solo bloquea las conexiones entrantes.

Advanced proxy: Otra de las extensiones más usadas, ya que el servidor proxy que trae por defecto este firewall es poco avanzado y con pocas opciones de configuración.

URL Filter: Esta extensión nos permite crear listas blancas y negras de las diferentes url's que queremos bloquear a los usuarios de IPCop, esta extensión se usa junto a la anterior puesto que se sirve de un proxy para bloquear dichas url's.

Topologías de red soportadas: Permite la implementación de diferentes topologías de red, ya sea desde la simple LAN que sale a internet, hasta la creación de una zona desmilitarizada (DMZ), soportando también la inclusión de una red inalámbrica.

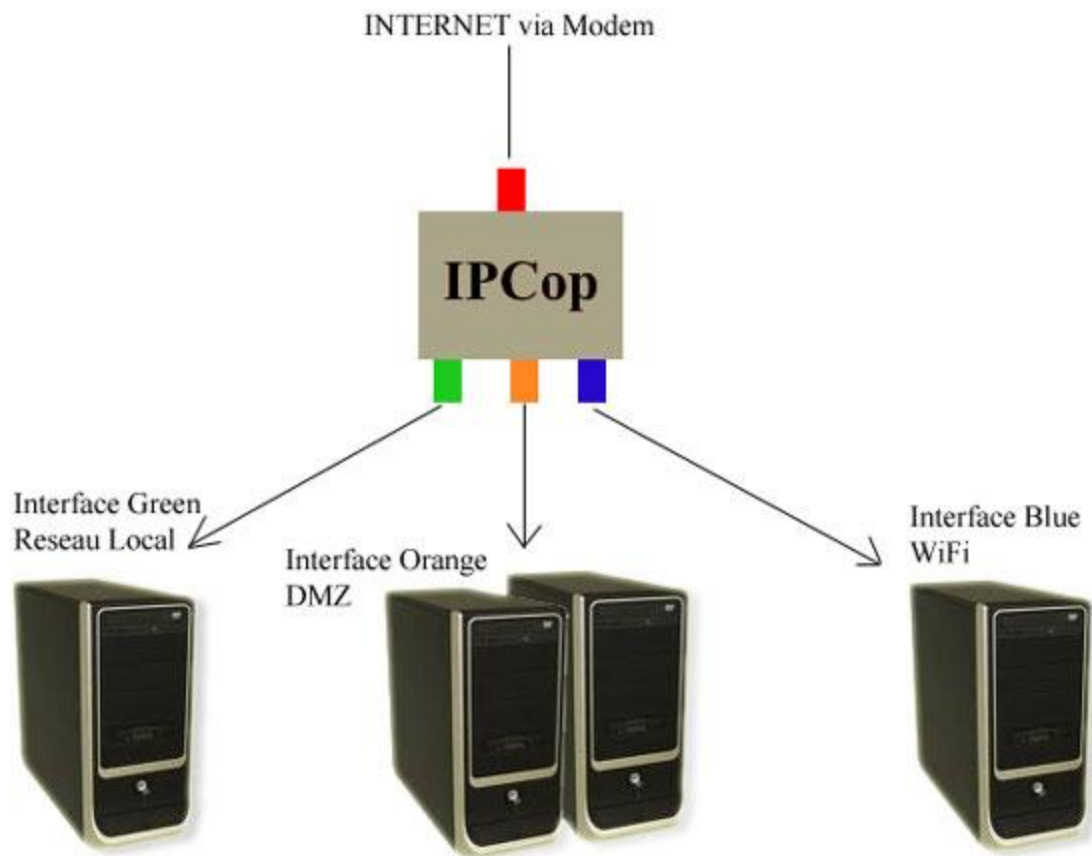
Las diferentes zonas las divide en colores, siendo:

Roja = zona de Internet,

Verde = Red de Área Local (LAN) cableada,

Naranja = zona desmilitarizada (DMZ, para la granja de servidores),

Azul = zona inalámbrica (Wireless).



4 Auditoria de seguridad

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información (SI) es el estudio que comprende el análisis y gestión de sistemas llevados a cabo por profesionales para identificar, enumerar y posteriormente describir las diversas vulnerabilidades que pudieran presentarse en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores.

Una vez obtenidos los resultados, se detallan, archivan y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo y/o corrección siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Las auditorías de seguridad de SI permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

La auditoría informática es un proceso llevado a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.



Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

En si la auditoria informática tiene 2 tipos las cuales son:

AUDITORIA INTERNA: es aquella que se hace adentro de la empresa; sin contratar a personas de afuera.

AUDITORIA EXTERNA: como su nombre lo dice es aquella en la cual la empresa contrata a personas de afuera para que haga la auditoria en su empresa. Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

4.1 Técnicas de auditoría

Una auditoría se realiza con base a un patrón o conjunto de directrices o buenas prácticas sugeridas. Existen estándares orientados a servir como base para auditorías de informática. Uno de ellos es COBIT (Objetivos de Control de la Tecnologías de la Información), dentro de los objetivos definidos como parámetro, se encuentra el "Garantizar la Seguridad de los Sistemas". Adicional a este estándar podemos encontrar el estándar ISO 27002, el cual se conforma como un código internacional de buenas prácticas de seguridad de la información, este puede constituirse como una directriz de auditoría apoyándose de otros estándares de seguridad de la información que definen los requisitos de auditoría y sistemas de gestión de seguridad, como lo es el estándar ISO 27001.



- Mejora la imagen pública.
- Confianza en los usuarios sobre la seguridad y control de los servicios de TI.
- Optimiza las relaciones internas y del clima de trabajo.
- Disminuye los costos de la mala calidad (reproceso, rechazos, reclamos, entre otros).
- Genera un balance de los riesgos en TI.
- Realiza un control de la inversión en un entorno de TI, a menudo impredecible.

La auditoría informática sirve para mejorar ciertas características en la empresa como:

Desempeño

- Fiabilidad
- Eficacia
- Rentabilidad
- Seguridad
- Privacidad



Generalmente se puede desarrollar en alguna o combinación de las siguientes áreas:

Gobierno corporativo

- Administración del Ciclo de vida de los sistemas
- Servicios de Entrega y Soporte
- Protección y Seguridad
- Planes de continuidad y Recuperación de desastres

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO eITIL.

Actualmente la certificación de ISACA para ser *CISA Certified Information Systems Auditor* es una de las más reconocidas y avaladas por los estándares internacionales ya que el proceso de selección consta de un examen inicial bastante extenso y la necesidad de mantenerse actualizado acumulando horas (puntos) para no perder la certificación.

4.2 Tipos de auditoría

Los servicios de auditoría pueden ser de distinta índole:

- Auditoría de seguridad interna. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno.
- Auditoría de seguridad perimetral. En este tipo de análisis, el perímetro de la red local o corporativa es estudiado y se analiza el grado de seguridad que ofrece en las entradas exteriores
- Test de intrusión. El test de intrusión es un método de auditoría mediante el cual se intenta acceder a los sistemas, para comprobar el nivel de resistencia a la intrusión no deseada. Es un complemento fundamental para la auditoría perimetral.
- Análisis forense. El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes, mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la par que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el análisis se denomina análisis postmortem.
- Auditoría de páginas web. Entendida como el análisis externo de la web, comprobando vulnerabilidades como la inyección de código SQL, Verificación de existencia y anulación de posibilidades de Cross Site Scripting (XSS), etc.

- Auditoría de código de aplicaciones. Análisis del código tanto de aplicaciones páginas Web como de cualquier tipo de aplicación, independientemente del lenguaje empleado

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría.

Dentro de la auditoría informática destacan los siguientes tipos (entre otros):

Auditoría de la gestión: la contratación de bienes y servicios, documentación de los programas, etc.

Auditoría legal del Reglamento de Protección de Datos: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

Auditoría de los datos: Clasificación de los datos, estudio de las aplicaciones y análisis del flujo gramas.

Auditoría de las bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.

Auditoría de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.

Auditoría de la seguridad física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc.) y protecciones del entorno.

Auditoría de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.

Auditoría de las comunicaciones. Se refiere a la auditoria de los procesos de autenticación en los sistemas de comunicación.

Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes.

Importancia de la Auditoria Informática

La auditoría permite a través de una revisión independiente, la evaluación de actividades, funciones específicas, resultados u operaciones de una organización, con el fin de evaluar su correcta realización. Este autor hace énfasis en la revisión independiente, debido a que el auditor debe mantener independencia mental, profesional y laboral para evitar cualquier tipo de influencia en los resultados de la misma.

La técnica de la auditoría, siendo por tanto aceptables equipos multidisciplinarios formados por titulados en Ingeniería Informática e Ingeniería Técnica en Informática y licenciados en derecho especializados en el mundo de la auditoría.

4.3 Fases de la auditoría

Los servicios de auditoría constan de las siguientes fases:

- Enumeración de redes, topologías y protocolos
- Verificación del Cumplimiento de los estándares internacionales. ISO, COBIT, etc.
- Identificación de los sistemas operativos instalados
- Análisis de servicios y aplicaciones
- Detección, comprobación y evaluación de vulnerabilidades
- Medidas específicas de corrección
- Recomendaciones sobre implantación de medidas preventivas.

En la realización de una auditoría informática el auditor puede realizar las siguientes pruebas:

- **Pruebas sustantivas:** Verifican el grado de confiabilidad del SI del organismo. Se suelen obtener mediante observación, cálculos, muestreos, entrevistas, técnicas de examen analítico, revisiones y conciliaciones. Verifican asimismo la exactitud, integridad y validez de la información.
- **Pruebas de cumplimiento:** Verifican el grado de cumplimiento de lo revelado mediante el análisis de la muestra. Proporciona evidencias de que los controles claves existen y que son aplicables efectiva y uniformemente.

Las principales herramientas de las que dispone un auditor informático son:

- **Observación**
- **Realización de cuestionarios**
- **Entrevistas a auditados y no auditados**
- **Muestreo estadístico**
- **Flujogramas**
- **Listas de chequeo**
- **Mapas conceptuales**

4.4 Informe de auditoría

Confección y redacción del Informe Final La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es el exponente de su calidad. Resulta evidente la necesidad de

redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

Estructura del informe final El informe comienza con la fecha de comienzo de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ostente. Definición de objetivos y alcance de la auditoría.

Enumeración de temas considerados: antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.

Cuerpo expositivo: Para cada tema, se seguirá el siguiente orden a saber:

- a. Situación actual. Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
- b. Tendencias. Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
- c. Puntos débiles y amenazas.
- d. Recomendaciones y planes de acción. Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.
- e. Redacción posterior de la Carta de Introducción o Presentación. Modelo conceptual de la exposición del informe final - El informe debe incluir solamente hechos importantes.

La inclusión de hechos poco relevantes o accesorios desvía la atención del lector. El Informe debe consolidar los hechos que se describen en el mismo. El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:

1. El hecho debe poder ser sometido a cambios.
2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
3. No deben existir alternativas viables que superen al cambio propuesto.
4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación. La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida.

I. FORMATO PARA EL PLAN DE LAS AUDITORÍAS INTERNAS				
Dependencia o proceso auditado: Responsable del proceso o dependencia: Auditor principal: Fechas de realización de la auditoría: Fecha de presentación del informe:				
1. OBJETO DE LA AUDITORÍA				
2. ALCANCE DE LA AUDITORÍA				
3. DOCUMENTOS DE REFERENCIA				
4. LOGÍSTICA DE LA AUDITORÍA				
5. EQUIPO DE AUDITORÍA				
6. FUNCIONARIOS ENTREVISTADOS				
7. PLAN DE ACTIVIDADES				
FECHA:				
HORA	SUBPROCESO	NUMERAL	AUDITOR	AUDITADO
8. APROBACIÓN				
AUDITOR PRINCIPAL		JEFE PROCESO O DEPENDENCIA AUDITADA		

El informe de auditoría tiene que estar basado en una metodología misma que debe estar soportando por mejores prácticas administrativas y tecnológicas. La información y observaciones vertido en el informe deben de contener un sustento y no pueden ser en ningún caso subjetivos.

5 ANÁLISIS DE VULNERABILIDADES Y BITÁCORAS (LOGS)

5.1 Análisis de vulnerabilidades

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

- Hardware: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,...).
- Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
- Otros: fungibles, personas, infraestructuras,.. aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

De ellos los mas críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.



Incluso de todos ellos, el activo mas crítico son los datos. El resto se puede reponer con facilidad y los datos ... sabemos que dependen de que la empresa tenga una buena política de copias de seguridad y sea capaz de reponerlos en el estado mas próximo al momento en que se produjo la pérdida. Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que conllevaría de pérdida de tiempo y dinero.

Vulnerabilidad: definición y clasificación

Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

La búsqueda de vulnerabilidades de seguridad es realizada principalmente por dos tipos de personas u organizaciones:

- Los atacantes de sistemas.-Pueden aprovechar las vulnerabilidades para hacer vulnerables a los sistemas y conseguir de forma ilegal beneficios monetarios de ello, ya sea directamente (Ej. permitiendo el uso de tarjetas de crédito ajenas) o indirectamente (Ej. vendiendo información privada sobre las víctimas). Por su propia naturaleza este tipo de investigadores de vulnerabilidades no están interesados en la revelación de las vulnerabilidades descubiertas ya que

así se aseguran de que la vulnerabilidad no sea arreglada y así puedan seguir beneficiándose de la misma.

- Profesionales de la informática y en especial de la seguridad.- Estos profesionales, por distintas motivaciones, estudian de forma legal los sistemas y muchas veces logran encontrar vulnerabilidades. Este tipo de personas están interesadas en la revelación de la información. De esta forma acreditan haber encontrado la misma y así pueden apuntarse el mérito. Las motivaciones que tienen estos profesionales para encontrar la vulnerabilidades podríamos resumirlas en:
 - Reputación.- El que una persona o organización sea acreditada como la primera en descubrir una vulnerabilidad particular es muy importante en el mundo de la seguridad informática. Por un lado a las personas les acredita de habilidades y esto puede usarse para aumentar sus ingresos o conseguir mejores trabajos. Para una empresa también es importante porque puede utilizarse para conseguir clientes en base al alto nivel del personal que trabaja para ella.
 - Perjudicar a competidores.- Por ejemplo un desarrollador o compañía puede tener especial interés en buscar vulnerabilidades a productos de la competencia para poner en dificultades al proveedor y desacreditar sus productos. De esta forma se consigue mejorar la posición en el mercado del producto propio.
 - Forzar al proveedor del productor a mejorar la calidad del producto y que tenga más interés en producir software más seguro.
 - Disfrutar del desafío intelectual de encontrar vulnerabilidades.
 - Obtener gratificaciones monetarias por parte del proveedor del producto o de otra entidad.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficientes e inexistentes.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.

- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

- Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe como explotarla.

5.1.1 Tipos de vulnerabilidades

- Vulnerabilidad de desbordamiento de buffer.

Si un programa no controla la cantidad de datos que se copian en buffer, puede llegar un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

En esta situación se puede aprovechar para ejecutar código que nos de privilegios de administrador.

- Vulnerabilidad de condición de carrera (race condition).

Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

- Vulnerabilidad de Cross Site Scripting (XSS).

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBScript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

- Vulnerabilidad de denegación del servicio.

La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

- Vulnerabilidad de ventanas engañosas (Window Spoofing).

Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

- Cross-site request forgery o falsificación de petición en sitios cruzados

Un ataque CSRF fuerza al navegador web validado de una víctima a enviar una petición a una aplicación web vulnerable, la cual entonces realiza la acción elegida a través de la víctima.

Las vulnerabilidades CSRF se conocen desde 1990. CSRF no se puede trazar porque es llevada a cabo por la dirección IP de un usuario legítimo.

5.1.2 Herramientas de análisis

La seguridad de una organización es un aspecto cambiante. Una empresa puede alcanzar un nivel de protección óptimo en un momento determinado y ser totalmente sensible poco después, tras cambios en la configuración de un servidor o luego de instalar nuevos dispositivos de red. Al mismo tiempo, continuamente aparecen nuevos fallos de seguridad en software existentes, que previamente se creían seguros.

Una política de realización de Análisis de Vulnerabilidades periódicas mitiga, en gran medida, el riesgo asociado a un entorno en constante cambio, tal como lo representan los sistemas informáticos de cualquier compañía.

Escáner de puertos

El "escáner de vulnerabilidad" (también denominado "analizador de red") es una aplicación que permite realizar una verificación de seguridad en una red mediante el análisis de los puertos abiertos en uno de los equipos o en toda la red. El proceso de análisis utiliza sondas (solicitudes) que permiten determinar los servicios que se están ejecutando en un host remoto.

Esta herramienta permite identificar los riesgos de seguridad. En general, con este tipo de herramienta es posible efectuar un análisis en una serie o lista de direcciones IP a fin de realizar una verificación completa de una red.

Funcionamiento

El escáner de vulnerabilidades permite identificar los puertos que están abiertos en un sistema al enviar solicitudes sucesivas a diversos puertos, además de analizar las respuestas para determinar cuáles están activos.

Mediante un análisis exhaustivo de la estructura de los paquetes TCP/IP recibidos, los escáneres de seguridad avanzados pueden identificar, a veces, qué sistema operativo está utilizando el equipo remoto, así como las versiones de las aplicaciones asociadas con los puertos y, cuando sea necesario, recomendar actualizaciones (esto se conoce como caracterización de la versión).

En general, se usan dos métodos:

- Adquisición activa de información, que consiste en enviar una gran cantidad de paquetes con encabezados característicos que normalmente no cumplen con las recomendaciones y analizar las respuestas para identificar la versión de la aplicación utilizada. Como todas ellas utilizan protocolos ligeramente diferentes, esto posibilita su diferenciación.

- Adquisición pasiva de informaciones (también denominado análisis pasivo o análisis no agresivo), un método mucho menos invasivo que reduce la probabilidad de ser detectado por un sistema detector de intrusiones. Funciona de modo similar, efectuando un análisis de los campos de datagramas IP que circulan en una red utilizando un rastreador de puertos. Dada su naturaleza pasiva, la versión analiza los cambios en los valores de campo dividiéndolos en una serie de fragmentos, lo que requiere un tiempo de análisis mucho más prolongado. Por ello, este tipo de análisis es muy difícil e incluso imposible de detectar en determinadas ocasiones.

Ventajas

Los escáneres de seguridad son herramientas sumamente útiles para los administradores de sistemas y redes, ya que les permite supervisar la seguridad de todos los equipos que están a su cargo.

Sin embargo, esta herramienta puede ser utilizada por los piratas informáticos para identificar las vulnerabilidades del sistema.

Nessus para servidores Linux/Unix

En el caso de servidores Linux/Unix para hacer el análisis de vulnerabilidades se suele utilizar el programa 'Nessus'.

Nessus es de arquitectura cliente-servidor OpenSource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades.

Existe software comercial que utiliza Nessus como motor para el análisis. Por ejemplo está Catbird (www.catbird.com) que usa un portal para la gestión centralizada de las vulnerabilidades, analiza externamente e internamente la red teniendo en cuenta los accesos inalámbricos. Además hace monitoreo de servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.

MBSA para Windows

En otros sistemas tipo Windows está el MBSA “Microsoft Baseline Security Analyzer” que permite verificar la configuración de seguridad, detectando los posibles problemas de seguridad en el sistema operativo y los diversos componentes instalados.

5.1.3 Gestión de vulnerabilidades

La informática ha sido tradicionalmente una materia compleja en todos sus aspectos, por lo que se hace necesaria la utilización de metodologías en cada doctrina que la componen, desde su diseño de ingeniería hasta el desarrollo del software, controlando todas estas áreas mediante la auditoria de los sistemas de información.

Esta metodología ha sido estructurada en 6 fases ; Planeación, Políticas de Seguridad, Aseguramiento Físico, Arquitecturas de Seguridad, Aseguramiento de Servicios y Auditoria de Sistemas, las cuales se han vislumbrado como las fases necesarias para la implementación y monitoreo de un ambiente de

seguridad apropiado no solo en las empresas a las que se ha enfocado la metodología, si no para cualquier empresa en general.

Una vez se haya finalizado el proceso de implantación de la metodología, la organización debería poseer las condiciones básicas de aseguramiento de sus recursos informáticos, de esta manera encontrarse preparada para reaccionar ante cualquier eventualidad, y lista para tomar medidas procedimentales o disciplinarias ante alguna irregularidad.

Fase 1: Planeación

Con el fin de crear un plan de aseguramiento de la compañía, inicialmente se debe estudiar el cometido de la misma para conocer su misión y visión, y de esta manera generar una solución de seguridad de acuerdo a sus necesidades y requerimientos. Posteriormente se ha de realizar un análisis de los datos y la información de la compañía, en donde se establecerán los recursos que se van proteger, priorizándolos de manera tal que se cuantifique el impacto en el caso de suspensión del servicio de las aplicaciones, definiendo medidas y procedimientos de seguridad; asimismo en esta etapa se debe hacer un análisis de los posibles riesgos que puede tener la compañía, en donde se identifiquen las amenazas y las vulnerabilidades tanto físicas como lógicas, proporcionándoles un valor de impacto y la probabilidad de que se materialicen.

Fase 2: Políticas De Seguridad

En esta fase se pretende implantar una serie de métodos, controles y directrices para el correcto uso de los recursos informáticos en general, para que de esta manera se pueda respaldar el plan de seguridad.

Al realizar esta labor, la organización debe ser conciente del nivel de responsabilidad que debe asumir, puesto que éstas se elaboran a la medida de cada organización y de acuerdo con su infraestructura tecnológica de información, así como de su cometido.

Desafortunadamente ésta no es una tarea sencilla ni rápida, ya que la elaboración de las políticas debe ser de tal manera que éstas sean breves y de fácil entendimiento, así como también de una implementación sencilla.

Además ha de tenerse en cuenta que las políticas deben apoyarse en estándares internacionales de seguridad tales como el BS-77992 y la ISO 177993, sin contradecir las diferentes regulaciones gubernamentales particulares para cada país. Una vez creadas las políticas, la implementación de las mismas se hace a través de procedimientos detallados, los cuales describirán los pasos a seguir, con el fin de cumplir el objetivo de la política de seguridad.

Sin embargo el proceso de documentación de procedimientos es extenso, ya que se requieren una serie de actividades con el fin de lograr el cumplimiento del estándar. La implantación de estas políticas, hará que el valor de la organización aumente así como su credibilidad y reputación, y por que no, conseguir el aval de una entidad certificadora, con el fin obtener una mayor competitividad, consiguiendo el mejoramiento de los procesos.

Una vez concluida la creación y/o modificación de las políticas, y procedimiento de seguridad se da inicio a las fases prácticas del ciclo de vida de la metodología.

Fase 3: Aseguramiento Físico

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

Ubicación física y disposición del centro de cómputo: Este es uno de los puntos de mayor cuidado y atención, puesto que aquí se encuentra la infraestructura central de la información y de comunicaciones de las cuales depende la compañía para sus labores diarias; control de acceso físico: Esta etapa refuerza la anterior, debido a que en ésta se dan parámetros para controlar el acceso de personas ajenas o no autorizadas a la organización; seguridad administrativa: Busca la capacitación de los empleados de la organización en cuanto al manejo y aseguramiento de los recursos en general. Por último la realización de Planes de Contingencia: Se ocupa de los procedimientos de recuperación del negocio, en caso de algún incidente de seguridad.

Fase 4: Arquitecturas De Red

Las arquitecturas de red se crearon para dividir las redes empresariales de las redes públicas, con el fin de mantener la información confidencial fuera del alcance de terceros. Para la metodología de análisis de vulnerabilidades se trabajó con diferentes tipos de arquitecturas de red, con el fin de proporcionar a las compañías opciones de acuerdo al plan de seguridad.

Dentro de los diferentes tipos de arquitecturas propuestas, existen las llamadas zonas desmilitarizadas o DMZ (demilitarized zone), las cuales protegen la red privada de la red pública, separando el tráfico de red interna en dos grupos, con el fin de asegurar el control de acceso a los servidores públicos desde la red pública y privada.

Las arquitecturas propuestas son:

- Arquitecturas sin DMZ
 - a. Red básica con un solo Firewall.
 - b. Red básica con un solo Firewall y un host bastión
- Arquitecturas con DMZ
 - c. Firewall básico con una DMZ
 - d. Firewall dual con una DMZ
- Arquitectura de Red con IDS
- Arquitectura de Red Inalámbrica (WLAN)

Una vez establecida la arquitectura, teniendo en cuenta sus ventajas y desventajas⁵, se procede con la implementación física de la misma, configurando y actualizando cada uno de los dispositivos que hacen parte de la arquitectura elegida, de tal manera que en su mayoría desaparezca las vulnerabilidades presentes en éstas, ya que solo con el montaje de la arquitectura no se obtiene un nivel suficiente de seguridad.

Fase 5: Aseguramiento Y Configuración De Sistemas Operativos Servicios, Herramientas Y Dispositivos

Gran parte del éxito de la metodología radica en el aseguramiento y buena configuración de los servicios que presta la organización, de las herramientas o aplicaciones que tiene la empresa para su protección, así como de los dispositivos que hacen parte de su arquitectura de red.

Dentro de las herramientas que se utilizan a diario en una organización se encuentra el sistema operativo, el cual controla el acceso y uso de los recursos de una máquina, siendo uno de los elementos más apetecibles para intentar explotar cualquier vulnerabilidad, por lo tanto, en un sistema operativo se debe contemplar:

- Identificación y autenticación de los usuarios.
- Control de acceso a los recursos del sistema.

- Monitorear las acciones realizadas por los usuarios.
- Auditoría de los eventos de posible riesgo.
- Garantía de integridad de los datos almacenados.
- Garantía de la disponibilidad de los recursos.

Además es necesario asegurar los recursos, y controlar su acceso y uso a través de sujetos remotos, tal como es el caso de los archivos compartidos; esta seguridad se debe implementar a través de políticas de seguridad en el sistema por parte de los administradores, con el fin de brindar la protección a los diferentes elementos del sistema

Fase 6: Auditoria De Sistemas

Una vez implementada la metodología y aseguradas todas las áreas que se tuvieron en cuenta en el plan de seguridad, se procede con la auditoría de sistemas, con el fin de verificar del éxito de la implementación y el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y contengan un buen nivel de seguridad. En la auditoría de sistemas se determina si los sistemas de información salvaguardan los activos, mantiene la integridad de los datos y utiliza eficientemente los recursos.

Dentro de las principales áreas que hacen parte de la auditoría de sistemas, se encuentran:

Auditoría Física

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

Auditoría de Bases de Datos

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

Auditoría de Redes

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

Auditoría de Aplicaciones

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

Auditoría de la Seguridad

En este tipo de auditoría se debe evaluar si los modelos de seguridad están en concordancia con las nuevas arquitecturas, las distintas plataformas y las posibilidades de las comunicaciones.

5.2 Análisis de bitácoras

Una bitácora o también llamado blog, es un sitio web que se encuentra periódicamente en actualización, en el se recopilan cronológicamente textos o artículos publicados por diferentes autores apareciendo primero el que fue publicado mas actualmente. El criterio de escritos se dejan a consideración de el autor, habitualmente en cada articulo los lectores pueden poner su opinión y comentarios para que de la misma

manera el autor pueda contestarles (establecen un dialogo)(no en todos los blogs se puede ya que esto esta habitualmente a consideración de el autor).

Una bitácora puede ser muy útil en temas que están en constante cambio y requieren de opinión.

5.2.1 Bitácoras de WEB, cortafuegos, routers, correo.

Las Bitácoras son páginas web de sencillo manejo, el cual permite incorporar herramientas multimedia, logrando producir un recurso en el que se integran texto, imágenes, audio y video.

Registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quien, que, cuando, donde y por que de un evento que ocurre para un dispositivo en particular o aplicación

La mayoría de los logs son almacenados o desplegados en el formato estándar ASCII. De esta forma logs generados por un dispositivo en particular puede ser leído y desplegado en otro diferente.

Propósito de los LOGS

Todos los sistemas pueden verse comprometidos por un intruso, de manera local o remota.

La seguridad no sólo radica en la prevención, sino también en la identificación. Entre menos tiempo haya pasado desde la identificación de intrusión, el daño será menor; para lograr esto es importante hacer un constante monitoreo del sistema.

De cualquier forma que se realice una proteccion de Unix debe incluir el monitoreo y revision de LOGS de una forma comprensiva, precisa y cuidadosa.

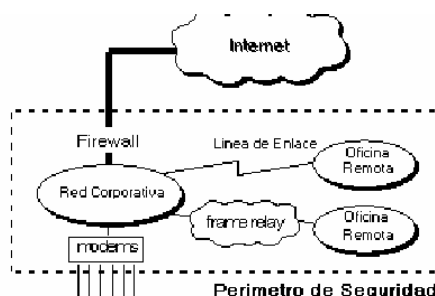
Los logs tienen numerosos propósitos:

- Ayudar a resolver problemas de todo tipo
- Proveer de avisos tempranos de abusos del sistema.
- Después de una caída del sistema, proporcionan datos de forensia.
- Como evidencia legal

Cortafuegos

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accedidos dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización.

Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración. Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.



Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, normas de dial-in y dial-out, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa, este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es “si” pero “cuando” ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del . También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

Concentra la seguridad Centraliza los accesos:

- Genera alarmas de seguridad.
- Traduce direcciones (NAT).
- Monitorea y registra el uso de Servicios de WWW y FTP.
- Internet.

Routers

Es un dispositivo que proporciona conectividad a nivel de red o nivel tres en el modelo OSI. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP que se pueden comunicar sin la intervención de un enrutador (mediante bridges), y que por tanto tienen prefijos de red distintos.

El funcionamiento básico de un router (en español 'enrutador' o 'encaminador'), como se deduce de su nombre, consiste en enviar los paquetes de red por el camino o ruta más adecuada en cada momento. Para ello almacena los paquetes recibidos y procesa la información de origen y destino que poseen. En base a esta información lo reenvían a otro enrutador o al host final en una actividad que se denomina 'encaminamiento'. Cada enrutador se encarga de decidir el siguiente salto en función de su tabla de reenvío o tabla de encaminamiento, la cual se genera mediante protocolos que deciden cuál es el camino más adecuado o corto, como protocolos basado en el algoritmo de Dijkstra.

Por ser los elementos que forman la capa de red, tienen que encargarse de cumplir las dos tareas principales asignadas a la misma:

- Reenvío de paquetes (Forwarding): cuando un paquete llega al enlace de entrada de un enrutador, éste tiene que pasar el paquete al enlace de salida apropiado. Una característica importante de los enrutadores es que no difunden tráfico difusivo.

- Encaminamiento de paquetes (routing): mediante el uso de algoritmos de encaminamiento tiene que ser capaz de determinar la ruta que deben seguir los paquetes a medida que fluyen de un emisor a un receptor.

Por tanto, debemos distinguir entre reenvío y encaminamiento. Reenvío consiste en coger un paquete en la entrada y enviarlo por la salida que indica la tabla, mientras que por encaminamiento se entiende el proceso de hacer esa tabla.

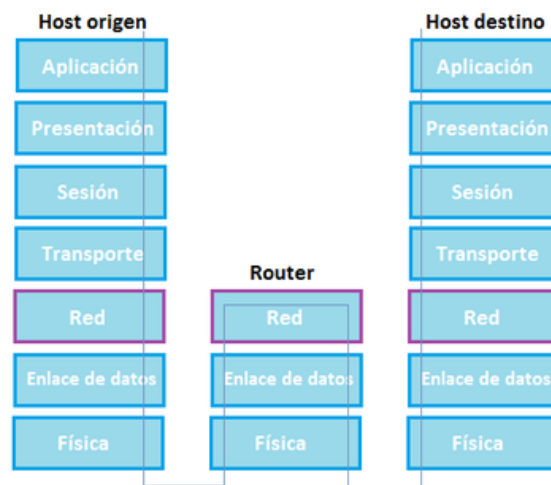
En un router se pueden identificar cuatro componentes:

Puertos de entrada: realiza las funciones de la capa física consistentes en la terminación de un enlace físico de entrada a un router; realiza las funciones de la capa de enlace de datos necesarias para interoperar con las funciones de la capa de enlace de datos en el lado remoto del enlace de entrada; realiza también una función de búsqueda y reenvío de modo que un paquete reenviado dentro del entramado de conmutación del enrutador emerge en el puerto de salida apropiado.

Entramado de conmutación: conecta los puertos de entrada del router a sus puertos de salida.

Puertos de salida: almacena los paquetes que le han sido reenviados a través del entramado de conmutación y los transmite al enlace de salida. Realiza entonces la función inversa de la capa física y de la capa de enlace que el puerto de entrada.

Procesador de encaminamiento: ejecuta los protocolos de encaminamiento, mantiene la información de encaminamiento y las **tablas de reenvío** y realiza funciones de gestión de red dentro del router.



Correo

Correo electrónico (en inglés: e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP, aunque por extensión también puede verse aplicado a sistemas análogos que usen otras tecnologías. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales dependiendo del sistema que se use. Su eficiencia, conveniencia y bajo coste están logrando que el correo electrónico desplace al correo ordinario para muchos usos habituales.

Para que una persona pueda enviar un correo a otra, cada una ha de tener una dirección de correo electrónico. Esta dirección la tiene que dar un proveedor de correo, que son quienes ofrecen el servicio de envío y recepción. Es posible utilizar un programa específico de correo electrónico (cliente de correo electrónico o MUA, del inglés Mail User Agent) o una interfaz web, a la que se ingresa con un navegador web.

5.2.2 Formatos

Un formato de archivo es un estándar que define la manera en que está codificada la información en un archivo.

Un formato de un archivo es una forma particular de codificar información para ser almacenamiento. Existen diferentes tipos de formatos para diferentes tipos de información. Por esto existen formatos de gráficos, formatos de audio, formatos de animación, formato de documentos, etc.

Los formatos suelen estar asociados a una o más extensiones de archivo que los identifica. Existen todo tipo de extensiones como:

- Extensiones de archivos audio
- De archivos de imagen
- De archivos comprimidos
- De archivos de texto
- De archivos del sistema
- De archivos de video

5.2.3 Centralización de bitácoras

Se pueden presentar dos escenarios principales:

Un único servidor central para la administración de Logs.

Al tener un único y común servidor de logs se establece también un único punto de falla o ataque. El sistema por completo dependería de la disponibilidad de este punto e igualmente un atacante al obtener acceso a este servidor pondría en duda la validez de los logs y la utilización de estos como evidencia en una investigación formal

Diferentes servidores que almacenan los logs de acuerdo a una clasificación de los mismos.

Tener un servidor para grupos de fuentes de logs, si el servidor de logs de los servidores con sistema operativo Windows NT falla, seguirá estando disponible el servidor de los de las maquinas Unix y desde luego los servidores de los demás dispositivos. Una forma de aumentar la disponibilidad es tener una replica de los logs en otros servidores de logs, alta redundancia.

– Ventajas

- Se requiere de un solo punto de almacenamiento de bitácoras.

– Desventajas

- Existe un solo punto de falla.
- Se necesitan muchos recursos para almacenamiento y redundancia.

5.2.4 Herramientas para análisis

Tripwire

Es una herramienta diseñada especialmente para Sistemas Operacionales UNIX. Dicha herramienta por medio de funciones se encarga de generar un Hash único por cada archivo que se le desee proteger su integridad. De esta forma cuando se presente un cambio en un log por parte del atacante, este cambio será notificado al administrador (enviándose un mail automático), ya que no reflejará el hash original. Para realizar dichas detecciones Tripwire también se basa en: CRC-32, MD5, SHA y HAVAL (firma digital de 128 bits).

logrotate

Esta herramienta alterna, comprime y envía logs de sistema. Está diseñada para facilitar la administración de los sistemas que generan un gran número de archivos de logs. Permite la rotación automática, comprensión, extracción y envío de los archivos de logs. Puede manipularse cada archivo log diaria, semanal o mensualmente, o cuando se haga demasiado grande.

SYSLOG

Es la principal herramienta de UNIX para llevar la bitácora de eventos. Con este sistema, se puede configurar el manejo de bitácoras a un nivel extremadamente alto de detalle y cada flujo de registros puede ir a un archivo diferente. Una habilidad muy buscada y muy potente del syslog es su capacidad de enviar registros de bitácoras a computadoras remotas. Esto permite centralizar las bitácoras en un solo servidor y fácilmente verificar los archivos de bitácora por razones de violaciones de seguridad y otras cosas extrañas en toda la red.

La mayoría del manejo de bitácoras esta provisto por dos programas principales: syslogd y klogd. El primero provee de un sistema de bitácoras para los programas y las aplicaciones, mientras que el segundo provee del manejo de bitácoras para el kernel.

Klogd actualmente envía la mayoría de los mensajes al syslogd, pero en ocasiones enviará mensajes a la consola.

Sysklogd actualmente maneja las tareas de procesar la mayoría de los mensajes y enviarlos al archivo o dispositivo apropiado; esto se configura dentro del archivo `/etc/syslog.conf`.

Sin embargo existen varios problemas con el syslogd y el klogd, la principal es que si un atacante logra acceso de root, podrá modificar los archivos de bitácoras y nadie lo notará.

Cada mensaje enviado al sistema de bitácoras tiene dos clasificadores: el servicio y el nivel. El servicio indica el tipo de programa que envió el mensaje y el nivel es el orden de importancia. Sysklogd y klogd no son los únicos sistemas para el seguimiento de bitácoras, existen otros, entre los cuales podemos nombrar:

modular syslog. Firma digitalmente los registros de bitácora para que cualquier alteración en ellos sea inmediatamente detectable.

next generation syslog. Permite el firmado digital y además puede clasificar los registros de otras maneras (como patrones en los registros) además del tipo de servicio y el nivel.

Nsyslogd. Añade soporte para SSL (Secure Socket Layer) en la transmisión de bitácoras a una computadora remota.

6 Manejo de incidentes de seguridad

6.1 Gestión de Incidentes

La Gestión de Incidentes tiene como objetivo resolver cualquier incidente que cause una interrupción en el servicio de la manera más rápida y eficaz posible.

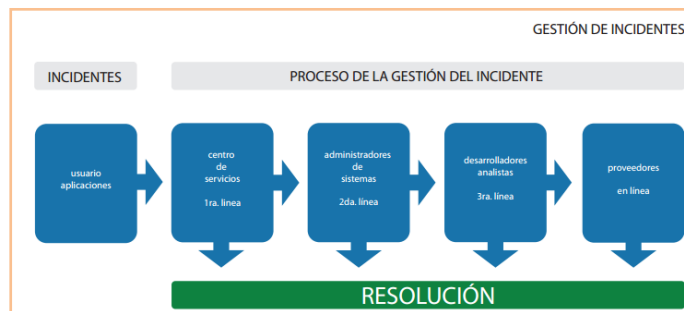
La Gestión de Incidentes no debe confundirse con la Gestión de Problemas, pues a diferencia de esta última, no se preocupa de encontrar y analizar las causas subyacentes a un determinado incidente sino exclusivamente a restaurar el servicio. Sin embargo, es obvio, que existe una fuerte interrelación entre ambas.

Los objetivos principales de la Gestión de Incidentes son:

- Detectar cualquiera alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio según se define en el SLA co-rrespondiente.

Esta actividad requiere un estrecho contacto con los usuarios, por lo que el Centro de Servicios (Service Desk) debe jugar un papel esencial en el mismo.

El siguiente diagrama resume el proceso de gestión de incidentes:



Aunque el concepto de incidencia se asocia naturalmente con cualquier malfuncionamiento de los sistemas de hardware y software según el libro de Soporte del Servicio de ITIL un incidente es:

“Cualquier evento que no forma parte de la operación estándar de un servicio y que causa, o puede causar, una interrupción o una reducción de calidad del mismo”.

Los principales beneficios de una correcta Gestión de Incidentes incluyen:

- Mejorar la productividad de los usuarios.
- Cumplimiento de los niveles de servicio.
- Mayor control de los procesos y monitorización del servicio.

- Optimización de los recursos disponibles.
- Una base de datos de gestión de configuraciones más precisa pues se registran los incidentes en relación con los elementos de configuración.
- Y principalmente: mejora la satisfacción general de clientes y usuarios.

Por otro lado una incorrecta Gestión de Incidentes puede acarrear efectos adversos tales como:

- Reducción de los niveles de servicio.
- Se dilapidan valiosos recursos: demasiada gente o gente del nivel inadecuado trabajando concurrentemente en la resolución del incidente.
- Se pierde valiosa información sobre las causas y efectos de los incidentes para futuras reestructuraciones y evoluciones.
- Se crean clientes y usuarios insatisfechos por la mala y/o lenta gestión de sus incidentes.

Las principales dificultades a la hora de implementar la Gestión de Incidentes se resumen en:

- No se siguen los procedimientos previstos y se resuelven las incidencias sin registrarlas o se escalan innecesariamente y/u omitiendo los protocolos preestablecidos.
- No existe un margen operativo que permita gestionar los “picos” de incidencias por lo que éstas no se registran adecuadamente e impiden la correcta operación de los protocolos de clasificación y escalado.
- No están bien definidos los niveles de calidad de servicio ni los productos soportados. Lo que puede provocar que se procesen peticiones que no se incluyan en los servicios previamente acordados con el cliente.

6.2 Grupos de respuesta a incidentes

Mantener seguros los activos de información en una organización en el actual medio de computación interconectado es un verdadero desafío que se toman más difícil con cada producto “e” nuevo y cada herramienta incrustada nueva.

La mayoría de las organizaciones se dan cuenta de que no hay solución o panacea para asegurar a los sistemas de datos; se requiere una estrategia de seguridad multicapa. Una de las capas que muchas organizaciones hoy están incluyendo en su estrategia es la creación del equipo de respuesta a incidentes de seguridad, generalmente llamado CSIRT.

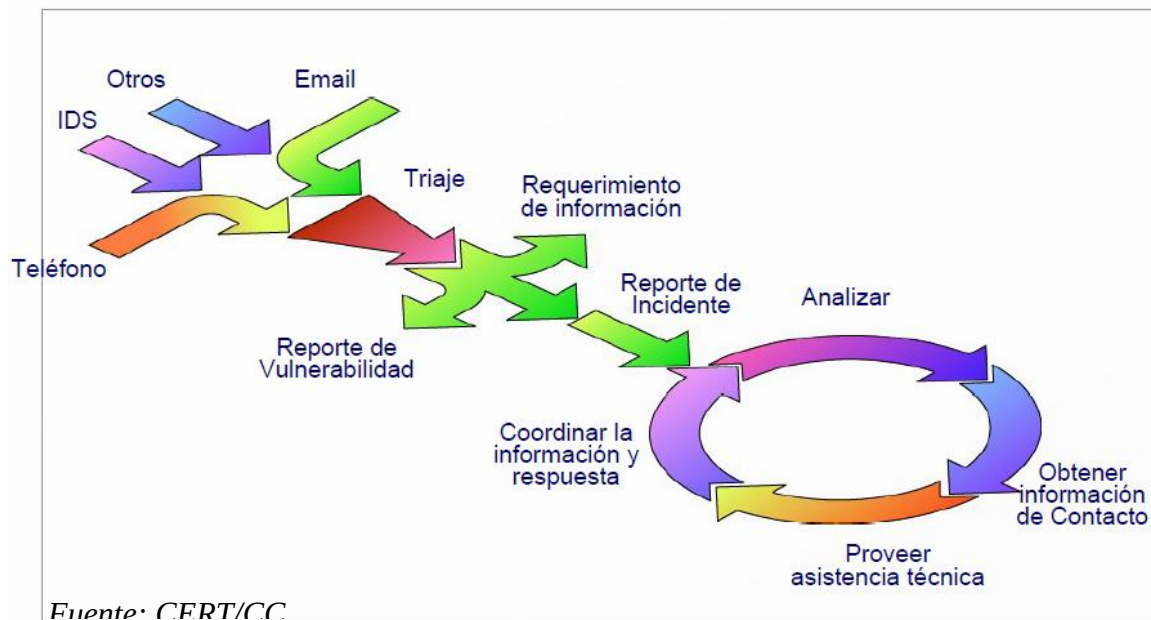
Los motivadores que conducen al establecimiento de CSIRTs incluyen:

- Un incremento general de la cantidad de incidentes de seguridad informados.
- Un incremento general de la cantidad y tipo de organizaciones que están siendo afectadas por incidentes de seguridad.
- Un reconocimiento o concientización por parte de las organizaciones sobre la necesidad de políticas y prácticas de seguridad como parte de sus estrategias generales de manejo del riesgo.
- Nuevas leyes y reglamentaciones que impactan en la forma en que las organizaciones requieren proteger sus activos informáticos. Comprender que los administradores de sistemas y de redes solos no pueden proteger los sistemas y activos de la organización.

CSIRT

Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

Ciclo de vida de un CSIRT



Es importante saber cuál va a ser el entorno de actuación y cuáles van a ser sus usuarios. Es por esto que se distinguen los siguientes sectores:

CSIRT del sector académico: prestan servicios a centros académicos y educativos, como universidades o centros de investigación, y a sus campus virtuales.

CSIRT comercial: prestan servicios comerciales a sus clientes. En el caso de un proveedor de servicios de Internet, el CSIRT presta principalmente servicios

relacionados con el abuso a los clientes finales (conexión por marcación telefónica, ADSL) y servicios de CSIRT a sus clientes profesionales.

CSIRT del sector CIP/CIIP: se centran principalmente en la protección de la información vital (CIP) y de la información y las infraestructuras vitales (CIIP). Por lo general, estos CSIRT especializados colaboran estrechamente con un departamento público de protección de la información y las infraestructuras vitales. Estos CSIRT abarcan todos los sectores vitales de las TI del país y protegen a los ciudadanos.

CSIRT interno: únicamente prestan servicios a la organización a la que pertenecen, lo que describe más su funcionamiento que su pertenencia a un sector. Por regla general, estos CSIRT no mantienen sitios web públicos.

6.3 Detección y análisis

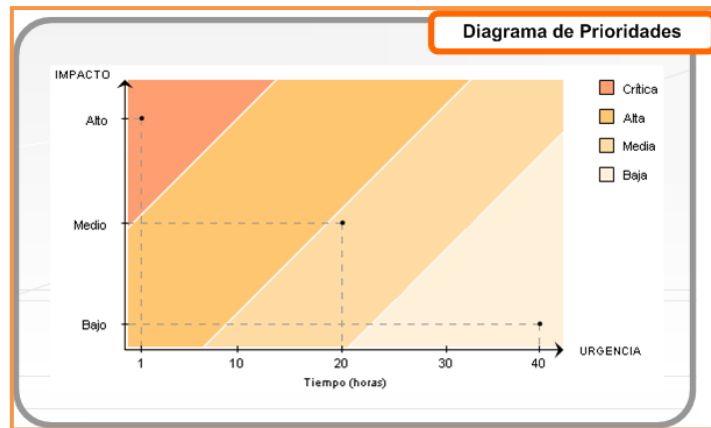
Es frecuente que existan múltiples incidencias concurrentes por lo que es necesario determinar un nivel de prioridad para la resolución de las mismas.

El nivel de prioridad se basa esencialmente en dos parámetros:

- Impacto: determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.
- Impacto: determina la importancia del incidente dependiendo de cómo éste afecta a los procesos de negocio y/o del número de usuarios afectados.

También se deben tener en cuenta factores auxiliares tales como el tiempo de resolución esperado y los recursos necesarios: los incidentes “sencillos” se tramitarán cuanto antes.

Dependiendo de la prioridad se asignarán los recursos necesarios para la resolución del incidente. La prioridad del incidente puede cambiar durante su ciclo de vida. Por ejemplo, se pueden encontrar soluciones temporales que restauren aceptablemente los niveles de servicio y que permitan retrasar el cierre del incidente sin graves repercusiones. Es conveniente establecer un protocolo para determinar, en primera instancia, la prioridad del incidente. El siguiente diagrama nos muestra un posible “diagrama de prioridades” en función de la urgencia e impacto del incidente:



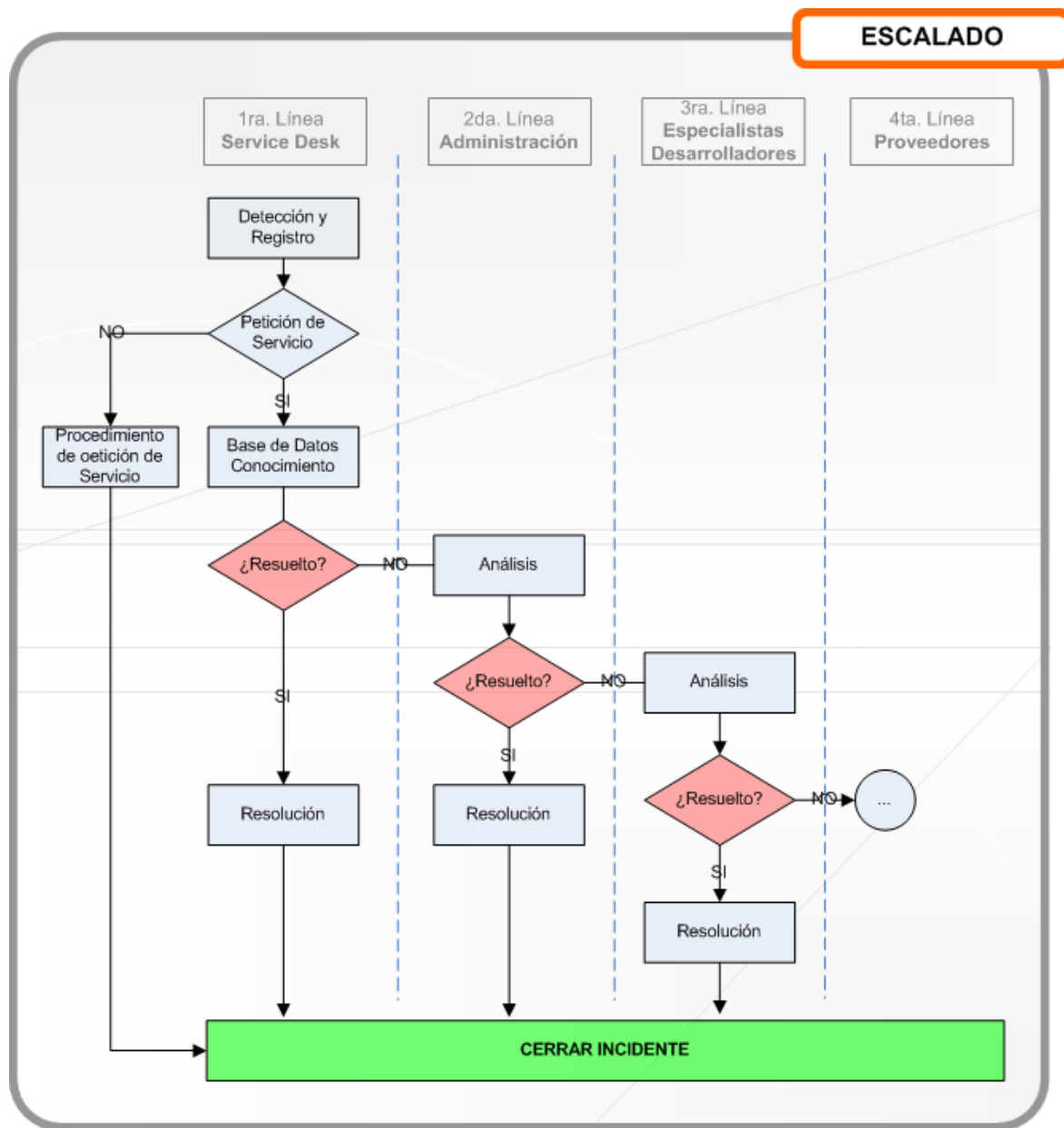
Escalonamiento

Es frecuente que el Centro de Servicios no se vea capaz de resolver en primera instancia un incidente y para ello deba recurrir a un especialista o a algún superior que pueda tomar decisiones que se escapan de su responsabilidad. A este proceso se le denomina escalado.

Básicamente hay dos tipos diferentes de escalado:

- **Escalado funcional:** Se requiere el apoyo de un especialista de más alto nivel para resolver el problema.
- **Escalado jerárquico:** Debemos acudir a un responsable de mayor autoridad para tomar decisiones que se escapan de las atribuciones asignadas a ese nivel, como, por ejemplo, asignar más recursos para la resolución de un incidente específico.

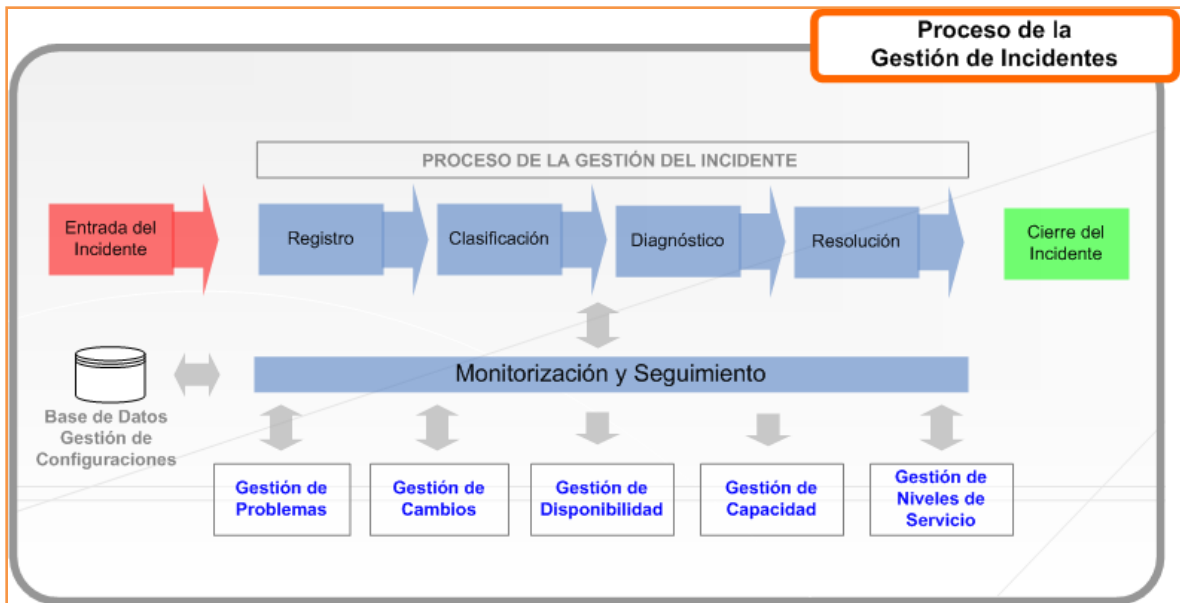
El proceso de escalado puede resumirse gráficamente como sigue:



El diseño de las políticas de escalonamiento va en función de qué tipo de escalamiento se adopte, queda a discreción de cada grupo CSIRT el diseñar su respectiva política.

Proceso

El siguiente diagrama muestra los procesos implicados en la correcta Gestión de Incidentes.



- **Gestión de Configuraciones:** la base de datos de Gestión de Configuraciones juega un papel clave en la resolución de incidentes pues, por ejemplo, nos muestra información sobre los responsables de los componentes de configuración implicados. La base de datos de Gestión de Configuraciones también nos permite conocer todas las implicaciones que pueden tener en otros servicios el malfuncionamiento de un determinado elemento de configuración.
- **Gestión de Problemas:** ofrece ayuda a la Gestión de Incidentes informando sobre errores conocidos y posibles soluciones temporales. Por otro lado, establece controles sobre la calidad de la información registrada por la Gestión de Incidentes para que ésta sea de utilidad en la detección de problemas y su posible solución.
- **Gestión de Cambios:** la resolución de un incidente puede generar una petición de cambio que se envía a la Gestión de Cambios. Por otro lado, un determinado cambio erróneamente implementado puede ser el origen de múltiples incidencias y la Gestión de Cambios debe mantener cumplidamente informada a la Gestión de Incidencias sobre posibles incidencias que los cambios realizados puedan causar en el servicio.
- **Gestión de Disponibilidad:** utilizará la información registrada sobre la duración, el impacto y el desarrollo temporal de los incidentes para elaborar informes sobre la disponibilidad real del sistema.
- **Gestión de la Capacidad:** se ocupará de incidentes causados por una insuficiente infraestructura IT. (Insuficiencia del ancho de banda, capacidad de procesamiento, etc.)
- **Gestión de Niveles de Servicio:** La Gestión de Incidentes debe tener acceso a los niveles de servicio acordados con el cliente para poder determinar el curso de las acciones a adoptar. Por otro lado, la Gestión de Incidentes debe proporcionar periódicamente informes sobre el cumplimiento de los niveles de servicio contratados.

6.4 Eliminación y recuperación del incidente

Pasos recomendados para el soporte de Incidentes

- Reporte de un incidente a ser atendido

Las personas autorizadas por parte de las Unidades de Negocio reportan situaciones o funcionamientos anormales en la infraestructura IT (equipos, redes, servidores, servicios, etc.) Los incidentes son reportados por diferentes medios: Email, personalmente, por Web utilizando el Portal de Autoservicio y por Teléfono.

- Registro y documentación del incidente reportado

El agente de soporte o usuario identifica el tipo de incidente (alertas, errores, caídas del sistema, actualizaciones, etc.) Que se reporta y la prioridad (alta, media, baja) que se debe asignar. Registra la persona que reporta el incidente y el elemento involucrado en el incidente, obtiene instantáneamente una visión de toda la información de la persona, ¿quién es?, ¿cómo debe ser atendida?, incidentes pendientes, etc. Realiza un diagnóstico inicial de lo que sucede.

- Preparación de la solución del incidente

Cuando el agente de soporte o usuario registra la información básica del incidente, se asigna el tiempo máximo de solución que depende de los acuerdos de nivel de servicio pactados. Se despliegan soluciones sugeridas tomadas de la historia de incidentes similares y de la Base de Conocimiento. Se sugieren tareas para planear la solución del servicio con tareas internas. Y se despliegan plantillas con ayudas para diagnosticar el problema y para comunicarse con el Cliente: plantillas para envío de email y para llamadas entrantes y salientes.

- Proceso de solución utilizando herramientas de software como apoyo.

Se envían alertas por email para listas de notificación previamente creadas. Se remite el incidente a otros usuarios (responsables de la solución) si es necesario. Se realizan tareas internas para completar actividades necesarias en la solución. Se le comunica a la unidad de negocio por diferentes medios los avances realizados en la solución del incidente. Todo el proceso se realiza teniendo en cuenta el tiempo máximo de solución asignado al incidente, para lo cual se envían alertas por email a los responsables.

- Identificación y solución de problemas

Como parte del proceso de solución se analiza toda la información de incidentes similares sobre los mismos elementos de la infraestructura IT, los diagnósticos realizados y las tareas o actividades internas realizadas para dar una solución. Si se identifican situaciones recurrentes, se registra la causa común como un problema, que

al ser solucionada, soluciona todos los incidentes que tienen esa causa en común. De esa manera se evita que se presenten incidentes similares y se mejora el nivel de satisfacción de las unidades de negocio con el soporte técnico que se presta.

- Cierre exitoso del incidente

Se comunica a la unidad de negocio el cierre del incidente reportado cumpliendo las políticas de servicio prometidas y respetando los tiempos máximos de solución pactadas según el tipo de incidente que se reportó y la prioridad asignada. Se documenta detalladamente el cierre del servicio para que enriquezca la Base de Conocimiento de la organización y pueda ser utilizada como una solución sugerida para un próximo servicio.

También es importante contar con procedimientos de mejora continua sobre las distintas actividades de soporte que se proveen. Para ello se recomiendan los siguientes puntos:

- Planeación de Cambios de Infraestructura IT:

Es coordinar cambios con mínimo impacto y riesgo aceptable. Ayuda a que los gerentes tecnológicos y los gerentes de áreas de negocio estén informados e involucrados sobre qué cambios se realizarán y que no haya lugar a sorpresas inesperadas. Se asignan responsables y niveles de autorización para aprobar los cambios propuestos. Un cambio soluciona problemas, que a su vez evita la ocurrencia de incidentes.

- Implementación de Cambios con Entregas Controladas:

Es planear y tener a todos informados de la implementación de cambios en la infraestructura con mínimas interrupciones y riesgos. La gestión de entregas complementa la gestión de cambios. En los cambios se planea y ejecuta en ambientes de calidad (pruebas) y en la entrega se ejecuta e implementa ya en sistemas de producción.

- Retroalimentación y Mejora del Proceso de Soporte Técnico:

Se analiza toda la información generada en la atención y solución de incidentes para mejorar continuamente el proceso de soporte técnico a las unidades de negocio. Se mejora la base de conocimientos, las soluciones y tareas sugeridas. Los índices de satisfacción de las unidades de negocio mejoran y se impulsa el crecimiento.

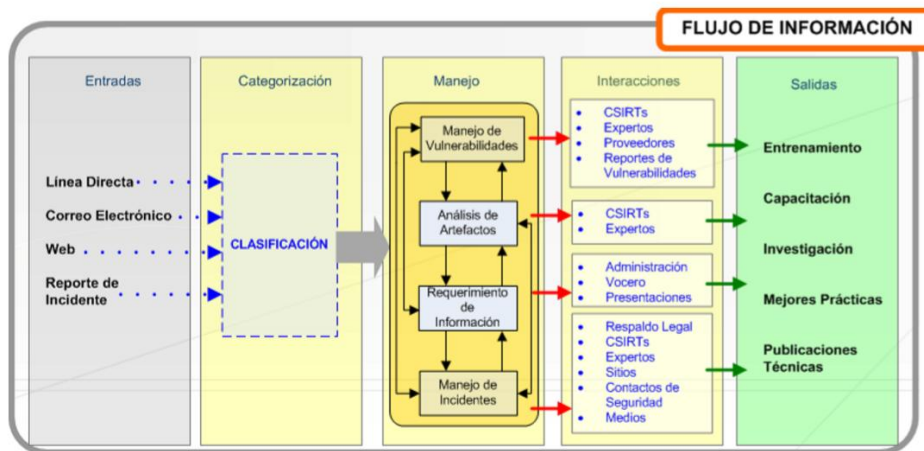


Figura 5: Flujo de Información en un CSIRT.

6.5 Informe de incidentes

En primera instancia se examina el incidente con ayuda de la base de datos de conocimiento para determinar si se puede identificar con alguna incidencia ya resuelta y aplicar el procedimiento asignado.

Si la resolución del incidente se escapa de las posibilidades del Centro de Servicios éste redirecciona el mismo a un nivel superior para su investigación por los expertos asignados. Si es-estos expertos no son capaces de resolver el incidente se seguirán los protocolos de escalado predeterminados.

Durante todo el ciclo de vida del incidente se debe actualizar la información almacenada en las correspondientes bases de datos para que los agentes implicados dispongan de cumplida información sobre el estado del mismo.

Si fuera necesario se puede emitir una petición de cambio. Si la incidencia fuera recurrente y no se encuentra una solución definitiva al mismo se deberá informar igualmente a la Gestión de Problemas para el estudio detallado de las causas subyacentes.

Cuando se haya solucionado el incidente se:

- Confirma con los usuarios la solución satisfactoria del mismo.
- Incorpora el proceso de resolución a la base de datos de conocimiento.
- Reclassifica el incidente si fuera necesario.
- Actualiza la información en la base de datos de gestión de configuraciones sobre los elementos de configuración implicados en el incidente.
- Cierra el incidente.

Registro

La admisión y registro del incidente es el primer y necesario paso para una correcta gestión del mismo. Las incidencias pueden provenir de diversas fuentes tales como usuarios, gestión de aplicaciones, el mismo Centro de Servicios o el soporte técnico, entre otros.

El proceso de registro debe realizarse inmediatamente pues resulta mucho más costoso hacer-lo posteriormente y se corre el riesgo de que la aparición de nuevas incidencias demore indefinidamente el proceso.

- **La admisión a trámite del incidente:** el Centro de Servicios debe de ser capaz de evaluar en primera instancia si el servicio requerido se incluye en el SLA del cliente y en caso contrario reenviarlo a una autoridad competente.
- **Comprobación de que ese incidente aún no ha sido registrado:** es común que más de un usuario notifique la misma incidencia y por lo tanto han de evitarse duplicaciones innecesarias.
- **Asignación de referencia:** al incidente se le asignará una referencia que le identificará unívocamente tanto en los procesos internos como en las comunicaciones con el cliente.

Registro inicial: se han de introducir en la base de datos asociada la información básica necesaria para el procesamiento del incidente (hora, descripción del incidente, sistemas afectados...).

- **Información de apoyo:** se incluirá cualquier información relevante para la resolución del incidente que puede ser solicitada al cliente a través de un formulario específico, o que pueda ser obtenida de la propia base de datos de la gestión de la configuración (hardware interrelacionado), etc.
- **Notificación del incidente:** en los casos en que el incidente pueda afectar a otros usuarios estos deben ser notificados para que conozcan como esta incidencia puede afectar su flujo habitual de trabajo.

Clasificación

La clasificación de un incidente tiene como objetivo principal el recopilar toda la información que pueda ser de utilizada para la resolución del mismo.

El proceso de clasificación debe implementar, al menos, los siguientes pasos:

- **Categorización:** se asigna una categoría (que puede estar a su vez subdividida en más niveles) dependiendo del tipo de incidente o del grupo de trabajo responsable de su re-resolución. Se identifican los servicios afectados por el incidente.

- **Establecimiento del nivel de prioridad:** dependiendo del impacto y la urgencia se de-termina, según criterios preestablecidos, un nivel de prioridad.
- **Asignación de recursos:** si el Centro de Servicios no puede resolver el incidente en primera instancia designará al personal de soporte técnico responsable de su resolución (segundo nivel).
- **Monitorización del estado y tiempo de respuesta esperado:** se asocia un estado al incidente (por ejemplo: registrado, activo, suspendido, resuelto, cerrado) y se estima el tiempo de resolución del incidente en base al nivel de servicio correspondiente y la prioridad.

7. REFERENCIAS

- [1] <http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=3>
- [2] <http://es.kioskea.net/contents/18-escaneres-de-vulnerabilidad-analisis-de-puertos>
- [3] <http://insecure.org/tools/tools-es.html>
- [4] <http://www.javeriana.edu.co/biblos/tesis/ingenieria/tesis181.pdf>
- [5] <http://tecnologiaedu.us.es/nweb../cursos/asig-nntt/html/pedro-web/6.htm>
- [6] http://www.capacinet.gob.mx/Cursos/Tecnologia%20amiga/desarrolladordesoftware/Seguridad_Internet_SE.pdf
- [7] <http://danielomarrodriguez.blogspot.com/2008/01/mejores-practicas-y-herramientas-para.html>
- [8] http://www.proyectoamparo.net/files/manual_seguridad/manual_basico_sp.pdf
- [9] http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica