SEGURIDAD INFORMÁTICA

2º DE SISTEMAS MICROINFORMÁTICOS Y REDES

Noelia Huguet Chacón

TOBALCAIDE

TEMA 1: SEGURIDAD INFORMÁTICA

1. Visión global de la seguridad informática
   - 1.1 Objetivos y riesgos de la seguridad
   - 1.2 Planes de seguridad
   - 1.3 Tecnologías de la seguridad
   - 1.4 Estándares de la seguridad
2. Seguridad física y lógica
   - 2.1 Seguridad física
   - 2.2 Seguridad lógica
   - 2.3 Niveles de seguridad para los SO
   - 2.4 Análisis forense

1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

- Llamamos **seguridad informática** al conjunto de medidas preventivas y reactivas que posibilitan la protección de la información con objeto de conseguir una elevada fiabilidad del sistema informático.
- No es posible garantizar la total seguridad de un sistema, por ello se suele hablar de fiabilidad o confiabilidad como el grado de seguridad que se puede alcanzar en un sistema, una vez adoptado un conjunto de medidas.

1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

- Seguridad es un concepto confuso porque se compone de muchos elementos interrelacionados entre sí, por ello el estudio de la seguridad se realiza considerando sus objetivos, que se pueden clasificar del siguiente modo:
  - Objetivos principales de la seguridad (CID en español o CIA en inglés)
  - Objetivos secundarios.

1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

- Objetivos principales (CID):
  - **Confidencialidad**. Previene que individuos, entidades o procesos no autorizados puedan interpretar la información a la que no tienen derecho.
  - **Integridad**. Previene contra posibles alteraciones no deseadas en la información, de modo, que se garantice que el mensaje enviado en origen es exactamente el mensaje que se recibe en destino.
  - **Disponibilidad**. Mantiene la capacidad de exponer los activos informáticos utilizables en todo momento a los agentes autorizados que los consumen.

1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

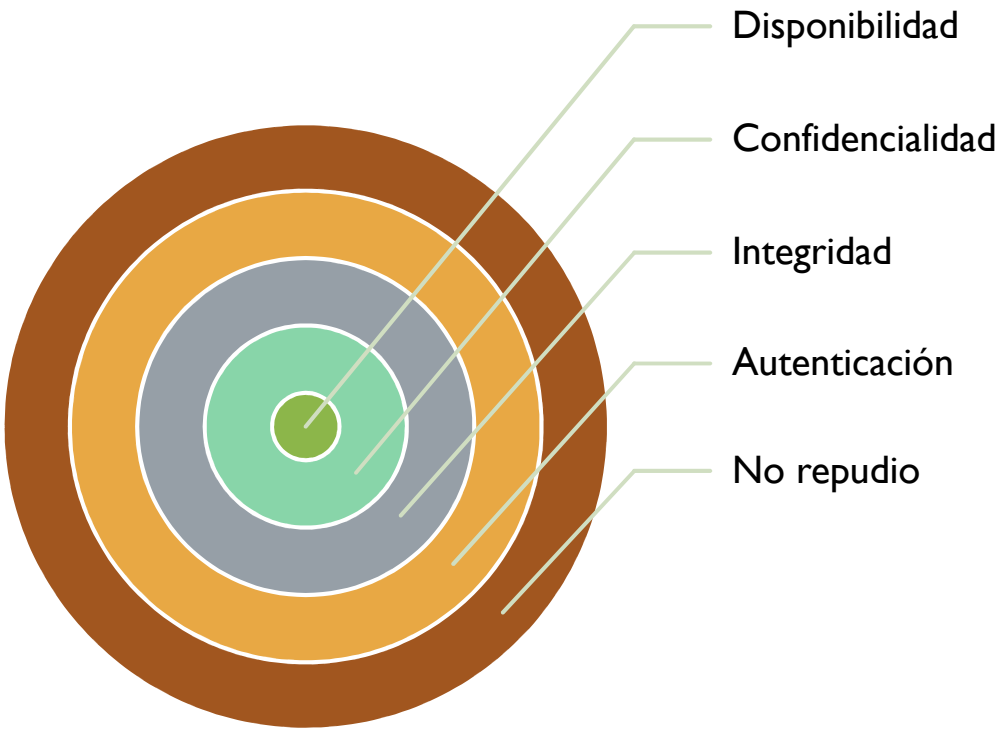
- Objetivos secundarios:
  - **Autenticidad y control de acceso**. Comprueba la identidad del agente que accede a un recurso y le facilita o deniega el acceso en función de esta identidad.
  - **Fiabilidad**. Mantiene la consistencia entre el comportamiento del sistema y los resultados obtenidos del mismo, es decir, evalúa si el sistema se comporta como se espera de él.
  - **No repudio o irrenunciabilidad**. Garantiza la autoría de una información o un proceso.
  - **Auditabilidad**. Registra el comportamiento del sistema para su evaluación posterior.

1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

- Objetivos secundarios:
  - **No repudio o irrenunciabilidad.** Es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación. La diferencia esencial con la autenticación es que la primera se produce entre las partes que establecen la comunicación y el servicio de no repudio se produce frente a un tercero, de este modo, existirán dos posibilidades:
    - **No repudio en origen:** el emisor no puede negar el envío porque el destinatario tiene pruebas del mismo, el receptor recibe una prueba infalsificable del origen de envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.
    - **No repudio en destino:** el receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

- **CIDAN** (las iniciales de los 5 objetivos más importantes de la seguridad).
- Relación de los diferentes servicios de seguridad, unos dependen de otros jerárquicamente, así no existe el de más abajo, no puede aplicarse el superior.
- De esta manera, la disponibilidad se convierte en el primer requisito de seguridad, cuando existe ésta, se puede disponer de confidencialidad, que es imprescindible para conseguir integridad, para poder obtener autenticación es imprescindible la integridad y por último el no repudio sólo se obtiene si se produce previamente la autenticación.



1.1 VISIÓN GLOBAL DE LA SEGURIDAD INFORMÁTICA

- La **estrategia de seguridad** se establece mediante políticas, controles de seguridad, tecnologías y procedimientos que detectan amenazas y que tratan de evitar o paliar los riesgos que conllevan estas amenazas.
- La seguridad de la información requiere la implementación de estrategias para cada uno de los procesos en donde debe tenerse en cuenta que "**la información es el activo primordial que debe protegerse**".
- En un contexto profesional, la seguridad de un sistema se refleja en un documento denominado **Plan de Seguridad** que contiene todas las especificaciones necesarias para conseguir el aseguramiento del sistema.
- El responsable de seguridad de un sistema debe formularse una serie de preguntas relacionadas con la seguridad sobre las que reflexionar para conseguir un plan de seguridad eficiente.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

- **AMENAZA**. La presencia de un factor de diversa índole (persona, máquina o suceso) que puede atacar al sistema y provocarle daños aprovechando alguna vulnerabilidad.
- **VULNERABILIDAD O BRECHA.** Es el grado de exposición del sistema amenazado a las amenazas de un ataque.
- **CONTRAMEDIDA**. Es la acción que pretende la prevención de una amenaza que actúa aprovechándose de una vulnerabilidad.
- **ATACANTE**. Es el agente activo que perpetra la amenaza que subyace a una vulnerabilidad.
- **RIESGO**. Es la valoración del daño que representan las amenazas a las que se está expuesto debido a las vulnerabilidades teniendo en cuenta las contramedidas que se implementan para la defensa.
- El riesgo se puede calcular:

$$\text{Riesgo} = \frac{\text{Amenazas x Vulnerabilidades}}{\text{Contramedidas}}$$

1.1.1 AMENAZAS RIESGOS Y ATAQUES

TIPOS DE AMENAZAS

- Dependiendo del lugar de procedencia de la amenaza (lugar en donde se sitúa el agente atacante):
  - **Amenaza interna.** Proceden del interior del sistema atacado. Los empleados o exempleados de la organización pueden realizar ataques intencionados (conocen el sistema y sus debilidades) o accidentales (causados por error o desconocimiento).
  - **Amenaza externa**. Procede del exterior del sistema atacado. Por ejemplo, el robo del servidor, una inundación o la actividad de un hacker desde Internet.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

GESTION DEL RIESGO

- Frente a un riesgo caben 4 posibilidades:
  - **Evitar el riesgo.**
  - **Reducir el riesgo.**
  - **Retener, asumir o aceptar el riesgo.**
  - **Transferir o compartir el riesgo.**

1.1.1 AMENAZAS RIESGOS Y ATAQUES

TIPOS DE AMENAZAS

- Dependiendo de la vía de ataque (el medio utilizado por el atacante para perpetrar el ataque):
  - **Amenaza física o ambiental.** Afectan al hardware o a las instalaciones en donde se ubica. Por ejemplo, una inundación, un fuego o un robo.
  - **Amenaza lógica**. Afectan al sistema en su software mediante la introducción de malware o por la ejecución de operaciones lógicas que comprometen la seguridad del sistema. Por ejemplo, un troyano o un virus.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

AMENAZAS FÍSICAS:

- **Personas**: la mayoría de los ataques a nuestro sistema van a provenir en última instancia de personas que, intencionada o no, puede causarnos enormes pérdidas.
  - **Atacantes pasivos**: aquellos que fisgonean por el sistema pero no lo modifican o destruyen.
  - **Atacantes activos**: aquellos que dañan el objetivo atacado, o lo modifican en su favor.
- **Personal**: cualquier persona de la organización, incluso el personal ajeno a la infraestructura informática puede comprometer la seguridad de los equipos.
- **Ex-empleados:** se trata de personas desconectadas con la organización que pueden aprovechar debilidades de un sistema que conocen perfectamente.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

AMENAZAS FÍSICAS:

- **Hackers**: es un término general que se ha utilizado históricamente para describir a un experto en programación. Recientemente, se ha utilizado con frecuencia con un sentido negativo, para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa, aunque no siempre tiene que ser esa finalidad.
- **Cracker**: es un término más preciso para describir a una persona que intenta obtener acceso no autorizado a los recursos de la red con intención maliciosa.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

AMENAZAS FÍSICAS:

- **Robos, sabotajes, destrucción de sistemas.**
- **Cortes, subidas y bajadas bruscas de suministro eléctrico.**
- **Condiciones atmosféricas adversas.** Humedad relativa excesiva o temperaturas extremas que afectan al comportamiento normal de los componentes informáticos.
- **Las catástrofes naturales o artificiales**, son las amenazas menos probables.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

AMENAZAS LÓGICAS:

- **Software incorrecto**: a los errores de programación se les denomina ***bugs***, y a los programas utilizados para aprovechar uno de estos fallos y atacar al sistema, ***exploits***.
- **Puertas traseras**: durante el desarrollo de aplicaciones grandes o de SO es habitual entre los programadores insertar "atajos" en los sistemas habituales de autenticación del programa o del núcleo que se está diseñando.
- **Bombas lógicas:** son partes de código de ciertos programas que permanecen sin realizar ninguna función hasta que son activadas; en ese punto, la función que realizan no es la original del programa, sino que generalmente se trata de una acción perjudicial.
- **Virus**: es una secuencia de código que se inserta en un fichero ejecutable, de forma que cuando el archivo se ejecuta, el virus también lo hace, insertándose a sí mismo en otros programas.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

AMENAZAS LÓGICAS:

- **Gusanos:** es un programa capaz de ejecutarse y propagarse por sí mismo a través de redes, en ocasiones portando virus o aprovechando bugs de los sistemas a los que conecta para dañarlos. El daño que pueden causar es muy elevado.
- **Caballos de Troya:** son instrucciones escondidas en un programa de forma que éste parezca realizar las tareas que un usuario espera de él, pero que realmente ejecute funciones ocultas sin el conocimiento del usuario.
- **Bacterias**: se conocen a los programas que no hacen nada útil, sino que simplemente de dedican a reproducirse hasta que el número de copias acaba con los recursos de sistema, produciendo una negación de servicio.

1.1.1 AMENAZAS RIESGOS Y ATAQUES

VULNERABILIDADES DE UN SISTEMA

- Todo componente de un sistema es vulnerable, a priori.
  - **El hardware.** Por ejemplo, una persona podría desconectar la alimentación de un servidor. Entre los equipos afectados por vulnerabilidades de hardware tendremos router, conmutadores y módems: cámaras web y servidores de vídeo; impresoras; teléfonos móviles…
  - **El software.** Por ejemplo, un virus podría dañar el sector de arranque del disco de sistema. Entre los elementos de software más vulnerables están los SO, servidores y bases de datos; los navegadores, las aplicaciones ofimáticas y las utilidades.
  - **Los datos.** Los datos podrían ser alterados, escuchados…

1.1.1 AMENAZAS RIESGOS Y ATAQUES

VULNERABILIDADES DE UN SISTEMA

- Para controlar y evaluar las vulnerabilidades, el responsable de seguridad cuenta con un conjunto de herramientas, procedimientos y tecnologías que le ayudan en su tarea:
  - Parches del SO y actualización de aplicaciones y utilidades.
  - Seguridad en los ficheros y control de acceso de los usuarios a los recursos.
  - Cuentas de usuarios y políticas de gestión de contraseñas.
  - Registro y auditoría de eventos.
  - Configuración de las herramientas de seguridad: antivirus, cortafuegos, copias de seguridad…
  - Test de penetración frente a ataques internos y externos.

1.1.2 PLANES DE SEGURIDAD

- La mejor solución contra un ataque es organizar una buena defensa, sobre todo a través de la prevención.
- Mantener un sistema seguro pasa por cumplir unos requisitos que básicamente se agrupan en torno a las siguientes políticas recomendadas:
  1. Tener un plan de seguridad de los sistemas de información, que debe haber sido probado antes de que se produzca un posible ataque.
  2. Respetar los códigos éticos de comportamiento personal y profesional.
  3. Proveer planes de contingencia específicos para cada activo informático, validados mediante pruebas.
  4. Disponer de un sistema eficaz de evaluación de la seguridad informática.

1.1.2 PLANES DE SEGURIDAD

- Toda la información de seguridad, las acciones preventivas y las reactivas después de sufrir un ataque se formulan en un plan de seguridad, también llamado a veces, plan de contingencia o plan de respuesta a incidentes.
- Un **plan de respuesta a incidentes** (reactivo no preventivo) tiene 4 fases:
  1. Acción inmediata para detener o minimizar el incidente de seguridad.
  2. Investigación del incidente.
  3. Restauración de los recursos afectados, dañados o comprometidos debido al incidente.
  4. Reporte del incidente y de los daños a los responsables de nivel superior.

1.1.3 TECNOLOGÍAS RELACIONADAS CON LA SEGURIDAD EN LOS SISTEMAS

- El material técnico con el que cuenta el administrador de la seguridad también es muy variado y está en constante evolución puesto que a cada nueva vulnerabilidad se abre una línea de investigación para tratar de atajarla. Por ejemplo:
  - Cortafuegos.
  - Administración de las cuentas de los usuarios y los servicios.
  - Detección y prevención de intrusos.
  - Antivirus y antimalware.
  - Infraestructura de clave pública, técnicas de cifrado y firma digital.
  - Biometría.
  - Redes privadas virtuales.
  - Técnicas de seguridad en el comercio electrónico.

1.1.4 ESTÁNDARES RELACIONADOS CON LA SEGURIDAD

- El estándar de seguridad de sistemas por antonomasia se recoge en la familia de normas ISO/IEC 27000.
- Esta norma contiene las mejores prácticas recomendadas sobre seguridad de la información para desarrollar, implementar y mantener especificaciones para los "Sistemas de Gestión de la Seguridad de la Información" (SGSI.
- Esta norma incluye la ISO/IEC 17799, que en España se denomina UNE-71501.
- La norma ISO/EIC 27000 contiene un conjunto de especificaciones.

1.1.4 ESTÁNDARES RELACIONADOS CON LA SEGURIDAD

- ISO/IEC 27000. Gestión de la Seguridad de la Información: fundamentos y vocabulario.
- ISO/IEC 27001. Especificaciones para un SGSI.
- ISO/IEC 27002. Código de buenas prácticas.
- ISO/IEC 27003. Guía de implantación de un SGSI.
- ISO/IEC 27004. Sistema de métricas e indicadores.
- ISO/IEC 27005. Guía de análisis y gestión de riesgos.
- ISO/IEC 27006. Especificaciones para organismos certificados de SGSI.
- ISO/IEC 27007. Guía para auditar un SGSI.
- ISO/IEC 2700X. Guías sectoriales.

1.2.1 SEGURIDAD FÍSICA Y AMBIENTAL

- La **seguridad física** consiste en la aplicación de contramedidas tales como barreras físicas o procedimientos de control que prevengan amenazas contra los recursos que se pretenden proteger, disminuyendo los riesgos.
- Los peligros físicos pueden ser intencionados o fortuitos.
- El **control físico de acceso** se trata de estudiar cómo será el acceso del personal a los equipos.
- El control de acceso no solo requiere la capacidad de identificación de usuarios, sino que debe proveer los mecanismos automáticos o domóticas para asociar la identificación de un sujeto con la apertura selectiva de puertas, el registro de acceso o la gestión de la respuesta de acceso en función de un horario.
- Las medidas de control físico de acceso deben ser conocidas por todos ya que tienen un propósito disuasorio.

1.2.1 SEGURIDAD FÍSICA Y AMBIENTAL

- Algunas de las técnicas de control de acceso son las siguientes:
  - Utilizar personal de seguridad y/o animales.
  - Detectores de metales.
  - Utilización de sistemas biométricos.
  - Sistemas de verificación automática de firma.
  - Sistemas de protección electrónica.
- El control del ambiente y el del acceso físico permite disminuir siniestros, generar la sensación de seguridad en el trabajo, disolver mejor las circunstancias en las que se producen los incidentes y disponer de medios más eficaces para disminuir los riesgos, incrementando la capacidad de tomar decisiones acertadas en momentos críticos para la seguridad.

1.2.2 SEGURIDAD LÓGICA

- La seguridad lógica consiste en la aplicación de barreras y procedimientos que protejan el acceso a los datos y aplicaciones a personas o agentes autorizados para ello, descartando a los demás.
- El aforismo clave para mantener la seguridad lógica, y que debe quedar claro en todos los niveles de la organización, es que "**todo lo que no está permitido debe estar expresamente prohibido".**
- El administrador de seguridad debe trabajar de modo que cualquier permiso o derecho de un usuario debe ser expresamente concedido, es decir, "todo lo que no está expresamente concedido, está implícitamente denegado".

1.2.2 SEGURIDAD LÓGICA

- **Las técnicas de seguridad lógica** persiguen los siguientes objetivos:
  - Restringir el acceso a los activos informáticos de software.
  - Garantizar que todo usuario puede acceder a los datos o aplicaciones que necesita, pero solo a los que necesita.
  - Asegurar que con cada información o dato con el que se trabaje se emplea el procedimiento adecuado y no alternativas no autorizadas.
  - Cuidar la integridad, confidencialidad y no repudio en las comunicaciones de mensajes.
  - Buscar alternativas redundantes para situaciones de fallos en equipos, por ejemplo, líneas de transmisión alternativas, pero controladas.
  - Tener la capacidad de restaurar los sistemas de información en poco tiempo después de un incidente a partir de backups, si fuera necesario.
  - Implementar sistemas redundantes de reparto de carga y alta disponibilidad.
  - Garantizar la continuidad del negocio.

1.2.2 SEGURIDAD LÓGICA

- **El control lógico de acceso** se pueden aplicar en los SO, en las aplicaciones, en las bases de datos o en cualquier elemento de software sobre los que se puedan definir alguno de los objetivos descritos anteriormente.
- Además, hay que tener en cuenta cuál será el procedimiento por el que un usuario puede solicitar un permiso para el acceso a un activo de software y cómo se decidirá si se le concede o no
- Esto suele ser complicado porque requiere la intervención activa de varios departamentos, no necesariamente técnicos.

1.2.2 SEGURIDAD LÓGICA

- **La NIST (National Institute for Standards and Technology)** ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad de cualquier sistema:
  - **Identificación y Autenticación.** Todos usuario debe ser identificado antes de concederle acceso mediante un proceso de autenticación suficientemente seguro.
  - **Roles**. Define el perfil de necesidades y obligaciones del usuario. En función del rol que desempeñe en la organización tendrá derecho o no a determinados servicios.
  - **Transacciones**. Para realizar ciertas operaciones delicadas es necesario disparar un procedimiento de seguridad específico, por ejemplo, disponer de contraseña.
  - **Limitaciones a los servicios**. Son los procesos de autorización que se siguen de una autenticación de usuario, que le autorizan a consumir ciertos servicios en función de su rol en la organización.

1.2.2 SEGURIDAD LÓGICA

- **Modalidad de acceso.** El acceso al dato será de lectura, ejecución, borrado… es decir, la modalidad de acceso define las operaciones permitidas sobre los datos y las aplicaciones.
- **Ubicación y horario.** Establece las restricciones de acceso a los recursos en función de un horario o calendario, o desde ciertas ubicaciones.
- **Control de acceso interno.** Contraseñas, métodos aceptables de cifrado, listas de control de acceso (ACL)…
- **Control de acceso externo.** Paso por contrafuegos, pasarelas de comunicaciones, creación de túneles…
- **Administración.** Recursos Humanos, definición de los puestos laborales, organización de personal…

1.2.3 NIVELES DE SEGURIDAD PARA SISTEMAS OPERATIVOS

- El estándar de niveles de seguridad para SO originario se describe en el **TCSEC** Orange Book de 1985.
- Cada sistema comercial sigue los estándares que más le benefician, dejando a TCSEC como un elemento de referencia.
- Los fabricantes someten sus productos a evaluación para establecer sus niveles estándar de seguridad, de modo que certifican sus productos en relación con unos patrones de seguridad de referencia.
- El estándar define varios niveles y subniveles de seguridad, cada uno de los cuales incluye a todos los anteriores.
- El nivel A implica mayor seguridad que B, y B2 es más seguro que B1 (subniveles dentro del mismo nivel)
- Estos niveles de seguridad han sido la base de desarrollo para otros estándares europeos como el ITSEC/ITSEM y los internacionales propuestos por la ISO/IEC.

1.2.3 NIVELES DE SEGURIDAD PARA SISTEMAS OPERATIVOS

- Características básicas de algunos de los niveles, en orden creciente de seguridad.

1. **Nivel D, sin protección**. Es el nivel de más baja seguridad. No cumplen ninguna especificación de seguridad, por tanto, son sistemas no confiables.
2. **Nivel C1, protección discrecional.** Requiere la autenticación de usuarios, quienes pueden manejar su propia información privada por separado. También permite la distinción de un usuario privilegiado que tiene la responsabilidad de la seguridad del sistema.
3. **Nivel C2, protección de acceso controlado**. Es una ampliación del nivel C1 que incorpora un sistema de auditoría de accesos e intentos fallidos de acceso o autorización. Permite establecer varios niveles de autorización (y no solo dos (usuario y superusuario) como en C1, por tanto, habrá usuarios que sin ser superusuarios podrán realizar algunas tareas restringidas de administración.

1.2.3 NIVELES DE SEGURIDAD PARA SISTEMAS OPERATIVOS

4. **Nivel B1, seguridad etiquetada.** Establece una seguridad multinivel repartida entre las distintas capas del sistema se le asigna una etiqueta que luego se asocia a un modelo de seguridad y que permitirá o no al usuario identificado el acceso a ese objeto.
5. **Nivel B2, seguridad estructurada.** Es una ampliación del B1 en la que se gestiona la herencia de permisos en objetos que están jerarquizados.
6. **Nivel B3, dominios de seguridad.** En este nivel se añaden, entre otros elementos, una auditoría exhaustiva sobre todas las estructuras de seguridad. También refuerza los dominios de seguridad con la instalación de hardware.
7. **Nivel A1, protección verificada**. Es el nivel más elevado que incluye procesos de diseño, control y verificación definidos mediante métodos matemáticos para asegurar todos los procesos del sistema. El software y hardware deben protegerse para evitar infiltraciones ante traslados o movimientos del equipamiento.

1.2.3 NIVELES DE SEGURIDAD PARA SISTEMAS OPERATIVOS

- La mayoría de los SO comerciales están por encima del nivel C2, aunque frecuentemente se añaden módulos específicos de seguridad para incrementar el nivel bajo ciertos aspectos operativos.

Niveles de seguridad del TCSEC						
SIN SEGURIDAD	Nivel D					
SEGURIDAD SIMPLE		Nivel C1	Nivel C2			
SEGURIDAD MULTINIVEL			Nivel B1	Nivel B2	Nivel B3	Nivel A1

1.2.3 NIVELES DE SEGURIDAD PARA SISTEMAS OPERATIVOS

- El estándar **ITSEC White Book** es el europeo, de 1991.
  - Define 10 clases de funcionalidades de las que 5 son equivalentes a las de TCSEC.
  - Las otras 5 funcionalidad están orientadas a aplicaciones en vez de a SO.
- El tercer tipo de estándar, mucho más actual y de mayor interés para los fabricantes es el **Common Criteria.**
  - Este estándar, creado en 1996, establece criterios comunes para Europa y EEUU como una iniciativa común para armonizar TCSEC o ITSEC.
  - La versión actual es la 3.1.

1.2.3 NIVELES DE SEGURIDAD PARA SISTEMAS OPERATIVOS

- El **Common Criteria** define un conjunto de niveles de seguridad o EALs entre los que podemos encontrar los siguientes:
  1. **Nivel EAL1.** Es el nivel básico en el que se evalúa la utilización apropiada de las funciones de seguridad, pero no su correcta implantación en el sistema.
  2. **Nivel EAL2.** Es el nivel moderado de seguridad. Se analizan las funciones de seguridad utilizando una batería de especificaciones funcionales.
  3. **Nivel EAL3.** Es el nivel medio de seguridad. Se analizan las funciones de seguridad y su diseño a alto nivel.
  4. **Nivel EAL4.** Es el nivel de alta seguridad en la que se añade a EAL3 el análisis del diseño a bajo nivel, es decir, su implantación. Es este nivel residen la mayor parte de los SO comerciales, por lo que podemos afirmar que si están actualizados y bien configurados son, en general, bastante seguros.

1.2.4 ANÁLISIS FORENSE

- No siempre las medidas tomadas para contrarrestar las amenazas son totalmente eficaces.
- El **análisis forense** se ocupa de que hay que hacer cuando se ha producido un ataque, se orienta a rastrear en el sistema comprometido, puesto offline, toda la información posible sobre el ataque de modo que se pueda diseñar una contramedida apropiada para evitarlo en el futuro o para determinar el agente que perpetró el ataque, así como una evaluación de los daños sufridos.
- Un análisis forense consta de las siguientes fases:
  1. **Identificación y evaluación del incidente (access)**
  2. **Preservación de la incidencia o adquisición de los datos (acquiere)**
  3. **Análisis de la evidencia (analyze)**
  4. **Documentación y reporte del incidente (report)**

1.2.4 ANÁLISIS FORENSE

Investigación y evaluación

- Notificaciones
- Autorizaciones
- Revisión de políticas
- Revisiones legales
- Preparación para examinar las evidencias

Adquisición de datos

- Herramientas de investigación
- Recoger datos
- Almacenar y archivar datos

Análisis de datos

- Analizar datos de red
- Analizar datos de host
- Analizar los medios de almacenamiento

Reportes

- Elección y organización de los reportes necesarios
- Confección de los reportes a partir de los datos

Siempre:
Preservar datos originales y custodiar las evidencias.
Documentar todas las fases del proceso.