NOMBRE VALENCIA ARRIBAS FRANCISCO - NIF 50103477R

Firmado digitalmente por NOMBRE VALENCIA ARRIBAS FRANCISCO - NIF 50103477R
Nombre de reconocimiento (DN): CN = NOMBRE VALENCIA ARRIBAS FRANCISCO - NIF 50103477R, C = ES, O = FNMT, OU = FNMT Clase 2 CA
Motivo: Soy el autor de este documento
Fecha: 2009.07.01 17:22:30 +02'00'

Francisco Valencia Arribas
www.francisco-valencia.es

1 INTRODUCCIÓN

Este documento ha sido elaborado al objeto de dotar de una guía sencilla que sirva como referencia para la obtención del Certificado CompTIA Security+.

Su contenido ha sido casi íntegramente obtenido del libro “CompTIA Security+ Deluxe Study Guide”, editado por Wiley Publishing y escrito por Emmett Dulaney, a quien reconozco y agradezco su obra.

Este documento me ha sido de ayuda para la obtención del certificado CompTIA Security+, y confío que, al estar redactado en castellano y plasmar sólo las ideas fundamentales de la certificación, te sea de ayuda a ti también.

En mi página encontrarás este documento y posibles mejoras o nuevas versiones sobre el mismo, además de otra documentación que voy preparando. Desde ella puedes contactar conmigo, estaré encantado de atenderte.

www.francisco-valencia.es.

Un cordial saludo, gracias por leer este documento y suerte con tu certificación.

Francisco Valencia Arribas

2 CONCEPTOS BÁSICOS DE SEGURIDAD

2.1 DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La definición de una correcta política de seguridad se enfrenta a dos problemas. El primero de ellos es que el propio concepto de seguridad tiene varias interpretaciones (robos, seguridad informática, protección de información, etc). El segundo es que las políticas de seguridad restan comodidad en el uso de las TIC, con lo que existe cierta oposición a su implementación.

Realmente el término de seguridad de la información implica tres áreas:

- **Seguridad física:** Proteger las propiedades de un modo físico, evitando que puedan ser robadas o dañadas. Para ello hay que evitar que el lugar donde se alojan los sistemas sea considerado un objetivo fácil. Hay que incluir en el mismo seguridad frente a la intrusión (cámaras, controles de acceso, etc). Por último, es necesario disponer de un plan para recuperar la información que haya podido ser robada.

- **Seguridad Operativa**: Hace referencia al modo de realizar las actividades de la empresa (acceso a la red, a la información, políticas de passwords, procesos de autenticación y control de acceso, etc)

- **Gestión de la seguridad**: La gestión de la seguridad es el establecimiento de unas políticas de seguridad, y la gestión del cumplimiento de las mismas. El, establecimiento de una política adecuada de seguridad debe incluir:

    - **Políticas administrativas**: Las políticas establecen la guía para realizar backups, upgrades, auditorías, monitorización, etc. Deben establecer claramente indicar la periodicidad y el momento de realizar upgrades, por ejemplo. Debe definir la persona responsable de cada actividad relacionada con la seguridad, y quien debe tomar las decisiones relativas a la misma. Debe establecer los procedimientos de actuación en caso de verse vulnerada la seguridad de la empresa.

    - **Planes de recuperación ante desastres**: El Plan de recuperación ante desastres (DRP) debería establecer el mecanismo de actuación ante cualquier posible evento que ponga en riesgo la continuidad de la empresa. Es caro y complicado de realizar, pero resulta imprescindible. Todas las personas o departamentos de la empresa deben conocerlo y deben conocer las acciones que ellos deben realizar de cara a un desastre.

    - **Políticas de información**: Hace referencia a aspectos relacionados con el flujo de la información (acceso, clasificación, marcado, almacenado, transmisión, destrucción, etc) . Niveles habituales son:

        - Pública
        - Interna
        - Privada
        - Confidencial

    - **Políticas de seguridad**: Describe la configuración de redes y sistemas, instalación de software, hardware, conexiones de red, cifrado, antivirus, etc. Definen también la seguridad de acceso al CPD (identificación y autenticación).

    - **Requerimientos de diseño de software**: Muchas compañías realizan sus propias aplicaciones para realizar funciones internas dentro de la empresa (producción, control, I+D..,). En el diseño de estas aplicaciones debe asegurarse que son integrables con las políticas de seguridad de la empresa.

    - **Políticas de uso**: Las políticas de uso definen el modo en que deben utilizarse la información y los recursos de la empresa. Incluyen aspectos como confidencialidad, propiedad intelectual, etc. Dentro de esta política pueden tomarse acciones de concienciación y/o legales para asegurar el correcto uso.

    - **Políticas de gestión de usuarios**: Definen el modo en que se tratan los aspectos relativos a los usuarios para realizar su función diaria habitual (altas de nuevos usuarios, bajas, cambios de funciones, ascensos, etc). Muchos ataques son provocados por personas con permiso de realizar su acción maliciosa o errónea.

2.2 OBJETIVOS PERSEGUIDOS CON LA SEGURIDAD DE LA INFORMACIÓN

Todas las políticas de la seguridad de la información deben perseguir tres objetivos fundamentales:

- **Prevención**: Estrategias orientadas a evitar que los ataques sucedan. Es mucho más fácil evitar que suceda un ataque que corregir sus efectos.
- **Detección**: Identificar los eventos en el momento que éstos suceden. Los peores ataques duran meses, incluso años, y nunca son detectados, por lo que es preciso, para poder protegerse, una correcta detección.
- **Respuesta**: Desarrollo e implantación de estrategias para evitar un ataque. Afectan a multitud de factores.

2.3 PROCESOS DE SEGURIDAD

La seguridad debe ser una combinación de procesos, procedimientos y políticas. Afecta a aspectos técnicos y a factores humanos. Los factores técnicos incluyen las herramientas que se instalan en los sistemas:

- **Antivirus:** Sofware instalado en los sistemas que previenen a los mismos ante ataques de virus, gusanos y otro malware. Es preciso asegurar la actualización de este software, ya que cada día aparecen nuevos métodos de ataques a los sistemas.
- **Control de acceso:** El control de acceso limita o controla el acceso a los recursos de la empresa:
    - **Mandatory Access Control (MAC):** Es un modelo estático que utiliza un conjunto de privilegios de acceso a los archivos de los sistemas. Los administradores establecen el control de un modo centralizado, que puede ser muy restrictivo. MAC utiliza etiquetas que identifican el nivel de sensibilidad de cada objeto. Al tratar de acceder a dicho objeto, se analiza la etiqueta para ver si debe autorizarse el acceso o no. En definitiva, solo se da acceso a los recursos a usuarios específicamente indicados.
    - **Discretionary Access Control (DAC):** El propietario del recurso establece los privilegios necesarios para acceder a su información. La diferencia entre DAC y MAC es que las etiquetas no son obligadas, aunque pueden utilizarse. En DAC, el propietario puede establecer una lista de acceso para permitir o denegar el acceso.
    - **Role-Based Access Control (RBAC):** Permite el acceso o no a los sistemas en base a un rol asignado a la persona que pretende acceder a los mismos.
- **Autenticación:** La autenticación es el modo de saber que quien se presenta a un sistema es quien dice ser. Se basa en tres métodos que pueden estar solos o combinados (Lo que sabe, lo que tiene, lo que es)
    - **Biometría:** Se usan características físicas para identificar al usuario (huella dactilar, voz, iris, etc)
    - **Certificados:** El empleo de certificados digitales consiste en un dispositivo de acceso (bien físico como tarjetas o bien solo software), que se presenta al tratar de acceder a un sistema. En este certificado consta una entidad de confianza corrobora la validez de dicho certificado.
    - **CHAP (Challenge Handshake Autentication Protocol):** CHAP no utiliza user/password. En lugar de eso, el cliente envía una petición de autenticación al servidor. Éste, le envía un Challenger (una trama) al cliente, el cual la cifra empleando su password. El resultado cifrado es enviado de vuelta al servidor, quien la comprueba con su propio resultado tras aplicar el mismo cifrado.
    - **Kerberos:** Kerberos es una muy segura forma de autenticación. Utiliza un KDC (Key Distribution Center). El KDC autentica al sistema y genera un ticket para él. El usuario que pretende acceder al sistema solicita antes un ticket al KDC, que luego presenta al sistema al que pretende acceder. De este modo ambos son autenticados, servidor y cliente. La criptografía utilizada para el intercambio de tickets es simétrica. El sistema necesita disponer de una buena fuente de tiempo (Servidor NTP o similar), ya que se basa en un análisis de tiempos para entregar tickets.

- **Autenticacion multi-factor:** Consiste en presentar una doble autenticación para poder acceder al sistema (password + certificado, por ejemplo).

- **Autenticación mutua:** Consiste en el sistema en el que el usuario debe autenticarse al servidor y viceversa.

- **PAP (Password Autentication Protocol):** Realmente no ofrece mucha seguridad. Con PAP el usuario y la password son enviados al sistema al que se desea acceder y éste lo comprueba con una lista, autorizando o no el acceso.

- **Tokens:** Son parecidos a los certificados, contienen el permiso de acceso al sistema. Aportan mayor seguridad que las passwords. Son de un solo uso, por lo que una vez que un usuario ha accedido empleando un token, éste deja de ser válido. Existen Tokens asíncronos y Tokens síncronos. Los asincronos generan una password que es válida hasta que se utiliza. Los síncronos generan una password que dura solamente un determinado tiempo, y necesitan estar sincronizados con el servidor. Dado que las passwords van cambiando en cada uso, no puede utilizarse como elemento de autenticación en un entorno de Single Sign-On.

- **Smart cards:** Es una tarjeta que da acceso a determinados recursos. Contiene información sobre los privilegios de acceso y la identidad del usuario. A menudo requieren ser acompañadas de una password personal (PIN)

- **User / password:** Se entrega una pareja de user/password para acceder al sistema.

2.4 TOPOLOGÍAS DE SEGURIDAD

En este apartado se describe el diseño, topología e implementación de la red desde un punto de vista de seguridad. Se tratan 4 áreas relativas con la topología de la red:

- **Objetivos de diseño:** Cuando se realiza el diseño de la red debe tenerse en consideración:
  - **Confidencialidad:** Asegurar que nadie es capaz de acceder a la información salvo su destinatario
  - **Integridad:** Asegurarse que nadie es capaz de modificar la información que recibe el receptor
  - **Disponibilidad:** Asegurarse que la información siempre esté disponible
  - **Contabilidad:** Registrar todos los accesos a la información, y quien ha hecho que con ella.

- **Zonas de seguridad:** Es necesario definir zonas que aíslen determinados sistemas de usuarios que no deben tener acceso a la misma. Pueden definirse cuatro tipos de zonas:

  - **Internet:** Es la red de redes. Insegura por definición.
  - **Intranet:** Redes privadas administradas por una misma entidad.
  - **Extranet:** Intranets extendidas a otras redes de confianza (clientes, Partners, etc).
  - **DMZ (Zona desmilitarizada):** Área para poner servicios públicos, a los que accederán usuarios no confiables.

- **Tecnologías:** Las estrategias de diseño de redes evolucionan según lo hacen las nuevas tecnologías. Nuevas tendencias como el empleo de máquinas virtualizadas, VoIP, y otras modifican el modo de analizar la seguridad en las redes

- **Requerimientos de negocio:** Es uno de los más importantes apartados de la seguridad, ya que en definitiva el objetivo de la seguridad es la protección del negocio soportado por los sistemas cubiertos. Un gestor de seguridad debe:

  - **Identificar propiedades:** Consiste en analizar y dar un valor a todas las propiedades de la empresa. El apartado más complicado suele ser hacerlo con la información, cuando ésta debe considerarse como la propiedad más importante de la empresa.

  - **Identificar riesgos:** Consiste en identificar lo que sucedería, en términos económicos, de negocio, etc cuando las propiedades identificadas son robadas, perdidas, no están disponibles, etc.

- **Identificar amenazas:** Es necesario identificar las amenazas reales a las que está sujeta la empresa. Las amenazas hay que dividirlas en amenazas externas (un hacker externo, una tormenta), y las internas (un empleado descontento, un mal administrador de sistemas)

- **Identificar vulnerabilidades:** Todos los sistemas TIC están sujetos a vulnerabilidades, que pueden ser aprovechados para acceder a los sistemas. Es responsabilidad de los técnicos de seguridad identificar estas vulnerabilidades para anticiparse a ellas.

Topologías de seguridad:

- **Screened host Gateway:** Firewall a nivel de red.
- **Circuit-level Gateway:** Firewall a nivel de session.
- **Bastion Host:** Es un firewall con dos interfaces que protege el paso por ellos a determinados puertos, direcciones, protocolos, etc.
- **Screened subnet Gateway:** Tiene dos firewalls que aíslan la LAN de Internet para crear una DMZ entre ellos

3 IDENTIFICACIÓN DE RIESGOS

Es necesario realizar un adecuado análisis de riesgos para conocer en qué medida se es vulnerable a ataques. Este análisis debe ser realizado en base a dos criterios:

- **Análisis de riesgos cuantitativo:** Se realiza un análisis en base a términos numéricos de probabilidades y consecuencias de que algo falle.

- **Análisis de riesgos cualitativo:** Se aplica valor a las amenas y sus consecuencias en base a medidas subjetivas, experiencias, etc.

3.1 CALCULANDO ESTRATEGIAS DE ATAQUES

Un ataque ocurre cuando un individuo o grupo intenta acceder, modificar o dañar propiedades. Los ataques pueden ser:

- **Ataque de acceso:** Alguien ha accedido a los datos o a los recursos por parte de alguien no autorizado a hacerlo. Algunos de los métodos que se emplea para realizar estos ataques son:

    - **Búsqueda en la basura:** Consiste en analizar los restos de las organizaciones, en busca de información.

    - **Robo de información en ruta:** Consiste en interceptar o leer información que se encuentra en el camino entre el emisor y el receptor.

    - **Eavesdropping:** Consiste en escuchar partes de una conversación o tráfico de red.

    - **Snooping:** Alguien busca en los ficheros o documentos esperando encontrar algo valioso, pero sin saber lo que busca exactamente.

    - **Interception:** Lectura de la información cuando ésta viaja del origen al destino.

- **Ataque de repudio:** Alguien quiere modificar información contenida en los sistemas. Son ataques difíciles de detectar. Un ataque típico es el WEB defacement, que cambia el contenido de una página WEB.. Una variación a este ataque es el ataque de reputación, que no modifica la información, pero hace ver que la fuente de la misma no es fiable. Para hacer estos ataques antes es necesario realizar un ataque de acceso.

- **Ataque de denegación de servicio (DoS):** Intentan hacer que el sistema sea incapaz de cumplir su función. Muchos se basan en consumir los recursos de la victima, hasta que no puede hacer su función normal. Una modalidad es el ataque de DoS distribuido (DDoS), donde muchas máquinas (zombies) controladas por un atacante, lanzan al mismo tiempo un ataque contra la víctima, multiplicando la potencia del mismo y dificultando la localización real de la fuente.

3.2 ATAQUES COMUNES

- **Ataques de backdoor:** Puede existir una puerta trasera bien por que se ha desarrollado para labores de mantenimiento o bien porque se ha desarrollado un software que la crea. La puerta trasera da acceso al sistema sin los mecanismos de control de acceso principales.

- **Ataques de spoofing:** Un spoofing es una suplantación de identidad. Los ataques más comunes son IP spoofing y DNS spoofing.

- **Ataques de hombre en el medio:** Son ataques más sofisticados. El método es poner un código entre el usuario y el servidor, y capturar el tráfico que circula entre ambos, haciendo creer a cada uno que está hablando con el otro.

- **Ataques de repetición:** En una red local, los datos como user y password son enviados por la red. un ataque de repetición consiste en capturar esa información y reenviarla. Puede ocurrir incluso con certificados como Kerberos.

- **Ataques de adivinación de password:** Son ataques de fuerza bruta o basada en diccionarios para tratar de lograr la password de acceso a un sistema.

- **Ataques de escalada de privilegios:** Están asociados con Bugs en el software, que le permitiría a la aplicación (y a quien la controle) obtener permisos superiores a los que originalmente tenia la aplicación.

- **HOAX:** No es realmente un ataque, sino un mensaje que avisa de la presencia de un ataque. Hace perder productividad y en ocasiones, al tratar de solucionar el falso ataque, se pueden causar daños.

3.3 ASPECTOS RELACIONADOS CON LA SEGURIDAD DE TCP/IP

3.3.1 INTRODUCCIÓN A TCP/IP

La pila TCP está basada en cuatro niveles:

- **Capa de Aplicación:** Permite a las aplicaciones utilizar la pila TCP/IP. Aquí hay protocolos como HTTP, FTP, SMTP, DNS, RIP, SNMP, POP, etc

- **Capa de Transporte:** En la capa de transporte se realiza la sesión y se ofrecen los servicios de comunicación de datos a las capas superiores. Trabajan en ella los protocolos TCP y UDP. Se establecen sesiones en unas direcciones internas al servidor llamados puertos. Hay 65536. Los primeros 1024 son los llamados well-know ports, registrados en IANA. UDP no establece conexión. TCP establece conexión mediante “trhree-way handshake”. EL cliente lanza una señal SYN al servidor, el cual contesta con una señal SYN/ACK, y el cliente contesta con ACK.

- **Capa de Internet:** Aquí se realiza el routing y direccionamiento. Protocolos de esta capa son IP, ARP, ICMP e IGMP.

- **Capa de Interface de red:** Es la capa donde los datos se convierten en señales eléctricas, comunicándose la pila con la tarjeta de red.

Para poder actuar con la pila TCP, los sistemas operativos establecen API’s (Application Programming Interface). El API de Windows que permite actuar con la pila IP se llama Windows socket (Winsock).

3.3.2 ATAQUES TCP/IP

- **Snifar la red:** Mediante un PC con una tarjeta en modo promiscuo, se puede recibir toda la información que circula por la red, y analizar su contenido

- **Escaneo de puertos:** Consiste en atacar a todos los puertos de una máquina determinada, para saber si están abiertos o no. Además, por muchos de ellos se prestará información que ayuda a conocer parámetros del sistema.

- **Ataque TCP SYN o TCP ACK Floyd atack:** El propósito es denegar el servicio. El ataque consiste en lanzar muchos inicios de sesión (paquetes ACK) pero no cerrar ninguna. Los servidores tienen un límite de sesiones que pueden tener en este estado, con lo que al llenarse deja de estar operativo.

- **Ataque de número de secuencia TCP:** El atacante coge el control en un extremo de una sesión TCP. Cada vez que se manda un paquete TCP, tanto el cliente como el servidor lo hacen con un número de secuencia. Entonces el atacante genera un paquete idéntico con un número de sesión distinto (por ejemplo superior). La sesión se cae o se hace inestable, al esperar las máquinas el paquete con el número adecuado.

- **Ataque TCP Hijacking:** También se llama sniffing activo. Consiste en desconectar la máquina de uno de los extremos y hacerse pasar por ella en una sesión TCP con un servidor.

- **Ataque por inundación de UDP:** Se envían largas tramas de UDP contra un servidor, para dejarlo inoperativo

- **Ataque ICMP "ping of death":** Se lanza un broadcast ICMP desde la dirección de la máquina a atacar. Al responder todas las máquinas contra ese origen, le crean un problema de disponibilidad.

- **ICMP Tunneling**: Los paquetes ICMP llevan determinada información, que puede utilizarse para pasar información entre dos máquinas, burlando niveles de seguridad como los firewalls.

3.4 EXPLOITS DE SOFTWARE

Son ataques lanzados contra aplicaciones de alto nivel. Los exploits pueden acceder a través de vulnerabilidades de la aplicación, mediante virus, etc:

- **Exploit contra Base de datos:** A pesar de que las bases de datos exigen autenticación del cliente, mediante un spoofing del cliente podrían enviarse comandos a una base de datos.

- **Exploit contra aplicación**: Determinadas aplicaciones soportan la ejecución de macros (como MSOffice). A traves de un macro virus puede realizarse un ataque que se ejecuta junto con las aplicación.

- **Exploit E-mail**: Una vulnerabilidad habitual en los clientes de correo electrónico permite el acceso a la agenda, con lo que es posible enviar correos que propaguen virus.

- **Spyware**: Intentan pasar inadvertidos en la máquina atacada. Monitoriza determinada información y la envía a un servidor, o hace entregar pop-ups , etc.

- **Rootkits**: Un rootkit es un programa que tiene la habilidad de ocultar funciones realizadas por el sistema operativo (por ejemplo, puede ocultarse para que el sistema operativo no vea su proceso funcionando). Puede instalarse a nivel de kernel, proceso y aplicación, y proporciona funcionalidad más avanzada que los backdoors.

- **Backdoors**:

3.5 CÓDIGOS MALICIOSOS

- **Virus:** Un virus es un pedazo de software diseñado para infectar un sistema. Pueden solo residir en la máquina o ser muy destructivos para ella. En la mayoría de los casos hacen el sistema inoperable y tratan de infectar a otros sistemas. Hay varios tipos de virus:

    - **Armored**: Es un virus de muy difícil detección. Se protegen de modo que los analizadores de código no lo interpretan como malicioso.

    - **Companion**: Se introducen dentro de código legítimo.

    - **Macro**: Son macros que se ejecutan en aplicaciones que las soportan (Como office)

    - **Multipartite**: Ataca al mismo tiempo varios elementos del sistema.

    - **Phage**: Infecta múltiples tipos de archivos, infecta varias aplicaciones y bases de datos. No hay forma de eliminarlo, salvo reinstalando el sistema infectado.

    - **Polymorphic**: Son virus capaces de cambiar de aspecto para evitar ser detectados.

    - **Retrovirus**: Es un virus que ataca al antivirus

    - **Stealth**: Virus que se enmascara en otras aplicaciones para evitar ser detectado.

    - Los virus realizan las siguientes funciones:
        - **Replication mechanism:** Un virus intenta copiar su propio código en otra aplicación, y esperar a que la nueva sea ejecutada en otras máquinas.

  - **Activation mechanism:** La mayor parte de los virus necesitan que el usuario haga algo (ejecutar un fichero, introducer un disquette, etc).
  - **Objective:** Muchos virus no tienen un objetivo concreto, pero otros buscan eliminar alguna información, bloquear el sistema, etc.

- **Caballos De Troya:** Son programas que entran en un sistema o red con apariencia de ser otro programa que si es autorizado por un usuario a entrar.

- **Bomba lógica:** Son programas que se ejecutan cuando sucede determinado evento. (por ejemplo hay conexión a Internet y además se ha iniciado un procesador de textos)

- **Gusanos:** La diferencia con un virus es que el gusano se reproduce a si mismo, es auto-contenido y no necesita una aplicación de host para ser transportado.

Para evitar estas amenazas, es necesario disponer de una aplicación antivirus, con el fichero de firmas actualizado. Además, es imprescindible la concienciación del usuario.

3.6 INGENIERIA SOCIAL

La ingeniería social es el ataque por medio de engaños a las personas, a los usuarios, y no a los sistemas. De este modo, se persigue lograr información, como usuarios/passwords y otros.Un modo de ingeniería social es el phishing, que hace que el usuario de determinada información a una página que está aparentando ser otra de confianza.

3.7 AUDITORIA DE PROCESOS Y ARCHIVOS

Muchos sistemas generan archivos de logs, en los que se registran muchos datos relacionados con los accesos al sistema, y los movimientos de dichos accesos dentro de los sistemas. Es una información valiosa que es necesario auditar de manera periódica. Los atacantes tratarán de eliminar estos ficheros, a fin de que no exista posibilidad de tracear sus acciones.

Debería disponerse de un software de auditoría, que analice los sistemas (escaneo de puertos, lectura de logs, etc), para detectar vulnerabilidades sobre el sistema.

4 INFRAESTRUCTURA Y CONECTIVIDAD

4.1 INFRAESTRUCTURA DE SEGURIDAD

La infraestructura de seguridad tiene que ver con el flujo que la información debe seguir entre los diferentes sistemas de la red y con éstos mismos, incluyendo elementos tanto hardware como software:

- **Elementos Hardware:** Elementos físicos como servidores, routers, switches, firewalls, etc. Desde el punto de vistas de seguridad, es necesario analizar la red desde el punto de vista de cada uno de los elementos hardware que la componen.

- **Elementos Software:** La función del software es hacer a los elementos útiles y fáciles de operar. Todos los elementos de la red disponen de su propio software. Muchas de las vulnerabilidades de seguridad surgen por que cada elemento trabaja de un modo independiente.

4.2 DISPOSITIVOS DE INFRAESTRUCTURAS DE RED

- **Firewalls:** El firewall es la primera línea de seguridad de una red. Pueden ser dispositivos stand-alone o estar embebidos en routers o servidores. La misión de un firewall es aislar una red de otra, permitiendo el flujo exclusivamente de la información autorizada. Hay varios tipos de firewall:

    - **Packet Firewall:** Bloquea o permite el paso de paquetes basándose en direcciones IP o aplicaciones (puertos de nivel 4). Este firewall no analiza el contenido de los paquetes, lo que quiere decir que permitirá pasar cualquier tráfico si su nivel 3 y 4 están en la lista de autorizados, aunque sea tráfico malicioso.

    - **Proxy Firewall o Aplication-Level Gateway:** Es un dispositivo que actúa como intermediario entre una red y el resto. El proxy analiza el tráfico y toma una decisión en cuanto a reenviar el tráfico o no. Proporciona mejor seguridad que un packet firewall por incrementar la inteligencia del mismo, ya que puede analizar la información a nivel de aplicación. De hecho, pueden existir proxy firewall dedicados exclusivamente a determinados protocolos.

    - **Statefull Inspection Firewall (SPI):** Mientras que la mayor parte de los dispositivos de networking y seguridad no almacena información de los paquetes que ha reenviado (en cuanto son reenviados o tirados son olvidados), un statefull inspection firewall almacena información relativa a los canales de comunicación que se han establecido y paquetes anteriores reenviados, especialmente UDP e ICMP. De este modo, puede detectar patrones de ataques en tiempo real.

    - **Circuit-Level Gateway:** Analiza las sesiones TCP a nivel de sesión, entre máquinas internas y máquinas de Internet. Es capaz de evitar ataques de DoS. Es igual que un proxy firewall, pero a nivel de sesión, no de aplicación.

- **Hub:** Un Hub es sólo un dispositivo que permite enlazar la red. Permite el paso de todas las tramas hacia todos los puertos. Permite escanear la información de la red.

- **Modem:** Dispositivo para establecer comunicaciones a través de línea telefónica. Como aceptan las llamadas entrantes, permiten establecer un camino inseguro de comunicaciones contra el sistema al que está conectado.

- **Remote Acccess Services:** Es el servicio que permite ser conectado por sistemas remotos. En servicio de Microsoft se llama RRAS (Routing and Remote Access Services). Con este servicio permite compartir su consola. Existen aplicaciones VNC (Virtual Network Computing) como PC Anywhere que permiten esta conexión. Todas estas aplicaciones dejan una puerta abierta para recibir conexiones, con lo que es necesario tener la precaución de activarlo sólo cuando vaya a usarse y de un modo controlado.

- **Routers:** Los routers establecen caminos de comunicación entre redes, y almacenan información acerca del camino que hay que seguir, de forma estática o dinámica. Los routers pueden ser configurados para actuar como un packet firewall.

- **Switches:** Los switches mejoran la eficiencia de la red frente a un firewall, e incrementa el nivel de seguridad al dirigir el tráfico sólo por el puerto en el que el destino está conectado.

- **PBX:** Una Private Branch Exchange (PBX) permite conectar redes de voz, datos, movilidad, etc. Se trata de un objetivo claro para un ataque. Las tecnologías de VoIP incrementan esta posibilidad.

- **Virtual Private Networks:** Una VPN es una conexión privada realizada a través de una red pública. Aparenta que las redes remotas sean la misma. El principal aspecto a considerar en las VPN es el cifrado.

- **Wireless Access Points:** Dispositivo que pemite el acceso a la red a dispositivos móviles (WIFI). Las redes WIFI pueden ser menos seguras que las redes cableadas, por lo que es preciso activar en ellas mecanismos de cifrado:

    - **WEP (Wired Equivalent Privacy):** Protocolo que cifra las comunicaciones empleando una clave que deben conocer el emisor y el receptor. Al ser la clave estática, cabe la posibilidad de ser descifrada:

    - **WPA (WIFI Protected Access):** Más difícil de romper que WEP, al tratarse de claves dinámicas. El intercambio de claves se realiza mediante el protocolo TKIP (Temporal Key integrity Protocol). Usando WPA puede establecerse una autenticación de las claves empleadas utilizando IEEE 8022.1x y un RADIUS. Usando WPA, la pila IP se sustituye por unos protocolos de seguridad diseñados especialmente para una red WIFI:

        - **WSP (Wireless Session Protocol):** Protocolo que gestiona las sesiones y la conexión entre dispositivos (Nivel 5)
        - **WTP (Wireless Transport Protocol):** Protocolo similar a TCP o UDP (Nivel 4)
        - **WDP (Wireless Datagram Protocol):** Proporciona El interface común entre los dispositivos (Nível 2)
        - **WTLS (Wireless Transport Layer Security):** Capa que gestiona La seguridad en las comunicaciones.

4.3 MONITORIZACION DE RED

La monitorización se realiza mediante dispositivos que capturan y analizan el tráfico que circula por la red. Existen dos tipos de dispositivos:

- **Sniffer:** Dispositivo software sobre un PC o servidor, que captura toda la información de la red (poniendo la tarjeta de red en modo promiscuo). Posteriormente esta información es analizada de múltiples maneras.

- **IDS (Intrussion Detection System):** Un IDS analiza el tráfico y busca sobre el mismo un comportamiento anómalo o tráfico malicioso, generando una alarma en caso de detectarlo. Un IDS puede instalarse sobre un firewall o integrado con el mismo, para que el firewall bloquee el tráfico que se ha clasificado como malicioso.

4.4 SEGURIDAD EN ESTACIONES DE TRABAJO Y SERVIDORES

Las estaciones de trabajo son especialmente vulnerables a ataques. En una red hay muchas estaciones de trabajo y pocos servidores, y tienen permisos para comunicarse con éstos en compartir ficheros, mail, etc.

El proceso de securizar una estación de trabajo se llama hardening. Algunos de los procedimientos para securizarlo son:

- Eliminar software, servicios y procesos no utilizados
- Asegurar que todas las aplicaciones y el sistema operativo se encuentren completamente actualizados
- Configurar las aplicaciones de un modo seguro
- Minimizar la información que ofrece el sistema sobre el sistema operativo, aplicaciones existentes, versiones, etc

El proceso es idéntico en un servidor. De echo, no existe ya apenas diferencia entre un servidor y un cliente, salvo por las aplicaciones que corren.

4.5 ACCESO REMOTO

Permiten a determinadas redes o sistemas acceder a otras remotas:

- **Point-to-Point Protocol (PPP):** Ofrece mecanismos para transportar protocolos como Apple Talk, IPX, DECnet, IP, etc. sobre diversos tipos de medio físico. Por si solo, no proporciona seguridad, pero proporciona autenticación utilizando CHAP. PPP no ofrece cifrado, por lo que hay que asegurarse que es transportado sobre un medio físico seguro. PPP tiene dos protocolos:
    - **Network Control Protocol (NCP):** Protocolo que encapsula el tráfico a transportar
    - **Link Control Protocol (LCP):** Protocolo donde se realiza La autenticación.
- **Túneles:** Un túnel permite una conexión segura entre redes. Soportan protocolos adicionales y establecen caminos virtuales entre las mismas.
    - **Point-to-Point Tunneling Protocol (PPTP):** Permite encapsular y cifrar tráfico PPP, por lo que es el más usado entre sistemas finales. Toda la negociación PPP se realiza en claro y, una vez que ha concluido, se cifra el canal (se mantienen PPP cifrado). PPTP fue desarrollado por Microsoft. Necesita conectividad IP, se monta sobre TCP, en el puerto 1723.
    - **Layer 2 Forwarding (L2F):** L2F fue creado por Cisco y tiene funciones similares a PPP. Tiene autenticación pero no cifrado. Se monta sobre el puerto 1701 de UDP.
    - **Layer 2 Tunneling Protocol (L2TP):** L2TP surge con un acuerdo de Cisco y Microsoft para unir PPTP y L2F. Es un protocolo punto a punto que soporta IPX, SNA e IP. Soporta autenticación pero no cifrado, y viaja sobre el puerto 1701 de UDP, igual que L2F. Se combina con ESP (Encapsulating Security Payload) para proporcionar autenticación y cifrado. Acaba en L2TP Access Concentrator (LAC) o L2TP Network Server (LNS).
    - **Secure Shell (SSH):** Es un protocolo de túnel desarrollado para UNIX, para montar encima protocolos como Telnet, FTP y otros. Utiliza el puerto 22 de TCP. Utiliza un mecanismo de cifrado entre cliente y servidor. El cliente inicia la sesión y el servidor responde diciendo que el cifrado es necesario. El cliente le manda entonces al servidor un certificado en el que se indican sus capacidades de cifrado. El servidor analiza esta información y le responde con una llave de sesión y una llave cifrada. El proceso es seguro hasta el final de la sesión.
    - **Internet Protocol Security (IPSec):** IPS no es un protocolo de túnel, pero puede montarse sobre otros protocolos de túnel. IPSec proporciona autenticación y cifrado de los datos y las cabeceras. Puede trabajar tanto en modo túnel como en modo transporte. En IPSec hay dos protocolos principales. Authentication Header (AH) y Encapsulating Security Payload (ESP). ESP trabaja en el puerto 50 y AH en el 51 de TCP. El protocolo de intercambio de llaves (ISAKMP/IKE o Internet Security Associations and key Management Protocol / Internet Key Exchange) utiliza el puerto 500 de UDP. Si se necesita utilizar NAT, debería aplicarse antes que IPSec.
        - **En modo túnel** se cifran tanto los datos como las cabeceras, y necesita una cabecera adicional para routing.
        - **En modo transporte** se cifran sólo los datos, dejando la cabecera original para routing.
- **RADIUS (Remote Authentication Dial-In User Service):** Protocolo del IETF que permite realizar la autenticación, autorización y accounting en accesos remotos. RADIUS se instala sobre un servidor centralizado al que se conectan los diferentes elementos de la red para identificar a los accesos a los mismos. Definido en la RFC 2865, se considera más robusto que TACACS.
- **TACACS/+ (Terminal Access Controller Access Control System):** Es entorno cliente servidor que opera de forma similar a RADIUS. Ha evolucionado a TACACS+, que implementa varios mecanismos de autenticación, incluyendo Kerberos. Cisco ha desarrollado múltiples funciones de autorización sobre TACACS+. TACACS utiliza el puerto 49 en TCP y UDP.

4.6 SEGURIDAD EN CONEXIONES A INTERNET

Muchos de los ataques de seguridad están centrados en la pila de protocolos TCP/IP porque es la forma en que funcionan todas las aplicaciones de Internet. Aquí se analizan alguna de ellas:

- **Correo electrónico:** Trabaja con 3 principales protocolos:
    - **SMTP (Simple Mail Transport Protocol):** Es un protocolo que transfiere correo electrónico entre un cliente y un servidor y entre servidores. Funciona en el puerto 25 de TCP.
    - **POP (Post Office Protocol):** Un cliente solicita al servidor que le entregue correo electrónico. Permite la transferencia en diferido de correos, con lo que el servidor debe soportar almacenar correos. La última versión (POP3) trabaja en el puerto 110 de TCP.
    - **IMAP (Internet Message Access Protocol):** Es la evolución de POP3, ya que permite determinadas funciones más avanzadas que POP (por ejemplo la descarga de correos basándose en criterios de búsqueda). La última versión (IMAP4) trabaja en el puerto 143 de TCP
    - **SMTP Relay:** Es una característica que permite a un servidor reenviar correo a otros sitios. Es utilizado por el SPAM. Debería ser desactivado en el servidor salvo que se esté usando de modo conocido y controlado.
- **Web:** La información de las páginas WEB está escrita en HTML (Un protocolo de presentación que permite integrar imágenes, textos y otros elementos con una presentación determinada), y se transporta sobre HTTP, protocolo de transferencia de HTML. HTML está evolucionando a XML (Extensible Markup Language) en muchos aspectos. Sobre el protocolo HTTP también pueden viajar otros elementos que pueden ser dañinos para el cliente, con lo que hay que controlarlos.
    - **Conexiones WEB seguras:** Existen dos protocolos de acceso seguro a la WEB:
        - **Secure Socket Layer (SSL):** Utiliza un mecanismo de cifrado entre cliente y servidor. El cliente inicia la sesión y el servidor responde diciendo que el cifrado es necesario. El cliente le manda entonces al servidor un certificado en el que se indican sus capacidades de cifrado. El servidor analiza esta información y le responde con una llave de sesión y una llave cifrada, que será la que se use en el cifrado, de forma simétrica. El proceso es seguro hasta el final de la sesión. Existen dos variaciones de renovación de certificado SSL. La primera es para revalidar las llaves actuales. La segunda es para renovar la pareja de llaves. SSL soporta llaves de 40 y de 128 bits. Después fue reemplazado por TLS.
        - **Transport Layer Security (TLS):** Es la evolución de SSL v3 con llaves de 1024 y 2048 bits. No es compatible con SSL, pero se han creado conectores que lo compatibilizan con SSL v3. Definido por la IETF. Permite otros protocolos de cifrado como 3DES. Ambos viajan por el puerto 443 de TCP.
        - **Hipertext Transport Protocol Secure (HTTPS):** Es la versión segura de HTTP. Utiliza SSL o TLS para transferencias seguras de tráfico HTML.
        - **Secure HTTP:** Se trata de un mensaje seguro sobre HTTP. Mientras que HTTPS asegura el canal, S-HTTP asegura el mensaje. Proporciona integridad y autenticación.
    - **Vulnerabilidades de los Add-ons WEB:** La mayor funcionalidad de las páginas WEB hacen que incluyan diversos tipos de contenidos potencialmente peligrosos:
        - **ActiveX:** Tecnología de Microsoft que permite incrementar la usabilidad de páginas WEB. Se descargan y ejecutan en el cliente, y pasan por un protocolo de autenticación llamado Authenticode. Muchos navegadores exigen al usuario que confirme su instalación, pero incluso así son peligrosos. El código fuente de ActiveX no es comprensible por una persona, se descarga en código máquina.
        - **Buffer overflow:** Este efecto se produce cuando una aplicación recibe más información de la que está programada para soportar. Existen múltiples ataques de buffer overflow.

- **Common Gateway Interface (CGI):** Es una técnica de ejecución de scripts en el servidor en base a parámetros de entrada facilitados por el cliente. Está siendo sustituido por scripts que se ejecutan en el cliente como ActiveX o Java.

- **Cookies:** Son ficheros de texto (aunque pueden tener otros formatos) escritos por los sitios WEB que almacenan en el PC del cliente determinada información al objeto de identificar al cliente y adaptar el contenido de la página al mismo. Su peligro radica en que el robo de esta información puede aportar mucha información relativa al usuario del PC. Pueden no ser aceptadas si se configura así en el browser.

- **Cross-site scripting (XSS):** Consiste en introducir en un sitio WEB código malicioso. Depués de puede "invitar" a los usuarios a visitar este sitio WEB empleando, por ejemplo, un SPAM.

- **Input Validation:** Se trata de vulnerabilidades en las aplicaciones por las que al introducir un usuario el user/password de una aplicación pueda o no tenerse en cuenta o bien existir una password de un backdoor

- **Java Applets:** Un applet java es un script java autocontenido que puede ser descargado desde un servidor WEB y se ejecuta en el cliente. Los applets de java se ejecutan en una máquina virtual de java, y en una zona cerrada de memoria llamada sandbox. Mientras que no se vulnere esta zona de memoria, no se corre peligro, pero vulnerabilidades en la máquina virtual de java podrían hacer que un applet ejecutara código fuera de esta zona de memoria.

- **JavaScrip:** Software que puede ejecutarse en un PC, sin necesidad de disponer la máquina virtual de java, y que tienen todos los permisos de cualquier software que se haya desarrollado en el PC. El código fuente de JavaScript es comprensible por una persona. El código de JavaScript puede ser ejecutado en cualquier tipo de máquina.

- **Pop-ups:** Consisten en que un sitio WEB abre una nueva instancia WEB forzando al cliente a visitar zonas que no han sido demandadas.

- **Signed Applets:** Son similares a los Java applets, pero no se ejecuta en el sandbox, con lo que tiene más acceso a los componentes del sistema. Incluyen una firma digital para certificar el origen del mismo, aunque el hecho de estar firmado no garantiza que sea inofensivo. Es necesario que esté firmado por una fuente de confianza para el usuario.

- **FTP (File Transfer Protocol):** Es un protocolo de transferencia de ficheros. Muchos servidores FTP aceptan un usuario anónimo con una dirección de email como fuente de acceso permitida para descargar ficheros. Existe un protocolo SFTP, que monta FTP sobre SSH para que la transferencia de datos sea cifrada entre el cliente y el servidor. Una evolución de FTP son los protocolos de compartir ficheros (Como los protocolos P2P).

4.7 PROTOCOLOS DE RED

- **SNMP (Simple Network Management Protocol):** Es un protocolo UDP utilizado con fines de gestión y monitorización de elementos de red

- **ICMP (Internet Control Message Protocol):** Es un protocolo usado para reportar errores en redes de datos. Muchos ataques de DoS se basan en bombardeos de paquetes ICMP.

- **IGMP (Intenet Group Management Protocol):** Es un protocolo utilizado para la gestión de grupos multicast.

4.8 CONCEPTOS DE CABLEADO

En redes de datos se utilizan los siguientes medios físicos. Hay que tener en cuenta que, según el tipo de medio que se emplee, podrán existir determinados modos de que un intrusos acceda al mismo, con mayor o menor dificultad.

- **Cable coaxial**
- **Cable UTP y STP**
- **Fibra óptica**
- **Infrarrojos**
- **Radio frecuencia**
- **Microondas**

4.9 SISTEMAS DE ALMACENAMIENTO PORTATIL

Un elemento importante para considerar desde el punto de vista de la seguridad es la información contenida en dispositivos de almacenamiento portátil, o almacenamiento de información en red.

- **CD-R/DVD-R**
- **Diskettes**
  - Hay que tener en cuenta el tiempo que duran los datos grabados, por su condición electromagnética
- **Tarjetas de memoria**
- **Discos duros**
  - No disponen de un mecanismo físico de protección contra escritura, como otros dispositivos
- **Smart Cards**
- **Cintas**
  - Hay que tener en cuenta el tiempo que duran los datos grabados, por su condición electromagnética
  - Deben almacenarse en una ubicación independiente
  - Cuando se borran datos de una cinta, según el Departamento de Defensa USA, es necesario pasar las cintas por el proceso de borrado al menos 7 veces (DoD-7, método 5220)
- **Thumb Drives (memoria USB)**
- **NAS (Network Attached Storage)**

5 MONITORIZACIÓN DE RED Y DETECCIÓN DE INTRUSOS

5.1 MONITORIZACIÓN DE RED

Las técnicas de monitorización de red permiten saber qué está sucediendo en la red. Puede realizarse en tiempo real (por ejemplo con un sniffer) o en base a logs y eventos (con un IDS, Sistema de Detección de Intrusos).

La monitorización de la red puede ser interna o externa. Idealmente, deberían analizarse ambas, y en un análisis del tráfico en ambas direcciones. El analizador se puede conectar a un tap o a un puerto de un hub o un switch que soporte mirror.

En la Red pueden existir protocolos de diferentes familias:

- **TCP/IP:** Se utiliza para transportar otro gran número de protocolos encima. Los ataques suelen estar dirigidos a IP, TCP, UDP, ICMP e IGMP. TCP abre un puerto por cada servicio que esté ofreciendo un sistema, lo que permite que sea atacado a través del mismo.

- **Protocolos Novell:** NetWare es un entorno basado en servidores que ofrecen diversos servicios y aplicaciones. Es susceptible de ataques de DoS. NetWare soporta dos protocolos propietarios:

    - **IPX (Internetwork Packet Exchange) / SPX (Sequenced Packet Exchange):** Protocolos similares a IP y TCP, que pueden ser monitorizados e interceptados en la red

    - **NDS (NetWare Directory Services) y eDirectory:** Protocolo que administra los recursos de la red, manteniendo una base de datos con los mismos. eDirectory es la evolución de NDS. Atacar a esta base de datos provocaría un DoS en la Red.

- **Protocolos Microsoft:**

    - **NetBIOS (Network Basic Input Output System):** Es el protocolo nativo de Windows. Proporciona el esquema de nombrado de los recursos de la red. Es un protocolo que trabaja en broadcast, con lo que toda la red conoce todos los mensajes que se mandan. NetBIOS puede ser transportado sobre NetBEUI, TCP/IP o IPX/SPX. Su principal vulnerabilidad es que abre varios puertos (del 135 al 139 y el 445).

    - **NetBEUI (NetBIOS Extended User interface):** Se utiliza para transportar NetBIOS sobre una LAN. No es enrutable, con lo que no puede atravesar los routers. Es fácil de interceptar en la red con un sniffer.

    - **WINS (Windows Internet Name Service):** Servicio que traduce nombres de NetBIOS a direcciones IP. Si el servidor WINS no está disponible, los Pc's comprueban e nombre en el fichero local LMHOSTS

- **Protocolo NFS (Network File System):** NFS es el protocolo de transferencia de ficheros de Unix. Permite a un usuario remoto montar en su PC una unidad de una máquina remota de la red.

- **Protocolos Apple:** Apple utiliza Apple Talk como protocolo de red. Es un protocolo enrutable, que carga mucho la red y es el protocolo empleado en sistemas Apple, aunque los más modernos también incorporan TCP/IP. La mayor parte de las vulnerabilidades no está en el protocolo en sí, sino en el software que explota este servicio.

5.2 SISTEMAS DE DETECCIÓN DE INTRUSOS

Para monitorizar la red puede utilizarse un sniffer o un IDS. Un Sistema de Detección de Intrusión (IDS) es un elemento fundamental en la seguridad y la monitorización de red. La detección de intrusismo es el proceso de monitorizar eventos de sistemas y de la red para determinar si ha ocurrido una intrusión. Una intrusión se define como cualquier acción que pueda comprometer la confidencialidad, integridad o disponibilidad de los recursos de la red.

Un IDS monitoriza la red y genera alarmas en caso de detectarse una intrusión, pero no lo corta. Esta función la realizan los firewalls.

Para que realice su función, el IDS puede instalarse detrás o delante del firewall (cada configuración aporta ventajas e inconvenientes) y debe configurarse adecuadamente en función de nuestra red. Es un fallo habitual dejar las opciones por defecto.

Algunos términos que hay que conocer para comprender esta tecnología de análisis de red son:

- **Actividad:** Un trozo de la fuente de datos que se considera necesario analizar.
- **Administrador:** La persona responsable de las políticas de seguridad.
- **Alerta:** Un mensaje del analizador notificando que ha detectado un evento de interés.
- **Analizador:** Componente que procesa los datos recogidos por el sensor.
- **Fuente de datos:** información origen que el IDS usará para buscar en ella actividad sospechosa
- **Evento:** Un evento es la detección de actividad sospechosa en la fuente de datos
- **Manager:** Es el elemento que gestiona la persona que administra el IDS, como la consola
- **Notificación:** una notificación es el proceso por el que el manager indica al operador que existe una alerta.
- **Operador:** Persona responsable del IDS
- **Sensor:** Es un componente del IDS que recoge datos de la red y se las entrega al analizador.

Un IDS analiza la red empleando dos métodos principales:

- **Signature-based detection o misuse-detection IDS (MD-IDS):** Analiza el tráfico en base a un archivo de firmas

- **Anomaly-detection IDS (AD-IDS):** Busca anomalías en el tráfico. Normalmente, un software inteligente analiza el comportamiento habitual de la red, y genera un aviso cuando éste se ve modificado (por ejemplo sube considerablemente el tráfico ICMP)

    - **Stateful Inspection:** Además de comprobar el tráfico con las firmas, realiza el reensamblaje de paquetes, detectando las firmas en toda la sesión.

    - **Protocol decode analysis:** Es igual a stateful inspection, pero además de añade un análisis de las normas RFC para detectar anomalías.

    - **Análisis heurístico:** Utiliza firmas y además analiza el tráfico para identificar patrones que anteriormente fueran marcadas como sospechosas.

Según su forma de conectarse a la red, un IDS puede ser de red o de host:

- **N-IDS (Network-based IDS):** Se conecta a un punto de la red donde se pretende analizar el tráfico. Debería conectarse antes del firewall, para tener información real de los ataques que pretenden realizarse contra la empresa. Si se conecta después del firewall no se tendrá la visión completa, sólo del tráfico no bloqueado por el firewall.

- **H-IDS (Host-based IDS):** Se instala como software dentro de un servidor, aunque esto tiene algunos problemas. El primero es que si se ataca al servidor, sería posible borrar la información del IDS, anulándolo. El segundo es que hacen falta tantos H-IDS como servidores, y hay que gestionarlos a todos. Un H-IDS normalmente solo puede hacer respuestas pasivas ante un incidente.

Un IDS puede, en principio, realizar acciones pasivas o activas ante un incidente:

- **Respuestas pasivas:** Una respuesta pasiva se basa en alguno de estos tres métodos:

    - **Logging:** Grabar el evento y las circunstancias en que se da el evento.
    - **Notificación:** Comunicar el evento al personal responsable de la seguridad.
    - **Shunning:** Ignorar el error (por ejemplo, se detecta un ataque contra un servidor web IIS pero el que está instalado es Apache)

- **Respuestas activas:** Una respuesta activa toma acciones para mitigar el evento:
    - **Terminar el proceso o sesión:** Si se detecta un ataque, un IDS puede forzar a un sistema a resetear todas las sesiones TCP abiertas (enviando señales de reset)
    - **Cambios en la configuración de red:** El IDS podría dar indicaciones a un firewall para aislar determinada IP o red que está siendo origen de los problemas, o bloquear el socket (IP+puerto) del servidor contra el que se está generando el ataque.
    - **Deception:** Consiste en hacer pensar al atacante que está teniendo éxito, cuando realmente el ataque se está derivando a un sistema preparado para ser atacado.

Existe un dispositivo denominado NIPS (Network Intrussion Prevention System) que está basado en un IDS, pero que es capaz de tomar acciones de bloqueo de tráfico (como un firewall).

Otro elemento interesante es el llamado honeypot, que es un elemento preparado para recibir ataques. Mientras los ataques tratan de acceder al mismo, se obtiene mucha información sobre los mecanismos empleados para ello, sin riesgo. Una de las iniciativas de honeypots más interesantes es una red completa, con servidores, estaciones de trabajo, comunicaciones, servicios y todo lo demás simulada por software y presentada a través de una única conexión a la red. permite analizar todo lo que sucede dentro de la misma con IDS virtuales colocados en los segmentos de la red.

Para hacer que los hackers caigan en el honeypot, hay dos métodos:

- **Enticepment (Seducción):** Es tratar de hacer que a los hackers les interese caer en la trampa, por ejemplo, ofreciendo software gratis, presumir de que tu sistema es invulnerable, etc.
- **Entrapment (Atrapamiento):** Se obliga a un hacker a romper un sistema (por ejemplo como parte de un proceso policial)

5.2.1 RESPUESTA ANTE UN INCIDENTE

El análisis forense es el proceso de identificar lo que ha sucedido en una red examinando los datos existentes (logs, etc). La respuesta a un incidente de seguridad es el proceso de identificar e investigar el incidente, solucionar los daños causados, documentar lo que ha sucedido y ajustar los procedimientos para evitar que vuelva a suceder. Todo este trabajo debería estar escrito en un documento llamado IRP (Incident Response Plan), que debería incluir los 5 puntos indicados:

- **Paso 1: Identificación del incidente:** Es necesario confirmar la existencia real de un evento de seguridad. Un IDS puede reportar falsos positivos, lanzando alarmas de eventos que realmente no son incidentes de seguridad. Después de confirmar que se trata de un evento de seguridad, hay que poner en marcha lo indicado en el Plan de respuesta de a incidentes (IRP). Por ejemplo, avisando al responsable de la gestión de dicho incidente.
- **Paso 2: Investigar el incidente:** El proceso de investigar hace referencia a analizar logs y otras fuentes de datos para conocer la naturaleza y fuente del incidente. Esta investigación permitirá conocer las siguientes acciones a tomar (analizar y corregir los daños, y modificar lo necesario para que el ataque no pueda volver a sucederse)
- **Paso 3: Reparar los daños causados por el incidente:** Hay que analizar que recursos han sido accedidos y como recuperar aquellos que hayan sido comprometidos. En ocasiones será necesario restaurar copias de seguridad. Si sólo ha sido un ataque de DoS, podría bastar con reiniciar el sistema afectado. Tal vez sea necesario un tratamiento con un antivirus, que repare los daños en el sistema.
- **Paso 4: Documentar la respuesta:** Durante todo el proceso, debe documentarse exactamente los pasos seguidos para la detección, investigación, reparación de daños, etc, y el resultado obtenido de estos pasos. Este documento será muy valioso si el ataque llegara a repetirse. Puede hacerse llegar información del ataque al CERT, o a los fabricantes de software o hardware afectado.

- **Paso 5: Ajustar los procedimientos:** Después de que un ataque haya sucedido, es necesario revisar los procesos, procedimientos o estructura de la empresa para evitar que vuelva a suceder. Deberían preguntarse al menos:

    - ¿Funcionaron adecuadamente las políticas de seguridad en esa situación?
    - ¿Se aprendió algo nuevo durante el evento?
    - ¿Qué debería ser diferente para la próxima vez?

5.3 SEGURIDAD WIFI

Los sistemas WIFI transmiten las señales de la red a través del aire, lo que provoca una serie de oportunidades para los hackers. Debido a ello, se han desarrollado una serie de protocolos que permiten securizar las redes WIFI. Primero vamos a repasar los protocolos del sistema WIFI, incluidos en el standard IEEE 802.11:

Protocolo	Banda	Velocidades soportadas
IEEE 802.11	2,4 GHz	1 Mbps 2 Mbps
IEEE 802.11a	5 GHz	54 Mbps
IEEE 802.11b	2,4 GHz	1 Mbps 2 Mbps 5,5 Mbps 11 Mbps
IEEE 802.11g	2,4 GHz	54 Mbps
IEEE 802.11n	2,4 GHz 5 GHz	300 Mbps

- **Wired Equivalent Privacy (WEP):** WEP permite cifrar los datos. WEP es vulnerable debido al mecanismo empleado para el cifrado, ya que, de echo, no fue concebido como protocolo de seguridad.

- **Wireless Protected Access (WPA):** WPA y la segunda versión (WPA2) utilizan lo indicado en el estándar IEEE 802.11i. La diferencia entre las dos versiones es su compatibilidad con determinados tipos de tarjetas WIFI. WPA soluciona los problemas de vulnerabilidad de WEP.

5.3.1 VULNERABILIDADES DE WIFI

Los sistemas WIFI tienen una serie de vulnerabilidades diferentes a los sistemas cableados. Las señales de radio pueden ser interceptadas, y existen determinados mensajes (Como el SSID de la red) que se transmiten de forma periódica y es posible obtener en base a ellos la password usada para cifrar. Además, un atacante puede conocer los sistemas que existen en la red, obteniendo información relativa a los mismos.

5.4 SEGURIDAD EN REDES DE ACCESO CON TELEFONOS MÓVILES

Existe un protocolo llamado WAP (Wireless Application Protocol), que ofrece soluciones similares a TCP/IP para dispositivos móviles. Permite el transporte de pequeñas páginas HTML escritas en un código llamado WML (Wireless Markup Language). WAP permite conectarse con redes IP gracias a gateways que traducen WAP por TCP/IP. Se utiliza más en redes celulares que en redes WIFI locales. Forman parte de WAP los siguientes protocolos:

- **WSP (Wireless Session Protocol):** Implementa los servicios orientados a conexión de WAP
- **WTP (Wireless Transport Protocol):** Proporciona transacciones cliente-servidor. Trabaja entre WSP y WTLS.

- **Wireless Transport Layer Security (WTLS):** Es la capa de seguridad en redes WAP. WTLS aporta servicios de autenticación, cifrado e integridad de los datos para dispositivos móviles. WTLS aporta un razonablemente bueno nivel de seguridad en dispositivos móviles, y también es incluido en sistemas WIFI.

5.5 SEGURIDAD BLUETOOTH

En Bluetooth existen los siguientes tipos de ataques:

- **Blue bugging:** Un ataque que permite tomar el control no autorizado de dispositivos bluetooth, sin notificación al usuario.
- **Blue snarfing:** Ataque que permite acceder a un dispositivo bluetooth y robar información de contactos, calendario, direcciones, etc
- **Blue jacking:** Es un ataque que consiste en mandar mensajes no autorizados a dipositivos bluetooth que se encuentran cerca.

5.6 MENSAJERIA INSTANTÁNEA

El auge de los sistemas de mensajería instantánea ha abierto nuevas vulnerabilidades que permiten robar información. Es fácil hacer ejecutar a un interlocutor software con troyanos, virus, gusanos y otros.

Además, la información enviada a través de los sistemas de mensajería instantánea es enviada en claro, con lo que pueden ser interceptados y leídos por un atacante. Esta es la principal preocupación. Otras están derivadas de la política de uso de la empresa y la pérdida de productividad.

5.7 CORREO ELECTRÓNICO

5.7.1 S/MIME

S/MIME (Secure Multipurpose Internet Mail Extensions) es un protocolo empleado para el cifrado de correo electrónico y ficheros. Se define en la RFC 2311.

Utiliza cifrado RSA. Se utiliza tanto en correo interno como a través de Internet, estando soportado por web browsers.

S/MIME es la versión segura de MIME, ya que utiliza cifrado asimétrico RSA y confía en certificados para la autenticación, mientras que MIME no.

5.7.2 PGP

PGP (Pretty Goog Privacy) es un mecanismo de envío de correo electrónico seguro. Puede utilizar llaves RSA y Diffie-Hellman.

PGP es una aplicación comercial, que puede adquirirse en formato corporativo o personal.

5.8 NOMBRES DE FICHEROS 8.3

Muchos sistemas operativos ocultan la extensión de los ficheros, con lo que el usuario podría estar pensando que abre un fichero de texto o imagen cuando realmente está abriendo, por ejemplo, un ejecutable. Debería forzarse al sistema operativo a mostrar siempre las extensiones de los ficheros.

5.9 ANÁLISIS E INTELIGENCIA DE RED

- **Footprinting:** Footprinting es el proceso de identificar la red y sus sistemas de seguridad. Un atacante puede obtener información sobre la red mirando los servidores que ofrecen servicios al exterior, analizando los dominios registrados, la información de direccionamiento IP vertida por los DNS's, etc. Con toda esta información el hacker puede hacerse un mapa de los elementos de la red.

- **Scanning:** Es el proceso de obtener datos de la red y los elementos vivos de la misma, mediante port scanning, ping, tracerouter y otras herramientas. La imagen que se obtiene de un sistema operativo medianteb estas técnicas es la llamada OS fingerprint.

6 IMPLEMENTACIÓN Y MANTENIMIENTO DE UNA RED SEGURA

Los sistemas operativos, aplicaciones y redes habitualmente son seguras cuando se instalan y se utilizan según los consejos del fabricante. Este capítulo trata del proceso de asegurar los productos.

6.1 AMENAZAS

Las redes, aplicaciones, sistemas operativos y demás elementos sufren vulnerabilidades que generan problemas de seguridad. Estas vulnerabilidades suelen ser corregidas en cuanto se detectan, por lo que es necesario asegurar que todos los sistemas están completamente actualizados.

El CERT Coordination Center analiza e informa acerca de nuevas amenazas de seguridad. Es conveniente analizar la información que el CERT publica.

Un buen método para detectar agujeros de seguridad es realizar un test de intrusión en la red (tratar de entrar como si se fuera un hacker en el exterior). Después del test de intrusión hay que realizar un test de vulnerabilidad, que consiste en tratar de explotar cada puerto abierto en la red con bases de datos de exploits conocidos.

6.2 SECURITY BASELINE

Una baseline define el nivel de seguridad que será implementada y mantenida. Puede elegirse una baseline poco segura o poco funcional, ningún extremo es bueno.

Una baseline siempre establece un nivel mínimo de standards de seguridad implementados.

El standard más aceptado en seguridad es el Common Criteria (CC) que ha definido un conjunto de baselines basado en 7 niveles llamados EAL (Evaluation Assurance Levels):

- **EAL 1:** Se utiliza cuando se desea que el sistema funcione correctamente, pero no se plantean que existan amenazas sobre el mismo
- **EAL 2:** La seguridad no se considera una prioridad. Se deben desarrollar productos con buenas prácticas de diseño.
- **EAL 3:** Requiere esfuerzos de desarrollo para lograr niveles moderados de seguridad.
- **EAL 4:** Requiere Ingeniería en seguridad basada en buenas prácticas comerciales en materia de seguridad.
- **EAL 5:** Se trata de asegurar que el equipo de ingeniería ha trabajado en el equipo de desarrollo desde el primer momento. Se buscan altos niveles de seguridad. Para alcanzar esta certificación hay que considerar consideraciones de diseño especiales.
- **EAL 6:** Proporciona muy elevados índices de seguridad contra los riesgos más importantes. También tiene un alto nivel de seguridad frente a ataques de penetración.
- **EAL 7:** Un nivel extremadamente alto de seguridad. La certificación requiere pruebas, medidas y un exhaustivo e independiente test de seguridad de la aplicación.

La más adecuada en software comercial es EAL 4, aunque pocos sistemas están certificados en este grado.

6.3 PROTECCIÓN DEL SISTEMA OPERATIVO

“Hardening” es el proceso de blindar o proteger un sistema para hacerlo más seguro frente a ataques e intrusos. Es necesario considerar tres elementos en la protección del sistema operativo:

- **Configurar adecuadamente los protocolos de red:** Casi todos los sistemas operativos trabajan con TCP/IP, NetBEUI o IPX/SPX. Sobre estos tres protocolos puede montarse NetBIOS de Microsoft. Cuando se

configuran los protocolos usados por el sistema operativo (en propiedades de red) hay que seleccionar exclusivamente los que vayan a ser utilizados. “Binding” es el proceso de encapsulado de unos protocolos sobre otros.

- **Utilizar las opciones de seguridad del sistema operativo:**
  - **Microsoft Windows Vista**
    - **Control parental de las cuentas de usuario:** web filter, horario de uso permitido, bloqueo de ficheros, etc.
    - **Panel de control de seguridad:** Firewall, escaneado automático del sistema, Windows defender
    - **Bitlocker (solo en la versión Enterprise):** Permite el cifrado completo del disco duro.
  - **Microsoft Windows XP**
    - Active Directory
    - Services pack
    - System Monitor, que permite ver contadores de uso del sistema
  - **Microsoft Windows Server 2003**
    - Firewall
    - Autenticación local y remota
    - Conexiones WIFI seguras
    - Políticas de restricción de software
    - Web Server seguro IIS 6
    - Mejoras de cifrado y criptografía
    - Conexiones VPN mejoradas
    - Soporte de certificados PKI y X.509
    - Grupos de políticas
    - Políticas locales
  - **Microsoft Windows 2000**
    - Actualizaciones
    - En la versión Server, arranca IIS, servidor FTP, y otros servidores, que pueden suponer problemas de seguridad.
    - Dispone de herramientas de monitorización y jogging
    - Flexibilidad en la gestión de grupos de usuarios, autenticación, control de acceso, etc.
    - Herramienta performance monitor
    - Active Directory
  - **Unix / Linux**
    - Elevado nivel de seguridad cuando se configuran correctamente
    - Permite tener iniciados muchas aplicaciones, servicios y protocolos. Hay que mantener parados los no usados.
    - Permisos en acceso a ficheros y directorios
    - Necesario mantener parches actualizados
    - Logging
    - TCP wrapper, herramienta que permite logear la actividad de bajo nivel en la red
  - **Novell NetWare**
    - La versión 6.5 permite compartir impresoras y ficheros, minimizando la seguridad
    - Es sensible a ataques de Denegación de Servicio
    - Consola de permisos de usuario
  - **Apple Macintosh**
    - Sistema muy vulnerable a través de su consola, que tiene passwords débiles**.**

- **Securizar los sistemas de ficheros:**

  - **Microsoft FAT (File Allocation Table):** diseñado para discos pequeños. Ha evolucionado a FAT16 y a FAT32. Sólo permite dos tipos de protección. Los permisos asociados a un directorio se extienden a todo su contenido.

  - **Microsoft NTFS (New Technology Fyle System):** Evolución más segura que FAT. Cada fichero o directorio tiene sus propios atributos de seguridad, incluyendo listas de acceso. Tiene tres niveles (Read-Only, Change o Full-control)

  - **Novell NetWare Storage Services:** Se suele llamara NetWare File System (NFS). Permite el control total de cualquier recurso presente en un servidor NetWare.

  - **Unix Filesystems:** Sistema jerárquico con tres niveles de permiso (lectura, escritura y ejecución). Es compleja de configurar al implantar el sistema.

  - **Unix Network Filesystems:** Es un protocolo que permite montar unidades remotas. Es difícil de asegurar, sobre todo por su autenticación.

  - **Apple File Sharing:** Es similar a Unix Filesystems, un protocolo sencillo para la gestión de recursos en Apple. Se considera seguro al no ser Apple un protocolo enrutable.

- **Actualización del sistema operativo:** Aunque es imprescindible realizar actualizaciones de los sistemas con los que se trabaja, en ocasiones hay que realizarlo cuando ya existe un feedback de otros usuarios. En ocasiones, los updates de los fabricantes pueden hacer que determinado sistema o parte de él deje de trabajar como hasta el momento. Hay tres tipos de upgrades:

  - **Hotfixes:** Sirven para solucionar un fallo de un sistema
  - **Service packs:** Es un conjunto de actualizaciones que se empaquetan en un simple producto
  - **Patches:** Es una solución temporal de un problema.

6.4 PROTECCIÓN DE LOS DISPOSITIVOS DE RED

La protección de los elementos de red, en aquéllos que sean configurables o actualizables (routers, firewalls, etc) pasa por:

- Mantener las versiones de sistema operativo actualizadas, especialmente la de aquéllos elementos (routers, firewalls) que tienen funcionalidades avanzadas y suelen ser primera línea al exterior de la red.

- Configurar adecuadamente los sistemas, habilitando sólo los protocolos y servicios necesarios, y protegiendo, con listas de acceso, que no atraviese por ellos ningún tráfico no autorizado.

6.5 PROTECCIÓN DE APLICACIONES

Los servidores son los puntos donde en primer lugar un hacker intentará acceder a la red, por lo que es necesario considerar en ellos los factores de riesgo que los comprometen:

- **Servidores WEB:** Aunque en principio entregaban texto e imágenes, actualmente un servicio WEB ofrece acceso a ficheros ejecutables, bases de datos, streaming y otro tipo de aplicaciones. Cada uno de estos servicios puede tener problemas de seguridad que comprometan el sistema. Es necesario tener las aplicaciones actualizadas y asegurar que se emplean sólo protocolos estándares. También pueden instalarse filtros que controlen el acceso a datos y a scripts. Muchos scripts ejecutables, como CGI's, necesitan permisos de administrador para ejecutarse. Aunque al concluir se regresa al nivel de permisos del usuario, es posible romper el sistema y dejar que un código se ejecute después de haber logrado escalada de privilegios.

- **Servidores e-mail:** El servidor de correo es un aliado de un posible atacante por su capacidad de distribuir a los usuarios SPAM, virus, etc. Por eso, es necesario instalar en el servidor de correo, además, un software antivirus y un sistema antispam.

- **Servidores FTP:** FTP no es un protocolo pensado para ser seguro. Muchos servidores permiten acceder a zonas del disco no autorizadas, escribiendo o leyendo ficheros que no le corresponden al usuario. Para asegurarlo un poco más, es necesario utilizar protocolos como SSH que permitan cifrar las comunicaciones. Además, hay que bloquear el acceso anónimo al servidor, y asegurar que los ficheros que sirve el servidor son limpiados de virus u otro malware.

- **Servidores DNS:** El servidor DNS entrega direcciones IP cuando le preguntan por nombres. Utiliza el puerto 53 de UDP para la resolución de nombres, y el puerto 53 de TCP para la transferencia de zonas (se utiliza para consultar toda la base de datos del DNS). El DNS puede ser público o privado, dando acceso a los sistemas internos de la red. El DNS está sujeto a ataques de:

    - **Ataques de DoS:** Los ataques de DoS de un DNS dejan inoperativa la red entera, por lo que son un claro objetivo. Para prevenir estos ataques hay que asegurar que el sistema operativo esté actualizado. También deben existir dos DNS, para que un ataque contra uno de ellos no afecte al sistema.

    - **Footprint:** El DNS es una fuente muy válida para realizar un footprint de la red, ya que puede aportar información de las IP's de todas las máquinas del dominio registradas.

    - **Comprometer integridad:** Lo que se escribe en el servidor DNS primario es escrito en el secundario y viceversa. Podría realizarse un ataque de spoofing modificando en uno de los dos un dato de un dominio, con lo que los datos de ambos serian distintos. Los servidores DNS deben exigir autenticación al otro.

- **Servidores NNTP:** El servidor NNTP (Network News Transfer Protocol) entrega mensajes de red. Suele ser usado en entornos privados para comunicaciones internas. Se puede atacar con DoS. Aunque para transmitir un mensaje a un grupo es necesaria la intervención de un moderador, puede inundarse de SPAM, haciendo que los moderadores no puedan gestionar tanto mensaje.

- **Servidores de ficheros e impresoras:** Son servicios Del sistema operativo (como Windows). Pueden ser objeto de ataques de DoS, por las vulnerabilidades de NetBIOS, con lo que debería bloquearse este protocolo.

- **Servidores DHCP:** Un DHCP permite configurar los datos de red de una máquina. En una red debe haber un solo DHCP. Si se instala el segundo podría comprometerse la estructura de red.

- **Servicios de directorio:** Son herramientas que permiten, a modo de lista, organizar los recursos de la red, para que sean rápidamente identificados. Los servicios de directorio tratan a todos los elementos de la red como objetos. Además, crean y almacenan datos que pueden ser publicados a otros elementos de red. La seguridad de los servidores de directorio es crítica, y el acceso a la misma suele estar protegido con autenticación. Algunos servicios de directorio son:

    - **Lightweight Directory Access Protocol (LDAP):** Es un protocolo estandarizado de acceso a servicios de directorios, como Ad o X.500. Utiliza el puerto 389 de TCP.

    - **Active Directory (AD):** Es el servicio de directorio de Microsost. Es el backbone para servicios de seguridad y otros. Para cada elemento de red permite definir para cada elemento:

        - **Distinguished Name (DN):** Valor único a cada objeto.
        - **Relative Distinguished Name (RDN)**: Valor que puede ser repetido. Forma parte del DN.
        - **User Prinicpal Name (UPN):** Nombre "amistoso" del recurso, como su dirección de correo, por ejemplo.
        - **Canonical name (CN):** Es el DN escrito de forma canónica

    - **X.500:** Es el servicio de directorio estandarizado por la ITU, y empleado por las redes Novell.

    - **eDirectory:** Servicio de directorio empleado en redes NetrWare.

- **Bases de datos:** La mayor parte de las bases de datos son accedidas utilizando SQL (Structured Query Language) que permite obtener un dato de una búsqueda que coincida con un determinado patrón con una sola línea de comando, lo que hace que sea muy funcional, pero más inseguro. Para mejorar la eficiencia y la

seguridad, se ponen aplicaciones entre el usuario y la base de datos, que son las autorizadas a consultar en la base de datos. Existen tres mecanismo de hacer esto:

- **Modelo One-Tier:** La aplicación y la base de datos están en la misma máquina.
- **Modelo Two-Tier:** La aplicación está en el PC del cliente
- **Modelo Threee-Tier:** La aplicación está en un servidor independiente, al que accede el cliente.

7 SEGURIDAD DEL ENTORNO

7.1 SEGURIDAD FISICA

La seguridad física protege a los sistemas frente a accesos no autorizados, es decir, previene que un intruso pueda acceder físicamente a los sistemas.

- **Barreras físicas:** El objetivo de poner barreras físicas es prevenir el acceso a los sistemas de red. Idealmente, debería existir al menos tres barreras (entrada al edificio, entrada a CPD y entrada a la sala de ordenadores). Cada barrera debería estar protegidas con cámaras, alarmas, puertas, etc. Cada barrera además debe ser monitorizada. Algunos centros de alta seguridad tiene instalados "mantrap" en sus accesos, que consisten en un sistema que solo permite pasar una persona a la vez, que además queda atrapada entre dos puertas hasta que se le autoriza el paso.

    - **Perímetro de seguridad:** El perímetro de seguridad es la primera línea de defensa del modelo de seguridad. No existen dispositivos de seguridad sin vulnerabilidades, por lo que será necesario implantar varios (cerraduras, sistemas de alarma, contactos magnéticos en puertas y ventanas, etc.

    - **Zonas de seguridad:** Una zona de seguridad es una zona del edificio donde los accesos son individualmente controlados y monitorizados. Puede dividirse el edificio o el entorno en zonas de seguridad diferenciadas, y cada una de ellas tendrá sus propias características de seguridad.

    - **Segmentación (partitioning):** Este proceso permite que la información sea almacenada en zonas más protegidas, aisladas físicamente de otras (muros, cerramientos, sistemas RF, etc)

- **Ubicación:** Los sistemas TIC deben estar ubicados en un entorno que sea fácil de asegurar, desde el punto de vista de acceso, pero también debe ser segura desde el puto de vista de condiciones ambiéntales (temperatura, humedad, etc). Por ello, es preciso disponer de control de HVAC (Heating, ventilating, and air conditioning). La humedad debería estar en torno al 50% de humedad. Por encima provoca condensación, y por debajo alto riesgo de descargas electrostáticas. Este entorno también debería contar con los sistemas antiincendios, anti inundación, etc.

- **Energía:** Los sistemas TIC son susceptibles a variaciones en la tensión de alimentación, por lo que hay que asegurar la estabilidad de la misma. A fin de asegurar este suministro continuo y estable pueden instalarse los siguientes elementos:

    - **Surge protectors:** Protegen a la instalación ante variaciones bruscas y transitorias de alimentación.

    - **Power conditioners:** son dispositivos activos que aíslan y regulan la entrada de alimentación eléctrica en un edificio. Pueden estar compuestos por filtros, medidores, reguladores, etc. puede activar el sistema de alimentación de emergencia.

    - **Backup Power:** Dispositivos que almacenan energía cuando la misma es recibida desde el exterior, y la generan cuando ésta falta. Puede ser sistemas de alimentación ininterrumpida (SAI), que genera la señal a partir de corriente almacenada en baterías, o generadores, que generan corriente a partir de un motor diesel.

- **Aislamiento electromagnético:** Consiste en aislar el perímetro donde se encuentran los sistemas TIC de emisiones electromagnéticas recibidas desde el exterior o de emitir al exterior señales procedentes del interior del recinto. Estas señales pueden afectar a los sistemas de cableado de datos, o a los propios sistemas TIC. Para ello pueden instalarse jaulas de Faraday. El objetivo es prevenir las EMI (Electromagnetic interferente) y la RFI (Radio Frequency Interference).

- **Extinción de incendios:** En los centros TIC hay que disponer de sistemas efectivos de extinción de incendios. Este sistema puede ser manual o automático.

    - Los sistemas manuales se basan en extintores portátiles, que deberán ser instalados en base al tipo de fuego que puede suceder en la sala (A: Madera y papel. B: Líquidos inflamables. C: Eléctrico. D: Metales inflamables). Hay extintores que cubren varios tipos de fuego (AB, BC, ABC, etc)

- Los sistemas automáticos utilizan detectores para detectar el punto en que se produce un incendio, y actúan dispersando en la sala agua nebulizada o gas (halón o dióxido de carbono) que expulsa el oxígeno del ambiente. El halón ya está en desuso, por lo dañino que rsulta para el ambiente.

- **Biometría:** Los sistemas biométricos utilizan alguna característica de la persona a la que se pretende autenticar para controlar el acceso a determinadas áreas. Algunas técnicas empleadas son la lectura de la huella dactilar, retina o huella de mano. Estas tecnologías son cada día más fiables y más usadas.

- **Tecnologías móviles:** La entrada de tecnologías móviles ha creado un problema de seguridad. Los nuevos dispositivos crean un atractivo escenario de trabajo para muchos trabajadores en movilidad. La tecnología se basa en transmisores ubicados de manera estratégica a través del área geográfica que se pretende cubrir. Estos elementos establecen comunicaciones entre ellos para gestionar de manera automática que dispositivo será el que atienda a un cliente. Esta tecnología es similar en entornos WIFI y en entornos de telefonía móvil. Global System for Mobile Communications (GSM) es un standard para comunicaciones celulares, que aporta cifrado y otros mecanismos de seguridad. GSM trabaja con una tarjeta denominada Subscriber Identification Module (SIM), que permite a los usuarios utilizar la red. Se trata realmente de un mecanismo de autenticación, aunque aporta otros servicios.

7.2 INGENIERIA SOCIAL

La ingeniería social es el proceso por el que un atacante obtiene información sobre la empresa o la red engañando a las personas que trabajan en ella, y basándose en la confianza natural de las personas. Un ataque de Ingeniería Social puede llegar por medio de una persona directamente o a través de un correo electrónico, WEB, u otros medios.

A priori es muy difícil averiguar si se trata de un ataque, y diagnosticar su fuente. Incluso si se utilizan mecanismos de autenticación robusta como tarjetas, biometría, etc, los ataques de ingeniería social son relativamente sencillos de llevar a cabo.

Una de las tareas del administrador es educar a las personas que utilizan los recursos de la red para evitar que sean victimas de ataques de ingeniería social. Esta educación es amplia y continua, ya que un ataque de ingeniería social puede ser muy complicado o puede ser simplemente mirra a alguien mientras mete sus passwords de acceso a un sistema.

Los daños ocasionados por un ataque de este tipo pueden ser muy elevados.

7.3 BUSINESS CONTINUITY PLAN (BCP)

Un Plan de Continuidad de Negocio es el proceso de implementar políticas, controles y procesos para contrarrestar el efecto de pérdidas, caídas o fallos de procesos críticos de negocio. El BCP es una documento que hace de herramienta de gestión que asegura que las funciones críticas de la empresa puedan estar operativas a pesar de que un evento ponga en riesgo la continuidad de las mismas.

Los dos componentes de un BCP son el BIA (Business Impact Analysis) y el documento de evaluación de riesgos (Risk Assessment). El BIA está relacionado con la identificación de los procesos de negocio, y el Risk Assessment con la identificación de los riesgos que pueden suceder.

- **Business Impact Analisys (BIA):** Es el proceso de evaluar todos los sistemas críticos que existen en la organización para determinar el impacto que su pérdida ocasiona para la empresa, y poder determinar un plan de recuperación adecuado. Los elementos que forman el BIA son:

    - **Identificación de funciones críticas:** Se listan todas las funciones de la empresa, para identificar entre ellas las que son críticas para el negocio.

    - **Priorización de funciones críticas de negocio:** Sobre la lista anterior, identificar aquéllas funciones que son críticas para el negocio, y priorizarlas.

    - **Calcular el tiempo de pérdida máxima de un proceso:** identificar para cada proceso, los puntos de RTO (tiempo de recuperación) y RPO (Punto de recuperación) que son soportados con un impacto

controlado en el negocio. Estos tiempos marcarán la prioridad a la hora de comenzar a recuperar servicios para la organización.

- **Estimar impacto en el negocio:** El impacto en el negocio puede ser tangible o intangible. De su análisis se obtendrá el impacto real que la pérdida de un proceso causa sobre el total del negocio. Este estudio permite dar un valor a los procesos, para la valoración de la empresa, por ejemplo, y también aporta una idea de las inversiones que pueden llevarse a cabo para una rápida recuperación.

- **Assessment Risk:** Analiza las amenazas y vulnerabilidades de los procesos y el impacto que pueden causar en los mismos. El documento incluye los siguientes elementos:

  - **Riesgos a los que la organización está expuesta:** Este componente permite desarrollar escenarios que ayudan a evaluar como tratar un riesgo determinado en caso de que suceda un evento.

  - **Riesgos que necesitan ser tratados:** Ayuda a la organización a proporcionar un chequeo real de qué riesgos están siendo analizados y cuales no, y ante cuales es necesario poner en marcha mecanismos de resolución de incidencias

  - **Coordinación con BIA:** Este documento complementa al BIA, de modo que para cada proceso analizado en el BIA, se debe asociar los riesgos a los que está expuesto.

  - **Priorización:** Lo más importante en la redacción de este documento es priorizar. Un método para priorizar es el llamado Annualized Rate of Ocurrente (ARO), que es las veces que un evento puede suceder a lo largo de un año. Este valor se mezcla con el Computer Single Loss Expectancy (SLE) que es un valor económico que calcula los costes derivados de una caída. El gasto total anual (ALE) es **ALE = SLE x ARO**

7.4 POLÍTICAS, ESTÁNDARES Y DIRECTRICES

El proceso de implementar y mantener una red segura es guiado por medio de políticas, standards y directrices. Estos tres elementos ayudarán a una organización a definir sus planes de seguridad, a involucrar a los recursos en los planes de seguridad y a esperar un resultado concreto de dicha política.

- **Políticas:** Una política proporciona a los recursos de una organización conocimiento acerca de lo que se espera de ellos. Las políticas deben ser documentos cortos, concisos, y bien escritos, y deben definir las consecuencias en caso de que no sean obedecidos. La ventaja de una política es que las decisiones son tomadas de antemano y ofrecen una mayor rapidez y serenidad de actuación en caso de crisis. Las áreas que deben ser cubiertas por una correcta política son:

  - **Policy Overview Statement:** proporciona información sobre la meta de la política, porqué es importante para la empresa y cómo cumplirla. Idealmente es un un simple párrafo.

  - **Policy Statements:** Define exactamente la política. Debe ser clara, sin ambigüedades.

  - **Accountability Statement:** Debe hacer referencia a las responsabilidades. Quien es responsable de cumplir determinada acción en la política, a quien se debe informar, etc.

  - **Exception Statement:** Algunas veces el evento no está definido en la política. O ésta no puede ser cumplida por algún motivo. Este apartado describe cómo hay que actuar para escoger un camino alternativo al marcado en la política 8documentar, informar, etc)

- **Standards:** Un standard trata con aspectos del negocio. Se derivan de las políticas. Aspectos que deben cubrir estos documentos son:

  - **Scope and purpose:** Debe explicarse el objeto y el alcance del documento.

  - **Roles and responsabilities:** Esta sección hace referencia a quien es el responsable de implementar, monitorizar y mantener el estándar.

  - **Reference documents:** Relaciona el estándar con las diferentes políticas, directrices y otros documentos de la organización que guarden relación con éste.
  - **Performance criteria:** Detalla lo que hay que realizar y como debe ser realizado.
  - **Maintenance and administrative requirements:** Hacen referencia a las tareas que es preciso realizar para mantener y administrar los sistemas o las redes afectadas por el estándar.

- **Directrices:** Ayudan a una organización a implementar o mantener standards, proporcionando información de cómo realizar políticas y mantener los estándares. Son documentos menos formales que las políticas o estándares porque su naturaleza es ayudar a los usuarios a cumplir con ellos. Proporcionan una guía paso a paso de cómo se han de realizar las funciones definidas en políticas y estándares. Debe contener, al menos:
  - **Scope and purpose:** Debe explicarse el objeto y el alcance del documento.
  - **Roles and responsabilities:** Esta sección hace referencia a quien es el responsable de realizar cada tarea contenida en la directriz.
  - **Guideline statements:** Identifica las tareas que hay que realizar y los pasos detallados para poder realizarls.
  - **Operacional considerations:** identifica cuando hay que realizar cada una de las tareas, su periodicidad, etc.

Una adecuada gestión de la seguridad pasa por definir unos roles y responsabilidades claros para quien está involucrado en el proceso de seguridad:

- **Propietario:** Es el responsable principal de establecer regls de protección y utilización del recurso. Se trata de un nivel alto o directivo en una organización
- **Custodio:** Es el responsable de mantener y proteger el recurso. En un entorno IT, suele ser el departamento TIC.
- **Usuario:** Es la persona que utiliza los datos. Realizan tareas de leer, escribir, modificar, borrar datos y otras acciones permitidas.
- **Profesional de seguridad:** Es la persona que aporta conocimientos de todos los aspectos del proceso, investiga riesgos, realiza medidas, desarrolla políticas, etc.
- **Auditor:** Es el perfil encargado de comprobar que las prácticas y políticas, que se han definido se cumplen dentro de la organización. Analiza documentos, revisa logs, realiza entrevistas, etc para poder verificar ese aspecto.

7.5 ISO 17799 (ISO 27001)

Uno de los estándares de seguridad más aceptados es la ISO 17799 (renombrado posteriormente a ISO 27002). La ISO 17799 fue publicado por la ISO y hace referencia a las bunas prácticas en la gestión de la seguridad de la información. El estándar hace referencia a 11 puntos que considera clave en la gestión de la seguridad. Para alcanzar el certificado ISO es necesario demostrar el cumplimiento de las 11 áreas:

- **Security policy:** Proceso para evaluar expectativas de seguridad y demostrar que existe un comité de seguridad apoyado por la dirección.
- **Organization and information security:** Se proporciona una estructura que demuestra la existencia de un responsable de seguridad, con funciones asignadas.
- **Asset Management:** Existe un proceso de inventariado de los sistemas TIC y la información de la empresa, con indicación de quien es el responsable de los mismos, y en qué nivel de seguridad deben encontrarse.

- **Human resources security:** Evalúa la gestión de los recursos humanos en su implicación con la seguridad (formación, contratos, etc)

- **Physical and environment security:** Demuestra la existencia de un plan de seguridad física, red y empleados que tienen que ver con ella (copias de backup, etc)

- **Communications and operations Management:** Demuestra la existencia de un plan con sistemas preventivos (como antivirus), un sistema de monitorización, logs, seguridad en las comunicaciones, y u plan de respuesta a incidencias (IRP).

- **Access control:** Mecanismos de protección ante intrusos externos e internos (passwords, autenticación, etc)

- **Information Systems acquisition, development and maintenance:** Mide las inversiones y recursos dedicados a las TIC en cuanto a renovaciones, actualizaciones y mejoras del parque de software y hardware.

- **Information security incident Management:** Define la existencia de un IRP, y lo indicado en el mismo en cuanto a acciones a tomar, escalados, etc.

- **Business continuity Management (BCM)**: Demuestra la existencia de planes de continuidad de negocio ante incidentes de todo tipo (por ejemplo naturales, terrorismo, informáticos, etc).

- **Compliance:** Demuestra el cumplimiento de aspectos legales, regulatorios, etc.

7.6 CLASIFICACIÓN DE LA INFORMACIÓN

La clasificación de la información es un aspecto fundamental en seguridad. En una organización, el 20% de la información es pública y el 80% de la misma es interna, pero en ambas existen determinadas limitaciones a cómo se divulga la información:

- **Información pública:** Es información que se ofrecerá al exterior de la organización, pero no toda ella debe estar disponible para todos el público:

    - **Distribución limitada:** Es información externa, no secreta, pero que no debería ser conocida por todo el mundo, por ejemplo la información prestada para obtener una línea de crédito.

    - **Distribución total:** Esta información si que es distribuida para que todo el mundo tenga acceso a ella, por ejemplo información que se entrega junto con una campaña de marketing.

- **Información privada:** Su destino es interno a la organización, y podría comprometer a la empresa en caso de ser sacada al exterior. Puede contener secretos, planes de estratégicos, datos de clientes o empleados, etc.

    - **Información interna:** La información interna incluye datos financieros, documentos de trabajo, y en general cualquier información relacionada con el funcionamiento del negocio. De ella depende la operativa de la empresa, por lo que debe ser valorada y protegida.

    - **Información restringida:** Esta información puede provocar graves daños a la empresa si fuera publicada. Incluye información estratégica, secretos, etc. Esta información puede ponerse bajo una política de “no la conoce quien no la necesita”

7.6.1 CONTROL DE ACCESO A LA INFORMACIÓN

Define el método utilizado para asegurar que los usuarios tengan acceso exclusivamente a la información a la que están autorizados. Hay varios modelos, pero comunes a todos son las siguientes reglas:

- Todo lo no indicado por la política de acceso, está implícitamente denegado

- Cuando se asignan permisos, se asigna el nivel de privilegios más bajos para que el usuario pueda hacer lo que realmente necesita.

- Los puestos de asignación de permisos deben rotar lo suficiente para evitar estar a merced de algún administrador.

Los modelos de control de accesos son los siguientes:

- **Modelo Bell La-Padula:** Es un modelo diseñado para gestionar información militar clasificada. Se basa en que un usuario de un nivel de privilegio no puede leer la información de niveles superiores, y no puede escribir en niveles inferiores.

- **Modelo Biba:** Es similar a Bell La-Padula, pero está más preocupado por la integridad de los datos. Un usuario o puede escribir en niveles superiores y no puede leer de niveles inferiores. De este modo se asegura que la información de niveles superiores no es afectada por información no del todo cierta que pueda haber en niveles inferiores.

- **Modelo Clark-Wilson:** En este modelo los datos no pueden ser accedidos directamente. Existe una aplicación de lectura en cada nivel y una aplicación de escritura en cada nivel. De este modo los usuarios sólo podrán hacer lo que les permita la aplicación a la que tienen acceso.

- **Modelo Information Flow:** En este caso la información tiene atributos que indica el nivel en el que debe estar alojada. Una aplicación se coloca como interface entre el usuario y la información, analiza las operaciones que se pretenden hacer y decide si éstas son o no legales, analizando los atributos contenidos en la misma información.

- **Modelo Noninterference:** Se basa en que en cada nivel hay información que es gestionada de manera separada. Si un usuario tiene un determinado nivel, no puede ver ni modificar informaciones de otros niveles.

8 CRIPTOGRAFÍA

8.1 INTRODUCCIÓN

La Criptografía es el hecho de cifrar mediante el empleo de un código un determinado mensaje para que no pueda ser desvelado a personas que no dispongan de dicho código y, por tanto, no estén autorizados a ello. Quien establece un código se llama criptógrafo y quien trata de romperlo se llama criptoanalista.

Hay tres tipos de códigos criptográficos:

- **Criptografía Física:** El método más común es el de sustitución o transposición de caracteres, palabras o trozos del mensaje. Otro método es el llamado esteganografía, que consiste en ocultar un mensaje dentro de otro (por ejemplo el mensaje real es la primera letra de cada palabra del mensaje que se lee). Puede haber sistemas híbridos, que hacen mucho más complejo de descifrar el mensaje real si se desconoce el código empleado. En general, es criptografía física aquella que no realiza operaciones matemáticas sobre el mensaje.

- **Criptografía Matemática:** Tiene que ver con la realización de operaciones matemáticas sobre el mensaje. La más común es la técnica de hashing, que consiste en la conversión de todo el mensaje a un valor de hash. Por ejemplo, sumar todos los códigos de las letras del mensaje y al valor resultante dividirlo por el número de letras que hay. A partir del valor de hash es imposible obtener el mensaje original, es utilizado para enviarlo con el mensaje y que el receptor pueda, calculando el mismo hash, comprobar la integridad y autenticación del mensaje (como un checksum). Este proceso se denomina one-way, porque no puede descifrarse en el destino. Uno de los usos que se da es el de transmitir de forma cifrada la password, de modo que cada extremo (que conocen la password) generan el mismo hash y éstos son comparados. La password real nunca se transmite.

- **Criptografía Cuántica:** La criptografía cuántica se basa en las características de las partículas más pequeñas conocidas. El proceso depende del modelo llamado Principio de Incertidumbre de Heisenberg, según el cual el mero hecho de observar o medir algo, hace que el resultado varíe (si se mide agua con un termómetro, al poner el termómetro en contacto con el agua ésta varía su temperatura). En la criptografía cuántica, empleada exclusivamente en transmisiones ópticas, el mensaje es enviado con una serie de fotones polarizados de determinado modo. El hecho de leer estos fotones hace que modifiquen su polaridad, con lo que el mensaje se ve alterado por el mero hecho de haberlo leído. Solo el receptor, preparado para recibir el mensaje de un determinado modo, puede leerlo correctamente.

Cuando se inventa un código, éste se hace, evidentemente, para ser irrompible, pero esto deja de ser así cuando alguien lo rompe. Algunas técnicas empleadas para ello son:

- **Análisis de frecuencia:** consiste en escuchar los mensajes cifrados durante el tiempo suficiente para observar en él patrones repetidos. Estos patrones pueden dar una idea de los protocolos que se están transmitiendo, y, conocidos ellos, obtener el código de cifrado empleado.

- **Errores en los algoritmos:** Los algoritmos de cifrado son modelos matemáticos que después son programados en ordenadores. En esta programación pueden existir errores o vulnerabilidades que permitan obtener información sobre el código empleado.

- **Fuerza bruta:** Consiste en tratar de encontrar la llave de cifrado mediante intentos con combinaciones de caracteres.

- **Errores humanos:** Por ejemplo, alguien que recibe un mail cifrado, luego lo reenvía sin cifrar, y el hacker, si lee ambos correos, tendrá la capacidad de descifrar el código.

8.2 ALGORITMOS CRIPTOGRÁFICOS

Existen tres tipos de algoritmos de cifrado: Hashing, algoritmos simétricos y algoritmos asimétricos.

- **Hashing:** Es el proceso de convertir un texto a un valor numérico llamado hash. La técnica de hashing puede ser tanto en un sentido como en ambos, es decir, algunos algoritmos no permiten reconstruir el valor original a partir del hash y otros si. Existen dos estándares principalmente empleados:

- **Secure Hash Algoritm (SHA):** Es un algoritmo empleado para dotar de integridad al mensaje. Se trata de un protocolo one-way que produce un hash. Posteriormente, este hash puede ponerse junto con el mensaje a transmitir y cifrarlo todo junto, firmando el mensaje. Fue desarrollado por NIST (National Institute os Standards and Technology) y produce un hash de 160 bits.

- **Message Digest Algoritm (MD):** Es un algoritmo one-way que genera un hash a partir de un valor, usado para mantener la integridad. Es más rápido que SHA, pero se ha visto comprometido (se han localizado colisiones, es decir, varios mensajes que dan el mismo hash). MD5 fue desarrollado por Ronald Rivest para crear un hash de 128 bits.

- **LANMAN y NTLM:** Son algoritmos de Microsoft (NTLM es la evolución de LANMAN) usados para autenticación. Emplean llaves SHA o MD5.

- **Algoritmos simétricos:** Requiere que en ambos extremos haya una llave para poder cifrar o descifrar los mensajes. Es la misma llave en ambos extremos. Esta llave simétrica debe ser protegida, porque su pérdida compromete al sistema completo. La llave no es enviada por el mismo canal por el que se mandan los mensajes, sino que debe ser enviada por otros medios. Este es un problema. El otro es que todas las personas que forman parte del grupo deben tener la llave. Algunos algoritmos de cifrado utilizados son:

  - **Data Encryption Standard (DES):** Algoritmo basado en llave de 56 bits, ya comprometido y sustituido por AES. DES ofrece integridad y confidencialidad.

  - **Triple DES (3DES):** Es un upgrade tecnológico de DES, aunque se utiliza más AES. Genera llaves de hasta 192 bits.

  - **Advanced Encryption Standard (AES):** Utiliza el algoritmo Rijndael y ha sustituido a DES. Soporta llaves de 128, 192 y 256 bits.

  - **CAST:** Utilizado en algunos de Microsoft e IBM, utiliza llaves de entre 40 y 128 bits, y es muy rápido y eficiente.

  - **Rivest's Cypher (RC):** Familia de algoritmos de cifrado de Laboratorios RSA. RC5 utiliza llaves de 2048 bits, consideradas muy robustas.

  - **Blowfish:** Trabaja con llaves de 64 bits a velocidades muy rápidas. Se ha evolucionado con Twofish, con llaves de hasta 128 bits.

  - **International Data Encryyption Algorithm (IDEA):** utiliza llaves de 128 bits, parecido a DES pero más seguro. Se utiliza con PGP (Pretty Good Privacy), sistema empleado en cifrado de correo electrónico.

- **Algoritmos asimétricos:** Utilizan dos llaves, una para cifrar (clave pública) y otra para descifrar (clave privada). Cuando se desea enviar un mensaje a un destino se utiliza la clave pública de ese destino para cifrar el mensaje, y sólo el destino, empleando su clave privada, podrá descifrarlo. La clave pública puede ser pública o puede ser compartida sólo en un grupo cerrado de dos o más estaciones, para cambiar mensajes seguros entre ellos. La clave privada debe mantenerse segura, su pérdida compromete al sistema. Esta arquitectura se llama PKC (Public Key Cryptography). Una PKI (Public Key Infraestructure) utiliza PKC como parte de su sistema. Se utilizan cuatro sistemas asimétricos:

  - **RSA:** RSA es un sistema de clave pública muy implementado, que utiliza grandes números enteros como base del proceso. Trabaja tanto para cifrado como para firma digital. RSA es muy utilizado en varios protocolos, incluyendo Secure Socket Layer (SSL)

  - **Diffie-Hellman:** Se utiliza para realizar el envío de certificados a través de redes públicas, no se utiliza para cifrar el mensaje, sólo para el cifrado de las llaves. La criptografía asimétrica fue concebida inicialmente por Diffie-Hellman.

  - **Eliptic Curve Cryptography (ECC):** Proporciona funciones similares a RSA. Se utiliza en dispositivos menos inteligentes como teléfonos. Necesita menos recursos que RSA.

- **El Gamal:** Algoritmo utilizado para el envío de firmas digitales y cambio de llaves. El método es similar a Diffie-Hellman, y se basa en cálculos logarítmicos.

8.2.1 TABLA RESUMEN

ALGORITMO	TIPO	TAMAÑO HASH / LLAVE	OBSERVACIONES
SHA1	HASH	160	
MD5	HASH	128	Más rápido que SHA1, pero tiene vulnerabilidades
LANMAN	HASH	160	Es de Microsoft. Utiliza MD5 o SHA1.
NTLM	HASH	160	Es la evolución de LANMAN
DES	SIMETRICO	56	Comprometido
3DES	SIMETRICO	192	Ha sustituido a DES
AES	SIMETRICO	256	Ha sustituido a 3DES
CAST	SIMETRICO	128	Usado por Microsoft e IBM. Es rápido y eficiente
RC5	SIMETRICO	2048	Es de RSA, Muy robusto
RC6	SIMETRICO	128	Desarrollado por RSA, es un standard
BLOWFISH	SIMETRICO	64	Muy rápido
TWOFISH	SIMETRICO	128	Ha sustituido a BLOWFISH, creado por Bruce Schneier
IDEA	SIMETRICO	128	Parecido a DES pero mas seguro. Se usa con PGP
RIJNDAEL	SIMETRICO	VARIABLE	Código de bloques desarrollado por joan Daemen y Vincent Rijmen
SERPENT	SIMETRICO	128	Código de bloques desarrollado por la Universidad de Cambridge
RSA	ASIMETRICO		RSA está basado en Diffie-Hellman, aunque ahora es el más utilizado.
DIFFIE-HELLMAN	ASIMETRICO		Es el origen de los códigos asimétricos.
ECC	ASIMETRICO		
El Gamal	ASIMETRICO		Parecido a RSA

8.3 SISTEMAS CRIPTOGRÁFICOS

Un sistema criptográfico debería ofrecer muchos de los servicios de la seguridad:

- **Confidencialidad:** La capacidad de un sistema criptográfico de dotar confidencialidad se llama robustez. Un sistema es robusto cuando su mecanismo de cifrado lo es. Se mide en el factor de trabajo, que aporta una medida del tiempo y esfuerzo necesarios para romper un cifrado.

- **Integridad:** Es asegurar que el mensaje no ha sido modificado. Para ello se puede agregar un MAC (Message Authentication Code) al mismo mensaje. Este MAC sale de una operación de hash sobre el propio mensaje. Si el mensaje es modificado, también lo es el MAC, con lo que es posible detectar esa situación.

- **Firma digital:** Una firma digital se obtiene a partir de un hash del documento, que posteriormente es cifrado utilizando la clave privada del emisor. El receptor para comprobar la integridad y autenticidad debe calcular el mismo hash del documento, y descifrar el hash recibido utilizando la clave pública del emisor. Si coinciden, el documento es originariamente del emisor y se garantiza su integridad. La autenticación se logra mediante firma digital, aunque también puede lograrse mediante la inserción de palabras clave en el mensaje, que respondan a un reto enviado por el receptor. RSA recomienda que cada persona tenga dos parejas de llaves, una pareja utilizada para cifrar las comunicaciones, y la segunda empleada para firmar.

- **No repudio:** El no repudio es evitar que se pueda negar una acción realizada. En estructuras de PKI se utilizan CA (Certificate Authorities), que gestionan las llaves públicas y gestionan la validación de los certificados.

- **Autorización (Control de Acceso):** El control de acceso son los mecanismos que se llevan a cabo para evitar que se acceda a sistemas que realizan la criptografía. Los certificados pueden ser perdidas o robadas. Deben incluirse métodos de seguridad física y lógica para evitar el comprometer las claves privadas de un sistema.

8.4 PUBLIC KEY INFRAESTRUCTURE (PKI)

Una PKI permite dotar de todos los servicios de seguridad indicados a los intercambios de mensajes. Es la respuesta a una necesidad global de soportar comercio electrónico y transacciones seguras entre distintas entidades.

PKI es un sistema que utiliza cifrado con dos claves y que trabaja con 4 componentes principales:

- **Autoridad Certificadora (CA):** Es un sistema u organización que es responsable de entregar, revocar y distribuir los certificados. El certificado asocia una pareja de claves a un individuo o sistema, con lo que se debe disponer de suficiente información del sistema. Las CA's pueden ser públicas o privadas. En el caso de las privadas, pueden generarse tantos certificados como se desee, pero hay que asegurar que exista una relación de confianza entre la CA y los posibles receptores de mensajes. Para establecer comunicaciones con un sistema, se debe conocer la clave pública del mismo. Quien desea cifrar un mensaje con esta clave pública puede comprobar en la CA a quien ha sido entregada esta clave pública, y asegurar de ese modo que se está manteniendo la comunicación con quien realmente se desea. Evidentemente hay que confiar en la autenticación aportada por la CA.

- **Autoridad Registradora (RA):** Este sistema apoya a la CA para prevenir demasiada carga en la misma. Puede distribuir certificados, aceptar registros de la CA y validar identidades.

- **Autoridad Registradora Local (LRA):** Se trata de una RA pero que además tiene la potestad de aceptar registros de nuevas identidades.

- **Certificados digitales:** Los certificados son utilizados para autenticar una identidad de un usuario o sistema. Pueden utilizarse también para almacenar determinada información relativa al mismo. También permiten saber si se está utilizando un software o sistema operativo adecuado. El certificado más empleado es X.509, estándar de la ITU. Un certificado X.509 tiene la siguiente forma:

    - **Versión**
    - **Número de serie**
    - **Algoritmo de firma**
    - **Nombre del editor**
    - **Fecha de inicio de validez**
    - **Fecha de fin de validez**
    - **Objeto (Nombre del propietario, sistema, etc)**
    - **Clave pública**
    - **Extensiones**

Para no caer en error, es importante indicar que la clave pública, aunque es necesaria para descifrar los mensajes enviados, no forma parte de una infraestructura de PKI.

8.5 POLÍTICAS DE USO DE LOS CERTIFICADOS

Los certificados deben estar sujetos a determinadas políticas de utilización, creación, revocación, confianza, etc. También la política de certificados indicará a las aplicaciones si deben considerar válido o no determinado certificado.

Un CPS (Certificate Practice Statement) es una declaración de la CA en la que indica en qué modo va a gestionar los certificados, a quien se los va a entregar y qué requisitos hará cumplir para ello. Con esta información, la CA puede generar confianza para que una organización la considere confiable en la autenticación de un certificado. Es mucho más detallado que una CP (Certificate Policy)

El proceso de revocar un certificado es el hacerlo inválido para el sistema antes de que su fecha de fin de validez haya llegado. Esto se hace, por ejemplo, cuando al seguridad de ese certificado se ha visto vulnerada (por ejemplo, se ha perdido el contenedor en el que va escrita la clave privada). La revocación de un certificado se realiza mediante la CRL (Certificates Revocation List) o mediante el protocolo OCSP (Online Certificate Status Protocol).

Cuando la CA conoce que un certificado se ha vulnerado, o hay algún motivo para revocar el certificado, escribe esta situación en la CRL. La CRL es enviada periódicamente a los sistemas que dependan de la CA y que lo hayan solicitado. Además, puede utilizar OCSP, más rápido en la comunicación, pero menos implementado.

Una CA puede mantener relaciones de confianza con otras CA's, lo que permite por un lado la unión confiable de sistemas PKI de diferentes organizaciones, o el crecimiento de una misma infraestructura PKI. Los mecanismos de confianza pueden ser:

- **Modelos de confianza jerárquica:** Aparece un root CA en lo alto de la pirámide, que confía en los CA que dependen de él, y estos en los que dependen de ellos, formando un árbol. Este sería el método empleado para implantar infraestructuras de PKA en organizaciones grandes.

- **Modelos de confianza en puente:** Son dos estructuras jerárquicas cuyos roots CA confían entre ellos, ampliando mucho más la estructura de la red

- **Modelos de confianza mallados:** Varias estructuras jerárquicas cuyos roots CA's confían entre ellos de un modo mallado (todos con todos).

- **Modelos híbridos:** Combinaciones de las tres anteriores, que hacen una estructura mucho más compleja (por ejemplo, confianzas en niveles inferiores o medios de las estructuras jerárquicas, semimalladas, etc)

8.6 ATAQUES CRIPTOGRÁFICOS

Hay tres tipos de ataques contra sistemas criptográficos:

- **Ataques a la llave:** Se trata de encontrar la clave directamente Esta clave puede ser una password, una clave privada de una PKC, un código conocido por ambos extremos, etc

- **Ataques al algoritmo:** Se trata de romper el algoritmo, descubrir su funcionamiento y obtener los datos cifrados que podrían ser descifrados. Muchos sistemas tienen vulnerabilidades ya reconocidas.

- **Interceptar la transmisión:** Consiste en escuchar las transmisiones en espera de que un error provoque la transmisión de información no cifrada, o el código utilizado, etc.

- **Birthday attack:** Se trata de encontrar dos mensajes con el mismo hash.

- **Weak Key attack:** Se basa en la realidad de que muchos passwords son sencillos y repetidos

- **Ataque matemático:** Ataques que utilizan modelos matemáticos para romper un código determinado.

8.7 ESTÁNDARES Y PROTOCOLOS EMPLEADOS EN CRIPTOGRAFÍA

Las más principales entidades que generan o proponen estándares en materia de seguridad son:

- **Agencias gubernamentales**
  - National Security Agency (NSA)
  - National Security Agency / Central Security Service (NSA/CSS)
  - National institute of Standards and Technology (NIST)

- **Asociaciones industriales**
  - Request for Comments (RFC) (no es una asociación, sino un mecanismo para proponer estandares)
  - American bankers Association (ABA)
  - Internet Engineering Task force (IETF)
  - Internet society (ISOC)
  - World Wide Web Consortium (W3C)
  - International Telecommunications Union (ITU)
  - Comite Consulatif International Telephonique et Telegraphique (CCITT)
  - Institute of Electrical and Electronics Engineers (IEEE)

8.7.1 ESTANDARES DE SISTEMAS CRIPTOGRÁFICOS

Public Domain Criptography hace referencia a los estándares y protocolos que tienen que ver con criptografía y que se hacen públicos al objeto de lograr un uso global. Dos iniciativas son PGP (Pretty Good Privacy) y RSA (Rivest, shamir and Adleman).

PKI X.509 (PKIX) es el trabajo del IETF para desarrollar modelos para el entorno PKI.

PKCS (Public Key Cryptography Standards) es un conjunto de estándares creados por RSA y otros líderes en seguridad como Microsoft, Apple, HP, Lotus, Sun… Hay 15 estándares PKCS:

- **PKCS#1: RSA Cryptography Standard**
- **PKCS#2: Incorporated in PKCS#1**
- **PKCS#3: Diffie-Hellman Key Agreement Standard**
- **PKCS#4: Incorporated in PKCS#1**
- **PKCS#5: Password-based Cryptography Standard**
- **PKCS#6: Extended-Certificate Syntax Standard**
- **PKCS#7: Cryptographyc Message Systax Standard. Define S/MIME**
- **PKCS#8: Private Key Information Syntax Standard**
- **PKCS#9: Selected attributes Types**
- **PKCS#10: Certification Request Syntax Standard**
- **PKCS#11: Cryptographic Token Interface Standard**
- **PKCS#12: Personal Information Exchange Syntax Standard**
- **PKCS#13: Elliptic Curve Cryptographic Standard**
- **PKCS#14: Pseudorandum Number Generators**
- **PKCS#15: Cryptographic Token information Format Standard**

El estándar X.509 define los formatos de los certificados y como deberían distribuirse las claves públicas. Los certificados actuales son X.509 versión 3 y hay dos tipos básicos:

- El más común es un certificado de entidad final, en el que una CA certifica a una entidad final. Una entidad final no gestiona certificados, sólo los utiliza.

- El otro tipo de certificado es el utiliza una CA para identificar a otra CA

8.8 GESTIÓN DE CERTIFICADOS Y CICLO DE VIDA DE LOS CERTIFICADOS

La gestión de los certificados se refiere al proceso desde que los certificados se crean hasta que son retirados. Las distintas fases de un certificado definen su ciclo de vida. La adecuada gestión de los certificados es clave para que una infraestructura PKI tenga valor.

- **Generación de certificados:** Puede ser centralizada o distribuida:

    - **Centralizada:** Sólo existe un generador de certificados, que en redes muy grandes podría tener problemas de rendimiento debido al consumo de CPU que tiene esta generación.

    - **Distribuida:** El sistema no es vulnerable a un simple ataque, y distintos servidores se encargan del proceso de gestión de claves. En un sistema distribuido hay una CA, una RA y varios sistemas de generación de certificados.

    - **Split:** En este sistema el servidor central genera las claves de cifrado, mientras que las claves de firma las genera el cliente o están grabadas en una smart card o similar.

- **Almacenado y distribución de certificados:** Puede ser realizado por un sistema de distribución de certificados como Kerberos KDC, o usando Key Exchange Algoritm (KEA) en el caso de PKI. KEA negocia una clave secreta entre las dos partes usada solamente para la distribución. KEA no debería ser utilizado para la transmisión de la clave privada. La llave privada necesita protección total, tanto a nivel lógico como físico.

- **Key scrow:** Es el almacenado de las claves públicas y privadas de modo que estén disponibles para aspectos legales. Este almacenado debe hacerse de manera independiente al almacenado operativo de las claves y habitualmente en una tercera empresa dedicada a esta actividad.

- **Expiración de certificado:** Un certificado expira cuando lo indica su fecha de expiración, indicada en el momento de creación del certificado. A partir de ese momento, el certificado no es válido.

- **Certificados revocados:** La CA puede revocar un certificado por ejemplo porque su seguridad se ha visto comprometida. Una vez que un certificado ha sido revocado no puede volver a utilizarse nunca.

- **Certificados suspendidos:** La CA puede suspender temporalmente la validez de un certificado. Por ejemplo, durante una ausencia temporal de un trabajador.

- **Recuperación y archivado de certificados:** consiste en el almacenado de certificados viejos para que la información que haya sido cifrada con ellos pueda ser recuperada. Estos certificados son accedidos mediante el nuevo certificado, el que les sustituye. De este modo puede accederse a información pasada. Habitualmente estos almacenes solo son accesibles mediante varios certificados válidos, por lo delicados que pueden llegar a ser.

- **Renovación de certificados:** Es el proceso de asignar un nuevo certificado a una entidad cuando su propio certificado está a punto de expirar. Existe un mecanismo llamado rollover que permite seguir usando el mismo certificado durante extensiones de tiempo, pero no debería utilizarse.

- **Destrucción de certificados:** Es el proceso de destruir físicamente los certificados no válidos y que han sido almacenados, por ejemplo, en una smart card.

- **Identificar el uso del certificado:** mientras que el certificado está vivo, puede hacerse un seguimiento de los lugares que han solicitado la autenticación del mismo, disponiendo de una trazabilidad de su utilización.

9 POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD

9.1 CONTINUIDAD DE NEGOCIO

La continuidad de negocio trata de gestionar los procesos, políticas y métodos de una organización para disminuir los efectos de un fallo en un elemento necesario para la operación de la propia empresa.

Los planes de contingencia y disaster-recovery son una parte importante del aseguramiento de la continuidad del negocio. Estos planes indican que hay que hacer ante determinados escenarios.

Un aspecto importante son las utilities (luz, agua, gas, etc) que puedan afectar al negocio, dado que pueden estar indisponibles un tiempo indeterminado. Deberían construirse infraestructuras sin puntos únicos de fallo. También deben considerarse efectos climatológicos.

El administrador de la red debe tener en cuenta todos los incidentes que puedan suceder y planear el modo de que no afecten al negocio. Algunas de las consideraciones a tener en cuenta son:

- **Alta disponibilidad:** Es el proceso de mantener los sistemas funcionando ante un incidente. La meta, al hablar de alta disponibilidad, es tener los sistemas funcionando el 99,999% del tiempo.

- **Redundancia:** Una de las herramientas para lograr alta disponibilidad. Consiste en disponer de dos elementos de modo que uno de ellos se haga cargo del servicio ante un fallo del otro. Los servidores soportan clustering como sistema de redundancia.

- **Tolerancia a fallos:** Es la habilidad de los sistemas de continuar trabajando incluso aunque algún componente crítico falle. Se basa en la redundancia interna de estos componentes. Hay que considerar el disponer de equipos de repuesto. Además, hay que asegurar la disponibilidad continua de potencia eléctrica.

- **Redundant Array of Independent Disks (RAID):** RAID es una tecnología que utiliza varios discos para proporcionar redundancia ante fallos. Hay varios niveles de RAID, que son gestionados por el software del servidor o por el hardware del grupo de discos:

    - **RAID 0:** Es un array que utiliza varios discos que trabajan juntos para parecer uno solo. No ofrece tolerancia a fallos, si un disco falla, el volumen entero falla.

    - **RAID 1:** Es disk mirroring. Proporciona redundancia porque cada dato es almacenado en dos discos del array. El problema es que también necesita el doble de capacidad para almacenar la misma información. Cuando un disco falla solo hace falta sustituirlo por otro.

    - **RAID 3:** Se trata de un RAID 0 más un disco adicional que almacena información de paridad. Esta información es un valor obtenido a partir de los datos almacenados en el disco. Gracias a ella, la información de un disco puede recuperarse en caso de un fallo. Lo soportan los sistemas UNIX y es el que se usa en muchos sistemas viejos.

    - **RAID 5:** Es como RAID 3, pero en lugar de aparecer un disco con la información de paridad, ésta está escrita en los mismos discos que forman el array. Evidentemente, la información de paridad de un disco no se almacena en el mismo, sino en otro del grupo. Está sustituyendo a RAID 3.

- **Recuperación ante desastres:** Es la capacidad de recuperar un sistema tras una catástrofe. Uno de sus elementos clave son los backups de información, y la gestión de los mismos. Este backup puede ser de copias digitales o de documentos en papel. En este último caso, sólo el hecho de su almacenamiento y su crecimiento pueden suponer el riesgo. Las copias digitales pueden ser:

    - **Copias de trabajo:** Son copias que se mantienen en el CPD para propósitos de recuperación inmediata. Se trata de los backups más recientes.

  - **Onsite storage:** Es una zona del CPD en la que se almacenan las copias de seguridad
  - **Offsite storage:** Localización fuera del CPD para almacenar las copias.

- **Plan de recuperación ante desastres (DRP):** Es un documento que realiza la empresa y que marca las acciones a tomar para recuperar la empresa ante determinadas catástrofes. Una parte importante de este plan es la indicación del mecanismo de backup y el acceso a dichas copias de backup. Este apartado se llama Backup Plan. Hay que realizar backup de los sistemas de bases de datos, archivos de usuario y aplicaciones. Hay tres tipos de backup:
  - **Backup completo:** Es una copia completa de los archivos de un disco o servidor
  - **Backup incremental:** Es una copia parcial con los ficheros que se han modificado desde el último backup (completo o no)
  - **Backup diferencial:** Es parecido al backup incremental, pero copia todos los ficheros cambiados desde el último backup completo y copia los ficheros que no han sido modificados. No puede mezclarse con un backup incremental.

- **Método de planificación de backups "abuelo, padre e hijo".** Se hace una copia en un periodo determinado, por ejemplo diario. Cada día de la semana se sobrescribe la copia de ese mismo día de la semana anterior. Estas copias son los hijos. Semanalmente, la última copia existente pasa a ser el padre. Se almacena una copia semanal durante un año y, anualmente, la última copia pasa a ser el abuelo. De este modo existe una copia diaria de la última semana, semanal del último año y varios años. El principal problema es el número de copias existentes, no saber donde está almacenado determinado fichero, etc.

- **Método de archivo completo:** Consiste en almacenar copias integrales de manera indefinida. Tiene los mismos problemas que el caso anterior.

- **Método de servidor de backup:** Es un servidor que realiza las copias en su disco duro, simplificando el sistema.

- Para recuperar un servicio, deberá existir un plan de recuperación de las copias almacenadas. Habitualmente, y disponiendo de los backups adecuados, un servidor es rápido de recuperar. Algunos sistemas operativos incluyen funciones de copia y restauración. Habrá que tener en cuenta qué aplicaciones son más críticas para el negocio y por tanto deben ser recuperadas antes.

- **Backup sites:** Un aspecto importante para asegurar la recuperación ante un desastre de gran escala es ubicar los datos también en otro centro alejado del centro principal. Este segundo centro se llama backup site, y uede ser de tres tipos en base a su funcionalidad, con costes diferentes. En el BCP se considerará la mejor alternativa, que puede ser diferente para cada servicio de la empresa.
  - **Hot site:** Es un centro que proporciona recuperación en sólo unas horas o menos. Tiene todos los elementos de comunicaciones, sistemas, software et para realizar esta función. Los datos podrían estar actualizados en el hot site con un backup realizado cada muy poco tiempo, o incluso por cada dato.
  - **Warm site:** Requiere que el cliente tome determinadas medidas para que el centro pase a ser activo, por ejemplo instalar o configurar el software de las aplicaciones en el nuevo centro. Los backups tienen menos exactitud que los del centro caliente.
  - **Cold site:** No está listo para ser utilizado. Podría no disponer de comunicaciones, o de los sistemas necesarios para hacer funcionar el sistema. En ocasiones, puede ser sólo un lugar en el que se almacenan las cintas con las copias de seguridad realizadas.

- **Vendor support:** Otro aspecto muy importante a considerar en en el BCP es la exigencia que se realiza a los proveedores en cuanto al servicio que los mismos ofrecen a la empresa. Es necesario considerar en los contratos con los mismos los siguientes parámetros:

- **Service Level Agreem,ent (SLA):** Se trata de un acuerdo por el que el proveedor se compromete a satisfacer un servicio de una forma y en un plazo concreto (por ejemplo asegurar que un técnico estará solucionando la incidencia en menos de 2 horas). En caso de no cumplirse, el proveedor podría estar obligado al pago de penalizaciones.

- **Mean Time Between Failures (MTBF):** Es el tiempo medio entre fallos que el fabricante dice que tiene su producto. Es decir, el tiempo medio que habrá entre intervenciones de reparación. Este dato debe conocerse para ajustar el tiempo de vida del equipo y en base a ello el tipo de servicio que se solicitará.

- **Mean Time To Repair (MTTR):** Es el tiempo medio que se necesita para solucionar una avería. Conocer este dato es importante ya que, junto con el tiempo de atención marcado en el SLA, establecerá el tiempo en que el sistema estará caído cada vez que pase el MTBF.

- **Code Scrow Agreement:** Es el acuerdo por el cual el proveedor en desarrollo de software hará entrega de la totalidad del código y la documentación asociada cuando la empresa así lo solicite, para asegurar que en caso de que el proveedor abandone el proyecto, la empresa pueda continuar con su aplicación y evoluciones sobre la misma.

9.2 POLÍTICAS

- **Políticas de recursos humanos**

  - **Políticas de contratación:** Definen el procedimiento que se seguirá para una nueva contratación (entrevistas, exámenes, etc), y el perfil de las personas a contratar (títulos, experiencia…)

  - **Políticas de finalización de contrato:** Definen el análisis que hay que realizar sobre las actividades que realiza una persona que va a rescindir su contrato, que actividades hay que realizar antes (como una copia de su PC), y después (como repartir las tareas que el mismo realizaba, eliminar sus permisos en sistemas, etc).

  - **Políticas de comportamiento ético:** Establece la forma de relación de las personas dentro de una organización y en su comunicación con el entorno. Existe una organización, llamada Computer Professionals for Social Responsibility (CPSR) que ha creado un documento llamado “Ten Commandments of Computer Ethics” que define unas reglas éticas generales.

  - **Políticas de utilización adecuada de recursos:** Acceptable-Use Policies (AUP) tratan acerca del uso de los sistemas TIC (ordenadores, teléfonos, etc) y de la información facilitada por la empresa. Debe marcar claramente lo que está permitido y lo que no. Una vez implementada, debe asegurarse su cumplimiento. Debe escribirse con soporte legal.

  - **Políticas de privacidad y Política de need-to-know:** Gestionan el uso de la información, en sus distintos niveles de confidencialidad.

  - **Política de investigación:** Consiste en investigar y obtener información acerca del pasado de empresas y personas que vayan a manejar información sensible, para verificar su idoneidad para permitirles hacerlo.

- **Políticas de Negocio:** Son también referidas a la seguridad de una organización. Entre ellas hay:

  - **Políticas de separación de funciones:** Previenen la aparición de fraude, ya que para realizar un trabajo en la empresa intervienen varias personas.

  - **Políticas de atención:** Definen el nivel de cuidado o atención que deben poner los recursos en la prevención de fuga de información. Especifica como debe gestionarse la información que se posee.

  - **Políticas de control de acceso:** Define las reglas de autorización de los individuos para acceder a sistemas que contienen información.

  - **Políticas de documentación:** Definen los planes de almacenamiento, distribución o destrucción de documentos dentro de la empresa.

- **Políticas de Certificados:** Las políticas de gestión de certificados definen como deben identificarse a los propietarios de los certificados, y como deben crearse, distribuirse, y gestionarse durante el ciclo de vida.

- **Políticas de respuesta ante un incidente:** Definen lo que debe hacer una organización cuando se detecta un incidente que pueda comprometer el funcionamiento normal de la misma. Deberia incluir, al menos:

  - Agencias externas que deben ser contactadas o notificadas
  - Recursos que deben involucrarse en la resolución del incidente
  - Procedimientos para recoger pruebas
  - Lista de información que debe ser recogida durante un incidente
  - Expertos externos que pueden ser utilizados si fuera necesario
  - Políticas y directrices sobre cómo tratar el incidente

9.3 GESTIÓN DE PRIVILEGIOS

La gestión de privilegios es la toma de decisiones acerca de qué información es accesible, para quién y cómo es accedida. El uso de una auditoria para realizar esta definición es importante. Algunos aspectos a considerar son:

- **Gestión de grupos y roles:** Después de la división de las acciones que hay que tomar en el normal funcionamiento de la empresa, se define que grupo o rol será el encargado de realizar esas funciones. Cada departamento puede tener distintas responsabilidades. El responsable de seguridad tendrá que dotar a cada Departamento y a cada persona dentro de él para que puedan acceder a la información que necesitan para realizar su trabajo.

- **Escalado de privilegios:** Es el proceso de incrementar los permisos de alguien. A menudo es temporal e inocente, pero otras veces responde a una vulnerabilidad.

- **Single Sign-On:** Es una gestión unificada de usuarios, de modo que con sólo introducir la password de acceso al PC, se dote al mismo automáticamente de acceso a todos los sistemas a los cuales se está autorizado. Estos se logra mediante el uso de Kerberos, Directorio Activo, PKI, etc.

- **Auditoría:** Es el procedimientos de comprobar que todas las políticas, procedimientos, regulaciones son llevadas a cabo de una forma adecuada. Se revisan los privilegios de cada usuario y los niveles de información a los que esos privilegios permiten acceder:

  - **Auditoría de privilegios:** Comprobar que los usuarios están correctamente asignados, que no existen perfiles de personas que ya no pertenecen a la empresa, y que cada perfil permite acceder a la información adecuada

  - **Auditoría de utilización:** comprobar que el hardware y software existente es conforme con las políticas de la empresa, que no hay software no licenciado en las estaciones de trabajo, etc.

  - **Auditoría de escalado:** Asegura que los procedimientos de informar a los niveles superiores en una organización es el que ha sido definido en las políticas.

  - **Auditoría administrativa:** Se trata de comprobar que todos los procedimientos de la empresa están escritos, accesibles, y que están expresados de forma clara. Los cambios que puedan existir sobre ellos deben haber sido indicados.

  - **Auditoría de archivos de log:** Evaluar los ficheros de log, para analizar si su tamaño es adecuado, y para analizar su contenido en la búsqueda de información que permita detectar un problema de seguridad Los sistemas, firewalls, routers, etc generan logs.

  - **Report:** Una auditoría debe concluir con un informe a la dirección de la empresa, donde se indiquen los procedimientos seguidos, datos obtenidos, y recomendaciones.

- **Control de acceso:** Hay cuatro métodos de control de acceso:
    - **Mandatory Access Control (MAC):** Método de control de acceso inflexible ene l que sobre el sistema se indica quien puede acceder y quien no. Solo el administrador del servicio puede modificarlo (Como una ACL)
    - **Discretionary Access Control (DAC):** Los usuarios tienen más flexibilidad para acceder a la información. Permite ser más ágil, pero es más inseguro
    - **Role-Based Access Control (RBAC):** Permite el acceso la información en función del rol que el individuo desempeñe en la empresa.
    - **Rule-Based Access Control (RBAC):** Permite el acceso a la información en base a un listado de personas autorizadas que satisfacen determinadas normas. El resto es denegado.

10 ADMINISTRACIÓN DE LA SEGURIDAD

La gestión de la seguridad pasa por la definición de las mejores prácticas en las diferentes políticas de la empresa que guardan relación con la seguridad:

- **Clasificación de información:** Define la política de cómo ha de clasificarse la información en los diferentes niveles (si es pública o interna, y el control de su distribución)
- **Notificación:** Define quien debe ser informado cuando se evalúan los niveles de clasificación de la información, o éstos deben ser actualizados, o se cambia o se actualiza la información de los mismos.
- **Retención y almacenado de la información:** Define cómo, donde y cuando se almacena la información, y quien es el responsable de la misma cuando se encuentra en ese estado.
- **Destrucción de la información:** Define cuando, cómo y quien deberá destruirse la información que se considere debe ser destruida (por ejemplo, borrar la información de discos duros o papeles antes de ser desechados).
- **Seguridad en los elementos:** Define los controles y acciones que deben ser realizados sobre las redes y sistemas.
- **Utilización de los sistemas por los usuarios:** Define como y quien puede usar los sistemas TIC de la empresa.
- **Backup:** Define qué información debe guardarse en un backup, quien debe hacerlo y con que frecuencia. Suele acompañar a un BCP.
- **Configuración:** Define los pasos que hay que realizar para realizar cambios en los sistemas o redes, su actualización, cambios de configuración, etc.
- **Logs:** Define la frecuencia y el modo en que los logs de los sistemas deben ser analizados y borrados para evitar que crezcan indefinidamente.
- **Inventarios:** Define el modo en que las propiedades (hardware, software, documentos, bienes materiales, etc) de la empresa deben ser listadas y controladas.
- **Documentos de red:** Define cómo se han de documentar y modificar los documentos relativos a la arquitectura y configuraciones de los sistemas y redes.
- **Gestión de Usuarios:** Identifica la autorización, control de accesos y métodos para monitorizar y controlar el acceso a los sistemas.
- **Uso de los recursos:** Define el modo en que van a repartirse los sistemas, inversiones existentes para proporcionar una estructura de seguridad.
- **Responsabilidad:** Define los roles y responsabilidades de las personas involucradas en la seguridad de la empresa
- **Errores:** En todos los sistemas de seguridad existirán errores, humanos, o por mal funcionamiento o configuración de los sistemas.
- **Aplicación de políticas y procedimientos:** Hay que asegurar que todas las políticas y procedimientos escritos son llevados a cabo, y si no lo es, analizar las razones de ello.
- **Simplificación:** Todas estas políticas, y su control en una organización grande puede convertirse en una tarea imposible. Además, las políticas no son iguales para todos los recursos de la empresa, lo que obliga a poner en las mismas multitud de excepciones, condicionantes, etc que las harán más complicadas. Un método para simplificar la tarea de gestionar la seguridad es aplicar estas políticas y procedimientos de manera reducida a grupos de la empresa, dividiendo ésta en grupos con políticas iguales.

- **Formación:** Uno de los trabajos del responsable de seguridad es formar y concienciar a los miembros de la empresa en materia de seguridad, para que colaboren en la consecución de la misma

- **Regulación:** Debe asegurarse el cumplimiento de las normas y regulaciones existentes en materia de seguridad (gestión de datos personales, responsabilidad civil, contratos con administración, etc)