Facultad de Ciencias Sociales y de la Comunicación

Diplomatura en Gestión y Administración Pública

Asignatura de:

Redes de datos

(Transparencias de clases)

Tema XIV

Seguridad en las redes

PARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS

Curso: 2008/2009

Profesor: Manuel Fernández Barcell
e-mail: manuel.barcell@uca.es

Índice de contenido

1 Seguridad

1.1 ¿Qué entendemos por seguridad?

Real Academia de la Lengua:

- SEGURIDAD: Cualidad de seguro
- SEGURO: libre y exento de todo peligro, daño o riesgo.

Unas definiciones de seguridad:

- Consejo Superior de Informática:
  - Conjunto de técnicas y procedimientos que tienen como misión la protección de los bienes informáticos de una organización
  - Conjunto de medidas encaminadas al mantenimiento de la confidencialidad, autenticidad, integridad y la disponibilidad de los bienes informáticos (*Hardware*, Datos, Programas)
- *La Internet Society*: Es un concepto multidimensional. Cuando pensamos en la seguridad nos referimos a uno o más de los siguientes aspectos:
  - Autentificación
  - Control de acceso
  - Auditoría de actividades
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - No repudiación
  - (Información en el RFC2828 en ftp.isi.edu/in-notes/rfc2828.txt)

1.2 Definiciones de conceptos

Autentificación

Dar y reconocer la autenticidad de ciertas informaciones del Dominio y/o la identidad de los actores y/o la autorización por parte de los autorizadores y la verificación. Es decir,que los datos, las personas y programas son auténticos. Verificar la identidad.

Control de acceso

Protección de los recursos del sistema contra accesos no autorizados. El uso de los recursos del sistema están regulados conforme a una política de seguridad. Solo es permitido a las entidades autorizadas(usuarios, programas, procesos, otros sistemas..), de acuerdo a la política de seguridad

Auditoría de actividades

Registro cronológico de las actividades del sistema que permitan la reconstrucción y examen de los eventos ocurridos. Registro de eventos

Confidencialidad

Condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. Acceso sólo a entes autorizados

Integridad

Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por personal autorizado. Modificación sólo por personal autorizado.

Disponibilidad

Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado.

Los bienes informáticos pueden ser utilizado cuándo y cómo lo requieran los usuarios autorizados

Integridad + disponibilidad = confiabilidad

No repudiación

No poder negar la intervención en una operación o comunicación.

¿Qué características determinan la seguridad de un sistema?

Según la Guía de Seguridad de los Sistemas de Información para Directivos de las Administraciones Públicas), la seguridad en un sistema viene determinado por los siguientes subestados:

- Autentificación
- Confidencialidad
- Integridad
- Disponibilidad

1.3 Niveles de seguridad

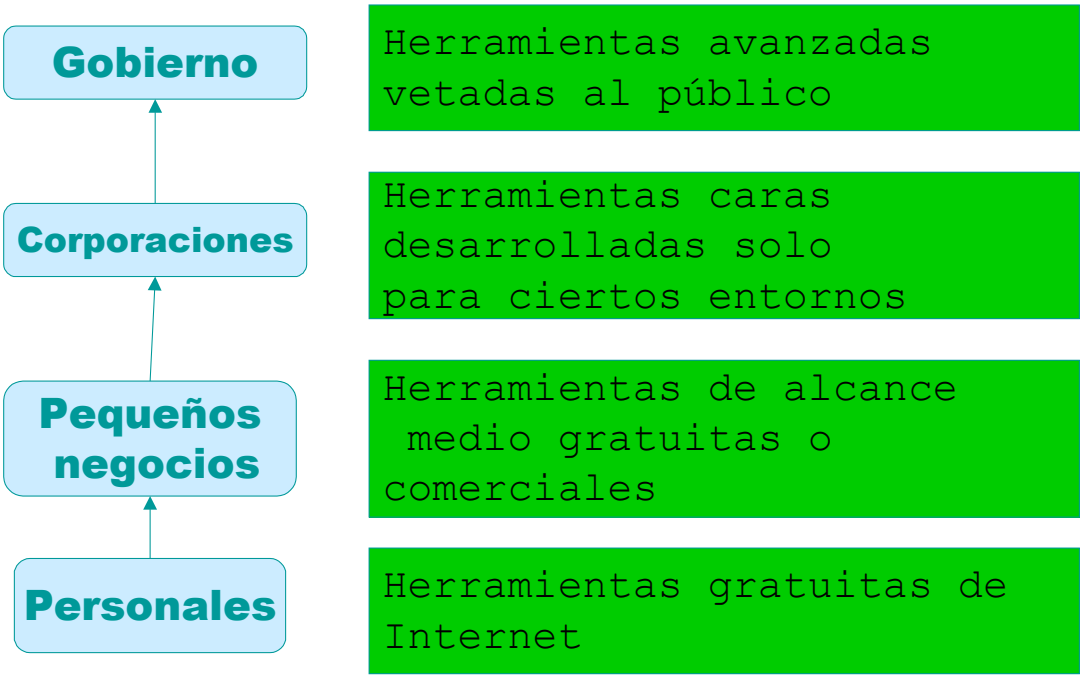
Seguro estaba y se murió. No existe la seguridad total. Existen grados de seguridad acorde con el bien a defender. La política de seguridad siempre es un compromiso entre el nivel de riesgo asumido y el coste requerido.

Evaluación de riesgo

Lograr que un ataque a nuestros bienes sea más costoso que su valor, invirtiendo menos de lo que vale.

Reglas:

- Toda política de seguridad debe ser holística.
- La política debe adecuarse a nuestras necesidades y recursos.



1.4 ¿De qué tipos de amenazas debemos defendernos?

Los tipos de amenazas más frecuentes se clasifican en algunas de las siguientes categorías:

Interrupción

Los recursos del sistema son destruidos, o no están disponibles o están inservibles. Afecta a la disponibilidad del sistema.

Ejemplo: Destrucción de un elemento del hardware del sistema.

Intercepción

Un elemento no autorizado accede a un recurso del sistema. Afecta a la privacidad del sistema.

Ejemplo: Pinchar una línea de comunicación de la red

Modificación

Acceso y modificación de un recurso del sistema. Afecta a la integridad del sistema

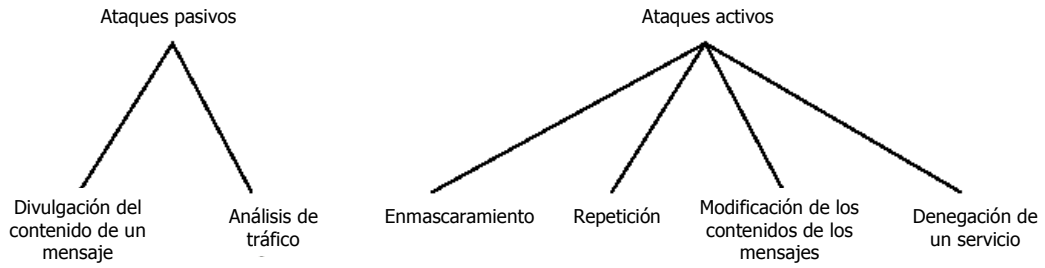
Ejemplo: Modificación de un programa o fichero.

Fabricación

Inserción de elementos ajenos al sistema. Afecta a la integridad del sistema.

Ejemplo: Añadir un registro a un fichero o generar un mensaje en la red

1.5 Modos de agresiones a la seguridad



Ataques pasivos

- Escuchas de las transmisiones.
  - Para obtener información.
- Divulgación del contenido del mensaje:
  - El intruso se entera del contenido de la transmisión.
- Análisis del tráfico:
  - Controlando la frecuencia y la longitud de los mensajes, incluso los cifrados, se puede adivinar la naturaleza de la conexión.
- Características
  - Difíciles de detectar.
  - Se pueden prevenir.

Ataques activos

- Enmascaramiento:
  - Una entidad pretende ser otra entidad diferente.
- Repetición.
- Modificación de mensajes.
- Denegación de un servicio.
- Características
  - Fácil de detectar: La detección tiene un efecto disuasivo.
  - Difícil de prevenir.

2 Políticas y mecanismos de seguridad

2.1 ¿Que podemos hacer para defendernos?

- Diseñar nuestra política de seguridad
  - Política (Diccionario de R.A.L): Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado. Indica qué hacer
- Implementar los mecanismos de seguridad para realizar la política diseñada
  - Mecanismo: Especifica cómo llevar a la práctica las políticas de seguridad y cómo hacerlas cumplir en un sistema determinado.

2.2 Principios de diseño para seguridad (*Saltzer y Schoeder*)

1. El diseño debe ser público.

   La seguridad no debe estar basada en la ignorancia del mecanismo por los atacantes.

2. Los derechos de acceso deben ser adquiridos sólo con permiso explícito.

   El valor por defecto debe ser la falta de acceso.

3. Verificar la autoridad actual de modo insistente.
4. El mínimo privilegio posible.
5. El mecanismo de protección debe ser sencillo y uniforme.
6. El esquema elegido debe ser psicológicamente aceptable por el usuario.
   - Implicación del factor humano
   - Debe conseguir concienciar a los usuarios (principio de conciencia)
7. Separación de privilegios.
   - Satisfacer más de una condición (tener una tarjeta y dar un PIN) Mínimo privilegio.
   - Dos o más personas con intereses contrapuestos sean necesarias para autorizar una operación que pueda poner en peligro la seguridad del sistema.
   - El mecanismo de protección debe ser sencillo y uniforme.
   - Rotación de roles.

   7. La Responsabilidad de la seguridad debe ser explícita
   8. Principio de proporcionalidad
   9. De obligado cumplimiento
   10. En constante revisión

2.3 Políticas de seguridad

2.3.1 Conceptos

- Especifica qué es lo que se desea desde el punto de vista de protección y seguridad.
- Generalmente engloban procedimientos y procesos que especifican:
  - Cómo se puede introducir y sacar información del sistema.
  - Quién está autorizado a acceder a qué información y con qué condiciones.
  - Cuáles son los flujos de información permisibles dentro del sistema.
- Las políticas de seguridad suelen estar guiadas por los principios de:
  - Mínimo privilegio.
  - Separación de deberes.

- Dos o más personas con intereses contrapuestos sean necesarias para autorizar una operación que pueda poner en peligro la seguridad del sistema.

– Rotación de roles.

- La política de seguridad siempre es un compromiso entre el nivel de riesgo asumido y el coste requerido.
- Las políticas se clasifican:

– Control de acceso discrecional:

– Definida por el propietario de los datos

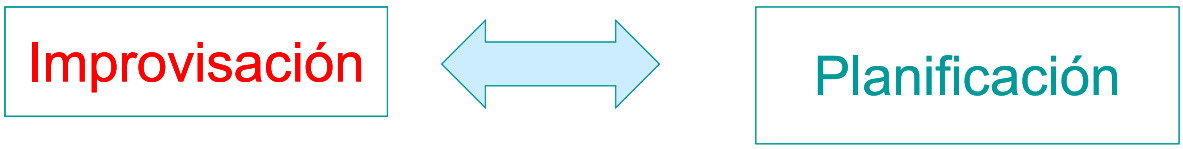
– Control de acceso obligatorio.

2.3.2 Estructura y contenido de la política de seguridad

- Introducción, propósito, importancia y necesidad
- Ámbito de la política
- Centro, plataforma, tipo de información, tipo de personas
- Clasificación de la información
- Necesidad de designar responsables
- Seguridad en las instalaciones (física)
- Seguridad lógica y de acceso
- Seguridad de redes
- Planificación de contingencia
- Uso adecuado del software
- Forma de difusión de la política

2.3.3 Los planes de seguridad

- Disponer de un plan de seguridad supone un enfrentamiento con la mentalidad mediterránea



-
- *¿Podría decirme qué camino debo tomar? Preguntó Alicia; esto depende de adonde quieras llegar, contestó el gato (Alicia en el País de las Maravillas)*
- ¿Dispone de un plan de seguridad formalizado y documentado, en el que se refleje las medidas que garanticen la seguridad de los datos de carácter personal y vitales para la empresa?. Los usuarios deben conocer:
- Derechos
- Deberes
- Sanciones
- El plan, para ser útil debe plasmarse en proyectos concreto

Definir + formalizar + aprobar

2.3.4 Estructura de cada proyecto

- Vendrá determinado por estándares y necesidades de la entidad
- Los proyectos se desglosarán en FASES, tareas y actividades
- Cada tarea debe especificar

- Descripción y código
- Productos a obtener
- Responsable o coordinador
- Partícipes
- Marco temporal
- Costes asociados
- Requerimientos específicos (contratos, cursos,...)

2.3.5 Direcciones donde encontrar informaión detallada

- Recomendaciones de seguridad
  - ftp://ftp.rediris.es/docs/security/
    - recomendaciones.pdf
    - rainbow-series
- Definición de una política de seguridad:
  - http://www.rediris.es/cert/doc/docu_rediris/poliseg.es.html#o14
- Información sobre estándares de seguridad
  - http://www.diffuse.org/secure.html

2.4 Mecanismos de seguridad:

Los mecanismos especifica como llevar a la práctica las políticas de seguridad y cómo hacerlas cumplir en un sistema determinado. Un objetivo del S.O es proporcionar mecanismos de seguridad. Los mecanismos nos indica como implantar las políticas de seguridad.

Los sistemas de información son unos elementos de cualquier corporación que tiene ya un alto valor. Deben de adoptarse medidas de seguridad como con cualquier objeto valioso. La seguridad de ordenadores y redes de datos es un área amplia que comprende la siguiente clasificación de las medidas seguridad (mecanismos):

2.4.1 Medidas técnicas

- Seguridad física (externa):
  - Se consigue adoptando una serie de medidas físicas y administrativas
  - Aspectos:
    - Intrusos físicos (“choris”)
    - Agentes físicos externos al sistema
- Seguridad lógica (Interna)
  - Se consigue adoptando una serie de medidas técnicas y administrativas
  - ASPECTOS:
    - De Sistemas
    - De red
    - Del software

2.4.2 Medidas Organizativas

  - Normas que determinan funciones como:
    - Las personas que pueden acceder.
    - Quién tiene derecho a utilizar el sistema
    - Horario etc

- Clasificación de los usuarios
  - Administradores
  - Usuarios
  - Personas ajenas al sistema
  - Personal de mantenimiento
  - Ejecutivos de grado medio
- Niveles
  - Todo el mundo tiene acceso a todo
  - Dos niveles: privilegiado y normal
  - Varios niveles de acceso
  - Todas las normas de "organización" (NO técnicas) necesarias para llevar a cabo el plan de seguridad

2.4.3 Medidas legales

- Legislación de protección de datos
- Normas de seguridad de obligado cumplimiento

2.4.4 Metodologías de seguridad

- Metodologías de análisis de riesgo
- Metodologías de nacionales e internacionales de seguridad
- Estándares: ISO 17799

3 Seguridad física o externa

Se consigue adoptando una serie de medidas físicas y administrativas.

3.1 Medidas anti intrusos

Las medidas anti -Intrusos sobre equipos, ordenadores y redes consisten en impedir el acceso físico de personas no autorizadas a las instalaciones y el equipamiento. Muchas medidas de seguridad tienen comprometida su eficacia si no se impide el acceso físico a los equipos.

- Medidas físicas
  - Puertas de seguridad, cerraduras, vallas
  - Vigilancia.
  - Control de acceso
  - Alarmas, circuitos cerrados de TV
- Medidas administrativas
  - Control de los visitantes
    - Acompañar al visitante hasta su destino
    - No entregar llaves
    - Las personas que pueden acceder.
    - Quien tiene derecho a utilizar el sistema
    - Horario etc.
  - Restricción de acceso a zonas determinadas
  - Uso de tarjetas identificativas

Seguridad física o externa

3.2 Seguridad Externa Agentes físicos

Medidas dirigidas a proteger los sistemas contra accidentes, agentes ambientales o físicos como el fuego, electricidad, inundación, temperatura, humedad, ambiente sin polvo etc...

- Medidas contra incendios.
- Aire acondicionado.
- Doble suelo
- Instalación eléctrica
  - Estabilizadores
  - SAI´s
- Directrices de construcción
  - Construcción de la sala de ordenadores por encima del primer piso
  - No debajo de conducciones de agua
  - Calidad de los materiales de construcción
- Consideraciones eléctricas
  - Suministro del panel principal
  - Independencia entre circuito ordenadores y otros equipos
  - Equipos de aislamiento eléctrico y SAI
  - Circuitos de emergencias
- Medidas administrativas: Son normas que determinan funciones como:
  - Plan de contingencia ante estos fenómenos
  - ¿Que hacer cuando se va la luz?

4 Seguridad lógica (interna)

Se consigue adoptando una serie de medidas técnicas y administrativas. Afectan a la configuración de los sistemas operativos y al diseño de los sistemas operativos. Deben de proporcionarse de un modo automático La implementación dependerá de cada sistema operativo:

- UNIX
- Windows

Ver documento de recomendaciones de seguridad para encontrar medidas concretas:

- ftp://ftp.rediris.es/docs/security

ASPECTOS

- De Sistemas
  - Autentificación
    - Políticas de contraseñas
    - Políticas de cuentas
  - Control de acceso
  - Seguridad en los sistemas de ficheros
  - Configuración de equipos y servidores
  - Configuración de servicios (www, FTP, correo, DNS, Servidores de ficheros)
  - Monitorización
  - Actualizaciones de software
- De red
  - Intranets

  - Internet
- Recomendaciones para usuarios finales
- De diseño del software

La seguridad de ordenadores y redes tiene cuatro requerimientos:

- Privacidad: La privacidad hace referencia a un mecanismo para controlar el acceso de programas, procesos o usuarios a los recursos definidos por un sistema informático.
  - Acceso a la información del sistema solo por parte de las entidades autorizadas.
- Confiabilidad:
  - Confiabilidad hace referencia a las medidas para conservar la integridad del sistema y sus datos.
- Integridad
  - No se pueda modificar la información por entidades no autorizadas realizando operaciones no autorizadas.
- Disponibilidad
  - Que el sistema esté en perfecto estado de funcionamiento, libre de averías y errores

4.1 Validación o autentificación de la identidad

El objetivo de la validación es permitir el acceso a los usuarios legítimos del sistema y denegarlo a los no autorizados. El principal problema de los sistemas operativos es el de la validación de la identidad.

Características

- Hacer una identificación única del usuario
- Independiente de la máquina

Métodos

- Características físicas:
  - Biométricos
- Secreto compartido:
  - Contraseña
- Posesión de un objeto (hardware o software)
  - Tokens o certificados digitales

La validación se basa en una combinación de tres conjuntos de elementos:

- Posesión por parte del usuario de algún elemento "llave"
  - Llave de acceso al puesto del ordenador.
  - Tarjeta magnética etc.
- Contraseña
- Atributos del usuario
  - Huellas dactilares.
  - Iris del ojo.
  - Firma.

4.1.1 Autentificación por contraseña

Se requiere que el usuario teclee una contraseña.

- Los problemas de la contraseña están relacionados con la dificultad de mantenerla secreta.

  - Deben de ser largas.
  - No se deben de anotar.
  - Posibles de recordar.
  - Deben de evitarse: Nombres familiares, fechas familiares, DNI, nombre de la novia/novio, del perro o del canario (pájaro).
  - Deben de caducar obligando al usuario a cambiarla.
  - Intercalar números, letras y signos de puntuación
  - NO USAR LA MISMA CONTRASEÑA PARA DISTINTOS SISTEMAS

¿Cómo guardamos las contraseñas? Las contraseñas se guardan cifradas. Hay diversos algoritmos de encriptación, con diferentes niveles de seguridad.

- UNIX utiliza el algoritmo crypt(16). La función E contraseña se realiza 25 veces. Es un algoritmo DES modificado. Una misma contraseña cifrada en distintas máquinas da un resultado diferente
- Windows NT Criptografía débil. Una función Hash

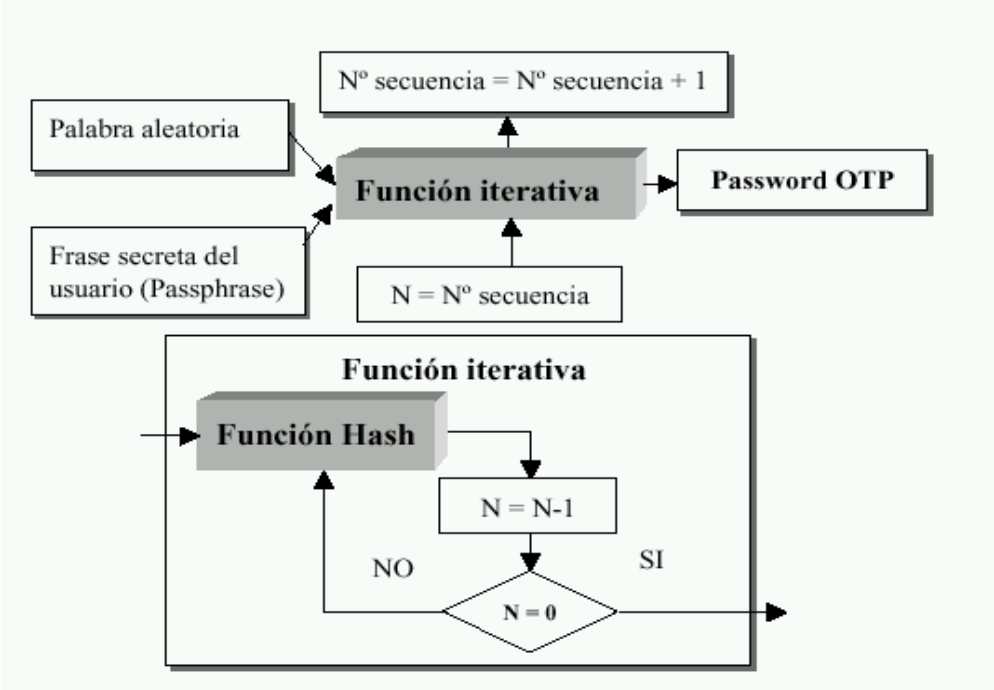
Ataques a las contraseñas

- Con acceso al fichero
  - Diccionario
  - Con 8 caracteres 1288= 7,2 * 1016
  - Un diccionario solo centenares de miles
- Prueba y ensayo (task force)
- Caballos de Troya
- Espías en la red (sniffer)
- Ingeniería social
  - Mirar el teclado, los post-tip...
- Bugs o errores en los programas

Políticas a ataques a contraseñas

- Se pueden asociar distintas contraseñas a distintos derechos de acceso.
- Sistemas de contraseña de un solo uso
  - OTP (One-time Password)
  - La contraseña de un usuario cambia cada vez que se usa
  - Servidor y usuario con dispositivo sincronizados

Seguridad lógica (interna)



- Algoritmos que conoce el usuario y el sistema aplicados a un número aleatorio proporcionado por el sistema después de introducir una primera contraseña.
- Control del número de intentos fallidos por parte de un usuario.
  - Cancelar cuentas con intentos fallidos
- Herramientas que comprueban la seguridad
  - Cracker (NEcXUS, SATAN)

4.1.2 Sistemas biométricos

Utilizan características físicas del usuario

- Las características deben ser únicas y que no cambien

Ventajas

- Son Intransferibles
- Muy seguros
- No necesitan gestión

Inconvenientes

- Necesitan electrónica adicional
- Rechaso del usuario
- Costo (100 dólares por contraseña)

Tipos de sistemas biométricos

- Medidas de acierto
  - FAR (False Acceptence Rate) % malos dados por buenos
  - FRR (False Rejet Rate) % buenos dados por malos
  - SR (Succes Rate) = 100 - (FAR+FRR)
- Emisión de calor o termograma

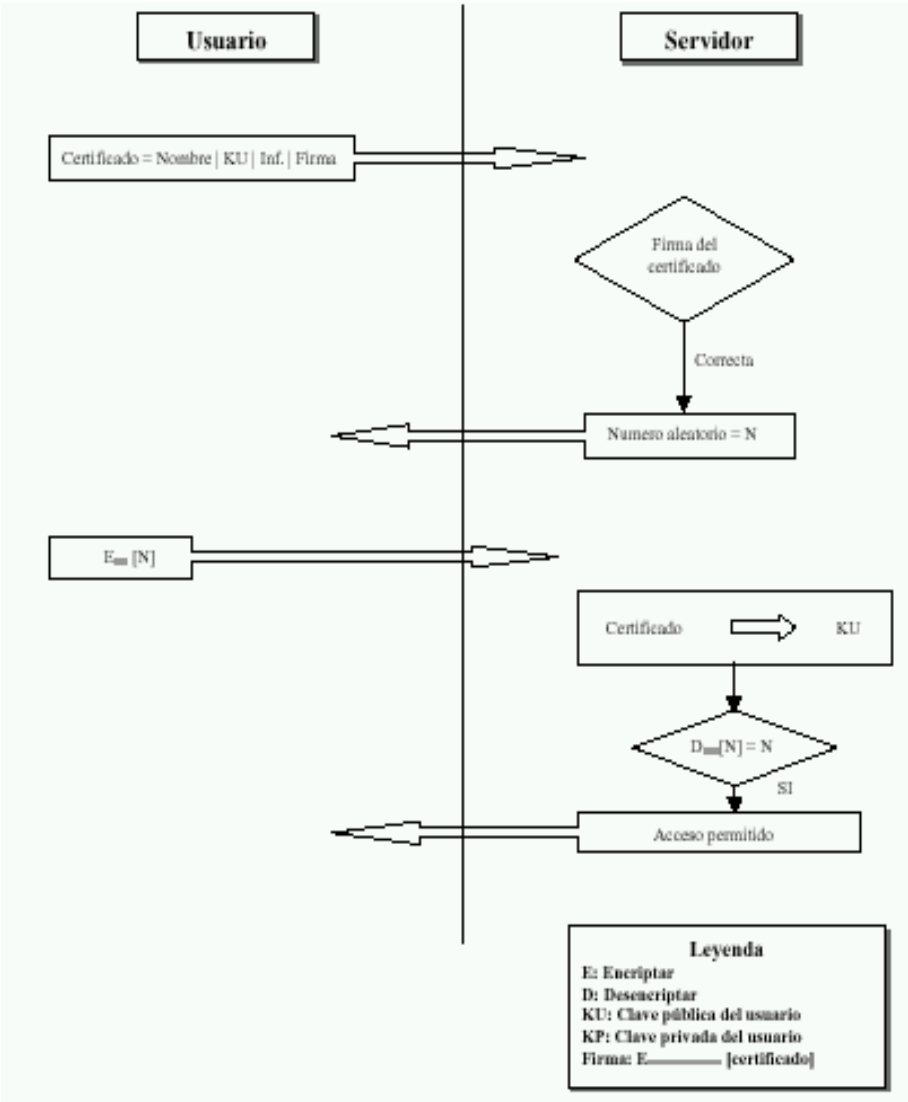
- Huellas dactilares FRR= 0,001 %
- Mano
- Iris del ojo. FAR 0,006 % FRR 0,0007 %
- Retina FAR 0 % FRR 12 %
- Firma
- Voz
- Reconocimiento facial.

4.1.3 Autentificación con objeto físico (Tokens)

- Tarjetas magnéticas
- Tarjetas Chip
- Memorias EPROM o Flash
- Pequeños ordenadores
- Estos sistemas complementan otros sistemas de acceso:
  - Contraseña, biométricos o certificados digitales
- Problema de la pérdida del objeto

4.1.4 Autentificación con certificados digitales

- Utiliza criptografía
- Es un objeto lógico, no físico
- El usuario debe tener
  - Un a clave privada de algún algoritmo asimétrico
  - Un certificado digital con la clave pública pareja de la privada y firmado digitalmente por el servidor
- Ejemplo: declaración de la renta por Internet

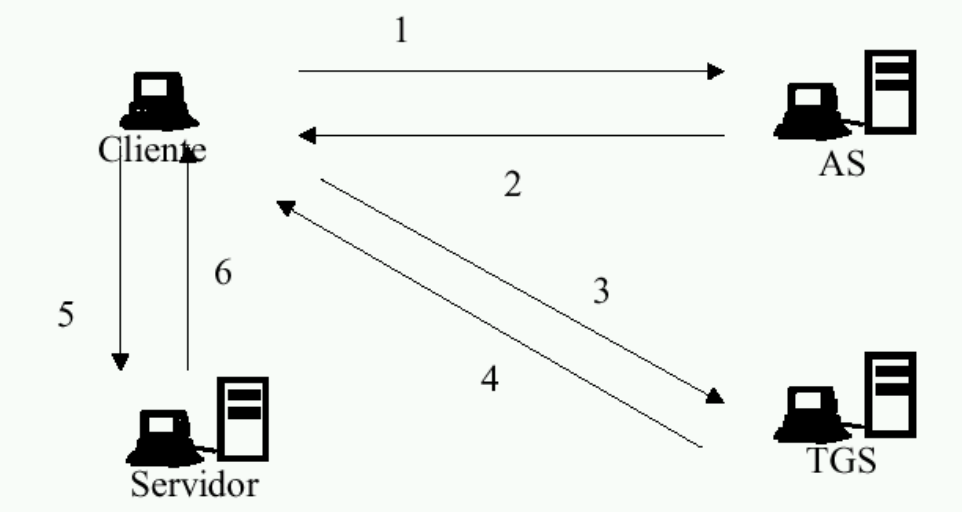


4.1.5 Autentificación Kerberos

- Sistema de control de acceso y autentificación para sistemas con muchos servidores
- Características
  - Utiliza claves simétricas
  - Los password nunca viajan por la red
  - Control de acceso individualizado por cada servicio
  - El password se introduce una sola vez por sesión
  - Se basa en un servidor de autentificación AS diferente de los servidores de información

Funcionamiento de Kerberos

Usuarios, servidor de servicios, servidor de autentificación (SA), servidor de concesión de tikets (TGS)



- El password del usuario genera una clave para encriptar el mensaje 1
- El $TICKET_{TGS}$ está cifrado con una clave conocida únicamente por TGS y AS
- Es un sistema costoso
- Otro ejemplo:
  - Sistema de windows NT
    - Trabajo en grupo
    - Dominios

4.2 Control de acceso

Una vez que autentifico puedo controlar los accesos

¿Que controlamos?

- Las máquinas: Que desde ciertos ordenadores se pueda o no acceder a recursos
- Los Usuarios (persona o programa)

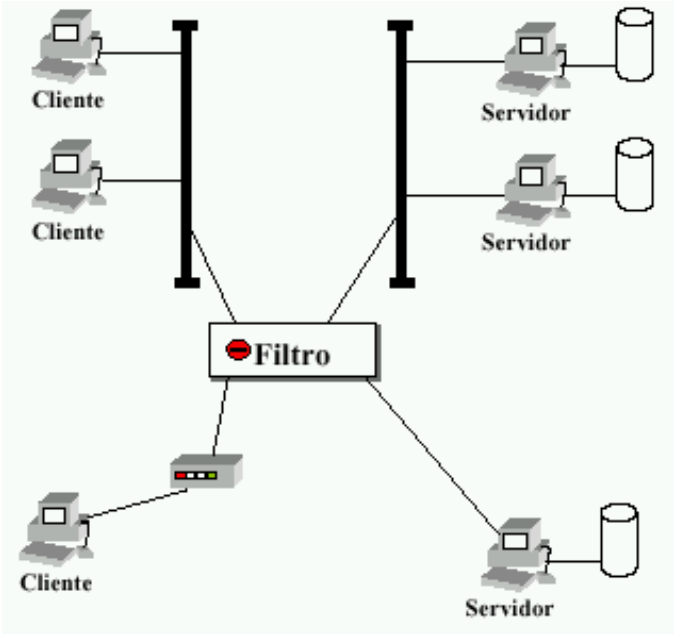
¿Dónde se pone el sistema de control?

- En la red
- En el servidor

4.2.1 Control en la red

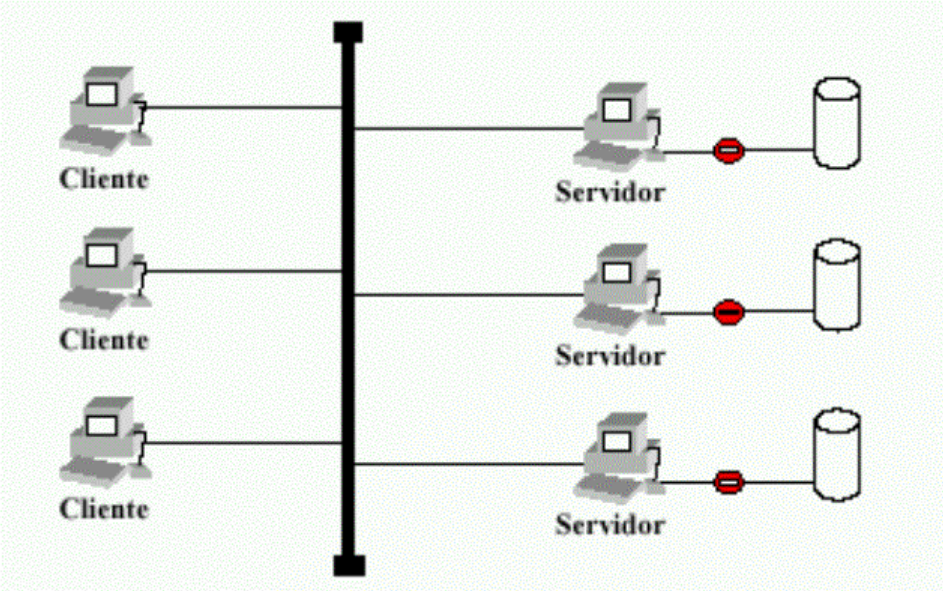
¿Quién lo realiza? Swichs LAN, Routers o Firewall. Los Inconveniente son que solo controla acceso desde máquinas remotas

Seguridad lógica (interna)



4.2.2 Control en el servidor

¿Quién lo realiza? El Sistema operativo o software. Las Ventajas son: Controla usuarios locales y remotos Inconvenientes: Difícil cuando son muchos los servidores.



4.2.3 Control de acceso por máquina

Identificadores posibles:

- Número de serie del procesador (Pentium III)
- Dirección MAC (física):
  - Solo funciona dentro de la red local.
  - No siguen ninguna norma
- Direcciones IP o de otros protocolos de red:

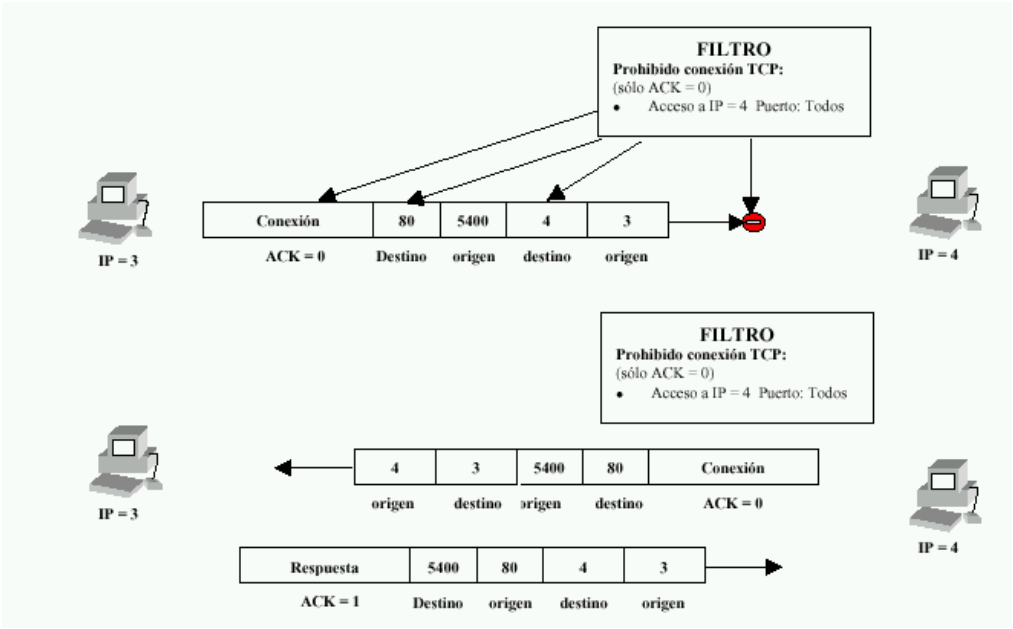
Seguridad lógica (interna)

- Permite control de acceso a servicios
- Obedecen a una lógica

- Nombre de Internet
  - Requiere el DNS

Control con firewall

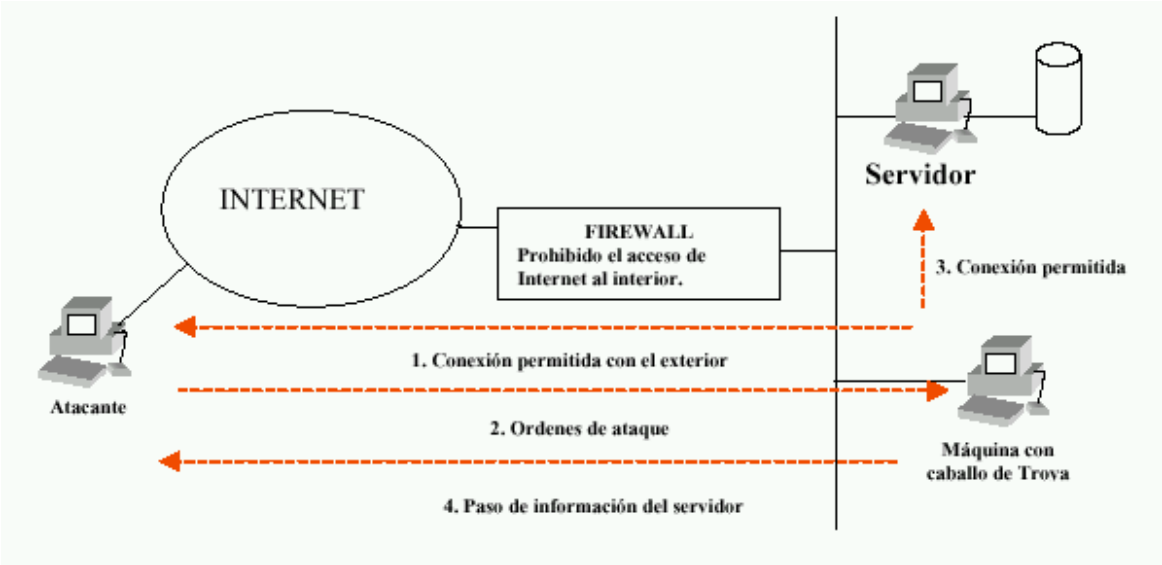
En esta dirección encontraremos toda la información sobre firewall http://www.wilyhacker.com/1e/



Ataques al control por IP o nombre

- Spoofing
  - Cambiar la dirección origen por una que es aceptada por el filtro
- Hijacking
  - Introducirse en la comunicación aprovechando una sesión abierto por un usuario con privilegio
- Denegación de servicios con paquetes UDP o ICMP
  - Destruye paquetes
- Ataques al DNS
  - Modifica la memoria cache del DNS (IP/nombre)
- Tunneling
  - Se aprovecha de un ordenador que está detrás del filtro

Seguridad lógica (interna)



Control de acceso de Usuarios

Clasificación de los tipos de acceso En función de quién organiza el control

- DAC (*Discretionary Access Control*)
  - El creador del fichero define los permisos
  - UNIX, Microsoft
- MAC (*Mandatory Access Control*)
  - La administración del sistema operativo asigna los permisos a los objetos
  - Cada objeto tiene una etiqueta
  - Los usuarios pertenecen a grupos que tienen definido permisos para cada etiqueta
- RBAC (*Role-Based Access Control*)
  - Por Roles
  - Lotus Notes

5 Seguridad del sistema de ficheros

- La pérdida de la información contenida en un sistema de ficheros puede ser irreparable y de costo infinito.
  - Un ordenador que se quema puede ser sustituido con la compra de otro. La información que contenía no.
- El control de acceso en un sistema de ficheros permite que el usuario determine quién y cómo puede acceder a sus ficheros.
- Un sistema orientado a la protección ofrece medios para distinguir entre uso autorizado y no autorizado.
- Sistemas de ficheros
  - Windows
    - FAT16
    - FAT32
    - NTFS
  - Uníx
    - EXT2FS
    - EXTFS
    - FAT16

- SMB
- 9660
- NFS
- SWAP
- MINIX
- XIAF
- Y MUCHOS MAS

5.1 Disponibilidad del sistema de ficheros

Vamos a comentar algunas medidas para garantizar la disponibilidad de los sistemas de ficheros. Un sistema de ficheros puede ser dañado por problemas de *hardware*:

- Errores de lectura
- Cortes o sobrecarga de corriente.
- Choque de las cabezas
- Polvo
- Temperatura
- Vandalismo

5.1.1 Listas de bloques defectuosos del disco.

- Solución *Hardware*: Mantener una pista donde señalar los sectores defectuosos. La controladora cuando va inicializar el disco lee primero esa pista.
- Solución *software*: Mantener un fichero con los sectores defectuosos.

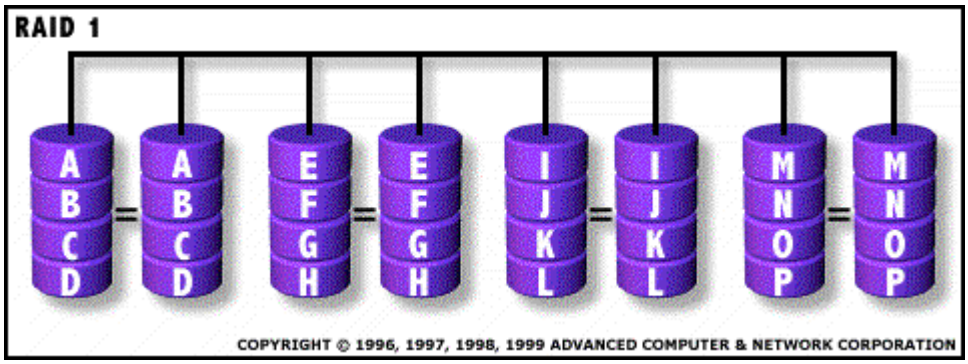
5.1.2 Copias de seguridad

Sistemas de copias

- Medios para pequeños sistemas
  - ZIP, LS-120, grabadoras y regrabadoras de CD, Discos mageto-ópticos, sistemas de cintas DAT
- Grandes sistemas
  - Librerías robotizadas de cintas
  - SAN (Storage Area Networks)
- Modos de copias
  - A cintas.
  - Discos espejos.
    - Almacenamiento estable: se implementa utilizando dos unidades de disco que contengan la misma información.
- Tipos de copias
  - Normales
  - Incrementales
  - Diferenciales (no marca como copiado)
- Sistemas de bases de datos
  - Registro de transacciones.
  - Ficheros de versión múltiple
    - Las actualizaciones se hacen sobre copias temporales de los ficheros. Está relacionado con las operaciones atómicas.

- Gestión de soportes
- Sistemas de copia padre, hijo, nieto

5.1.3 Sistemas RAID (redundant array of independent [inexpensive] disks)



El RAID (*redundant array of independent [inexpensive] disks*) es una forma de almacenar los mismos datos en distintos lugares (por tanto de modo redundante) en múltiples discos duros. Al colocar los datos en discos múltiples, las operaciones I/O (*input/output*, de entrada y salida) pueden superponerse de un modo equilibrado, mejorando el rendimiento del sistema. Dado que los discos múltiples incrementan el tiempo medio entre errores (*mean time between failure*, MTBF), el almacenamiento redundante de datos incrementa la tolerancia a fallos.

Un RAID, para el sistema operativo, aparenta ser un sólo disco duro lógico. El RAID emplea la técnica conocida como "*striping*" (bandeado o creación de bandas), que incluye la partición del espacio de almacenamiento de cada disco en unidades que van de un sector (512 bytes) hasta varios megabytes. Las bandas de todos los discos están interpaginadas (*interleaved*) y se accede a ellas en orden.

En un sistema de un solo usuario donde se almacenan grandes registros (como imágenes médicas o de otro tipo), las bandas generalmente se establecen para ser muy pequeñas (quizá de 512 bytes) de modo que un solo registro esté ubicado en todos los discos y se pueda acceder a él rápidamente leyendo todos los discos a la vez.

En un sistema multiusuario, un mejor rendimiento demanda que se establezca una banda lo suficientemente ancha para contener el registro de tamaño típico o el de mayor tamaño. Esto permite acciones I/O superpuestas en los distintos discos.

Hay al menos nueve tipos de RAID además de un grupo no redundante (RAID-0):

RAID-0. Esta técnica tiene bandeado paro no tiene redundancia de datos. Ofrece el mejor rendimiento pero no tolerancia a los fallos.

RAID-1. Este tipo también se conoce como creación de discos espejo y consiste de al menos dos discos duros que duplican el almacenamiento de datos. No hay bandeado. El rendimiento de la lectura se mejora pues cualquiera de los dos discos puede leerse al mismo tiempo. El rendimiento de escritura es el mismo que el del almacenamiento en un solo disco. El RAID-1 proporciona el mejor rendimiento y la mejor tolerancia a fallos en un sistema multiusuario.

RAID-2. Este tipo usa bandeado en todos los discos, con algunos de estos dedicados a almacenar información de verificación y corrección de errores (*error checking and correcting*, ECC). No tiene ninguna ventaja sobre el RAID-3.

RAID-3. Este tipo usa bandeado y dedica un disco al almacenamiento de información de paridad. La información de verificación de errores (ECC) incrustada se usa para detectar errores. La recuperación de datos se consigue calculando el O exclusivo (XOR) de la información registrada en los otros discos. Dado que una operación I/O accede a todos los discos al mismo tiempo, el RAID-3 no puede traslapar I/O. Por esta razón, el RAID-3 es mejor para sistemas de un solo usuario con aplicaciones que contengan grandes registros.

RAID-4. Este tipo usa grandes bandas, lo cual significa que podemos leer registros de cualquier disco individual. Esto nos permite aprovechar la I/O traslapada para las operaciones de lectura. Dado que todas las operaciones de escritura tienen que actualizar el disco de paridad, no es posible la superposición I/O para ellas. El RAID-4 no

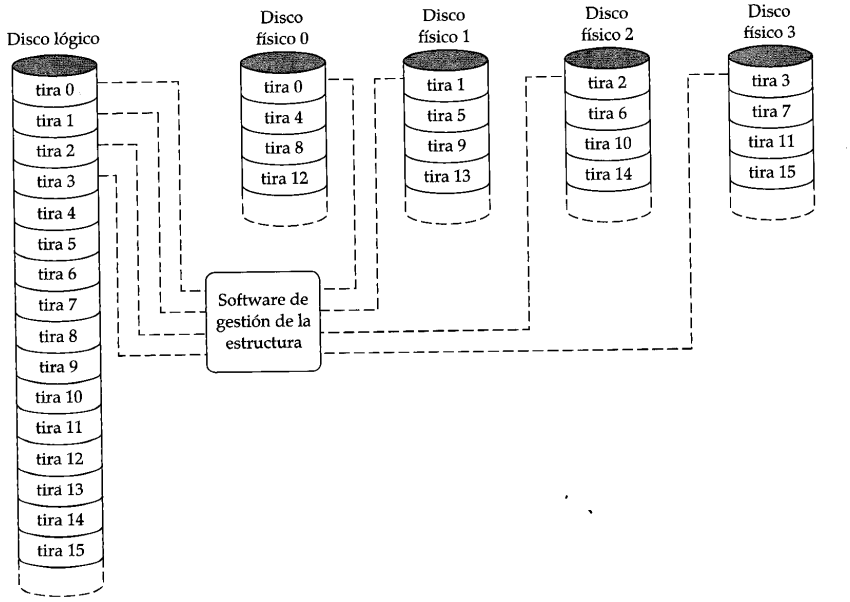
ofrece ninguna ventaja sobre el RAID-5. RAID-5. Este tipo incluye un grupo rotatorio de paridad, con lo que resuelve las limitaciones de escritura en RAID-4. Así, todas las operaciones de lectura y escritura pueden superponerse. El Raid 5 almacena información de paridad pero no datos redundantes (aunque la información de paridad puede usarse para reconstruir datos).

RAID-5 exige al menos tres y usualmente cinco discos en el conjunto. Es mejor para los sistemas multiusuario en los cuales el rendimiento no es crítico, o que realizan pocas operaciones de escritura.

RAID-6. Este tipo es similar al RAID-5, pero incluye un segundo esquema de paridad distribuido por los distintos discos y por tanto ofrece tolerancia extremadamente alta a los fallos y las caídas de disco. Hay pocos ejemplos comerciales en la actualidad.

RAID-7. Este tipo incluye un sistema operativo incrustado de tiempo real como controlador, haciendo las operaciones de caché a través de un bus de alta velocidad y otras características de un ordenador sencillo. Un vendedor ofrece este sistema.

RAID-10. Este tipo ofrece un conjunto de bandas en el que cada banda es un grupo de discos RAID-1. Esto proporciona mejor rendimiento que el RAID-1, pero a un costo mucho mayor.



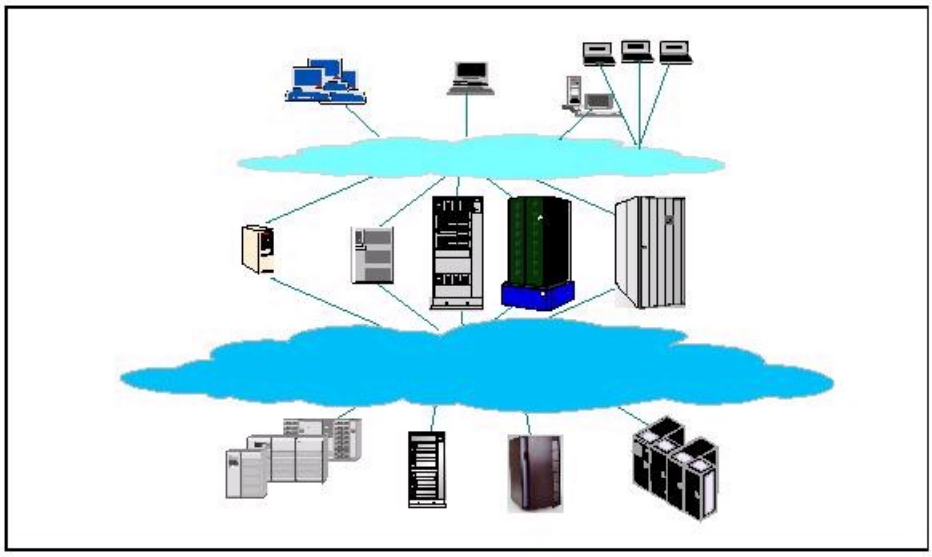
RAID-53. Este tipo ofrece un conjunto de bandas en el cual cada banda es un conjunto de discos RAID-3. Esto proporciona mejor rendimiento que el RAID-3, pero a un costo mucho mayor.

En resumen:

- El RAID mejora el rendimiento y la disponibilidad
- Hay muchos tipos de RAID (0-7, 10, 53)
- Se basan en las bandas (*striping*), redundancia (Discos espejos) y control de errores (CCR)

5.1.4 Storage Area Networks (SAN)

El nuevo concepto se define como "redes de dispositivos de almacenamiento gestionados de forma centralizada, conectados entre sí y con todos los servidores de la empresa a través de sistemas de alta velocidad y que permiten a las empresas explotar al máximo sus sistemas información".



5.2 Sistemas tolerantes a fallos

Para garantizar la disponibilidad y confiabilidad en todo momento de un sistema se recurre a los sistemas tolerantes a fallos.

Un sistema tolerante a fallos sigue funcionando aunque falle alguno de sus componentes. Se emplean en instalaciones críticas.

- Líneas aéreas.
- Bancos.
- Central nuclear.

El aspecto fundamental de la tolerancia a fallos es la **redundancia.**

- Hay sistemas que cuando falla uno se activa el de reserva y otros que funcionan siempre en paralelo.
- Degradación paulatina.

Los sistemas tolerantes están diseñados para poder sustituir y reparar un elemento sin parar el sistema.

6 Problemas de protección

6.1 Ejemplos

- Terminal con sesión abierta.
  - El terminal queda desatendido por el usuario.
    - Programa que imita la entrada de *login*.
- Puerta secreta.
  - El diseñador del *software* deja una puerta para poder usarla cuando quiera.
- Sospecha mutua.
  - Rutinas o funciones comunes que para su ejecución obtiene los permisos del invocante, utilizándolos posteriormente con intenciones perversas.
- Búsqueda de basura.
  - Información sensible borrada que queda en el dispositivo y puede ser husmeada y reconstruida con las herramientas adecuadas (pc-tools).

6.2 Software maligno (malware)

6.2.1 Caballo de Troya

Un Caballo de Troya es un programa maligno que se oculta en otro programa legítimo, encargado de encontrar datos o palabras de acceso y enviarlas a otra persona. Produce sus efectos perniciosos al ejecutarse el programa donde se oculta. En este caso, no es capaz de infectar otros archivos o soportes, y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

6.2.2 Bomba Lógica

Se trata simplemente de un programa maligno que permanece oculto en memoria y que solo se activa cuando se produce una acción concreta, predeterminada por su creador: cuando se llega a una fecha en concreto (Viernes 13), cuando se ejecuta cierto programa o cierta combinación de teclas, etc.

6.2.3 Gusano o Worm

Un gusano en un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la RAM, siendo ésta su única acción maligna.

- Son programas que son capaces de reproducirse y propagarse a otros ordenadores.
- No causan generalmente ningún daño directo a otros programas o ficheros del sistema informático que invaden.
- Los gusanos se distinguen de los virus en la forma de propagación. Los gusanos lo hacen exclusivamente a través de las redes informáticas.

6.2.4 Bacterias

Programas que consumen recursos del sistema por autoreplicación.

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos.

6.2.5 VIRUS

Es un código. Un virus en simplemente un programa que se adhiere a otros programas. Una secuencia de instrucciones y rutinas creadas con el único objetivo de alterar el correcto funcionamiento del sistema y, en la inmensa mayoría de los casos, corromper o destruir parte o la totalidad de los datos almacenados en el disco.

- Los virus informáticos recorren típicamente 4 etapas:
  - Letargo.
  - Propagación.
  - Activación.
  - Daño.

La clasificación es la siguiente:

- Virus parásito. Ataca a los ficheros ejecutables y se replica cuando se ejecutan.
- Virus residentes en memoria.
- Virus del sector de arranque.
- Virus sigilosos. Virus especialmente diseñados para no poder ser detectados.
- Virus mutantes.

Los virus ataca a los ficheros ejecutables y se replica cuando se ejecutan. Un verdadero virus tiene como características más importantes la capacidad de copiarse a sí mismo en soportes diferentes al que se encontraba originalmente, y por supuesto hacerlo con el mayor sigilo posible y de forma transparente al usuario; a este proceso de autorréplica se le conoce como "infección", de ahí que en todo este tema se utilice la terminología propia de la medicina: "vacuna", "tiempo de incubación", etc. Como soporte entendemos el lugar donde el virus se oculta, ya sea fichero, sector de arranque, partición, etc.

Un virus también debe modificar el código original del programa o soporte objeto de la infección, para poder activarse durante la ejecución de dicho código; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar así de forma trasparente al usuario.

La barrera entre virus puros y el resto de programas malignos es muy difusa, prácticamente invisible, puesto que ya casi todos los virus incorporan características propias de uno o de varios de estos programas: por ejemplo, los virus como el Viernes 13 son capaces de infectar otros archivos, siendo así virus puro, pero también realizan su efecto destructivo cuando se da una condición concreta, la fecha Viernes 13, característica propia de una bomba lógica; por último, se oculta en programas ejecutables teniendo así una cualidad de Caballo de Troya. De ahí la gran confusión existente a este respecto.

Formas De Infección

Antes de nada, hay que recordar que un virus no puede ejecutarse por si solo, necesita un programa portador para poder cargarse en memoria e infectar; asimismo, para poder unirse a un programa portador necesita modificar la estructura de este, para que durante su ejecución pueda realizar una llamada al código del virus.

Las partes del sistema más susceptibles de ser infectadas son el sector de arranque de los disquetes, la tabla de partición y el sector de arranque del disco duro, y los ficheros ejecutables (*.EXE y *.COM). Para cada una de estas partes tenemos un tipo de virus, aunque muchos son capaces de infectar por sí solos estos tres componentes del sistema.

En los disquetes, el sector de arranque es una zona situada al principio del disco, que contiene datos relativos a la estructura del mismo y un pequeño programa, que se ejecuta cada vez que arrancamos desde disquete.

En este caso, al arrancar con un disco contaminado, el virus se queda residente en memoria RAM, y a partir de ahí, infectara el sector de arranque de todos los disquetes a los que se accedan, ya sea al formatear o al hacer un DIR en el disco, dependiendo de cómo esté programado el virus).

El proceso de infección consiste en sustituir el código de arranque original del disco por una versión propia del virus, guardando el original en otra parte del disco; a menudo el virus marca los sectores donde guarda el boot original como en mal estado, protegiéndolos así de posibles accesos, esto suele hacerse por dos motivos: primero, muchos virus no crean una rutina propia de arranque, por lo que una vez residentes en memoria, efectúan una llamada al código de arranque original, para iniciar el sistema y así aparentar que se ha iniciado el sistema como siempre, con normalidad. Segundo, este procedimiento puede ser usado como técnica de ocultamiento.

Normalmente un virus completo no cabe en los 512 bytes que ocupa el sector de arranque, por lo que en éste suele copiar una pequeña parte de si mismo, y el resto lo guarda en otros sectores del disco, normalmente los últimos, marcándolos como defectuosos. Sin embargo, puede ocurrir que alguno de los virus no marquen estas zonas, por lo que al llenar el disco estos sectores pueden ser sobrescritos y así dejar de funcionar el virus.

La tabla de partición esta situada en el primer sector del disco duro, y contiene una serie de bytes de información de cómo se divide el disco y un pequeño programa de arranque del sistema. Al igual que ocurre con el boot de los disquetes, un virus de partición suplanta el código de arranque original por el suyo propio; así, al arrancar desde disco duro, el virus se instala en memoria para efectuar sus acciones. También en este caso el virus guarda la tabla de partición original en otra parte del disco, aunque algunos la marcan como defectuosa y otros no. Muchos virus guardan la tabla de partición y a ellos mismos en los últimos sectores de disco, y para proteger esta zona, modifican el contenido de la tabla para reducir el tamaño lógico del disco. De esta forma el DOS no tiene acceso a estos datos, puesto que ni siquiera sabe que esta zona existe.

Casi todos los virus que afectan la partición también son capaces de hacerlo en el boot de los disquetes y en los ficheros ejecutables; un virus que actuara sobre particiones de disco duro tendría un campo de trabajo limitado, por lo que suelen combinar sus habilidades.

Con todo, el tipo de virus que más abunda es el de fichero; en este caso usan como vehículo de expansión los archivos de programa o ejecutables, sobre todo .EXE y . COM, aunque también a veces .OVL, .BIN y .OVR. AL ejecutarse un programa infectado, el virus se instala residente en memoria, y a partir de ahí permanece al acecho; al ejecutar otros programas, comprueba si ya se encuentran infectados. Si no es así, se adhiere al archivo ejecutable, añadiendo su código al principio y al final de éste, y modificando su estructura de forma que al ejecutarse dicho programa primero llame al código del virus devolviendo después el control al programa portador y permitiendo su ejecución normal.

Este efecto de adherirse al fichero original se conoce vulgarmente como "engordar" el archivo, ya que éste aumenta de tamaño al tener que albergar en su interior al virus, siendo esta circunstancia muy útil para su detección. De ahí que la inmensa mayoría de los virus sean programados en lenguaje ensamblador, por ser el que genera el código más compacto, veloz y de menor consumo de memoria; un virus no seria efectivo si fuera fácilmente detectable por su excesiva ocupación en memoria, su lentitud de trabajo o por un aumento exagerado en el tamaño de los archivos infectados. No todos los virus de fichero quedan residentes en memoria, si no que al ejecutarse se portador, éstos infectan a otro archivo, elegido de forma aleatoria de ese directorio o de otros.

Efectos destructivos de los Virus

Los efectos perniciosos que causan los virus son variados; entre éstos se encuentran el formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, ralentización del sistema hasta limites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos.

Técnicas utilizadas por los Virus

Cada uno de los miles de virus existentes utiliza diferentes mecanismos, tanto para realizar la infección como para ocultarse y pasar desapercibido. Estas técnicas evolucionan con el tiempo, como las técnicas utilizadas por los programas antivirus para detectarlos. En esta sección presentamos los mecanismos utilizados por los virus:

- ***Ocultamiento*** (*Stealth*): los virus que utilizan esta técnica intentan pasar desapercibidos ante los ojos del usuario, no levantando ninguna sospecha sobre la infección que ya ha tenido lugar. Los virus residentes son los que más la utilizan, aunque no es exclusivamente este tipo de virus quienes la aplican. Cuando un virus infecta un determinado fichero, suele dejar signos evidentes de su actuación, como los siguientes: aumento de tamaño en el fichero infectado, modificación de la fecha y hora de creación en el fichero infectado, secciones marcadas como defectuosas, disminución de la capacidad en la memoria, ...etc. El virus se encargará de que cada una de estas pistas no puedan ser visualizadas. Para ello vigilará peticiones de información que requiere el sistema operativo acerca de estas características, interceptándolas y ofreciendo un información falseada e irreal.
- ***Sobrepasamiento*** (*Tunneling*): se trata de una técnica especialmente diseñada para imposibilitar la protección antivirus en cualquier momento. Mientras el análisis permanente, o residente, del programa antivirus que se encuentre instalado intenta realizar detecciones, el virus actúa en su contra. Todas las operaciones que se realizan sobre cualquiera de los archivos son inspeccionadas por el antivirus mediante la interceptación de las acciones que el sistema operativo lleva a cabo para hacerlas posible. De la misma manera, el virus interceptará estas peticiones o servicios del sistema operativo, obteniendo las direcciones de memoria en las que se encuentran. Así el antivirus no detectará la presencia del virus. No obstante, existen técnicas antivirus alternativas que permiten la detección de virus que realicen este tipo de operaciones.
- ·***Autoencriptación***: los programas antivirus se encargan de buscar determinadas cadenas de caracteres (lo que se denomina la firma del virus) propias de cada uno de los posibles virus. Estos, por su parte y mediante la técnica de autoencriptación, infectarán de forma diferente en cada ocasión. Esto significa que el virus utilizará una cadena concreta para realizar una infección, mientras que en la siguiente infección utilizará otra distinta. Por otro lado, el virus codifica o cifra sus cadenas para que al antivirus le sea difícil encontrarlo. Sin embargo, los virus que utilizan este tipo de técnicas, emplean siempre la misma rutina o algoritmo de encriptación, con lo que es posible su detección.
- ·***Polimorfismo***: basándose en la técnica de autoencriptación, el virus se codifica o cifra de manera diferente en cada infección que realiza (su firma variará de una infección a otra). Si sólo fuese así estaríamos hablando de un virus que utiliza la encriptación, pero adicionalmente el virus cifrará también el modo (rutina o algoritmo) mediante el cual realiza el cifrado de su firma. Todo esto hace posible que el virus cree ejemplares de sí mismo diferentes de una infección a la siguiente, cambiando de "forma" en cada una de ellas. Para su detección, los programas antivirus emplean técnicas de simulación de descifrado.
- ·***Armouring***: mediante esta técnica el virus impide ser examinado. Para conocer más datos sobre cada uno de ellos, éstos son abiertos como ficheros que son, utilizando programas especiales (*Debuger*) que permiten descubrir cada una de las líneas del código (lenguaje de programación en el que están escritos). Pues bien, en un virus que utilice la técnica de Armouring no se podrá leer el código.

Técnicas Antivirus

– Detección

- Identifiicación
- Eliminación

A medida que evolucionan las técnicas empleadas por los virus y éstas son investigadas, los programas antivirus incorporan medidas de búsqueda de virus y protección más avanzadas como las siguientes:

- ***Búsqueda de cadenas***: cada uno de los virus contiene determinadas cadenas de caracteres que le identifican. Estas son las denominadas firmas del virus. Los programas antivirus incorporan un fichero denominado "fichero de firmas de virus" en el que guardan todas las cadenas correspondientes a cada uno de los virus que detecta. De esta forma, para encontrarlos, se analizarán todos los ficheros especificados comprobando si alguno de ellos las contiene. Si un fichero no contiene ninguna de estas cadenas, se considera limpio, mientras que si el programa antivirus la detecta en el interior del fichero avisará acerca de la posibilidad de que éste se encuentre infectado.
- ***Excepciones***: una alternativa a la búsqueda de cadenas es la búsqueda de excepciones. Cuando un virus utiliza una determinada cadena para realizar una infección pero en la siguiente emplea otra distinta, es difícil detectarlo mediante la búsqueda de cadenas. En ese caso lo que el programa antivirus consigue es realizar la búsqueda concreta de un determinado virus.
- ***Análisis heurístico***: cuando no existe información que permita la detección de un nuevo o posible virus desconocido, se utiliza esta técnica. Se caracteriza por analizar los ficheros obteniendo información sobre cada uno de ellos (tamaño, fecha y hora de creación, posibilidad de colocarse en memoria,...etc.). Esta información es contrastada por el programa antivirus, quien decide si puede tratarse de un virus, o no.
- ***Protección permanente***: durante todo el tiempo que el ordenador permanezca encendido, el programa antivirus se encargará de analizar todos los ficheros implicados en determinadas operaciones. Cuando éstos se copian, se abren, se cierran, se ejecutan,...etc., el antivirus los analiza. En caso de haberse detectado un virus se muestra un aviso en el que se permiten la desinfección. Si no se encuentra nada extraño, el proceso recién analizado continúa.
- ***Vacunación***: mediante esta técnica, el programa antivirus almacena información sobre cada uno de los ficheros. En caso de haberse detectado algún cambio entre la información guardada y la información actual del fichero, el antivirus avisa de lo ocurrido. Existen dos tipos de vacunaciones: Interna (la información se guarda dentro del propio fichero, de tal forma que al ejecutarse él mismo comprueba si ha sufrido algún cambio) y Externa (la información que guarda en un fichero especial y desde él se contrasta la información).

LOS QUINCE CONSEJOS ANTI-VIRUS

1.- Utiliza un buen antivirus y actualízalo frecuentemente.

La mejor manera de estar protegido contra los virus es instalar un buen antivirus en tu ordenador.

Un antivirus es un programa informático específicamente diseñado para detectar y eliminar virus. Porque los conoce, sabe cómo actúan y también sabe cómo eliminarlos.

Sin embargo, cada día aparecen más de 20 nuevos virus que los antivirus no son capaces de reconocer. Para la detección y eliminación de estos virus es necesario actualizar frecuentemente nuestro antivirus.

Por lo tanto, la efectividad de un programa antivirus reside, en gran medida, en su capacidad de actualización, preferentemente diaria.

2.- Comprueba que tu antivirus incluye soporte técnico, resolución urgente de nuevos virus y servicios de alerta.

Si bien un antivirus perfectamente actualizado es la mejor arma para luchar contra los virus, es aconsejable contar con servicios adicionales.

El servicio de soporte técnico, bien a través de correo electrónico o por teléfono, es de gran ayuda ante cualquier problema o duda que pueda surgir relacionado con virus o con el funcionamiento del antivirus.

En el supuesto de verse afectado por algún virus de reciente creación, se debe contar con un servicio de resolución urgente de nuevos virus capaz de eliminarlos en el menor tiempo posible.

Otro servicio fundamental son las alertas sobre nuevos virus peligrosos, por ejemplo, a través de listas de correo.

3.- Asegúrate de que tu antivirus esté siempre activo.

Un antivirus está activo cuando dispone de una protección permanente capaz de vigilar constantemente todas las operaciones realizadas en el ordenador.

Existen dos maneras para comprobar que esta protección permanente está activa; a través de un icono fijo en la barra de tareas, junto a la información horaria, o en la propia configuración del programa antivirus.

Estar protegido contra los virus requiere una protección permanente, tanto de archivos como de correo electrónico.

4.- Verifica, antes de abrir, cada nuevo mensaje de correo electrónico recibido.

El correo electrónico es el medio de transmisión preferido por los virus, por lo que hay que tener especial cuidado en su utilización.

Cualquier correo recibido puede contener virus aunque no le acompañe el símbolo de datos adjuntos (el habitual "clip"). Además, no es necesario ejecutar el archivo adjunto de un mensaje de correo para ser infectado; en algunos sistemas basta únicamente con abrir el mensaje, o visualizarlo mediante la 'vista previa'.

Para prevenir esto, lo mejor es verificar los mensajes inesperados o que provengan de una fuente poco habitual. Un indicativo de posible virus es la existencia en el asunto del mensaje de palabras en un idioma diferente al utilizado normalmente por el remitente.

5.- Evita la descarga de programas de lugares no seguros en Internet.

Muchas páginas de Internet permiten la descarga de programas y archivos a los ordenadores de los internautas. Cabe la posibilidad de que estos archivos estén infectados con virus.

Como no existen indicadores claros que garanticen su fiabilidad, debemos evitar la descarga de programas desde sitios web que no nos ofrezcan garantías. Por lo general, son sitios seguros aquellos que muestran una información clara acerca de su actividad y los productos o servicios que ofrecen; también los avalados por organizaciones tales como editoriales, organismos oficiales, etc.

6.- Rechaza archivos que no hayas solicitado cuando estés en chats o grupos de noticias (news).

Gracias a Internet es posible intercambiar información y conversar en tiempo real sobre temas muy diversos mediante los grupos de noticias y los chats, respectivamente.

Los grupos de noticias o "news", como no son listas de correo y usan su propio sistema de transmisión por Internet (NNTP), también necesitan de una protección eficaz y constante.

Ambos sistemas, además de permitir la comunicación con otras personas, también facilitan la transferencia de archivos. Aquí es donde hay que tener especial cuidado y aceptar sólo lo que llegue de un remitente conocido y de confianza.

7.- Analiza siempre con un buen antivirus los disquetes que vayas a usar en tu ordenador.

Además de Internet, otra de las vías de infección de virus más frecuente son los disquetes.

Es una buena norma analizar, mediante un buen antivirus, todos aquellos disquetes que entren y salgan de nuestro ordenador.

Al utilizar nuestros disquetes en otros ordenadores es aconsejable protegerlos contra escritura, bajando la pestaña de la parte inferior derecha del disquete, en su parte trasera.

8.- Retira los disquetes de las disqueteras al apagar o reiniciar tu ordenador.

A pesar de que Internet es uno de los medios de propagación de virus más habituales, cabe resaltar que los disquetes siguen siendo una vía de infección de gran magnitud.

Además de analizar con un antivirus todos los disquetes utilizados, una forma de evitar que se activen los ya clásicos virus de boot o de arranque consiste en retirar los disquetes de las disqueteras al apagar o reiniciar el ordenador.

Por si se nos olvida hacerlo, es conveniente contar con un antivirus capaz de comprobar en tales circunstancias la existencia de disquetes infectados.

9.- Analiza el contenido de los archivos comprimidos.

Los archivos comprimidos, muy útiles por contener en su interior múltiples archivos y ocupar menos espacio, son un caldo de cultivo para los virus.

En primer lugar, hay que demandar a nuestro antivirus que detecte el mayor número de formatos comprimidos posible.

Antes de abrir directamente uno de estos archivos, como los de formato ZIP, es aconsejable guardarlos en carpetas temporales -creadas por los usuarios y cuyos ficheros pueden ser posteriormente borrados- en lugar de abrirlos sobre directorios de trabajo, por ejemplo, la carpeta Windows, Mis Documentos, el Escritorio, etc.

10.- Mantente alerta ante acciones sospechosas de posibles virus.

Mediante el simple uso del ordenador, hay numerosos síntomas que pueden delatar la presencia de nuevos virus: aumento del tamaño de los archivos, avisos de macros en documentos Word o Excel que en principio no deberían contenerlas, recepción por parte de otras personas de mensajes nuestros de correo que no hemos enviado…

Como solución más completa a estas sospechas de posibles infecciones, se debe recurrir al servicio de resolución urgente de nuevos virus de nuestra compañía antivirus.

11.- Añade las opciones de seguridad de las aplicaciones que usas normalmente a tu política de protección antivirus.

Los programas informáticos más utilizados se convierten, precisamente por esa razón, en blanco de los autores de virus. Sus fabricantes suelen incluir en ellos opciones de seguridad contra virus.

Tal es el caso de los navegadores de Internet, procesadores de texto, programas de correo, etc., que disponen de características para asegurar un poco más la información.

Si no estamos familiarizados con ellas, podemos acudir a la ayuda del propio programa y realizar una búsqueda del término 'seguridad' para saber cómo utilizarlas.

Es conveniente aprovechar estas opciones específicas de seguridad, además de contar con un antivirus constantemente actualizado.

12.- Realiza periódicamente copias de seguridad.

Una muy buena forma de minimizar el impacto de un virus, tanto a nivel corporativo como particular, es restaurar las copias de seguridad de nuestra información.

Realizar copias periódicas y frecuentes de nuestra información más importante es una magnífica política de seguridad. De esta manera, una pérdida de datos, causada por ejemplo por un virus, puede ser superada mediante la restauración de la última copia.

13.- Mantente informado.

Una buena manera de protegerse contra los nuevos virus es estar continuamente informado sobre lo que acontece en el sector de la Seguridad Informática.

Sin embargo, ante la gran cantidad de información recibida por diferentes medios, es aconsejable contrastar estos datos con la información completa, actualizada y experta difundida por determinadas compañías y organismos: compañías antivirus, empresas consultoras de seguridad, organismos que informan de alertas tempranas, organismos gubernamentales, universidades, etc.

14.- Utiliza siempre software legal.

A la hora de instalar nuevos programas en el ordenador, el riesgo de infección es menor si se trata de software legal.

Sin embargo, si el software nos ha llegado en CDs piratas, o se trata de software legal manipulado posteriormente para "saltarse" la protección de los propios fabricantes, nadie nos puede asegurar que esté libre de virus.

Además, si se trata de software antivirus, su legalidad nos permite disfrutar de todos los servicios adicionales que garantizan su eficacia y seguridad.

15.- Exige a los fabricantes de software, proveedores de acceso a Internet y editores de publicaciones, que se impliquen en la lucha contra los virus.

En la lucha contra los virus se precisa la participación de todos los agentes implicados en el sector informático: empresas, usuarios finales, compañías antivirus, medios de comunicación, etc.

Como Internet es el medio más utilizado por los virus para su propagación, la colaboración de los proveedores de acceso a Internet es muy importante.

Así mismo, es aconsejable que los fabricantes de software y las publicaciones que ofrecen CD-ROMs adopten medidas para no difundir virus.

La contribución de todos ellos ayudará a minimizar el problema de las infecciones provocadas por virus. (**Fuente: Pandasoftware**)

6.2.6 La ingeniería social

¡¡¡ Yo no he comprado nada !!! Publicado en Kriptonomicon Un numeroso grupo de internautas españoles recibieron un correo electrónico que les confirmaba la compra en Internet de una mercancía, cargada en su cuenta corriente, que recibirían en un breve plazo de tiempo. Además de dar las gracias al supuesto cliente, la misiva indicaba que si tenía alguna duda llamaran al teléfono que aparecía al final del mensaje, donde también se atendería cualquier queja o reclamación. El número en cuestión era una especie de 906, aunque con llamada internacional, donde respondía una grabación que solicitaba unos momentos de espera a la víctima de la estafa. No había ninguna empresa al otro lado de la línea, ni compra efectuada en Internet, ni mercancía alguna que recibir. La carta era falsa. Su objetivo: asustar al inocente internauta para que llamara al teléfono del timador, que cobraría por cada segundo que las víctimas pasaran con el auricular pegado a la oreja.

La Ingeniería Social no es exclusiva de los virus: es habitualmente empleada por los hackers para engañar a los usuarios, aunque también ayuda a los virus a infectar a más ordenadores.

La Ingeniería Social no se emplea ningún programa de software o elemento de hardware, sólo grandes dosis de ingenio, sutileza y persuasión para así lograr datos de otra persona sin que se dé cuenta de que está revelando información importante con la que, además, el atacante puede dañar su ordenador.

Un claro ejemplo de Ingeniería Social es el del hacker que llama por teléfono a una empresa para decir que necesita ayuda o hablar con el administrador de la red porque hay que modificar algún aspecto de la configuración. Durante la conversación, y a través de escogidas y cuidadas preguntas, el atacante obtendrá los datos (como los códigos de acceso a los equipos) que necesita para vulnerar la seguridad del sistema.

En la práctica, los autores de virus emplean la Ingeniería Social para que sus creaciones se propaguen rápidamente. Para ello atraen la atención del usuario y consiguen que realice alguna acción (que, normalmente, consiste en abrir un fichero que es el que procede a realizar la infección), mediante variados trucos, entre los que destacan los siguientes:

1) Emplear como señuelos mensajes o ficheros con explícitas referencias eróticas.

- - HomePage llama la atención del usuario aludiendo a una sugestiva página. Además se autoenvía de manera masiva por e-mail e intenta acceder a determinados sitios web pornográficos.
- - W32/Hybris reclama la curiosidad de los usuarios mediante un mensaje sugerente sobre una posible versión erótica del cuento de Blancanieves y los Siete Enanitos. Además, para aumentar su propagación, el asunto del mensaje se presenta en diferentes idiomas.
- - W32/Naked intenta atraer la atención del usuario ofreciéndole un archivo cuyo nombre (NakedWife.exe) sugiere la imagen de una mujer desnuda.

2) Aludir a personajes famosos, tal y como ha sucedido con:

- - "AnnaKournikova" alias VBS/SST.A o "I-Worm/Lee.O"- intenta engañar al usuario haciéndole creer que ha recibido un fichero que contiene una fotografía de la tenista Anna Kournikova.
- - Trojan.Butano aprovecha la imagen del conocido locutor de radio José María García para esconder un programa que elimina todos los archivos existentes en el directorio raíz del disco duro.
- - I-Worm/Pikachu se envía por correo electrónico en un mensaje cuyo asunto es "Pikachu Pokemon", en clara referencia al popular personaje infantil de videojuegos y series de animación.

3) Servirse de "ganchos" vinculados a las relaciones amorosas.

- - W32/Matcher utiliza como reclamo -en el cuerpo del mensaje en el que se envía- un texto que ofrece una alternativa para encontrar pareja.
- - VBS/LoveLetter -alias "Iloveyou"- se envía por correo electrónico en un mensaje cuyo asunto es "ILOVEYOU" y el fichero que incluye se denomina "LOVE-LETTER-FOR-YOU.TXT.VBS".

Habría mucho que hablar sobre la ingeniería social en Internet, aunque en este número nos hemos centrado en el uso que los virus suelen hacer de ésta disciplina.

6.3 Spyware: software espía en Internet El precio de la gratuidad

(fuente:Criptonomicon http://www.iec.csic.es/criptonomicon **)**

Problemas de protección

Los programas gratuitos son muy frecuentes en Internet. ¿Nunca se ha preguntado por qué contra toda lógica una empresa puede decidir ofrecer software gratis? ¿Qué obtiene a cambio? A menudo, la respuesta es simple y aterradora a la vez: sus datos personales. El pagar con su privacidad a cambio de obtener un programa en apariencia gratuito se está convirtiendo en moneda de cambio común en Internet. Con eso de que cada vez más usuarios tienen su ordenador conectado a la Red, incluso de forma permanente gracias a tarifas planas de cable y ADSL, muchas compañías optan por distribuir sus productos de forma totalmente gratuita y cobrarse el servicio espiando la actividad del usuario.

Siempre que instala un programa en su ordenador, éste necesariamente tiene acceso a todos los recursos del sistema: puede leer cualquier rincón del disco duro, registrar cada pulsación de teclado realizada por el usuario o guardar un histórico de cada programa y documento abiertos. Claro que una cosa es la posibilidad de llevar a cabo todas estas tareas y otra, que se haga de verdad.

Los programas que rastrean la información sobre hábitos de consumo y navegación de los internautas pueden realizar todas o alguna de las actividades anteriores de manera sigilosa, sin que nadie lo advierta. A intervalos de tiempo programables, el programa se conecta a través de Internet con un servidor de la compañía que lo distribuyó y transmite diligentemente toda la información que ha recopilado. Uno de los primeros casos conocidos de software espía fue el de Aureate/Radiate, que funcionaba en conjunción con programas que incluían publicidad para financiarse, lo que se conoce como software de distribución adware, esto es, el usuario no paga por usar el programa, pero debe soportar la presencia de banners. Con la excusa de que necesitaban conectarse a un servidor central para descargar los banners que vería el usuario, establecían conexiones sin despertar mayores sospechosas. Lo que no imaginaba el usuario era que el programa no sólo descargaba banners, sino que también enviaba de vuelta a Aureate información de su actividad en Internet. El hecho resultaba aún más grave si se tiene en cuenta que al desinstalar el programa de Aureate dejaban de funcionar las otras aplicaciones que había descargado, como GetRight o Go!zilla.

Desde luego que Aureate/Radiate no es la única compañía metida en este negocio. Otros programas similares a Aureate/Radiate que puede encontrar en su ordenador son Webhancer, Customer Companion, Conducent/Timesink, Cydoor, Comet Cursor o Web3000. Otras aplicaciones de gran popularidad y uso muy extendido hoy día entre los internautas que recaban información sobre los usuarios para enviarla a las casas publicitarias son, además de las ya citadas, Audiogalaxy, Babylon Tool, Copernic 2000, CrushPop, CuteMX, EZForms, Gator, FlashGet, Gif Animator, iMesh, JPEG Optimizer, MP3 Downloader, MP3 Fiend, NeoPlanet Browser, Net Scan 2000, Net Tools 2001, NetMonitor, Odigo Messenger, Opera Freeware, Oligo Browser, Real Audioplayer, Spam Buster, TIFNY, TypeItIn, WebCopier, ZipZilla. Si le entra la duda y quiere saber si un software concreto esconde o no programas que recopilan su información, consulte la base de datos de Spychecker en www.spychecker.com o el completo listado en www.infoforce.qc.ca/spyware.

Por otro lado, las barras de navegación constituyen la última vuelta de tuerca en las novedosas estrategias maquinadas por las empresas punto com, para recabar subrepticiamente información sobre los usuarios. Existen docenas de barras gratuitas que asisten al internauta en su navegación: le facilitan las búsquedas en Internet, le proporcionan información extendida sobre el sitio que está visitando, le ayudan a comparar precios sobre productos, en definitiva, colaboran para que su vida en la Red sea más sencilla.

Lo que el internauta desconoce es que, silenciosamente entre bastidores, algunas barras también registran cada página que visita, cada formulario que rellena, sin distinguir si se trata de páginas cifradas o no. Cada cierto tiempo, las barras envían toda esta información a la empresa de software, que ve así recompensados con creces sus esfuerzos por desarrollar el producto "gratis". Otra forma de recopilación solapada de datos de los internautas que se ha visto en Internet consiste en la utilización de los "Web bugs" o "escuchas Web", de las que ya se habló en un editorial anterior (http://www.iec.csic.es/criptonomicon/susurros/susurros32.html). Mientras algunas compañías avisan acerca de su intención de recopilar información sobre hábitos de navegación del usuario en la letra pequeña de sus licencias de uso, ese texto que nadie lee cuando instala los programas, otras obvian toda referencia clara a su actividad espía. Obtener datos privados sobre los usuarios sin pedir su consentimiento y, lo que es peor, sin ni siquiera informarles sobre ello, representa un grave atentado contra la privacidad que se está volviendo cada vez más frecuente en Internet. La próxima vez que descargue un programa sin que le cobren por ello, piense que a lo mejor no es tan gratuito como se anuncia en la publicidad. Sus datos personales pueden suponer el precio que pagará por él.

6.4 Seguridad en Redes de ordenadores

- Hitos de seguridad en las transacciones Electrónicas
  - Evitar monitorizaciones ilegales

- Evitar la modificación de los mensajes y/o modo de demostrar que la alteración ha sucedido
- Determinar que la transmisión es de una fuente auténtica
- No repudio: evitar que niegue haber emitido o recibido un mensaje

7 Criptografía

El conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido. Es el arte de escribir en clave. Protege la información del acceso de quien no está autorizado a conocerla. La criptografía oculta datos

- Encriptación: ocultación de datos
- Desencriptación: liberación de datos
- Elementos:
  - clave y algoritmos

El cifrado es un método común de proteger la información que se transmite por enlaces poco fiables. El método es:

- La información se cifra de su formato legible inicial (llamado texto limpio) a un formato interno (llamado texto cifrado). Este formato interno del texto aunque es legible, no tiene ningún sentido.
- El texto cifrado se almacena o se transmite.
- El texto cifrado es descifrado por el receptor a fin de recuperar el texto limpio.

La encriptación de los mensajes se puede hacer por codificación o por cifrado.

- Codificación: Utiliza una tabla o diccionario para hacer sustituciones de palabras o letras.
- Cifrado: utiliza un algoritmo para transformar el mensaje.

Los criptosistemas que se basan en mantener secreto el algoritmo son fáciles de descifrar utilizando métodos estadísticos.

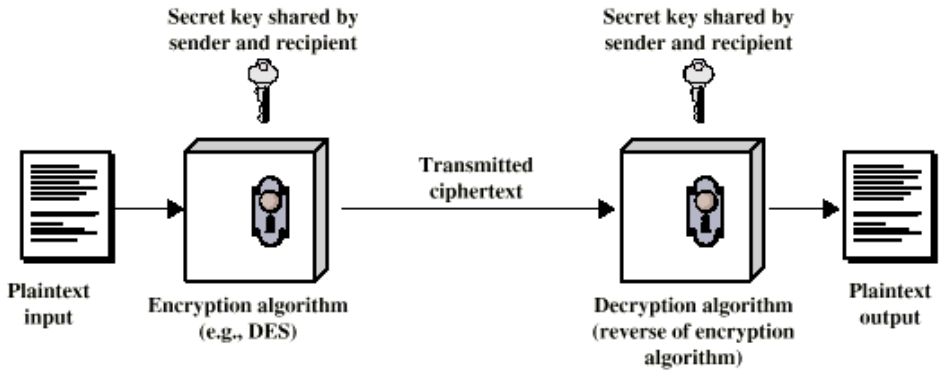
Los sistemas actuales basan su seguridad en mantener en secreto una serie de parámetros, llamados claves, de forma que el algoritmo puede ser conocido.

- Es imposible descifrar un mensaje basándose en el texto cifrado y al conocimiento del algoritmo de encriptación/desencriptación.
- El algoritmo no tiene que ser secreto: lo que hay que mantener secreto son las claves.

Sistema criptográfico **simétrico**: es aquel que utiliza la misma clave para cifrar y descifrar. Sistema criptográfico **asimétrico**: utiliza claves diferentes para cifrar y descifrar un mensaje. Hay que distinguir entre:

- **Sistemas de clave secreta**, en que el emisor y el receptor del mensaje utilizan una misma clave para cifras y descifrar respectivamente el mensaje. Ambos deben mantener la clave en secreto.
- **Sistemas de clave pública**. Los usuarios están en posesión de un par de claves, una que mantiene en secreto y otra que hacen pública.

7.1 Cifrado convencional



Ingredientes

- Texto nativo.
- Algoritmo de cifrado.
- Clave secreta.
- Texto cifrado.
- Algoritmo de descifrado

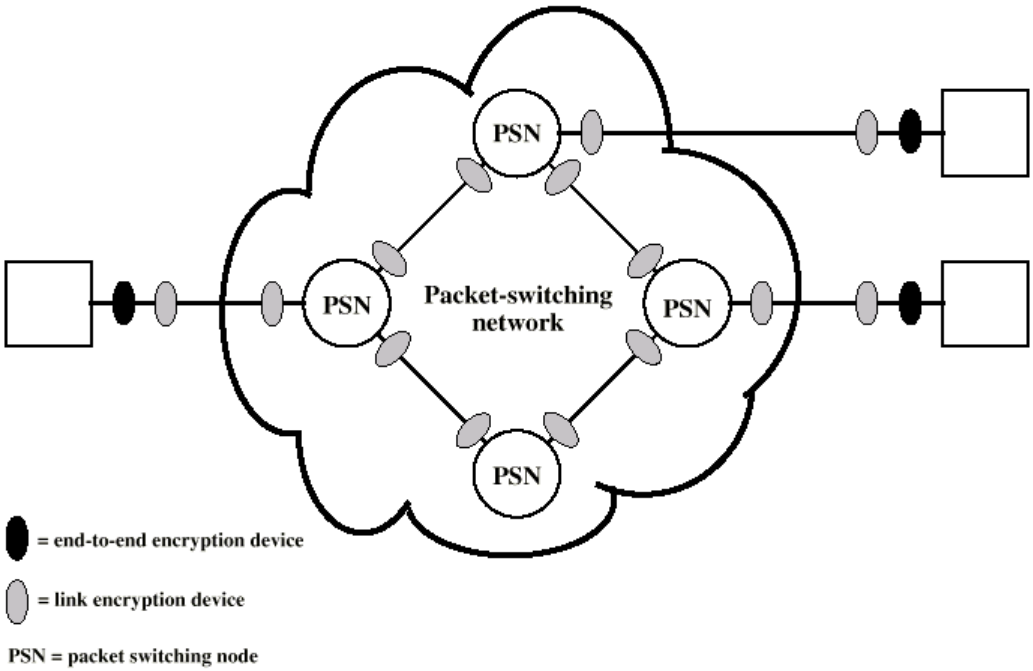
Requisitos de seguridad

- Algoritmo de cifrado robusto:
  - Incluso si conoce el algoritmo, no debería ser capaz de descifrar el texto o describir la clave.
  - Incluso si posee un determinado número de textos cifrados junto con los textos nativos que produce cada texto.
- El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura.
- Una vez que se conoce la clave, todas las comunicaciones que utilicen esta clave pueden ser leídas.

Ataques al cifrado convencional

- Criptoanálisis:
  - Se basa en la naturaleza del algoritmo más algún conocimiento de las características generales del texto nativo.
  - Intento de deducir un texto nativo o la clave.
- Fuerza bruta:
  - Intentar cada clave posible hasta que se obtenga una traducción inteligible del texto nativo.

7.2 Localización de los dispositivos de cifrado



Cifrado de enlaces

- Cada enlace de comunicación tiene un dispositivo de cifrado a ambos lados.
- Todo el tráfico se protege.
- Alto grado de seguridad.
- Requiere muchos dispositivos de cifrado.
- El mensaje debe ser descifrado en cada conmutador para leer la dirección (número de circuito virtual).
- El mensaje es vulnerable en cada nodo:
  - Especialmente si la red es de conmutación de paquetes pública.

Cifrado extremo-extremo

- El cifrado se hace en los dos sistemas finales.
- Los datos cifrados se transmiten sin alteraciones a través de la red.
- El destino comparte una clave con el origen para descifrar los datos.
- El computador sólo puede descifrar los datos del usuario:
- Si no, los nodos de conmutación no podrían leer la cabecera o paquete de encaminamiento.
- Modelo de tráfico no seguro.
  - Uso de cifrado de enlace y extremo-a-extremo.

7.3 Encriptación de datos estándar. (DES *Data Eencryption Standar*)

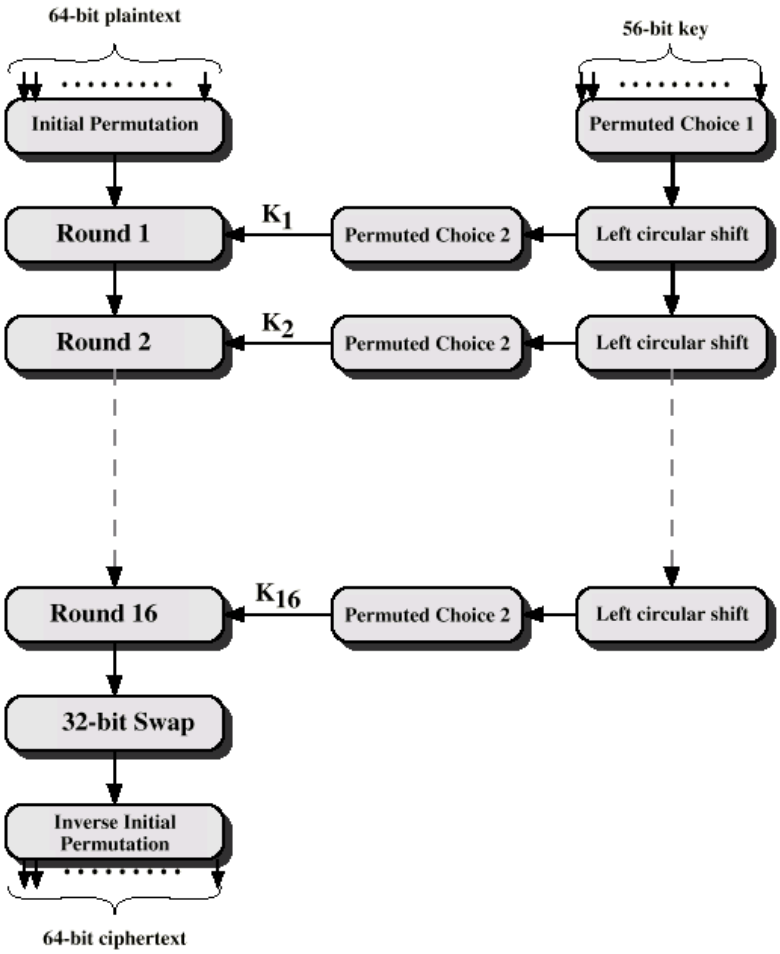
Desarrollado por la oficina nacional de normas de EE.UU. (*National Bureau of Standar*- NBS 1.977). La información se cifra en bloques de 64 bits usando una clave de 56 bit. Utiliza la misma clave para en cifrado y descifrado.

E_k --> algoritmo de encriptación con clave **k**.

D_k --> algoritmo de desencriptación con clave **k**.

$D_k(E_k(m))=m$

El problema es la transmisión de la clave. Dos usuarios que quieran comunicarse deben transmitirse la clave. En una red de **n** usuarios, cada pareja necesita tener su clave secreta particular, lo que hacen un total de $2^{n(n-1)}$ claves para esa red.



Necesario para trabajar

- El mismo algoritmo y la misma clave debe de usarse para la encriptación/desencriptación.
- El emisor y el receptor deben de compartir el algoritmo y la clave.

Necesario para la seguridad.

- La clave debe de mantenerse secreta.
- Debe ser imposible o al menos impracticable descifrar un mensaje sin otra información.
- El conocimiento del algoritmo mas un ejemplo de texto cifrado debe ser insuficiente para determinar la clave.

Potencia de DES

- Declarada insegura en 1998.
- Fundación las Fronteras Electrónicas (EFF, *Electronic Frontier Foundation*).
- Máquina saboteadora de DES.
- Actualmente, DES no tiene ningún valor.
- Entre las alternativas está el DEA Triple.

7.4 Triple DES (DEA)

- ANSI X9.17 de 1985.
- Incorporado como una parte del Estándar de Cifrado de Datos en 1999.
- Utiliza tres claves y tres ejecuciones del algoritmo DES.

- Longitud de clave efectiva de 168 bits.
- Actual Algoritmo AES (NIST Instituto Nacional de Estándares y Tecnología)
  - Autor: el belga Rijndael
  - Utiliza bloques y claves de 128 bits
  - http://www.kriptopolis.com/luc/20010522.html

7.5 CAST

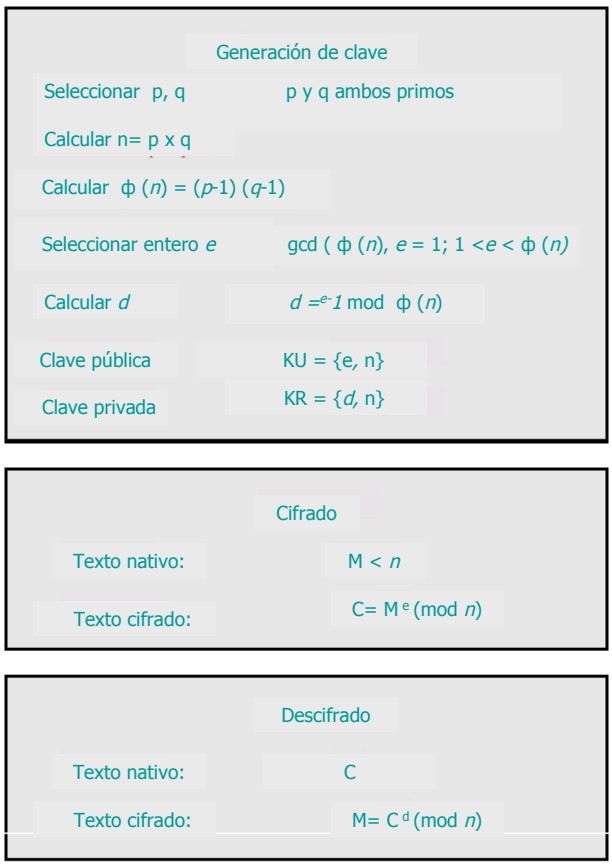
- Creadores: Carliste Adams y Stafford Tavares
- CAST utiliza valores variables de claves entre 40 y 128 bits
- Posible exporta CAST 64

7.6 Encriptación mediante clave pública **(RSA** *Rivest, Shamir, Adelman***)**

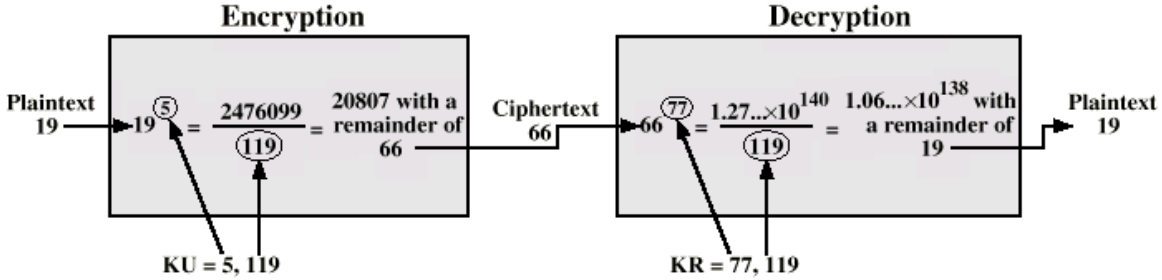
Marco de certificación y encriptación de clave pública. Autor es Ron Riverst, Adi Shamir, Leonard Adleman. RSA (1977 MIT)

- Característica:
  - Uso de parejas de claves públicas y privadas
- Cada usuario tiene dos claves, una pública y otra privada.
  - Es un sistema asimétrico.
- Si el usuario A quiere mandarle un mensaje al usuario B, encripta el mensaje usando la clave publica de B y se lo remite a B.
- Sólo B que conoce la clave secreta puede descifrar la información.
- No hay problema de distribución de claves.
  - Las secretas se generan localmente.

7.6.1 Algoritmo RSA



- La clave pública y la privada están compuesta por un exponente y un módulo que es el producto de dos números primos grandes.
- Para cada usuario A, la transformación privada D_A, se describe mediante una clave privada.
- La clave pública E_A se deduce de la clave privada utilizando una transformación unidireccional cuya inversa es excepcionalmente difícil de calcular.



$$D_A(E_A(P))=P$$

Para un número P ε [0, n-1] puede demostrarse que la ecuación

$$C = P^e \bmod n$$

es inversa de

$$P = C^e \bmod n$$

si

$$e*d \bmod \Phi(n) = 1, \text{ donde } \Phi(n) = (p - 1)(q - 1) \text{ para } n = p*q \text{ y } p \text{ y } q \text{ primos}$$

- Para determinar **n, d, e** se siguen los siguientes pasos:

1. Elegir dos primos grandes, **p** y **q**, cada uno superior a 100^{100}.
2. Calcular $n = p * q$ y $\Phi(n) = (p - 1)(q - 1)$
3. Elegir un número **d** como número aleatorio grande que sea primo relativo con $\Phi(n)$, es decir, tal que (el máximo común divisor de) $mcd (d, \Phi(n)) = 1$.
4. Hallar **e** tal que $e*d \bmod \Phi(n) = 1$.

- La seguridad de RSA es la dificultad de factorizar números grandes.
- Factorizar un número de 200 dígitos requeriría 4.000 millones de años en un ordenador con tiempo de instrucción de 1 μs.

Necesario Para funcionar

- Un algoritmo para encriptación/desencriptación.
- Un par de claves: una para la encriptación y otra para desencriptación.
- El emisor y el receptor tienen que tener un par de claves.

Necesario para la seguridad

- Una de las dos claves debe ser guardada en secreto.
- El conocimiento del algoritmo, más un ejemplo de texto cifrado y una de las claves debe ser insuficiente para determinar la otra clave.

Validación

- Si el receptor B, desea validar a un emisor A, propone un reto aleatorio a A y la cifra utilizando la clave pública de A, E_A.
- A, descifra el reto utilizando su clave privada D_A, y lo devuelve como "texto llano" a B.
- Si el mensaje devuelto corresponde con el que le envió, B puede estar seguro de la identidad de A.

Firma digital

- Suponiendo que B recibe un mensaje M firmado por A, la firma digital debe satisfacer los siguientes requisitos.
    1. Debe ser posible para B validar la firma de A sobre M.
    2. Debe ser imposible que nadie falsifique la firma de A.
    3. Debe ser imposible para A, repudiar el mensaje M.
- El emisor aplica primero su propia transformación privada para obtener $D_A(M)$ y luego cifra el resultado utilizando la clave pública de B, E_B.
- El mensaje doblemente transformado, $C = E_B(D_A(M))$ es enviado a B.
- El receptor aplica primero su transformación de descifrado privada y luego aplica la transformación pública de A para obtener el mensaje M.

$$\begin{aligned} E_A(D_B(C)) &= E_A(D_B(E_B(D_A(M)))) \\ &= E_A(D_A(M)) \\ &= M \end{aligned}$$

7.6.2 Cifrado de clave pública

Se basa en funciones matemáticas. Es asimétrica porque usa dos claves independientes.

Los Ingredientes son:

- Texto nativo.

- Algoritmo de cifrado.
- Clave pública y privada.
- Texto cifrado.
- Algoritmo de descifrado.

Técnica de Cifrado de Clave Pública

Una clave se hace pública: Se usa para el cifrado.

Otra clave se mantiene privada:Se usa para el descifrado.

No es factible determinar la clave de descifrado dadas la clave de cifrado y el algoritmo. Cualquiera de las claves se puede usar para cifrar, la otra para descifrar.

Pasos

1. Cada usuario genera un par de claves.
2. Cada usuario publica una de las dos claves.
3. Para enviar un mensaje al usuario, se cifra el mensaje utilizando la clave pública.
4. El usuario descifra el mensaje utilizando su clave privada.

Firmas Digitales

Necesitamos algo más:

Las firmas digitales son un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje

Las firmas digitales son un método de verificar que un documento ha sido creado por una persona y que no ha sido alterado

Los pasos básicos para la firma digital son tres:

1. El emisor cifra el mensaje con su clave privada.
2. El receptor puede descifrar el mensaje utilizando la clave pública del emisor.
3. Esto autentifica al emisor, que es la única persona que tiene la clave que coincide.

No proporciona privacidad a los datos:

La clave de descifrado es pública.

Ejemplo Firmas digitales:

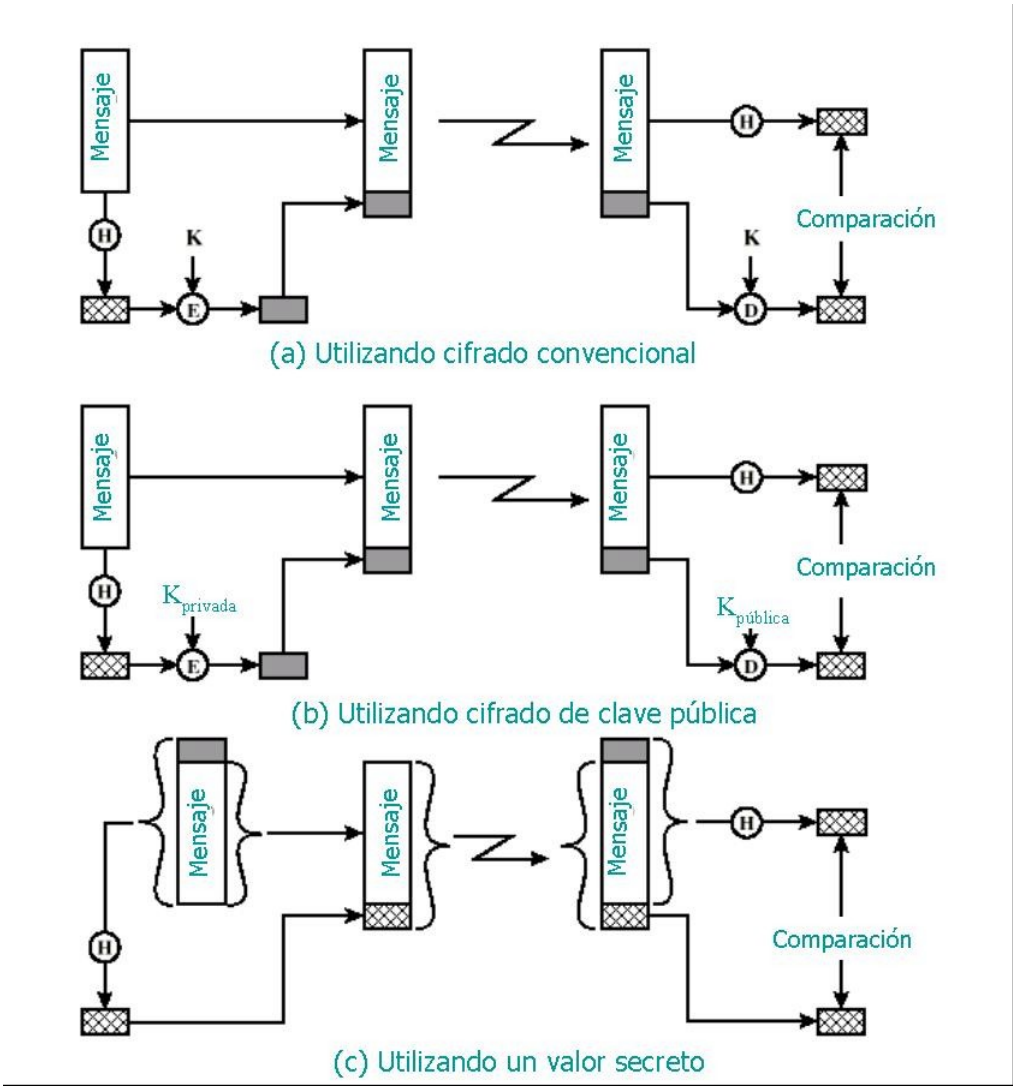
- paso 1
  - Juan crea un testigo especial cifrado con información del propio mensaje
  - Encripta el mensaje y el testigo con su clave privada
  - Envía el mensaje a Susana
- Paso 2
  - Susana utiliza la clave pública de Juan para desencriptar el mensaje
  - Crea un testigo similar usando la clave pública de Juan para desencriptar la información del mensaje
- Paso 3:
  - Susana compara su testigo con el enviado por Juan
  - Si encajan, el mensaje es considerado auténtico

¿Qué es una huella digital?

Un conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado. Se obtiene aplicando una función, denominada *hash*.

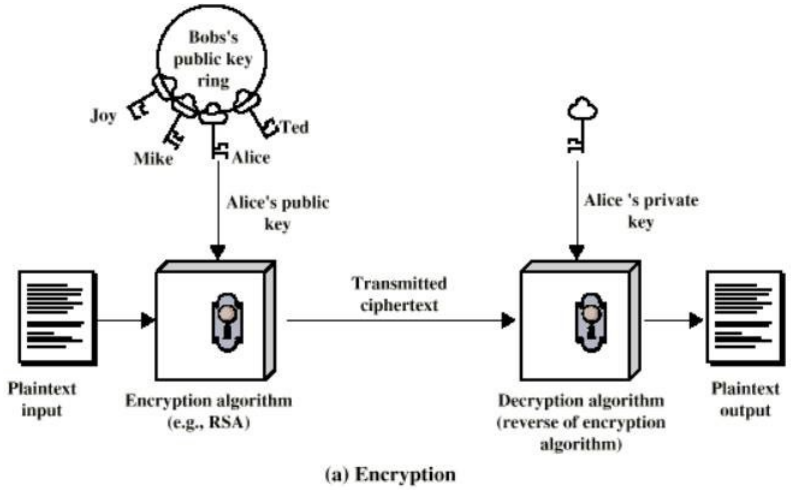
1. Dos mensajes iguales producen huellas digitales iguales.
2. Dos mensajes parecidos producen huellas digitales completamente diferentes.

3. Dos huellas digitales idénticas pueden ser el resultado de dos mensajes iguales o de dos mensajes completamente diferentes.
4. Una función *hash* es irreversible

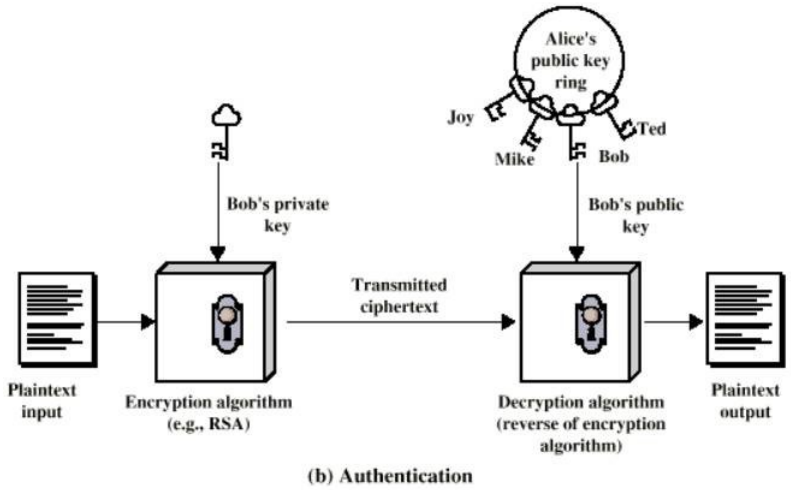


Comparación DES RAS

- DES
  - Adecuado para casos donde se pueda comunicar la clave secreta sin problemas
- RAS
  - Adecuado para las transacciones electrónicas



(a) Encryption



(b) Authentication

8 Protocolos Estándares

- SSL (Secure Socket Layer): Establece un canal seguro de intercambio de información
- SET (Secure Electronic Transaction): Además impide la manipulación de la información en los extremos. Adecuado para el comercio electrónico
- PGP (Pretty Good Privac):Correo electrónico)

SSL Secure Socket Layer

Proporciona:

- Cifrado de datos
- Autenticación de servidores
- Integridad de mensajes
- Autenticación de clientes

EJEMPLO: Correo electrónico para los alumnos en titanic.uca.es

SSL pasos para crear un canal seguro

1 Elección de algoritmo: DES, RC2,RC4..

2 Autenticación: intercambio certificado x.509v3

3 Generación de clave de sesión

4 Verificación de canal seguro

Si el sitio es seguro:

- Aparece un candado cerrado
- El protocolo es https
- Pinchando sobre el candado aparece información sobre el sitio y su certificado

9 Iniciativas públicas

- GTA :Grupo de Usuarios de Telecomunicaciones en la administración
- CITAD: Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento automatizado de datos. URL: www.map.es/csi (Consejo Superior de Informática)
- CERES: URL:www.fnmt.es

9.1 Infraestructuras de Clave Pública (ICPs o PKIs, *Public Key Infrastructures*).

El modelo basado en Terceras Partes Confiables . Es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública. Algunos de los servicios

- Registro de claves: emisión de un nuevo certificado para una clave pública.
- Revocación de certificados: cancelación de un certificado.
- Selección de claves: publicación de la clave pública
- Evaluación de la confianza: determinación sobre si un certificado es válido
- Recuperación de claves: posibilitación de recuperar las claves de un usuario.

Las ICPs están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:·

- Autoridad de Certificación
- Autoridad de Registro
- Otras Terceras Partes Confiables como por ejemplo las Autoridades de Fechado Digital.

CERES. Autoridad de Registro en la Entidad Pública de Certificación

La autoridad de Certificación:

- Responsable de la gestión de los certificados digitales
- Emisión
- Publicación y
- Revocación

Entidad FNMT :URL:www.FNMT.es

¿Qué es un certificado?

Un certificado en un documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con su propietario.

Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

¿Qué es un certificado raíz?

Un certificado raíz es un certificado emitido por la Autoridad de Certificación para sí misma.

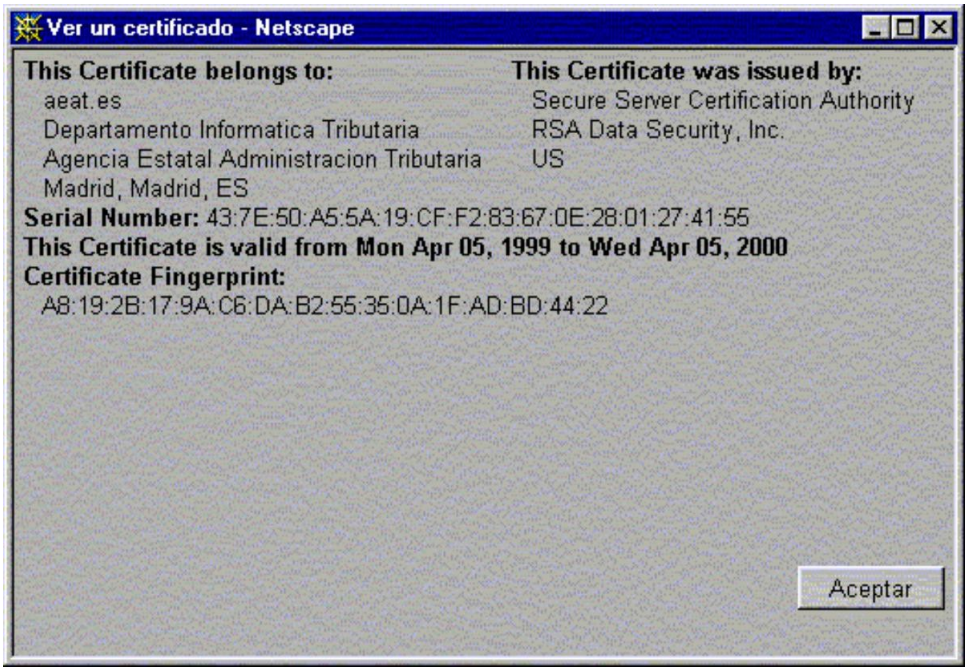
En este certificado consta la clave pública de la Autoridad de Certificación y por tanto será necesario para comprobar la autenticidad de cualquier certificado emitido por ella.

Es el certificado origen de la cadena de confianza.

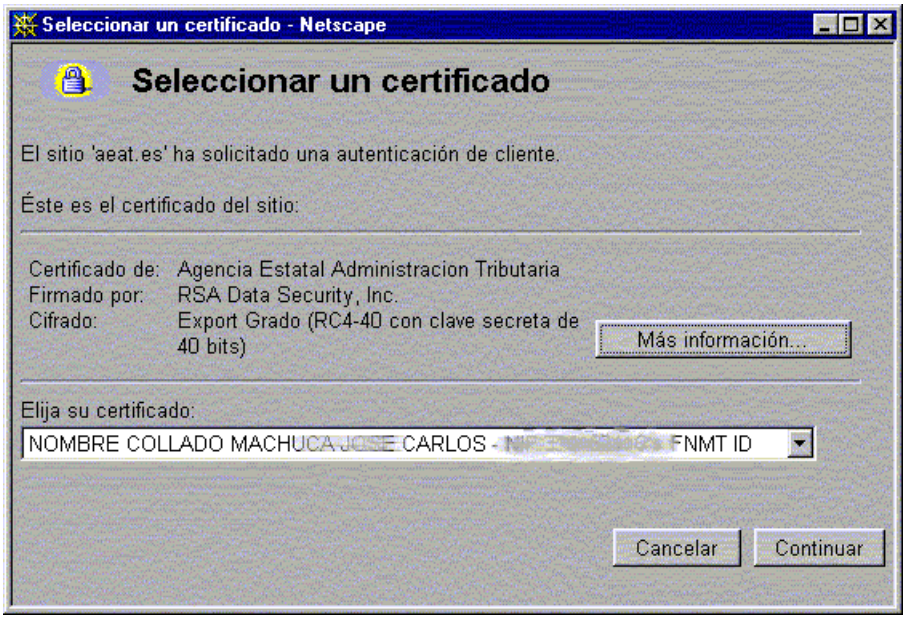
¿Qué información contiene un certificado ?

- Nombre habitual del propietario de la clave de firma
- Identificador único del propietario
- Clave pública correspondiente a la clave privada de firma
- Identificación de los algoritmos de clave pública
- Número del certificado
- Nombre de la Entidad Certificadora
- Limitaciones de aplicación de las claves
- Capacidad de representación por terceras partes
- Fecha y hora de emisión y aceptación del certificado
- Fecha y hora de expiración del certificado
- Firma de la Autoridad Pública de Certificación como emisora del certificado
- Versión de la DPC bajo la cual se haya emitido el certificado

Ejemplo de la AEAT (hacienda)

-
  - 

-

- 

- Autoridad de Registro: Responsable de la autenticación de la identidad del ciudadano y de los datos que aporta para su inclusión en los certificados digitales. **Entidad** *Correos y telégrafos*
- Entidad Final: Un ciudadano propietario de una tarjeta inteligente donde almacena sus claves (PIN) y sus certificados. **Entidad**: *El ciudadano*
- EQUIPAMIENTO NECESARIO
  - Tarjeta inteligente de APC
  - Ordenador con 8 Mb
  - Procesador Pentium
  - Lector compatible PC/SC de tarjetas inteligentes con criptoprocesador
  - Acceso a Internet

9.2 Normas de seguridad publicas

Pregunta:¿Hay alguna norma sobre seguridad de los sistemas de información para las Administraciones Públicas? Respuesta:si

- Magerit
- Métrica V3

9.2.1 MAGERIT

EL Consejo Superior de Informática ha elaborado la Metodología de Análisis y GEstión de los Riesgos de los sistemas de Información de las Administraciones Públicas: MAGERIT

Objetivos

- Estudiar los riesgos que soporta un sistema de información y el entorno asociable con él
- Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados

Guía de Aproximación a la Seguridad de los sistemas de información

Donde conseguirla?:URL:http://www.map.es/csi

Elementos de MAGERIT. Un conjunto de Guías, compuesto básicamente por:

- Guía de Aproximación
- Guía de Procedimientos

Iniciativas públicas

- Guía de Técnicas
- Guía para Desarrolladores de Aplicaciones
- Guía para Responsables del Dominio protegible
- Referencia de Normas legales y técnicas
- Un panel de herramientas de apoyo, con sus correspondientes Guías de Uso y con la Arquitectura de Información y Especificaciones de la Interfaz para el Intercambio de datos

Magerit indica que las Salvaguardas preventivas mínimas de seguridad son:

1. Documentación de políticas de seguridad de la información
2. Asignación de funciones y responsabilidades de seguridad
3. Responsabilidades del usuario en el acceso al sistema
4. Educación y formación en la seguridad de la información
5. Comportamiento ante incidentes de seguridad
6. Controles físicos de seguridad
7. Gestión de la seguridad del Equipamiento
8. Cumplimiento de las obligaciones y restricciones jurídicas vigentes
9. Protección, transporte y destrucción de la Información
10. Gestión Externa de servicios

9.2.2 Métrica versión 3 (octubre 1999)

Metodología de planificación y desarrollo de sistemas de Información

Autor: Consejo Superior de Informática

Fase1

Interfaz de seguridad

El objetivo de la interfaz de seguridad MAGERIT – Métrica V.3 es

- Ayudar en la consideración de los requisitos de seguridad de los sistemas de información durante todas los procesos que cubre la metodología Métrica V.3:
- Planificación de Sistemas de Información, Estudio de Viabilidad, Análisis, Diseño, Construcción, Implantación y Aceptación del sistema de información.

10 Legislación sobre seguridad informática

10.1 Legislación estatal (España)

- Constitución Española (diciembre 1978) Art. 18.4 la ley limitará el uso de la informática para garantizar el honor...
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan datos personales.
- Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal. Derogada por la Ley Orgánica 15/1999
- Real Decreto 1332/1994, 20 de junio, por el que se desarrollan determinados aspectos de la Ley Orgánica 5/1992, de 29 de octubre.
- Real Decreto 428/1993, de 26 de marzo, Estatuto de la Agencia de Protección de Datos.

- Instrucción 1/1995, de 1 de marzo, de la Agencia de Protección de Datos, relativa a prestación de servicios de información sobre solvencia patrimonial y crédito.
- Instrucción 2/1995, de 4 de mayo, de la Agencia de Protección de Datos, sobre medidas que garantizan la intimidad de los datos personales recabados como consecuencia de la contratación de un seguro de vida de forma conjunta con la concesión de un préstamo hipotecario o personal.
- Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.
- Instrucción 2/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los casinos y salas de bingo.
- Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación.
- Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos.
  - *TELECOMUNICACIONES*
- Ley 11/1998, de 24 de abril, General de Telecomunicaciones.
- Real Decreto-Ley 1736/98, de 31 de julio, en el que se aprueba el Reglamento del Título III de la Ley General de Telecomunicaciones.
- Real Decreto-Ley 14/1999, de 17 de septiembre, sobre firma electrónica.
- Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico.
- **Comentarios sobre la legislación española**

De todas estas leyes vamos a estacar las que mayor repercusión tienen en los Sistema de Gestión de la Seguridad de la Información

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos Personales.

10.1.1 Ley Orgánica 15/1999

Vamos a definir algunos términos utilizados en esta norma.. En el Anexo C de Definiciones de conceptos de la Ley Orgánica 15/1999 y del Real Decreto 1332/1994, podrá encontrar los términos para entender mejor estas leyes.

Datos accesibles al público

Los datos que figuren en censos, anuarios, bases de datos públicas, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, los títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

Autoridad controladora del fichero

Significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuales operaciones se les aplicará (convenio 108 Consejo Europa).

Datos de carácter personal

Toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada e identificable.

Responsable del fichero

Persona física, jurídica de naturaleza pública o privada y órgano administrativo que decida sobre la finalidad y contenido y uso del tratamiento.

Responsable de Seguridad

Persona o personas de la organización a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables en dicha organización.

Obligaciones de Seguridad de la L.O. 15/1999

- Art. 9: 1. El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
- Art. 9 (2): 2 En relación con la seguridad física la norma indica que no se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
- Art. 43.3. h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen. ¡falta grave!
- Artículo 45. Tipo de sanciones

  1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

  2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

  3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas
- Una obligación general para toda empresa o institución que solicita datos personales es que los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

  a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.

  b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

  c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

  d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

  e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

10.1.2 Real Decreto 994/1999 Reglamento de seguridad

Destacar Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos Personales sujetos al régimen de la Ley Orgánica 15/1999. El objetivo del Reglamento es establecer las medidas obligatorias técnicas y organizativas, necesarias para garantizar la seguridad de los ficheros, centros de tratamiento, locales, equipos, sistemas, programas y personas que intervengan en el tratamiento.

El reglamento indica que hay que proteger la información en:

- Acceso en modo local
- Acceso a través de redes de comunicaciones
- Trabajos fuera del local de ubicación del fichero
- Los Ficheros temporales

El responsable del fichero elaborará e implantará la normativa de seguridad mediante un documento de obligado cumplimiento. Atendiendo al tipo de datos contenidos en su ficheros, deberá adoptar las diferentes medidas de seguridad recogidas en el Reglamento.

- Nivel básico: todos los ficheros con datos personales
- Nivel medio :datos relativos a solvencia patrimonial y crédito
- Nivel alto: datos de ideología, religión, creencias, etnia, salud, sexualidad

El Documento de Medidas de Seguridad es de carácter interno, no teniendo la obligación de ser presentado ante la Agencia, sino tan solo tenerlo disponible por si éste fuera requerido. Los niveles medio y alto exigen auditorias.

Medidas de seguridad de nivel básico que establece el reglamento son:

- Documento de seguridad (art. 8) Políticas y reglamentos
- Funciones y obligaciones del personal (art. 9)

- Registro de incidencias (art. 10)
- Identificación y autenticación (art. 11)
- Control de acceso (art. 12)
- Gestión de soporte (art. 13)
- Copia de respaldo y recuperación (art. 14) semanal

El Documento de Seguridad indicado en el apartado uno debe contener al menos los siguientes apartados:

1. Ámbito de aplicación
2. Medidas, normas, procedimientos, reglas y estándares
3. Funciones y obligaciones
4. Estructura de los ficheros y sistemas que los tratan
5. Procedimiento de notificación ante incidencias
6. Procedimientos de copias de seguridad y de recuperación de los datos

Medidas de seguridad de nivel medio

Las medidas de seguridad de nivel medio son las siguientes

- Documento de seguridad (art. 15)
- Responsable de seguridad (art. 16)
- Auditoria (art. 17) cada dos años
- Identificación y autenticación (art. 18)
- Limitar el número de intentos
- Los controles periódicos que se deben realizar para verificar el cumplimiento de lo dispuesto
- Control de acceso físico (art. 19)
- Gestión de soportes (art. 20) La medidas que sea necesario adoptar cuando un soporte vaya a desechado o reutilizado. Impedir poder recuperar información borrada
- Registro de incidencia (art. 21)
- Pruebas con datos reales (art. 22) Está prohibido

Medidas de seguridad de nivel alto

- Distribución de soporte (art. 23) Cifrado de los soportes
- Registro de acceso (art. 24)
- Copias de respaldo (art. 25) Copia en lugar diferente a donde se encuentren los equipos.
- Telecomunicaciones (art. 26) Cifrado de la información.

Las medidas comentadas son acumulativas, es decir, la información de tercer nivel debe implementar las medidas de nivel tres, dos y uno.

El régimen de protección de los datos de carácter personal no será de aplicación:

1. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
2. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
3. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

Tabla 1 Cuadro resumen de tipos de datos

	DATO	FICHEROS EN LOS QUE SE PUEDE ENCONTRAR

DATOS DE NIVEL ALTO	Ideología	Nómina
	Religión y creencias	Liquidación de renta
	Origen racial	Seguridad e higiene
	Salud	Salud del personal
	Vida sexual	Clientes de productos eróticos
	Datos recabados para fines policiales sin el consentimiento de las personas afectadas	
DATOS DE NIVEL MEDIO	Infracciones administrativas o penales	Clientes de abogados, gestores etc
	Hacienda Pública	Agencia Estatal de Administración Tributaria
	Servicios Financieros	Bancos
	Solvencia patrimonial y crédito	ASNEF
	Evaluación de la personalidad	Selección de personal
DATOS DE NIVEL BÁSICOS	Resto	Todos

Desde el pasado 26 de junio de 2002 la obligación de cumplir con las medidas expresadas en el reglamento, afecta a todas las empresas, administraciones o profesionales.

El reglamento, a nivel técnico, es difícil de cumplir de forma exhaustiva. Tampoco es fácil deducir la información precisa que requieren los documentos requeridos. Un ejemplo de ello es el denominado Documento de seguridad, que debe de tenerse en todos los casos. Podemos encontrar un ejemplo de documento de seguridad de cada uno de los niveles en la Agencia de Protección de Datos de la Comunidad de Madrid. Esta referencia es muy valiosa porque no existe otros ejemplos de documentos "oficiales"

La obligación legal de su cumplimiento, aunque la norma no sea de muy reciente creación, sigue siendo desconocida para la inmensa mayoría de las micro-PYME´s, y PYME de este país. La Agencia de Protección de Datos está siendo, por ahora, "generosa" y solo actúa en este tipo de empresas bajo demanda expresa. La aplicación estricta de la norma, debido a la cuantías de las sanciones, avocaría al cierre de muchos pequeños negocios. A modo de ejemplo comentar que un pobre video-club de barrio requiere las medidas de seguridad de máximo nivel.

¿Hay algún organismo encargado de velar por el cumplimiento de las normas?

El organismo en España encargado de velar por el cumplimiento de las leyes de protección de datos personal es la Agencia de protección de datos. Regulada por el título VI de LOPDCP 15/1999 y Estatutos de APD (R.D. 428/1993 de 26 de marzo BOE 106 de 4 de mayo de 1.993). Son funciones de la agencia: inspectora, ordenadora, de publicidad, sancionadora, inmovilizadora, reguladora, unificadora y de relaciones con el exterior.

En el sitio de la Agencia de Protección de Datos (URL:www.agenciaprotecciondatos.org) en el apartado legislación, podemos encontrar los textos de las principales normas legales. También podemos encontrar "Guía práctica para ciudadanos" donde nos aclara los derechos básicos que tiene cualquier ciudadano en relación con la protección de sus datos personales. Por último señalar el apartado de "Recomendaciones e instrucciones" donde podremos encontrar recomendaciones sectoriales sobre el tema y las "Instrucciones" dictada por esta autoridad.

10.2 Comunidad EUROPEA

Estrategias europeas

- Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas en lo que respecta al tratamiento automatizado de los datos personales
- Acuerdo de *Schengen* (14 junio de 1985)

- Tratado de Niza, de 26 de febrero de 2002, modificativo de los Tratados Consultivos de la Unión Europea, introduciendo en los mismos la Carta de Derechos Fundamentales. (Entrada en vigor prevista para el año 2004, cuando sea ratificado por los 15 estados de U.E.).
- Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las regiones sobre "Seguridad de las redes y de la información: Propuesta para un enfoque político europeo"
- Informe "Bangemann"(94); Cumbres (Corfú94, ...)
- eEurope 2005
- **Directivas europeas**
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Directiva 2002/58/CE, de 12 de julio de 2002 del Parlamento Europeo y Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas.

TELECOMUNICACIONES

- Directiva 97/66/CE, del Parlamento Europeo
- Directiva 2000/31/CE, del Parlamento Europeo y Consejo sobre determinados aspectos jurídicos de la sociedad de la información, en particular, el comercio electrónico en el mercado interior.
- Orden ECO/1758/2002, de 9 de julio, por la que se establecen los criterios generales de tramitación telemática de determinados procedimientos en materia de personal
- **Decisiones europeas**
- ITSEC (91), ITSEM (93), CC-SEC ...

11 Gestión de la seguridad de los sistemas de información

Para la Gestión de la seguridad de los sistemas de información hay que tener en cuenta cada vez más normas legales y técnicas . Una forma de facilitar la gestión de la seguridad de sistemas de información es aplicar las normas internacionales existentes al respecto.

Algunas empresas podrán considerar importante la adecuación a una norma para obtener la certificación correspondiente porque su proceso de negocio (o clientes) lo demanden. Sin embargo, aunque esto pueda ser el caso para otras normas ISO (como la ISO 9000) no lo es tanto para la norma ISO/IEC 17799. ¿Por qué, entonces, puede ser necesario adecuarse a una norma como el ISO/IEC 17799?

La utilización de una norma de seguridad permite cerciorarse de que se cubren todos los aspectos de seguridad que debe abordar una organización, desde la especificación de una política de seguridad a la definición de necesidades de seguridad física o de recuperación de desastres. Claramente, una organización puede abogar por definir su política de seguridad y realizar su implementación sin seguir ninguna norma. El beneficio de utilizar una norma es el de acceder al conocimiento de expertos reflejado en una guía accesible a cualquier responsable de seguridad.

En este y siguientes niveles nos vamos a basar, además de las normas legales, en los estándares y recomendaciones internacionales.

11.1 Principios en Seguridad de la OCDE

Podemos empezar analizando los nueve Principios en Seguridad del de la OCDE (PARIS 2002)

Tabla 2 principios de seguridad de la OCDE

8. Principio 1: Concienciación	**Los participantes deben ser conscientes de la necesidad de contar con sistemas de información y redes seguros, y qué es lo que pueden hacer para promover y fortalecer la seguridad.**
9. Principio 2: Responsabilidad	**Todos los participantes son responsables de la seguridad de los sistemas de información y redes.**
10. Principio 3: Respuesta	**Los participantes deben actuar de manera oportuna y cooperativa para prevenir, detectar y responder a incidentes**

	que afecten la seguridad.
11. Principio 4: Ética	**Los participantes deben respetar los intereses legítimos de los otros.**
12. Principio 5: Democracia	**La seguridad de los sistemas de información y redes debe ser compatible con los valores esenciales de una sociedad democrática.**
13. Principio 6: Evaluación de riesgos	**Los participantes deben llevar a cabo evaluaciones de riesgo.**
14. Principio 7: Diseño e implementación de seguridad.	**Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas de información y redes.**
15. Principio 8: Administración de la Seguridad.	**Los participantes deben adoptar una visión integral de la administración de la seguridad.**
16. Principio 9: Evaluación continua de la seguridad	**Los participantes deben revisar y reevaluar la seguridad de sus sistemas de información y redes y hacer las modificaciones pertinentes a sus políticas, prácticas, medidas y procedimientos de seguridad.**

11.2 Nivel del análisis de riesgo

En relación con el análisis de riesgo, en el apartado 8 de UNE-71501-3 IN se establecen diversos niveles para su realización: mínimo, informal, detallado y combinado). Entendemos que el análisis descrito como combinado es el adecuado para este nivel. El nivel mínimo sería adecuado para el nivel anterior.

11.3 Instituciones de normalización

- Internacionales
  - ITU-T (recomendaciones -series-)
  - ISO/IEC (normas)
- Europeas
  - CEN/CENELEC
  - ETSI

11.4 Normas de Organismos internacionales

La implantación de la seguridad de la información, en la medida de lo posible, se consigue mediante un conjunto adecuado controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones *software*. Estas medidas de control sirven para asegurar que se cumplen los objetivos específicos de seguridad de la Organización. En el campo normativo voluntario de la gestión de la seguridad de las TI existen actualmente, como más relevantes, destacamos como fundamentales para este nivel las siguientes:

- La norma ISO/IEC 17799:2000 que ofrece las recomendaciones para realizar la gestión de la seguridad de la información, las versión española de esta norma es la norma espejo UNE-ISO/IEC 17799:2000.
- La norma multiparte ISO/IEC 13335 conocidas como las GMITS donde se recogen las etapas del ciclo de gestión de la seguridad proporcionando orientaciones organizativas y técnicas, la versión española de esta norma multiparte es la UNE 71501 IN 2001. Generalmente cada Organización en base a los riesgos a que esté expuesta y los aspectos intrínsecos de su funcionamiento, define e implanta un Sistema propio para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de TI.
- BS 7799:1 "*Information Security Management*- Part 1: *Code of practice for information security management*"
- BS 7799-2 (*British Standards Institution*): buenas prácticas de gestión de seguridad. Para algunas organizaciones puede ser orientativa la norma Británica BS-7799-2, la cual fija requisitos para establecer, implementar y mantener un sistema de gestión de la seguridad de los sistemas de información (ISMS: *Information Systems Management System*). Aquellas organizaciones que quieran ser conformes a la norma BS-7799-2 deberán cumplir estrictamente los requisitos según se indican en su texto. Dada la riqueza de variantes presentes en el mundo real, para algunas organizaciones la norma resulta meramente orientativa.

- Norma ISO-OSI 7498-2: Arquitectura de Seguridad (Interconec. .S. Abiertos)
- Norma IS 17799-2 en preparación, para evaluar y certificar los Sistemas de Gestión de Seguridad que cumplan la IS 17799-1.
- Guías de la OCDE para la seguridad de los sistemas de información y redes. Hacia una cultura de seguridad. (*Organisation For Economic Co-Operation And Development*. Paris 2002).
    - Un cuadro-resumen de estas normas ordenadas separando las nacionales de las internacionales:

Normativas estándaresde Seguridad de la Información en España

- UNE-ISO/IEC 17799:2002 "Código de buenas prácticas de la Gestión de la Seguridad de la Información" Traducción en castellano de la ISO/IEC 17799:2000 Equivale a la BS7799:1
- UNE 71501 IN "Guía para la Gestión de la Seguridad de TI" Equivale a ISO/TR 13335 parte 1, 2 y 3
  – Parte 1: Conceptos y modelos para la Seguridad de las TI ;
  – Parte 2: Gestión y planificación para la Seguridad de las TI
  – Parte 3: Técnicas para la Gestión de la Seguridad de las TI
- PNE 71502 (Proyecto de Norma Española) "Requisitos para la gestión de la seguridad de TI" Norma certificable actualmente en proyecto, en previsión para 2003, estará fundamente extraída de la BS7799-2:2002
- Metodologías: Magerit y Métrica V·3

Normativas estándares de Seguridad de la Información internacionales

Normativas ISO desarrolladas por el comité JTC1/SC27 [1]

- ISO/IEC 17799:2000 "*Information Technology- Code of Practice for Information Security Management*"
- ISO/IEC TR 13335 "*Information Technology - Guidelines for the management of IT security*" (GMITS) -
  – Part 1: *Concepts and models for IT security*
  – Part 2: *Managing and planning IT security*
  – Part 3: *Techniques for the management of IT security*
  – Part 4: *Selection of safeguards*
  – Part 5: *Management guidance on network security*

Reino Unido [2]

- BS7799:1 " *Information Security Management*- Part 1: *Code of practice for information security management*"
- BS7799-2:2002 "*Information Security Management*- Part2: *Specifications for an ISMS*" revisión 2 / 5 septiembre de 2002
- Metodología: CRAMM
- Comentamos las normas que consideramos mas importantes para su aplicación en este nivel.

11.4.1 La Norma UNE 71501 IN

La Norma UNE 71501 IN se ha elaborado para facilitar la comprensión de la seguridad de las Tecnologías de la Información (TI), y proporcionar orientación sobre los aspectos de su gestión.

Los objetivos principales de esta norma son:

- Definir y describir los conceptos relacionados con la gestión de la seguridad de TI
- Identificar las relaciones entre la gestión de la seguridad de TI y la gestión de las TI en general
- Presentar varios modelos Útiles para explicar la seguridad de TI,

[1] Otras normas ISO: listado completo en: http://www.din.de/ni/sc27/doc7.html

Disponibles en www.iso.ch

[2] Disponibles en www.bsi-global.com

- Proporcionar orientación general sobre la gestión de la seguridad de TI, y proporcionar orientación en relación con la selección de salvaguardas.

La Norma UNE 7 150 1 IN está estructurada en varias partes:

- UNE 71501-1 IN que proporciona una visión general de los conceptos fundamentales y de los modelos utilizados para describir la gestión de la seguridad de TI. Sus contenidos van dirigidos a los responsables de la seguridad de TI y a quienes son responsables del plan global de seguridad de la organización.
- UNE 71501-2 IN que describe los aspectos de gestión y planificación de la seguridad de TI. Va dirigida a los directivos con responsabilidades relacionadas con los sistemas de TI de la organización. Pueden ser: directivos de TI responsables del diseño, desarrollo, pruebas, adquisición o explotación de sistemas de TI, o directivos responsables de actividades que hacen un uso sustancial de los sistemas de TI.
- UNE 71501-3 IN que describe técnicas de seguridad indicadas para quienes se encuentran implicados en actividades de gestión durante el ciclo de vida de un proyecto, como planificación, diseño, desarrollo, pruebas, implantación, adquisición o explotación.

UNE 71501-1 IN

Fundamento

Las organizaciones, tanto del sector público como del sector privado, dependen crecientemente de la información para el desarrollo de sus actividades. Así, la pérdida de autenticidad, confidencialidad, integridad y disponibilidad de su información y servicios puede tener para ellas un impacto negativo. En consecuencia, es necesario proteger la información y gestionar la seguridad de los sistemas de TI dentro de las organizaciones. Este requisito de proteger la información es particularmente importante, dado que numerosas organizaciones están conectadas a redes de sistemas de TI interna y externamente.

La gestión de la seguridad de TI es el proceso para alcanzar y mantener niveles apropiados de autenticidad, confidencialidad, integridad y disponibilidad. Las funciones de gestión de la seguridad de TI incluyen:

- Determinación de los objetivos, estrategias y políticas organizativas de la seguridad de TI,
- Determinación de los requisitos organizativos de la seguridad de TI,
- Identificación y análisis de amenazas a activos de la organización (análisis de riesgos),
- Como consecuencia del punto anterior, especificación de las salvaguardas apropiadas (gestión de riesgos),
- Seguimiento de la implantación y operación de las salvaguardas necesarias para proteger la información y los servicios de la organización,
- Desarrollo e implantación de un plan de concienciación en la seguridad, y
- Detección y reacción ante incidentes.

La información es un activo organizativo. Puede existir en múltiples formas. Es vulnerable. Está sometida a una amplia variedad de amenazas. Debe ser protegida frente a impactos mediante la eliminación o minimización de los riesgos asociados. Se protege mediante el establecimiento de salvaguardas o elementos de control.

Aspectos de la gestión de la seguridad

La gestión de la seguridad de TI es una acción permanente, cíclica y recurrente. Vamos a comentar algunos de sus aspectos.

Gestión de la configuración

La gestión de la configuración es el proceso de seguimiento de los cambios en el sistema y puede hacerse formal o informalmente. El objetivo primordial de la gestión de la configuración, en relación a la seguridad, es garantizar que los cambios en el sistema no reducen la efectividad de las salvaguardas, ni la seguridad global de la organización.

Gestión de cambios

La gestión de cambios es el proceso que ayuda a identificar nuevos requisitos de seguridad cuando tienen lugar cambios en los sistemas de TI.

Análisis y gestión de riesgos

Persigue el equilibrio entre la naturaleza de los riesgos a los que están sometidos los datos y los tratamientos y el coste de las salvaguardas.

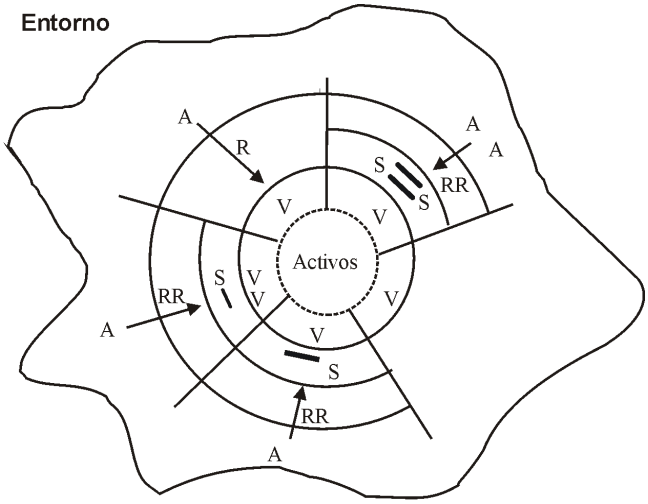
En el análisis y gestión de riesgos se identifican dos procesos:

- *El análisis de riesgos* es el proceso que permite la identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como "activos"), para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.
- *La gestión de riesgos* es el proceso que, basado en los resultados obtenidos en el análisis de riesgos, permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

MODELOS

Si bien existen diversos modelos para la gestión de la seguridad en TI, los modelos presentados en esta parte 1 de la Norma UNE71501 IN proporcionan los conceptos necesarios para su comprensión. Se presentan los siguientes modelos:

- Las relaciones entre elementos de seguridad
- Las relaciones en el análisis y gestión de riesgos
- La gestión del proceso de seguridad de TI



Leyenda
R Riesgo
RR Riesgo residual
S Salvaguarda
A Amenaza
- V Vulnerabilidad

figura 11-1 relaciones entre elementos de seguridad. Fuente: AENOR

El modelo representa:

- Un entorno sometido a amenazas que cambian constantemente y que son parcialmente conocidas,
- Los activos de una organización,
- Las vulnerabilidades de dichos activos,
- Las salvaguardas seleccionadas para proteger los activos y para reducir las consecuencias de la posible materialización de las amenazas,
- Las salvaguardas que reducen los riesgos, y
- Los riesgos residuales aceptables para la organización.
  -

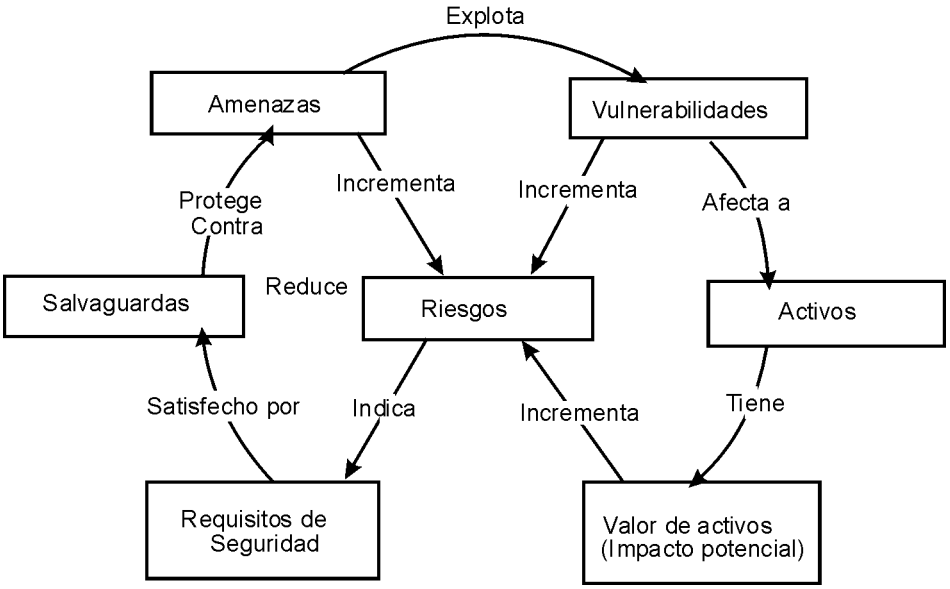


figura 11-2 Las relaciones en el análisis y gestión de riesgos Fuente: AENOR

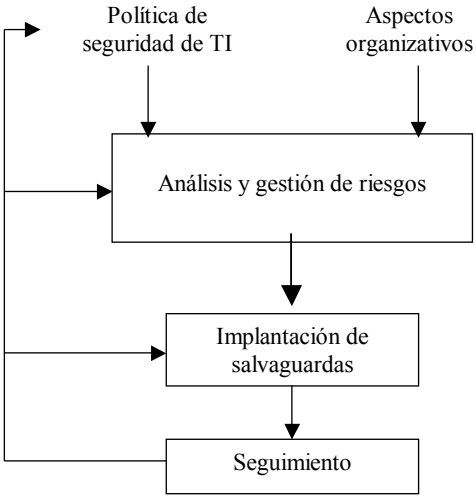


figura 11-3 La gestión del proceso de seguridad de TI

UNE 71501-2 IN

Trata sobre la gestión y las responsabilidades asociadas a un plan eficaz de seguridad de TI. Persigue familiarizar a los gestores con los principales procesos y funciones en la gestión de la seguridad de TI. La información proporcionada en esta parte puede no ser directamente aplicable a todas las organizaciones. En particular, las organizaciones pequeñas probablemente no dispongan de todos los recursos para llevar a cabo por completo algunas de las funciones descritas. descritas. En estos casos, es importante que los conceptos y funciones básicos sean adaptados de forma adecuada a la organización.

UNE 71501-3 IN

Examina diversas técnicas que son importantes para la gestión de la seguridad de TI. Estas técnicas están basadas en los conceptos y modelos aportados por la Norma UNE 71501-1 IN y en el proceso de gestión y responsabilidades tratados en la Norma UNE 71501-2 IN. La discusión en esta parte muestra las ventajas y desventajas de cuatro posibles

estrategias para el análisis de riesgos. Se describe en detalle el enfoque combinado, y las diversas técnicas útiles para su implantación. Es el apartado mas concreto con unos anexos con ejemplos precisos.

11.4.2 UNE 71502 Especificaciones para los Sistemas de Gestión de la Seguridad de la Información

Los apartados son los siguientes:

1 OBJETO Y CAMPO DE APLICACIÓN (SGSI Controles Buenas Prácticas

2 NORMAS PARA CONSULTA

3 TÉRMINOS Y DEFINICIONES

- Un SGSI comprende la estructura organizativa, los procedimientos, los procesos y los recursos para implantar la gestión de la seguridad de la información.
- El sistema es la herramienta de que dispone la Dirección de las organizaciones para llevar a cabo las políticas y los objetivos de seguridad (integridad, confidencialidad y disponibilidad, asignación de responsabilidad, autenticación, etc.)
- Proporciona mecanismos para la salvaguarda de los activos de información y de los sistemas que los procesan, en concordancia con las políticas de seguridad y planes estratégicos de la organización.

4 MARCO GENERAL DEL SGSI

- Requisitos generales
- Establecimiento del entorno de gestión (requisitos legales)
- Selección de controles
- Pasos para el establecimiento del entorno de gestión
- Documentación
- Control documental
- Registros
- Responsabilidades de la Dirección (Compromiso y Política)

Pasos para el establecimiento del entorno de gestión

- FASE 1 Definición de la Política
- FASE 2 Definición del alcance del SGSI
- FASE 3 Desarrollo del Análisis de Riesgos
- FASE 4 Gestión de Riesgos
- FASE 5 Selección de controles a implantar y objetivos a cubrir
- FASE 6 Preparar la relación de controles

5 IMPLANTACIÓN DEL SGSI

- Implantación de los controles
- Eficacia y calidad de los controles

6 EXPLOTACIÓN

- Provisión de recursos materiales y humanos

7 REVISIÓN DEL SGSI

- Auditorías y Revisión por Dirección

8 PROCESO DE MEJORA

PROCESO DE CERTIFICACIÓN

- Reglamento en preparación (similar a otros)
- Auditores con formación específica (legislación y tecnologías de información)

11.4.3 Norma UNE-ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información

Basada en los tres conceptos fundamentales de confidencialidad, integridad y disponibilidad de la información, ya sea escrita, hablada o almacenada en un computador, la ISO/IEC 17799 define las mejores prácticas para manejar la seguridad de la información, en términos de procesos, no de tecnología.

La ISO/IEC 17799 es una metodología estructurada, internacionalmente reconocida, orientada a la seguridad de la información que reconoce un proceso para evaluar, implantar, mantener y administrar la seguridad de la información.. La norma proporciona recomendaciones a los a los responsables la gestión de la seguridad de la información en las organizaciones.

Pretende proporcionar:

- Una base para el desarrollo de normas de seguridad organizativas
- Prácticas efectivas de gestión
- Confianza en los acuerdos entre organizaciones.

Contiene10 secciones de salvaguardas

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

además de 36 objetivos, 127 controles detallados.

La ISO/IEC 17799, que se basa en la norma BS 7799 debe ser utilizada como un documento de referencia, pues proporciona un completo conjunto de controles de seguridad.. A diferencia de ella, la BS 7799 especifica los requerimientos para establecer, implementar y documentar un Sistema de Gestión de Seguridad de Información (*Information Security Management System, ISMS*) y para que los controles de seguridad sean implementados de acuerdo a las necesidades particulares de cada organización.

12 Gestión global de riesgos del sistema

Como ya hemos comentado en el apartado anterior, de los niveles de riesgos establecidos el UNE 71501-3 IN, a este nivel le correspondería el análisis de riesgo detallado, con la ayuda de metodologías de análisis de riesgo. Existen muchas herramientas y metodologías disponibles para la medición de riesgos. Podemos enumerar

- CRAMM
- MAGERIT
- OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability EvaluationSM*)
- InfoSecure [3] metodología y herramientas de análisis de riesgo.
- COBIT [4] (*Control Objetives For It*)

[3] http://www.infosecuregroup.com/

[4] http://www.netconsul.com/

FUENTE: WWW.ISACA.ORG

- COBRA: Risk Consultant. *Software* de análisis de riesgo

Vamos a comentar las tres primeras.

12.1 CRAMM

Es el método de análisis y control de riesgos del Gobierno Británico (*CCTA Risk Analysis and Management Method*). CRAMM es un método estructurado y coherente para la identificación y la evaluación de riesgos en redes y sistemas de información. Abarca escenarios técnicos y no técnicos (por ejemplo, aspectos físicos de la seguridad de la tecnología de la información) y proporciona un método riguroso por etapas que permite programar adecuadamente las revisiones. Hay herramientas de software disponibles para CRAMM. La última versión es CRAMM Versión 5 de enero de 2003. Esta metodología se aplica con la norma BS 7799.

12.2 MAGERIT. Versión 1.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas

La versión 1.0 de MAGERIT se presenta mediante un conjunto de guías:

- Guía de Aproximación a la Seguridad de los Sistemas de Información,
- Guía de Procedimientos, Guía de Técnicas,
- Guía para Desarrolladores de Aplicaciones,
- Guía para Responsables del Dominio Protegible,
- Referencia de Normas legales y técnicas,
- Arquitectura de la Información y especificaciones de la interfaz para el intercambio de datos.

MAGERIT, Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones Públicas, fue elaborado con un doble objetivo: Estudiar los riesgos y recomendar las medidas. Es un método formal para investigar los riesgos que soportan los Sistemas de Información.

La estructura de MAGERIT permite realizar:

- ***El análisis de los riesgos*** para identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el Sistema de Información (conocidos como 'activos'); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.
- ***La gestión de los riesgos***, basada en los resultados obtenidos en el análisis anterior, que permite seleccionar e implantar las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

El Análisis y Gestión de Riesgos es el 'corazón' de toda actuación organizada de materia de seguridad. Influye, incluso, en las fases y actividades de tipo estratégico (implicación de la dirección, objetivos, políticas) y condiciona la profundidad de las fases y actividades de tipo logístico (planificación, organización, implantación de salvaguardas, sensibilización, acción diaria y mantenimiento).

Submodelos de MAGERIT

El modelo normativo de MAGERIT se apoya en tres submodelos:

- *Submodelo de Elementos de Seguridad*, con 6 entidades básicas: Activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas.
- *Submodelo de Eventos de Seguridad*, con 3 tipos principales: Estático, dinámico organizativo y dinámico físico.
- *Submodelo de Procesos de Seguridad*, con 4 etapas tipificadas: Planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas.

Submodelo de Elementos

Activos. Se definen como los "recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección". Se pueden estructurar en las siguientes categorías: En el entorno del Sistema de Información necesario para su funcionamiento, en el sistema de

información, la propia información, las funcionalidades de la organización y otros activos como, por ejemplo, la credibilidad de una persona jurídica o física, su intimidad, la imagen.

Amenazas. Se definen como "los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos". Las amenazas se pueden materializar y transformarse en agresiones. MAGERIT ve las amenazas como acciones capaces de modificar el "Estado de seguridad" del activo amenazado; acciones de tipo "evento", pues hay otras de tipo "decisión" humana.

Vulnerabilidad. Definida como la "ocurrencia real o frecuencia de materialización de una amenaza sobre un activo", la vulnerabilidad es una propiedad de la relación entre un activo y una amenaza. Ejerce entre ambos una función de 'mediación' en el cambio del 'estado de seguridad' del activo; siendo también el mecanismo de paso desde la amenaza a la agresión materializada. La vulnerabilidad tiene así dos aspectos: el estático, ligado a la función (forma parte del "estado de seguridad" del activo); y el dinámico, ligado al mecanismo (convierte la amenaza en agresión).

Impacto. Se define como "daño producido a la organización por un posible incidente" y es el resultado de la agresión sobre el activo, o visto de manera más dinámica, "la diferencia en las estimaciones de los estados (de seguridad) obtenidas antes y después del evento". El impacto puede ser cuantitativo (si representa pérdidas cuantitativas monitorizables directas o indirectas); cualitativo con pérdidas orgánicas (por ejemplo, de fondo de comercio, daño de personas); y cualitativo con pérdidas funcionales (o de los subestados de seguridad).

Riesgo. Se ha definido como la "posibilidad de que se produzca un impacto dado en la organización". Su importancia como resultado de todo el análisis organizado sobre los elementos anteriores (activos, amenazas, vulnerabilidades e impactos) queda velada por su apariencia como indicador resultante de la combinación de la vulnerabilidad y el impacto que procede de la amenaza actuante sobre el activo. Este riesgo calculado permite tomar decisiones racionales para cumplir el objetivo de seguridad de la organización. Para dar soporte a dichas decisiones, el riesgo calculado se compara con el umbral de riesgo, un nivel determinado con ayuda de la política de seguridad de la Organización. Un riesgo calculado superior al umbral implica una decisión de reducción de riesgo. Un riesgo calculado inferior al umbral queda como un riesgo residual que se considera asumible.

Salvaguardas. Para reducir el riesgo se necesita la mejora de salvaguardas existentes o la incorporación de otras nuevas. MAGERIT distingue entre la llamada Función o Servicio de Salvaguarda y la llamada Mecanismo de Salvaguarda. Se define la función o servicio de salvaguarda como "reducción del riesgo"; y el mecanismo de salvaguarda como "dispositivo, físico o lógico, capaz de reducir el riesgo". Una función o servicio de salvaguarda es así una acción para reducir un riesgo de tipo actuación u omisión (es una acción fruto de una decisión, no de tipo evento). Esa actuación se concreta en un mecanismo de salvaguarda que opera de dos formas: la salvaguarda preventiva ejerce como acción sobre la vulnerabilidad y la salvaguarda curativa actúa sobre el impacto.

En resumen:

- Activo: dominio de elementos afectables por el riesgo y la seguridad
- Amenazas: Factores de Riesgo sobre los activos del dominio
- Vulnerabilidad: probabilidad de que se materialice cada amenaza en cada activo
- Impacto: consecuencia de que se materialice cada amenaza en cada activo
- Riesgo: composición de Impactos en los activos y de vulnerabilidades a las amenazas
- Salvaguardas: medidas técnicas y/u organizativas para reducir el riesgo bajo un umbral aceptable

Submodelo de Eventos

Refleja las relaciones generales entre las 6 entidades reseñadas en el Submodelo de Elementos.

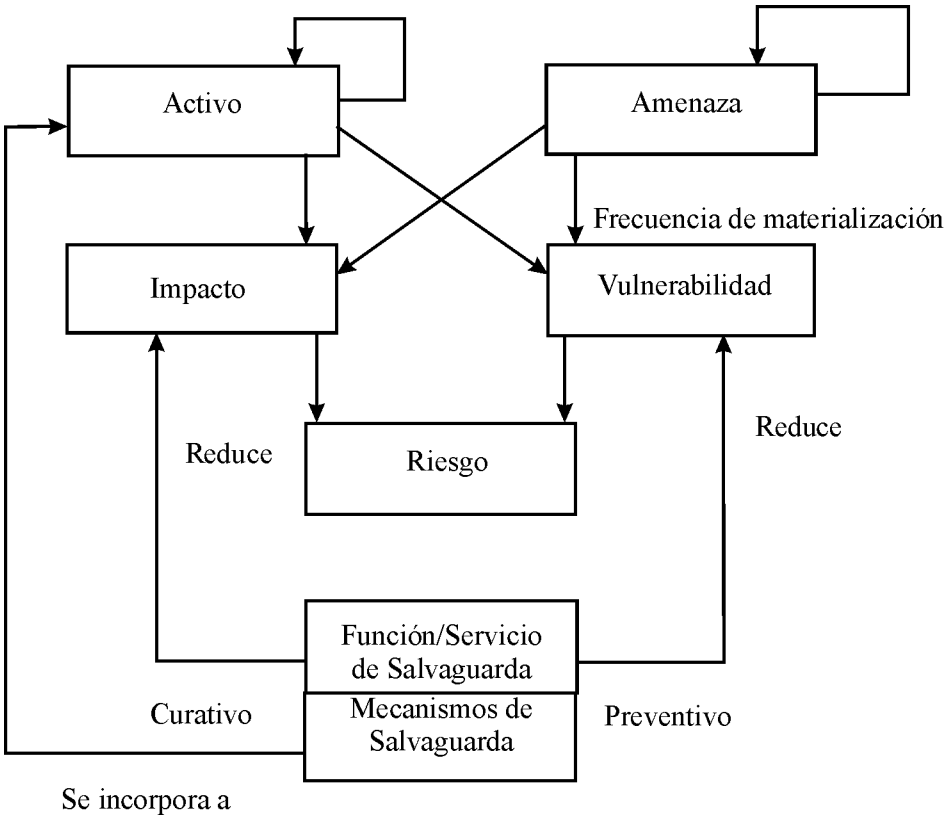


figura 12-4 Relaciones entre elementos

Submodelo de Procesos

El Submodelo de Procesos de MAGERIT está dividido en etapas, compuestas por actividades y éstas se desglosan en tareas (y en caso necesario en subtareas).

El Submodelo de Procesos de MAGERIT comprende 4 etapas:

1. Planificación del Proyecto de Riesgos. Como consideraciones iniciales para arrancar el proyecto de análisis y gestión de riesgos, se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto.

2. Análisis de riesgos. Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.

3. Gestión de riesgos. Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.

4. Selección de salvaguardas. Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del AGR, para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

Herramientas:

- Herramienta RIS2K *Magerit*. La utilización de esta herramienta RIS2K, que data de 1998, es únicamente recomendable a efectos de demostración o de aplicación a entornos o situaciones no muy complejas. Para los demás usos, conviene emplear otros instrumentos de mayor flexibilidad y potencia, como las hojas de cálculo de propósito general.
- La herramienta CHINCHON versión 1.3, elaborada por D. José Antonio Mañas, Profesor de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid. CHINCHON es una herramienta que sigue la metodología MAGERIT. La entrada se escribe en XML y realiza un análisis de la

posición de riesgo, sirviendo de apoyo a su gestión. Los derechos de propiedad intelectual pertenecen al autor, quien ha puesto la herramienta en el dominio público.

Seguridad para el desarrollo de aplicaciones

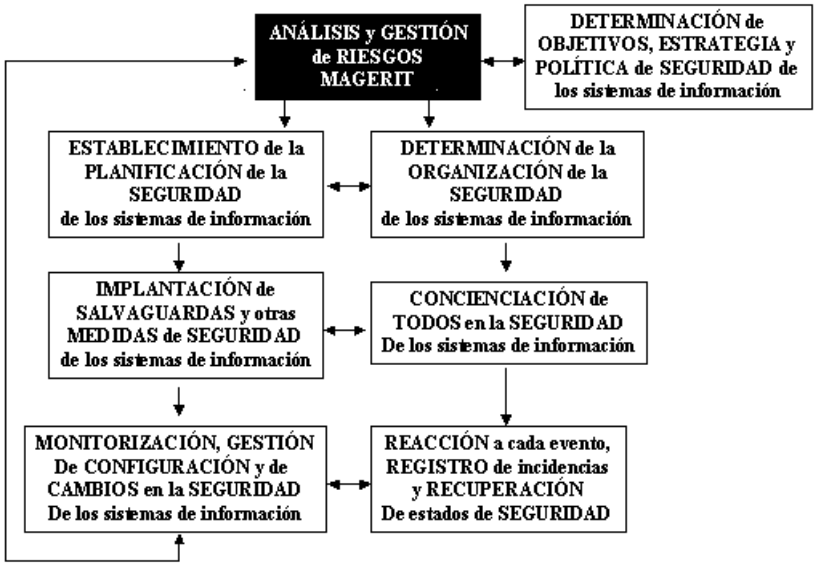


figura 12-5 análisis y gestión de riesgos Magerit

Para poder construir proyectos específicos de seguridad, MAGERIT posee interfaces de enlace con MÉTRICA V 3. MAGERIT permite añadir durante el desarrollo del Sistema la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento. Estas interfaces tienen ventajas inmediatas: analizar la seguridad del Sistema antes de su desarrollo, incorporar defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

La Guía para Desarrolladores de Aplicaciones. Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica.

Productos y servicios complementarios

"Los Criterios de seguridad, normalización y conservación" recogen los requisitos, criterios, y recomendaciones relativos a la implantación de las medidas de seguridad organizativas y técnicas para asegurar la autenticidad, confidencialidad, integridad, disponibilidad y conservación de la información en el diseño, desarrollo, implantación y explotación de las aplicaciones que la Administración General del Estado utiliza para el ejercicio de sus potestades. Estos Criterios pueden ser complemento de MAGERIT y útiles para otras organizaciones que no pertenecen a las Administraciones Públicas. Podemos encontrar criterios de normalización, seguridad, y conservación aplicables a muchos entornos. Aconsejamos la consulta de este documento.

12.3 OCTAVE (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM)

OCTAVE es una metodología estadounidense desarrollada por el Centro de Coordinación CERT del Instituto de Ingeniería del Software de la Universidad Carnegie-Mellon. Un segundo método está en desarrollo el OCTAVE-S, dirigido a pequeñas organizaciones.

13 Certificación

El siguiente nivel correspondería a la Certificaciones de productos. Entendemos que este es el nivel superior, después de implantar un Sistema de Gestión de la Seguridad de la Información según una norma estándar, lo que procede es

Certificar que cumple con dicha norma. No está disponible todavía la norma para la certificación de la norma UNE 17799. Comentamos en este apartado la norma ISO/IEC 15408 (Criterios Comunes), para certificación de componentes.

13.1 Normas de evaluación y certificación

Son el conjunto de normas que sirven para evaluar o certificar que, instalaciones, normas, o programas poseen certificaciones de seguridad. Nos encontramos con normas de diversos ámbitos:

- Estadounidenses
  - TCSEC-Trusted Computer SECurity (libro naranja)
- Europeos
  - ITSEC/ITSEM
- Internacionales
  - ISO/IEC 15408-1 (CC v2.1)

Un poco de historia

Common Criteria es el resultado final de importantes esfuerzos en el desarrollo de criterios de evaluación unificados para la seguridad de los productos IT y ampliamente aceptado por la comunidad internacional.

A principios de los años 80, se desarrollaron en Estados Unidos los criterios de seguridad recogidos bajo el nombre de TCSEC (*Trusted Computer System Evaluation Criteria*) y editados en el famoso "libro naranja". En las décadas posteriores, varios países tomaron como base el TCSEC americano y evolucionaron las especificaciones para hacerlas mas flexibles y adaptables a la constante evolución de los sistemas de IT.

De ahí la comisión europea, en el año 1.991 publicó el ITSEC (*Information Technology Security Evaluation Criteria*), desarrollado conjuntamente por Francia, Alemania, Holanda y el Reino Unido. En Canada, igualmente se desarrollaron en 1.993 los criterios CTCPEC (*Canadian Trusted Computer Product Evaluation*) uniendo los criterios americanos y europeos. En ese mismo año el Gobierno americano publico los *Federal Criteria* como una aproximación a unificar los criterios europeos y americanos.

Tal escenario comienza a aclararse con la decisión de estandarizar internacionalmente estos criterios para uso general, y en esa labor ISO comienza a trabajar a principios de los años 90. Esta tarea fue asignada al grupo de trabajo 3 (WG 3) del subcomité 27 (SC 27) del Comité Técnico ISO/IEC JTC 1 dedicado a Tecnologías de la Información.

La culminación del proceso ocurrió en Junio de 1999, cuando ISO estableció el *Common Criteria* versión 2.0 como estándar, estableciéndolo como ISO 15408 con el título de "*Evaluation Criteria for Information Technology Security*" (ISO-IEC 15408).

Es el resultado de una laboriosa e intensa negociación entre países para obtener un acuerdo de reconocimiento mutuo de las certificaciones de seguridad de productos IT realizadas entre un grupo de 14 países entre los que figura España como firmante del acuerdo a través del Ministerio de Administraciones Publicas[5].

Estos 14 países signatarios de los acuerdos de *Common Criteria*, llegaron a este arreglo porque permitiría establecer un único criterio con el que evaluar la seguridad de los productos de IT, contribuyendo a aumentar la confianza de los usuarios en los mismos.

[5] (http://www.map.es/csi/pg3432.htm)

Certificación

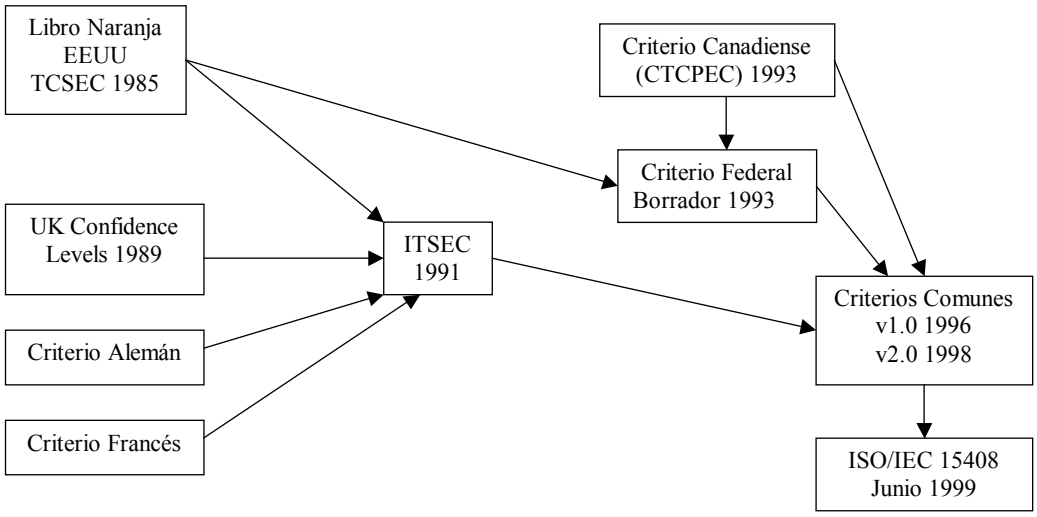


figura 13-6 Evolución de los criterios comunes

Vamos a ver con un poco de más detalles cada una de las normas anteriores.

13.2 CRITERIOS EVALUACIÓN EEUU: TCSEC (Trusted Computer SECurity)

El propósitos de estos criterios de evaluación son:

- Suministrar normas de seguridad a los fabricantes.
- Definir métricas de evaluación y certificación.
- Establecer condiciones para la adquisición de sistemas.

Los requisitos establecidos son:

- Funciones a implementar
- Adecuación de las implementaciones

Las divisiones establecidas

- D, C, B, A

Las clases establecidas son:

- D protección mínima
- C1, C2 protección discrecional
- B1, B2, B3 protección preceptiva
- A1 protección verificada

13.3 ESTÁNDAR EUROPEO DE EVALUACIÓN Y CERTIFICACIÓN

En es estándar Europeo de Certificación y Evaluación podemos distinguir entre:

- Los criterio de evaluación: ITSEC *Information Technology SECurity*
- La metodología: ITSEM.

Una característica de esta norma Europea es la existencia de un esquema nacional de evaluación y certificación. Cada país tiene su autoridad de Evaluación y Certificación.

Criterios de Evaluación ITSEC (*Information Technology SECurity***)**

Los Criterios de Evaluación ITSEC se fijan sobre los Objetivo de seguridad, las Funciones de seguridad y los Mecanismos de seguridad sobre el Objeto a evaluar (TOE).

Los aspectos de la evaluación se realizan sobre:

Certificación

- La funcionalidad. Establece 10 niveles funcionales de F1-F10(Conjunto de funciones de seguridad: F-DX, F-DC, F-DI, F-AV, F-IN, F-B3, F-B2, F-B1, F-C2, F-C1).
- La confianza. Establece 7 niveles de garantía (Efectividad y Corrección: E0, E1, E2, E3, E4, E5, E6).

Metodología ITSEM

Las partes implicadas que se reconocen en esta metodología son:

- El patrocinador del producto que queremos certificar
- El Productor
- Las Instalaciones de evaluación
- La Comisión nacional de certificación

Funciones de la Comisión nacional de certificación

- Las funciones de las comisiones nacionales de Certificación son las siguientes:
- Acreditación de instalaciones
- Supervisión de la evaluación
- Revisión Informes Técnicos
- Emisión de certificados
- Publicación de certificados

Acuerdo de reconocimiento mutuo de certificados (Nov. 1997)

Organismos de certificación reconocidos:

- Reino Unido
- Francia
- Alemania

13.4 ISO/IEC 15408 (Criterios Comunes[6])

La Norma internacional ISO 15408, también conocida como "*Common Criteria*" 16 establece unos criterios de evaluación y certificación de la seguridad en Tecnologías de la Información. Quedan fuera de su marco de normalización los siguientes aspectos:

- Medidas administrativas
- Medidas físicas
- Marco legal de la evaluación
- Calidad intrínseca de los algoritmos de cifrado

Justificación

Muchos sistemas y productos de Tecnologías de la Información están diseñados para satisfacer y realizar tareas específicas y puede ocurrir, normalmente por razones económicas, que determinados aspectos de seguridad se encuentren delegados en funciones de seguridad de otros productos o sistemas de propósito general sobre los cuales ellos trabajan como pueden ser sistemas operativos, componentes *software* de propósito específico o plataformas *hardware*.

Por tanto, las medidas de salvaguarda dependen del correcto diseño y funcionamiento de los servicios de seguridad que implementan otros sistemas o productos IT más genéricos.

Sería deseable por tanto, que éstos estuvieran sometidos a evaluación para conocer en que medida nos ofrecen garantías y podemos depositar confianza en ellos. Muchos clientes y consumidores de sistemas y productos IT carecen de los conocimientos necesarios o recursos suficientes para juzgar por ellos mismos si la confianza que depositan en estos sistemas o productos IT es adecuada y desearían no obtener esa certeza solamente en base a la información que proporcionan los fabricantes o las especificaciones de los desarrolladores.

[6] ISO/IEC 15408 http://www.commoncriteria.org/

Certificación

La norma ISO/IEC 15408 define un criterio estándar a usar como base para la evaluación de las propiedades y características de seguridad de determinado producto o sistema IT. Ello permite la equiparación entre los resultados de diferentes e independientes evaluaciones, al proporcionar un marco común con el que determinar los niveles de seguridad y confianza que implementa un determinado producto en base al conjunto de requisitos de seguridad y garantía que satisface respecto a esta norma obteniendo de esa forma una certificación oficial de nivel de seguridad que satisface.

Por tanto, la norma ISO/IEC 15408 proporciona una guía muy útil a diferentes perfiles relacionados con las tecnologías de la seguridad.

Desarrolladores de productos o sistemas de tecnologías de la información (fabricantes).Pueden ajustar sus diseños y explicar lo que ofrecen.

Los evaluadores de seguridad, que juzgan y certifican en que medida se ajusta una especificación de un producto o sistema IT a los requisitos de seguridad deseados. Es decir, puede certificar lo que asegura.

Los usuarios que pueden conocer el nivel de confianza y seguridad que los productos de tecnologías de la información y sistemas le ofrecen y puede explicar lo que quiere.

1. Los usuarios pueden comparar sus requerimientos específicos frente a los estándares de *Common Criteria* para determinar el nivel de seguridad que necesitan.
2. Los usuarios pueden determinar mas fácilmente cuando un producto cumple una serie de requisitos. Igualmente, *Common Criteria* exige a los fabricantes de los productos certificados publicar una documentación exhaustiva sobre la seguridad de los productos evaluados.
3. Los usuarios pueden tener plena confianza en las evaluaciones de *Common Criteria* por no ser realizadas por el vendedor, sino por laboratorios independientes. La evaluación de *Common Criteria* es cada vez mas utilizada como condición necesaria para concurrir a concursos públicos. Por ejemplo, el Departamento de Defensa Americano ha anunciado planes para utilizar exclusivamente productos certificados *por Common Criteria*.
4. Debido a que *Common Criteria* es un estándar Internacional, proporciona un conjunto común de estándares que los usuarios con operaciones internacionales pueden utilizar para escoger productos que se ajusten localmente a las necesidades de seguridad.

En definitiva, proporcionando un conjunto de estándares en seguridad como los recogidos por *Common Criteria*, se crea un lenguaje común entre los fabricantes y los usuarios, que ambos pueden entender. Los fabricantes utilizarán este lenguaje para contar a sus clientes potenciales las características de sus productos evaluadas en *Common Criteria*, e igualmente habilita a los usuarios a identificar y comunicar adecuadamente sus necesidades de seguridad. Se proporcionan unos medios y mecanismos objetivos que nos permitirán tomar decisiones en base algo más sólido que las meras percepciones.

Diferentes partes del Estándar

El ISO/IEC 15408 se presenta como un conjunto de tres partes diferentes pero relacionadas. A continuación, describimos cada una de ellas:

Parte 1. Introducción y modelo general. IS 15408-1:1999(2002) *Introduction and general model*

Define los principios y conceptos generales de la evaluación de la seguridad en tecnologías de la información y presenta el modelo general de evaluación. También establece cómo se pueden realizar especificaciones formales de sistemas o productos IT atendiendo a los aspectos de seguridad de la información y su tratamiento.(la estructura y lenguaje comunes para expresar los requisitos de seguridad de productos o sistemas de TI).

- PP –*protection profile* –perfil de protección
  – lo que se quiere: requisitos para una categoría de productos
- ST –*security target* –objetivo de seguridad
  – fabricante: lo que ofreceré: especificaciones de un producto
- TOE –*target of evaluation* –objetivo de evaluación
  – una implementación de ST

Parte 2. Requisitos Funcionales de Seguridad IS 15408-2: 1999(2002) *Security functional requirements*

Este tipo de requisitos definen un comportamiento deseado en materia de seguridad de un determinado producto o sistema IT.

Parte 3. Requisitos de Garantías de Seguridad IS 15408-3:1999(2002) *Security assurance requirements*

Este tipo de requisitos establecen los niveles de confianza que ofrecen funciones de seguridad del producto o sistema. Trata de evaluar que garantías proporciona el producto o sistema en base a los requisitos que se satisfacen a lo largo del ciclo de vida del producto o sistema.

- **Evolución del estándar**

Las normas que se están elaborando para el futuro inmediato son:

- IS 15292:2001(2005) *Protection profile registration procedures*
- WD 18045 *Methodology for IT security evaluation*

Niveles de garantía

- *Common Criteria* o ISO/IEC 15408, proporcionan también unos niveles de garantía (EAL) como resultado final de la evaluación. EAL –*Evaluated Assurance Level*
- EAL0: sin garantías
- EAL1: probado funcionalmente
- EAL2: probado estructuralmente
- EAL3: probado y chequeado metódicamente
- EAL4: diseñado, probado y revisado metódicamente
- EAL5: diseño y pruebas semi-formales
- EAL6: diseñado, probado y verificado semi-formalmente
- EAL7: diseñado, probado y verificado formalmente Constituyen la base para el reconocimiento mutuo

Organización de los requisitos de Seguridad

Los CC establecen unos criterios de evaluación basados en un análisis riguroso del producto o sistema IT a evaluar y los requisitos que este satisface. Para ello, establece una clasificación jerárquica de los requisitos de seguridad. Se determinan diferentes tipos de agrupaciones de los requisitos siendo sus principales tipos los que vemos a continuación:

- Clase: Conjunto de familias comparten un mismo objetivo de seguridad.
- Familia: un grupo de componentes que comparten objetivos de seguridad pero con diferente énfasis o rigor.
- Componente: un pequeño grupo de requisitos muy específicos y detallados. Es el menor elemento seleccionable para incluir en los documentos de perfiles de protección (PP) y especificación de objetivos de seguridad (ST).

13.5 Metodología abierta para la verificación de la seguridad (OSSTMM)

Existe una metodología de código abierto para la verificación de la seguridad de los sistemas. Esta metodología es de ISECOM 16 (*Institute for security and Open methodologies*) La metodología se conoce por las siglas OSSTMM – (*Open Source Security Testing Methodology Manual*).

Isecom es una organización internacional, sin ánimo de lucro, que tiene como objetivo desarrollar conocimientos y herramientas relacionadas con la seguridad, ofreciéndolas bajo una licencia de código abierto que permite su libre utilización.

OSSTMM es el estándar más completo existente en la actualidad con una metodología para la verificación de la seguridad de los sistemas y las redes que disponen de una conexión a Internet.

Esta metodología, se encuentra en constante evolución y es fruto de la colaboración de más de 150 colaboradores de todo el mundo. Gracias a este número de colaboradores, el documento incorpora los más recientes cambios y nuevos desarrollos relacionados con la seguridad informática.

La OSSTMM es una metodología para la realización de las verificaciones de seguridad en Internet. Se trata del principal proyecto existente en la actualidad para definir una metodología formal que permita verificar la seguridad informática de los equipos, desarrollado de una forma independiente y totalmente abierto. Otros proyectos en los que se está trabajado son la metodología para la programación segura y la "*Hacker High School*".

El disponer de una metodología de trabajo estandarizada significa que permita garantizar el nivel de pruebas que se realizan en el momento de verificar la seguridad. No pretende especificar una lista de pruebas concretas a realizar, sino los elementos que deben verificarse, tanto desde el exterior como el interior.

Un aspecto importante a señalar es que la OSSTMM ha sido diseñada para cubrir los aspectos técnicos establecidos por diversas legislaciones. Así, en el caso concreto de España, la OSSTMM incluye los requerimientos establecidos tanto por la ley de protección de datos y la LSSICE.

Es un proyecto interesante pero que no es adecuado para la elaboración de los planes de seguridad que por normativa legal hay que realizar.

Son mas recomendable la norma ISO 17799 ayudada de la metodología Magerit. La metodología OSSTMM esta orientada a evaluar la seguridad de un sistema. Esta orientada a realizar una auditoría de seguridad de los sistemas.

13.6 Metodología del Computer Security Resource Center (CSRC-NIST)

El *Computer Security Resource Center* (organismo que depende del NIST, *National Institute of Standards and Technology* del departamento de comercio de los Estados Unidos) ha publicado su metodología para la verificación de la seguridad de los sistemas y de las políticas de seguridad 16.

Este documento está dividido en cuatro secciones: una introducción a la metodología, la descripción de los métodos de verificación y el conjunto de seguridad, la definición de los métodos y objetivos de las pruebas de seguridad y, en la última sección, que elementos deben tener prioridad cuando se realizan las verificaciones con unos recursos limitados.

Los pasos que debe seguir una organización que desea implementar una normativa de este tipo son: primero, establecer los requisitos de seguridad de la organización, identificando riesgos, amenazas, vulnerabilidades y posibilidades de impacto, principalmente. Luego, es necesario establecer principios y políticas para lo que queremos proteger. Además, se debe considerar un ítem de entrenamiento para que los empleados de la empresa comprendan cómo se debe establecer la norma. También, es clave definir un calendario de trabajo con tiempos determinados y el alcance de las políticas que se han de implementar.

Certificación

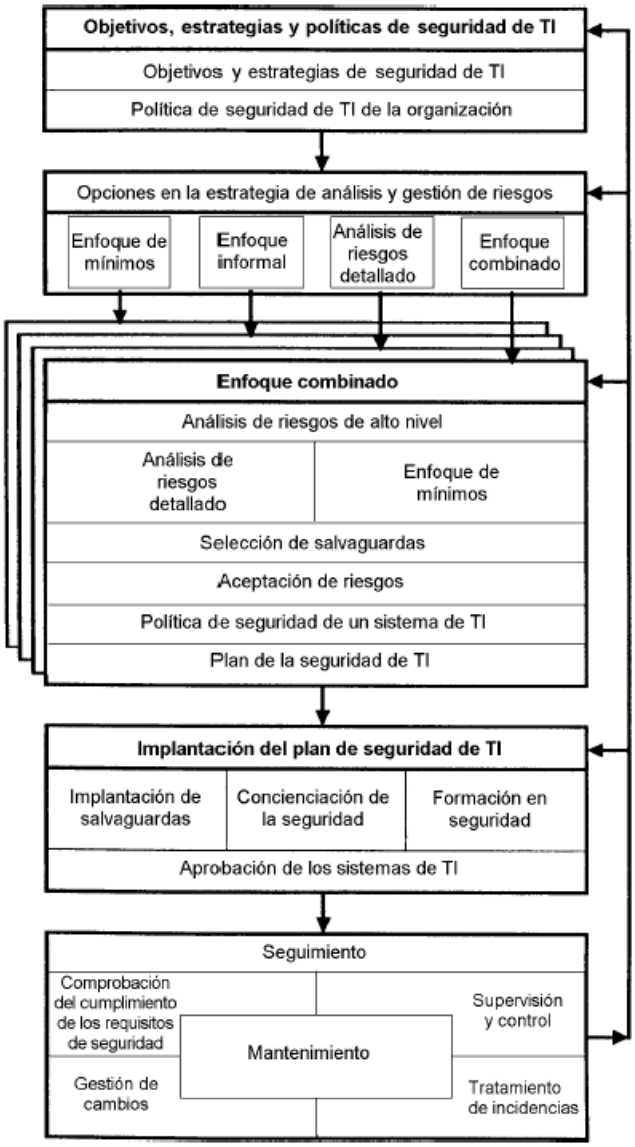


figura 13-7 PNE 71502

La ISO/IEC 17799:2000 es un Código de Prácticas que no proporciona el necesario nivel de detalle para dar soporte a un esquema de certificación. En otros países se emplea la norma BS-7799-2.

Se trata del único estándar con aceptación mundial que satisface los requerimientos del mercado. Es una forma de reducir los costos de las primas de las pólizas de seguros; y mejora la efectividad de la seguridad de la información

Debe ser utilizada considerando el marco legal aplicable en cada país. Es importante señalar que el carácter de norma nacional idéntica a la Norma Internacional ISO/IEC 17799:2000, si se consideran apartados aislados, podríamos tener la visión que la norma incurre puntualmente en aspectos que pueden ser objeto de conflicto con la legislación aplicable en el marco español.

Pero si la norma se contempla en su totalidad, se verá que sí tiene en cuenta los mencionados aspectos, indicando el debido cumplimiento de la legislación aplicable en cada estado.

Certificación

Recientemente las compañías dedicadas a la seguridad han lanzado una iniciativa que precisamente está orientada a concienciar a los responsables de la seguridad sobre la importancia del factor humano y las políticas de seguridad dentro de una organización [7].

13.7 La Norma BS 7799

BS 7799 permite definir y mantener un Sistema de Gestión de la Seguridad de la Información (ISMS). Esta norma define los controles y las responsabilidades que más se adecuen a una organización, de acuerdo a su realidad, para administrar mejor la seguridad de la información. BSI, como fundadora de la norma BS 7799 es la principal entidad certificadora en dicho estándar.

Obtener la certificación BS 7799 es claramente un beneficio para las organizaciones de hoy, ya que representa una oportunidad para identificar las debilidades; permite al gerente general conocer y controlar la seguridad de la información de su compañía, además de una revisión permanente de la misma y de forma independiente del sistema de gestión de seguridad de la información que se tenga

Acerca de BSI (*British Standard*)

Fundada en 1901, BSI ha llevado más de 35,500 proceso de registro sobre 90 países. es miembro fundador de la Organización Internacional para la Estandarización (ISO), BSI facilitó y publicó el primer estándar para sistemas de administración de calidad, sistemas de administración ambiental, salud y administración de proyectos. También construyo la norma de seguridad BS 7799, base del estándar de buenas prácticas ISO/IEC 17799:2000. Actualmente cuenta con registro del 35% de la certificación de seguridad BS7799-2[8].

Por la proliferación de normativa legal en el ámbito nacional e internacional se hace necesario la elaboración de algún tipo de guía u orientación para poder aplicar prácticamente todas estas normas y recomendaciones.

14 Consejos sobre seguridad

INFORMÁTICA PERSONAL SEGURA

==========

Por Bruce Schneier (schneier@counterpane.com)

Traducido por José Manuel Gómez

(jmg@kriptopolis.com)

http://www.kriptopolis.com/criptograma/0037_8.html

****

Se me pregunta con frecuencia qué puede hacer el usuario medio de Internet para garantizar su seguridad. Mi primera respuesta suele ser "Nada; no hay forma". Pero en realidad es más complicado que eso.

Contra el gobierno no hay nada que se pueda hacer. El desequilibrio de poder es demasiado grande. Incluso si se utiliza el mejor cifrado del mundo, la policía puede instalar un espía de teclado mientras uno está fuera (Si usted es lo bastante paranoico para dormir con su pistola y su portátil bajo la almohada, este artículo no es para usted). Hasta es difícil protegerse de las grandes empresas. Si tienen su número de tarjeta de crédito, por ejemplo, no hay forma de hacer que se les olvide. Pero hay algunas cosas que usted puede hacer para mejorar su seguridad en Internet.

Ninguna de ellas es perfecta; ninguna es infalible. Si la policía secreta desea obtener sus datos o acceder a sus comunicaciones, ninguna de ellas se lo impedirá. Pero todas constituyen buenas medidas preventivas para la red y harán que usted sea más difícil de controlar que el ordenador del vecino.

1. Contraseñas. Las contraseñas suficientemente buenas no son fáciles de memorizar, pero no se preocupe. Cree contraseñas largas y aleatorias, y anótelas. Guárdelas en su cartera, o en un programa como Password Safe. Guárdelas como haría con su dinero. No deje que los navegadores web almacenen sus contraseñas por usted.

[7] Puedes consultarla en http://www.humanfirewall.org/ y tiene un cuestionario que permite evaluar tu organización respecto de la iso17799

[8] (www.bsi-global.com)

No transmita contraseñas (o PINs) mediante formularios web o correos sin cifrar. Asuma que todos los PINs pueden romperse fácilmente, y actúe en consecuencia.

2. Antivirus. Utilícelo. Descargue e instale las actualizaciones cada dos semanas, y en cualquier momento en que lea algo sobre un nuevo virus en los medios de comunicación. Algunos productos antivirus comprueban automáticamente si existen actualizaciones.
3. Cortafuegos personales. Utilícelos. Habitualmente no existe ninguna razón para permitir conexiones entrantes de nadie.
4. Correo electrónico. Borre el spam (correo basura) sin leerlo. No abra, y borre inmediatamente, mensajes con ficheros adjuntos, a menos que sepa lo que contiene. No abra, y borre inmediatamente, viñetas, vídeos y ficheros del tipo "bueno para echar unas risas" enviados por bienintencionados amigos. Desactive el correo HTML. No utilice Outlook ó Outlook Express. Si debe utilizar Microsoft Office, active la protección frente a virus de macro; en Office 2000 cambie el nivel de seguridad a "Alto" y no confíe en ninguna fuente a menos que tenga que hacerlo. Si está utilizando Windows, desactive la opción "Ocultar extensiones de fichero para tipos de fichero conocidos"; esa opción permite que los troyanos se hagan pasar por otros tipos de ficheros. Desinstale "Windows Scripting Host" si puede pasar sin ello. Si no puede, al menos cambie sus asociaciones de ficheros, para que los ficheros de script no sean enviados automáticamente al Scripting Host si se hace doble click sobre ellos.
5. Sitios web. SSL no proporciona ninguna seguridad sobre si el comerciante es fiable o si su base de datos de información de clientes es segura. Piensélo antes de hacer negocios con un sitio web. Limite los datos personales y financieros que envíe a los sitios web; no proporcione ninguna información a no ser que lo considere imprescindible. Si no quiere dar información personal, mienta. No acepte recibir anuncios de marketing. Si el sitio web le da la opción de no almacenar su información para usos posteriores, márquela.
6. Navegación. Limite el uso de cookies y applets a esos pocos sitios que le dan servicios que necesita. Limpie con regularidad sus carpetas de cookies y ficheros temporales (yo tengo un fichero BAT que lo hace cada vez que arranco). Si eso no es posible, no utilice Microsoft Internet Explorer.
7. Aplicaciones. Limite los programas en su máquina. Si no lo necesita, no lo instale. Si no va a necesitarlo más, desinstálelo. Si lo necesita, compruebe con regularidad si hay actualizaciones e instálelas.
8. Copias de Seguridad. Hágalas regularmente. Haga copias al disco, cinta o CD-ROM. Guarde por lo menos un juego de copias fuera de su ordenador (una caja de seguridad es un buen lugar) y al menos un juego en el ordenador. Recuerde destruir las copias antiguas; destruya físicamente los discos CD-R.
9. Seguridad en portátiles. Mantenga su portátil con usted siempre que no esté en casa; piense en él como si fuera su cartera o su bolso. Elimine regularmente los ficheros de datos que ya no necesite. Lo mismo puede aplicarse a los dispositivos Palm; la gente tiende a dejar en ellos incluso más datos personales, incluyendo contraseñas y PINs, que en los portátiles.
10. Cifrado. Instale un cifrador de correo y ficheros (como PGP). Cifrar todo su correo no es realista, pero algún correo es demasiado sensible para enviarlo sin cifrar. De igual forma, algunos ficheros de su disco duro son demasiado sensibles para dejarlos sin cifrar.
11. General. Apague su ordenador cuando no lo utilice, sobre todo si tiene una conexión permanente a Internet. Si es posible, no utilice Microsoft Windows.

Sinceramente, todo esto resulta difícil. Ni siquiera puedo decir que yo siga escrupulosamente mis propios consejos. Pero sigo la mayoría, y probablemente eso ya resulta suficiente. Y "probablemente suficiente" es casi lo mejor que se puede obtener hoy en día.

Recomendaciones del CERT

“Recomendamos, con toda rotundidad, que windows 95/98/ME se considere comprometido desde el mismo momento que se arranca. Ninguna versión de Windows 9x/ME debería ser jamás utilizada en cualquier ordenador de una red donde algún recurso necesite ser asegurado”

Pag. 37 Recomendaciones de seguridad. V.0.1 Noviembre 2000

Seguridad en red

1. No comparta recursos si no es necesario

2. Si necesita compartirlo hágalo con una buena contraseña
3. Siempre que sea posible compártalo como “solo lectura”
4. NUNCA comparta su disco duro con privilegio de escritura ni siquiera con contraseña.

Problemas y casos

- Cookies
- Herramientas comercio one-to-one: i-sell
- Data mining
- NTFSDOS
- Historias clínicas del SAS en contenedores de basura
- Casos datos del Gran Hermano
- Correo electrónico no deseado
    - **La red ultrasecreta Echelon**
- Se creó a principios de la década de los setenta
- Está dirigida por la NSA norteamericana y la agencia británica Comunicaciones Gubernamentales (GCHQ) y en ella participan Canadá, Australia y Nueva Zelanda.
- red de 120 satélites
    - Cada hora más de dos millones de mensajes pasan bajo el tamiz de Echelon
    - **Sitios sobre seguridad**
- www.kriptopolis.com
- www.cica.es
- www.rediris.es

15 Cuestiones Tema IX

1. ¿Cuáles son los cuatro subestados que determinan las características de seguridad de un sistema?
2. ¿Qué significa autentificación?
3. ¿Qué significa confindencialidad?
4. ¿Qué significa no repudio o irrenunciabilidad?
5. ¿Qué significa integridad?
6. ¿Qué diferencia hay entre políticas y mecanismos?
7. Clasificación de las medidas de seguridad
8. La validación de la identidad se basa en la combinación de tres elementos.
9. Nombra al menos tres tipos de ataques a las contraseñas
10. ¿Qué son los sistemas biométricos?
11. Nombra los tres tipos de copias de seguridad de los ficheros
12. ¿Qué es criptografía?
13. Características de la criptografía de clave privada
14. ¿Qué es la criptografía de clave pública?
15. ¿Qué es la encriptación o cifrado?
16. Características de clave pública
17. ¿Qué es una firma digital?
18. ¿Qué es un certificado digital?
19. ¿Qué es un certificado raiz?
20. ¿Qué es la huella digital?
21. Nombra tres protocolos estándares de seguridad en redes. Di sus características más destacadas.
22. ¿En qué consiste el proyecto CERES?
23. ¿Qué es una autoridad de certificación?
24. ¿Qué es una autoridad de registro?
25. Normas de seguridad para las administraciones públicas. Nómbralas
26. ¿Qué ley orgánica define la protección de los datos de carácter personal?

16 Referencias:

[1] ISO/IEC 15408 (Criterios Comunes) parte 1, 2 y 3 [consulta 11junio de 2003] http://www.commoncriteria.org/docs/PDF/CCPART1V21.PDF

[2] ISO/IEC 17799:2000 *Information Security Management, Code of Practice for Information Security Management. International Standard*. [consulta 11 junio de 2003] http://www.iso17799software.com/

[3] BS 7799-1:1999 *Information security management –Part 1: Code of practice for information security management. British Standard*.

[4] BS 7799-2:2002 *Information Security Management. Part 2 Specification for information security management systems. British Standard*.

[5] UNE ISO/IEC IS 17799 – Tecnologías de la información – Código de buenas prácticas para la gestión de la seguridad de la información (*Information technology – Code of practice for information security managment*)

[6] ISO/IEC 13335-1 IT- *Security techniques - Guidelines for the management of IT security - Part 1: Concepts and models for managing and planning IT security*

[7] ISO/IEC 13335-2 IT- *Security techniques - Guidelines for the management of IT security - Part 2: Managing and planning IT security*

[8] ISO/IEC 13335-3 IT- *Security techniques - Guidelines for the management of IT security - Part 3: Techniques for the management of IT security*

[9] ISO/IEC 13335-4 IT- *Security techniques - Guidelines for the management of IT security - Part 4: Selection of safeguards*

[10] ISO/IEC 13335-5 IT- *Security techniques - Guidelines for the management of IT security - Part 5: Management guidance on network security*

[11] UNE 71501-1 IN Parte 1: Conceptos y modelos para la seguridad de TI

[12] UNE 71501-2 IN Parte 2: Gestión y planificación de la seguridad de TI

[13] UNE 71501-3 IN Parte 3: Técnicas para la gestión de la seguridad de TI

[14] INFORMATION TECHNOLOGY *Baseline Protection* Manual [consulta 4 junio de 2003] http://www.bsi.bund.de/gshb/english/etc/inhalt.htm

[15] Guía de seguridad informática (SEDISI) [consulta: 11 junio de 2003] http://www.sedisi.es/06_index.htm ,

[16] MAGERIT V.1.0 Metodología de análisis y gestión de riesgos de los sistemas, 1997 Ministerio de Administraciones Públicas Boletín Oficial del Estado ISBN 84-340-0960-9; [consulta 6 de junio de 2003] http://www.map.es/csi/pg5m20.htm

I. Guía de aproximación a la seguridad de los sistemas de información
II. Guía de procedimientos
III. Guía técnica
IV. Guía para desarrolladores de aplicaciones
V. Guía para responsable del dominio protegible
VI. Arquitectura de la información y especificaciones de la interfaz para intercambio de datos
VII. Referencia de normas legales y técnicas CD-ROM

[17] LORTAD Reglamento de seguridad. E. Del Peso Navarro – M. A. Ramos González, Diaz de Santos, 1999 ISBN 84-7978-412-1

[18] LORTAD análisis de la ley. E. Del peso – M. A. Ramos González, Díaz de Santos, 1998 ISBN 84-7978-343-5 2º edición.

[19] Ley de protección de datos. La nueva LORTAD. Del peso navarro, E, Díaz de Santos, 2000 ISBN 84-7978-446-6

[20] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité

Referencias:

de las Regiones sobre seguridad de las redes y de la información: Propuesta para un enfoque político europeo [consulta: 4 de junio de 2003]. y http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_es.pdf

[21] REAL DECRETO 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal [consulta 5 de junio de 2003] http://www.map.es/csi/pg3415.htm

[22] Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal [consulta 5 de junio de 2003] https://www.agenciaprotecciondatos.org/datd1.htm

[23] Real Decreto 195/2000, de 11 de febrero, por el que se establece el plazo para implantar las medidas de seguridad de los ficheros automatizados previstas en el Reglamento aprobado por el Real Decreto 994/1999, de 11 de junio. .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3417.htm

[24] Legislación sobre ficheros de tratamiento automatizado de datos de carácter personal. .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3419.htm

[25] Legislación sobre protección de datos de carácter personal (Disposiciones generales). .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3418.htm

[26] PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (Otras disposiciones). .[consulta 4 de junio de 2003] http://www.map.es/csi/pg3426.htm

[27] PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL (Aprobación de Documentos de seguridad en aplicación del reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal. .[consulta 4 de junio de 2003] http://www.csi.map.es/csi/pg3425.htm

[28] Evaluación y certificación de la seguridad de las tecnologías de la información. MAP.[consulta 11 junio de 2003] http://www.csi.map.es/csi/pg3432.htm

[29] Adopting a multi-annual programme (2003-2005) for the monitoring of eEurope, dissemination of good practices and the improvement of network and information security (MODINIS). Brussels, 26.07.2002 COM(2002) 425 final 2002/0187 (CNS). .[consulta 4 de junio de 2003] http://www.map.es/csi/pdf/modenis_en.pdf

[30] A R R E G L O sobre el Reconocimiento de los Certificados de Criterios Comunes en el campo de la Seguridad de las Tecnologías de la Información. .[consulta 4 de junio de 2003] http://www.map.es/csi/pdf/acuerdo.pdf

[31] Special Pub 800-12 -- An Introduction to Computer Security: The NIST Handbook .[consulta 4 de junio de 2003] ; http://csrc.nist.gov/publications/nistpubs/800-12/

[32] Estrategia para la Seguridad de los Sistemas de Información. Madrid 22 de octubre del 2002. Julián Marcelo Cocho. Universidad Politécnica de Valencia. [consulta: junio 2003] http://www.grupodoxa.com/html/grupodoxa/pdf/estrategias.pdf

[33] eEurope 2005: Una sociedad de la información para todos. junio de 2002. Bruselas, 28.5.2002 COM(2002) 263 final [consulta: 5 junio 2003] http://www.guiafc.com/documentos/2002-COM-263.pdf

[34] Documentos de seguridad. Agencia de Protección de Datos de la Comunidad de Madrid [consulta: 6 de junio 2003] https://www.madrid.org/apdcm/contenidos/documento_box00.html

[35] Estándares Internacionales de seguridad en sistemas de información. I Consecri (Congreso Nacional de Seguridad en Sistemas Teleinformáticos y Criptografía). Arturo Ribagorda Garnacho. Catedrático de Universidad. Universidad Carlos III Madrid. [Consulta: 6 de junio de 2003] http://www.consecri.com.ar/pdf/Consecri%2025-09-01/Exposiciones/05%20-%20Est%E1ndares%20internacionales%20de%20seguridad%20en%20Sist%20Inf.pdf

[36] Certificación de la Seguridad. José A. Mañas jmanas@dit.upm.es Dpto. de Ingeniería de Sistemas TelemáticosUniversidad Politécnica de Madrid. [Consulta: 6 junio 2003] http://jungla.dit.upm.es/~pepe/ec/2003/02-certificacion.pdf

[37] eEurope 2005: Propuesta de Reglamento de la Agencia de Seguridad de la Información y de las Redes Europeas presentada por la Comisión. (COM(2003) 63 final (Febrero 2003) (en inglés) [consulta 14 de junio de 2003] http://www.csi.map.es/csi/pdf/nisa_en.pdf

[38] REDI Revista Electrónica de Derecho Informático.[Consulta 6 junio de 2003]

Referencias:

http://v2.vlex.com/es/ppv/doctrina/fuente_29

[39] Guías de la OCDE para la seguridad de los sistemas de información y redes Hacia una cultura de seguridad. *Organisation For Economic Co-Operation And Development*. (Paris 2002).[consulta 7 junio 2003]http://www.oecd.org/pdf/M00033000/M00033189.pdf

[40] CRAMM del Gobierno Británico (CCTA *Risk Analysis and Management Method*).[consulta 7 junio de 2003] http://www.cramm.com/ y Para obtener más información, consulte: http://www.crammusergroup.org.uk/

[41] Recomendaciones de seguridad. Chelo Malagon Poyato (chelo.malagon@rediris.es) Francisco Monserrat Coll (francisco.monserrat@rediris.es) David Martinez Moreno (david.martinez@rediris.es) 15 de diciembre de 2000. Versi on 0.1 [consulta 7 junio 2003] http://www.rediris.es/cert/doc/docu_rediris/recomendaciones/recomendaciones.pdf

[42] Documentación sobre seguridad en la Comunidad RedIRIS [consulta 7 junio 2003] http://www.rediris.es/cert/doc/docu_rediris/

[43] Definición de una política de seguridad José R. Valverde JRValverde@es.embnet.org onsulta 7 junio 2003] http://www.rediris.es/cert/doc/docu_rediris/poliseg.es.html

[44] Gestión de la seguridad de la información. Noviembre 2002, Mario López de Ávila Muñoz. [consulta 8 junio 2003] www.a-nei.org/documentos/PS17799.pdf

[45] Adecuándose a la norma ISO/IEC 1799 mediante software libre * José Fernando Carvajal Vión Grupo de Interés en Seguridad de ATI (ATI-GISI) carvaco@ati.es Javier Fernández-Sanguino Peña Grupo de Interés en Seguridad de ATI (ATI-GISI) jfs@computer.org 28 de octubre de 2002 [consulta 9 junio de 2003] http://www.ibiblio.org/pub/Linux/docs/LuCaS/Presentaciones/200211hispalinux/jfs2/linux-iso17799.pdf y en http://www.opensource.org.mx/lucas/Presentaciones/200211hispalinux/jfs2/linux-iso17799.html

[46] Criterios de seguridad, normalización y conservación de las aplicaciones utilizadas para el ejercicio de potestades. Ministerios de Administraciones Públicas. Madrid, febrero de 2003. [consulta 10 junio 2003] http://www.map.es/csi/pg5c10.htm.

[47] Magerit V1.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas. Consejo Superior de Informática y para el impulso de la Administración electrónica [Consulta 9 de junio de 2003]. http://www.map.es/csi/pg5m20.htm

[48] CHINCHON - Análisis del Riesgo. D. José Antonio Mañas, Profesor de la Escuela Técnica Superior de Ingenieros de Telecomunicaciones de la Universidad Politécnica de Madrid. [Consulta 9 junio de 2003] http://jungla.dit.upm.es/~pepe/chinchon/README.htm

[49] MÉTRICA. Versión 3. Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información. Ministerio de Administraciones Publicas 2002. CSIAE.[Consulta 9 de junio de 2003] http://www.map.es/csi/metrica3/index.html

[50] Cuarto informe anual situación de la protección de las personas en lo que respecta al tratamiento de datos personales y a la protección de la vida privada en la comunidad y en terceros países relativo al año 1999. 5019/02/es WP 46. [consulta: 11 junio de 2003] http://www.aece.org/docs/recogida.datos.internet.wp29.pdf

[51] COBRA ISO 17799 COMPLIANCE & SECURITY RISK ANALYSIS [consulta 11 junio de 2003] http://www.iso17799software.com/download.htm

[52] Alerta-antivirus centro de atención temprana de virus y seguridad informática. Ministerio de Ciencia y Tecnología. [consulta 11 junio 2003] http://www.alertaantivirus.es/index.html

[53] ISECOM *Institute for security and Open methodologies OSSTMM* - Open Source Security Testing Methodology Manual [consulta 11 junio de 2003] http://www.isecom.org/

[54] Metodología del *Computer Security Resource Center* (CSRC-NIST) [consulta 12 junio de 2003] http://csrc.nist.gov/

[55] El Comité técnico del Consejo Superior de Informática de Seguridad de los Sistemas de Información y Protección de Datos Personalizados Automatizados (CITAD) [consulta 12 junio de 2003] http://www.map.es/csi/fr340001.htm

[56] OCTAVE (*Operationally Critical Threat, Asset, and Vulnerability EvaluationSM*) [consulta 12 junio de 2003] URL: http://www.cert.org/octave/

Referencias:

[57] Documento de seguridad. Manual Práctico. Martín Manent González. Derecho.com 2003 .ISBN 84-95996-05-7

[58] Las Tecnologías de la Sociedad de la Información en la Empresa Española, 2002. SEDISI. [Consulta 8 junio de 2003] http://www.sedisi.es/05_index.htm

[59] SSITAD – seguridad y legislación. Ministerio de Administraciones Públicas, [consulta 14 junio de 2003] http://www.csi.map.es/csi/pg6000.htm

[60] Adopción de un programa plurianual (2003-2005) para el seguimiento del Plan eEurope, la difusión de las mejores prácticas y la mejora de las redes y la seguridad de la información (MODINIS)". Propuesta de Decisión del Consejo (COM(2002) 425 final) (Julio 2002) (en inglés) [consulta 14 de junio de 2003] http://www.csi.map.es/csi/pdf/modenis_en.pdf

[61] La protección de datos personales. La solución en entornos Microsoft. D. Gonzalo Gallo Ruiz, D. Iñigo Coello de Portugal Martínez del Peral, D. Fernando Parrondo García, D. Héctor Sánchez Montenegro. 2003 [consulta 12 junio 2003] http://www.microsoft.com/spain/technet/seguridad/otros/libro_lopd.asp

[62] I Programa sectorial ANEI de gestión de la Seguridad de la Información. Mario López de Ávila Muñoz. 2002 [consulta 6 junio de 2003. http://www.a-nei.org/documentos/PS17799.pdf

[63] Satan 1.1.1 Dan Farmer and Wietse Venema [consulta 6 junio de 2003] http://www.trouble.org/satan/ plataformas: Linux, Solaris

[64] Tripwire 2.3.1-2 Tripwire, Inc. info@tripwire.com [consulta 6 de junio de 2003] http://www.tripwire.org plataforma: Linux

[65] INFORMÁTICA FORENSE : GENERALIDADES, ASPECTOS TÉCNICOS Y HERRAMIENTAS Autores : Óscar López, Haver Amaya, Ricardo León Coautora : Beatriz Acosta Universidad de Los Andes

[66] Equipo de Seguridad para la Coordinación de Emergencias en Redes Telemáticas [consulta 5 de junio de 2003] http://escert.upc.es/

[67] Máquinas trampas y análisis forense. F.J. Monserrat Coll Equipo de seguridad de Red Iris. J.M. Navarro Meseguered. Universidad de Murcia. Boletín de la red nacional de I+D, Rediris, nº 61, septiembre 2002

17 Anexo A: Estándares internaciones ISO

El Comité Técnico ISO que trata sobre seguridad en las tecnologías de la Información es el **JTC 1 / SC 27**. El número de estándares publicados son de 47. El comité está dividido en tres grupos de trabajo

Grupos de trabajo	Título
JTC 1/SC 27/WG 1	*Requirements, security services and guidelines*
JTC 1/SC 27/WG 2	*Security techniques and mechanisms*
JTC 1/SC 27/WG 3	*Security evaluation criteria*

Relación de estándares: Fuente: http://www.iso.ch/

NORMA	DESCRIPCIÖN
ISO/IEC 7064:2003	Information technology -- Security techniques -- Check character systems
ISO 8372:1987	Information processing -- Modes of operation for a 64-bit block cipher algorithm
ISO/IEC 9796-2:2002	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms
ISO/IEC 9796-3:2000	Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms
ISO/IEC 9797-1:1999	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
ISO/IEC 9797-2:2002	Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
ISO/IEC 9798-1:1997	Information technology -- Security techniques -- Entity authentication -- Part 1: General
ISO/IEC 9798-2:1999	Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms
ISO/IEC 9798-3:1998	Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques
ISO/IEC 9798-4:1999	Information technology -- Security techniques -- Entity authentication -- Part 4: Mechanisms using a cryptographic check function
ISO/IEC 9798-5:1999	Information technology -- Security techniques -- Entity authentication -- Part 5: Mechanisms using zero knowledge techniques
ISO/IEC 9979:1999	Information technology -- Security techniques -- Procedures for the registration of cryptographic algorithms
ISO/IEC 10116:1997	Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
ISO/IEC 10118-1:2000	Information technology -- Security techniques -- Hash-functions -- Part 1: General
ISO/IEC 10118-2:2000	Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher

Anexo A: Estándares internaciones ISO

NORMA	DESCRIPCIÖN
ISO/IEC 10118-3:2003	Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
ISO/IEC 10118-4:1998	Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic
ISO/IEC 11770-1:1996	Information technology -- Security techniques -- Key management -- Part 1: Framework
ISO/IEC 11770-2:1996	Information technology -- Security techniques -- Key management -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 11770-3:1999	Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC TR 13335-1:1996	Information technology -- Guidelines for the management of IT Security -- Part 1: Concepts and models for IT Security
ISO/IEC TR 13335-2:1997	Information technology -- Guidelines for the management of IT Security -- Part 2: Managing and planning IT Security
ISO/IEC TR 13335-3:1998	Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
ISO/IEC TR 13335-4:2000	Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards
ISO/IEC TR 13335-5:2001	Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security
ISO/IEC 13888-1:1997	Information technology -- Security techniques -- Non-repudiation -- Part 1: General
ISO/IEC 13888-2:1998	Information technology -- Security techniques -- Non-repudiation -- Part 2: Mechanisms using symmetric techniques
ISO/IEC 13888-3:1997	Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques
ISO/IEC TR 14516:2002	Information technology -- Security techniques -- Guidelines for the use and management of Trusted Third Party services
ISO/IEC 14888-1:1998	Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General
ISO/IEC 14888-2:1999	Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Identity-based mechanisms
ISO/IEC 14888-3:1998	Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Certificate-based mechanisms
ISO/IEC 14888-3:1998/Cor 1:2001	
ISO/IEC 15292:2001	Information technology - Security techniques - Protection Profile registration procedures
ISO/IEC 15408-1:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
ISO/IEC 15408-2:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements

Anexo A: Estándares internaciones ISO

NORMA	DESCRIPCIÖN
ISO/IEC 15408-3:1999	Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements
ISO/IEC 15816:2002	Information technology -- Security techniques -- Security information objects for access control
ISO/IEC 15945:2002	Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures
ISO/IEC 15946-1:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General
ISO/IEC 15946-2:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 2: Digital signatures
ISO/IEC 15946-3:2002	Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 3: Key establishment
ISO/IEC TR 15947:2002	Information technology -- Security techniques -- IT intrusion detection framework
ISO/IEC 17799:2000	Information technology -- Code of practice for information security management
ISO/IEC 18014-1:2002	Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework
ISO/IEC 18014-2:2002	Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens
ISO/IEC 21827:2002	Information technology -- Systems Security Engineering -- Capability Maturity Model (SSE-CMM®)

18 Anexo B: Glosario según la Norma UNE 71501 IN

activo: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

amenaza: Evento que puede desencadenar un incidente en la Organización, produciendo daños o pérdidas materia- les o inmateriales en sus activos.

análisis de riesgos: Proceso que permite la identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como "activos"), para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

autenticidad: Característica que se refiere a la comprobación y confirmación de la identidad real de los activos (procesos, sistemas, información) y/o actores (usuarios) y/o de la autorización por parte de los autorizadores, así como la verificación de estas tres cuestiones.

confidencialidad: Característica que evita el acceso o la divulgación de activos del dominio (información) a individuos, entidades o procesos no autorizados. Concierne sobre todo a activos de tipo información, y a menudo se relaciona con la intimidad o "privacidad", cuando esa información se refiere a personas físicas, contemplada en la LOPD, Ley Orgánica de Protección de Datos 15/1999

controles básicos: Conjunto mínimo de salvaguardas establecidas para un sistema o una organización

disponibilidad: Característica que previene contra la denegación no autorizada de acceso a los activos. La disponibilidad se asocia a la fiabilidad técnica (tasa de fallos) de los componentes del sistema de información.

fiabilidad: Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

gestión de riesgos: Proceso basado en los resultados obtenidos en el análisis de riesgos, que permite seleccionar e implantar las medidas o "salvaguardas" de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados reduciendo de esta manera al mínimo su potencialidad o sus posibles perjuicios.

impacto: Consecuencia sobre un activo de la materialización de una amenaza.

integridad: Característica que previene contra la modificación o destrucción no autorizadas de activos del dominio. La integridad está vinculada a la fiabilidad funcional del sistema de información (o sea su eficacia para cumplir las funciones del sistema de organización soportado por aquél) y suele referirse (aunque no siempre) a activos de tipo información. Por ejemplo, son típicos los problemas causados por la amenaza de un virus (llegado con un disquete externo o a través de la red) a la integridad de los datos almacenados en el disco duro de un ordenador personal.

política de seguridad de TI: Conjunto de normas reguladoras, reglas y prácticas, que determinan el modo en que los activos, incluyendo la información considerada como sensible, son gestionados, protegidos y distribuidos dentro de una organización.

responsabilidad: Propiedad de una entidad que garantiza que las acciones de ésta (como violaciones o intentos de violación de la seguridad) queden asociadas inequívocamente a ella.

riesgo: Es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio (conjunto de activos) o en toda la organización.

riesgo residual: Es el riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.

salvaguarda: Acción, procedimiento **o** dispositivo, físico o lógico que reduce el riesgo.

seguridad de TI: Conjunto de aspectos relacionados con la autenticidad, confidencialidad, integridad y disponibilidad.

vulnerabilidad: Debilidad de un activo que puede ser explotada por una amenaza para materializar una agresión sobre dicho activo.

19 Anexo C: Definiciones de conceptos de la Ley Orgánica 15/1999 y del Real Decreto 994/1999

Tanto la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y, Real Decreto 994/1999, de 11 de junio de Medidas de Seguridad, recogen en su articulado definiciones de conceptos que facilitan la comprensión de estas leyes.

Datos de carácter personal: toda información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, susceptible de recogida, registro, tratamiento o transmisión concerniente a una persona física identificada o identificable.

Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento.

Identificación del afectado: cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, psíquica, económica, cultural o social de la persona física afectada.

Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.

Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.

Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

Cesión de datos: toda obtención de datos resultante de la consulta de un fichero, su interconexión con otros ficheros y la comunicación de datos realizada por una persona distinta de la afectada.

Transferencia de datos: el transporte de datos entre sistemas informáticos por cualquier medio de transmisión, así como el transporte de soportes de datos por correo o por cualquier otro medio convencional.

Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Datos accesibles al público: datos que se encuentran a disposición del público en general, no impedida por cualquier norma limitativa, y están recogidos en medios tales como censos, anuarios, bases de datos públicas, repertorios de jurisprudencia, archivos de prensa, repertorios telefónicos o análogos, así como los datos publicados en forma de listas de personas pertenecientes a grupos profesionales que contengan únicamente los nombres, títulos, profesión, actividad, grados académicos, dirección e indicación de su pertenencia al grupo.

Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.

Sistemas de información: conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Usuario: sujeto o proceso autorizado para acceder a datos o recursos.

Recurso: cualquier parte componente de un sistema de información.

Accesos autorizados: autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

Identificación: procedimiento de reconocimiento de la identidad de un usuario.

Autenticación: procedimiento de comprobación de la identidad de un usuario.

Control de acceso: mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Contraseña: información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

Incidencia: cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Soporte: objeto físico susceptible de ser tratado en un sistema informático y sobre el cual se pueden grabar o recuperar datos.

Responsable de seguridad: persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

Copia del respaldo: copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

20 Anexo D: sitios de seguridad

En estas direcciones hay antivirus el línea

www.pandasoftware.es (*panda active scan*)

http://es.trendmicro-europe.com/enterprise/products/housecall.php

www.trendmicro.es (products housecall)

http://www.zonavirus.com/Antivirus_on_line.asp lista de antivirus *on line*

http://www.ravantivirus.com/scan/indexn.php

http://scan.sygatetech.com/prestealthscan.html

http://www.bitdefender.com/scan/licence.php

SNORT http://www.snort.org/

http://www.spychecker.com/

Anexo D: sitios de seguridad

http://www.hormiga.org/hack/scaners.htm

NESSUS: http://www.nessus.org/

NMAP: http://www.insecure.org/nmap/ y http://www.insecure.org/links.html

Landguard: http://www.gfi.com/lannetscan/index.htm

Shadow Security Scanner: http://www.safety-lab.com/en/

RETINA: www.eeye.com

http://www.securityfocus.com/ Excelente sitio de seguridad

Centro de Alertas del MAP http://www.map.es/csi/pg7060.htm

Servicio de seguridad IRIS-CERT http://www.rediris.es/cert

Para detección de problemas de seguridad en centros de Red-IRIS y actuación coordinada para resolverlos Universidad Politécnica de Cataluña http://escert.upc.es

Sitio con listas de distribución e información sobre la ISO 17799

http://www.ictnet.es/ICTnet/cv/comunidad.jsp?area=tecInf&cv=sgsi

www.microsoft.com/spain/seguridad

ISO 17799 Directory www.iso-17799.com

Information Systems Auditand Control Association www.isaca.org

National Institute of Standards and Technology www.nist.gov

Disaster Recovery Journal www.drj.com

Business Continuity Institute www.thebci.org

Contingency Planning Exchange Inc www.cpeworld.org

Contingency Planning World www.business-continuity-world.com

Disaster Recovery Institute International www.drii.org

Globalcontinuity www.globalcontinuity.com

www.agenciaprotecciondatos.org

www.delitosinformaticos.com

www.ips.es

www.ipsca.com

http://www.criptonomicon.com/

http://www.iana.org/assignments/port-numbers relación de puertos

http://www.simovits.com/nyheter9902.html relación de puertos usados por los troyanos más frecuentas

http://scan.sygate.com/ escan de seguridad

http://www.iec.csic.es/criptonomicon/default2.html criptonomicon

21 Anexo E: Direcciones de interés de Criterios Comunes

Common Criteria

http://www.commoncriteria.org

Consejo Superior de Informática, SISTAD

http://www.map.es/csi/pg6000.htm

Anexo E: Direcciones de interés de Criterios Comunes

Perfiles de Protección Evaluados

http://www.radium.ncsc.mil/tpep/library/protection_profiles/index.html

http://niap.nist.gov/cc-scheme/PPRegistry.html

Productos Comerciales Evaluados

http://www.commoncriteria.org/epl/index.html