CAPÍTULO1.
PRINCIPIOS DE SEGURIDAD Y ALTA DISPONIBILIDAD

Autor: Jesús Costas Santos

SEGURIDAD Y ALTA DISPONIBILIDAD

Índice de contenidos

SEGURIDAD Y ALTA DISPONIBILIDAD

1.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- Hoy en día un sistema informático totalmente seguro es imposible, la conectividad global, extiende el campo de posibles amenazas.

- *La seguridad informática: asegurar que los recursos del sistema de información sean utilizados de la manera que se decidió y que el acceso y modificación a la información, solo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización.*

SEGURIDAD Y ALTA DISPONIBILIDAD

1.1 INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

- **Objetivos** de la seguridad informática:
  - Detectar los posibles problemas y amenazas.
  - Garantizar la adecuada utilización de los recursos y de las aplicaciones de los sistemas.
  - Limitar las pérdidas y conseguir una adecuada recuperación en caso de un incidente.
  - Cumplir con el marco legal y con los requisitos impuestos a nivel organizativo.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- **Seguridad absoluta no es posible**
- Seguridad informática: **técnicas** para obtener **altos niveles de seguridad** → FIABILIDAD.
- Sistema seguro (o fiable), garantizar CIDAN: Confidencialidad, Integridad y Disponibilidad + Autenticación y No Repudio.

SEGURIDAD Y ALTA DISPONIBILIDAD

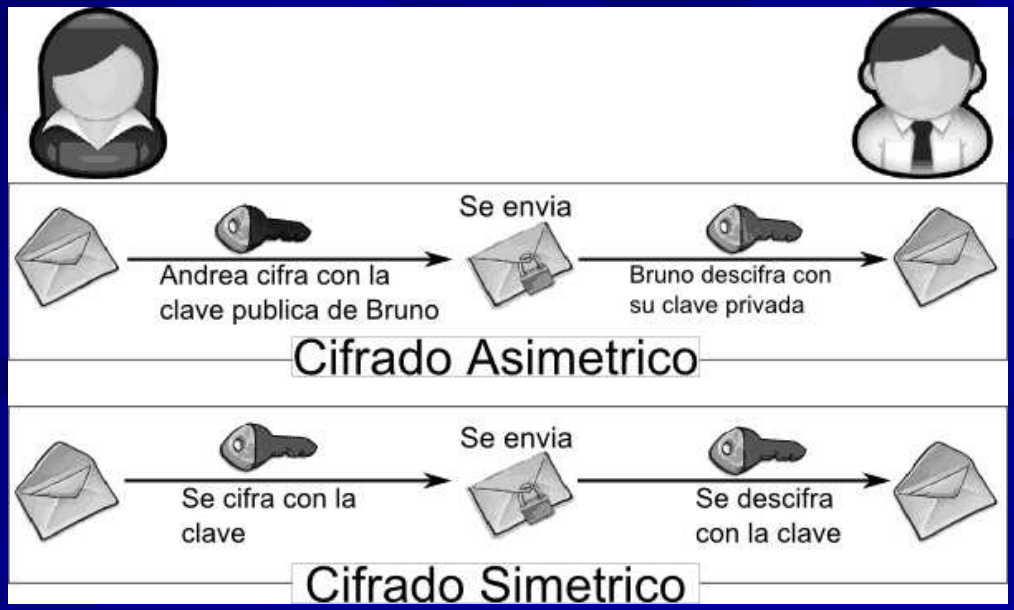
1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- **Confidencialidad**: privacidad o protección de información o comunicación.
- **Integridad**: comprobar que no ha sido alterada cierta información o comunicación.
- **Disponibilidad**: capacidad de un servicio, datos o sistema, a ser accesible.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.2 CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

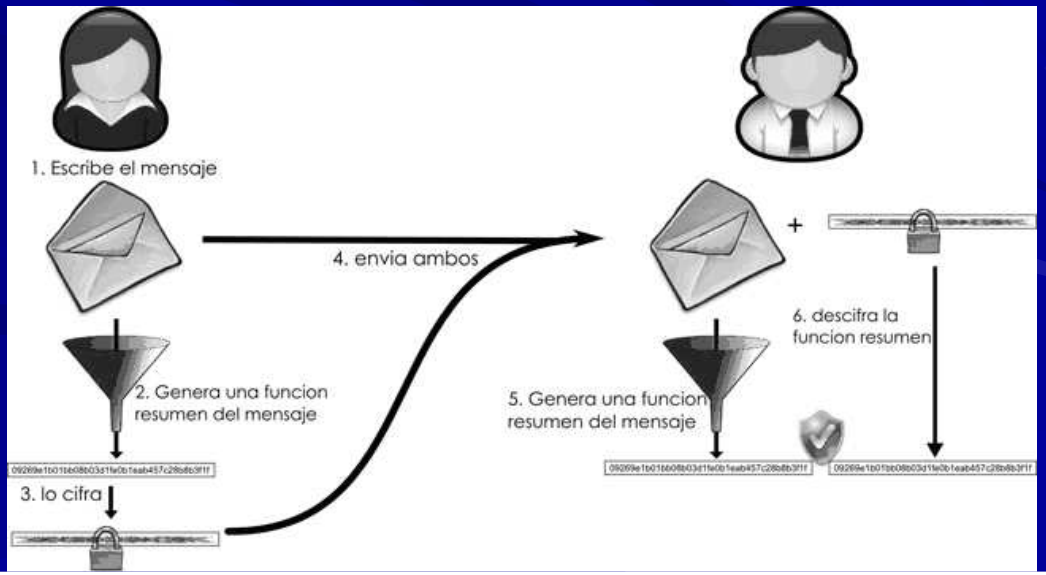
- **Ejemplos Confidencialidad**:
  - EFS. Cifrado de archivos en sistema operativo Windows.
  - Cifrado asimétrico/simétrico en comunicaciones



SEGURIDAD Y ALTA DISPONIBILIDAD

1.2 CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- **Ejemplos de Integridad**:
  - Comprobación de integridad, no falsificación o modificación, de archivos del sistema (anti-rootkit). Windows (SFC) – GNU/Linux (Rootkit Hunter)
  - Firma digital y funciones resumen o hash en comunicaciones.



SEGURIDAD Y ALTA DISPONIBILIDAD

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- **Ejemplos de Disponibilidad**:
  - Comprobación de disponibilidad de servicios, protocolos y aplicaciones inseguras: NMAP, NESSUS, MBSA, etc.
  - Alta disponibilidad (*High Availability*): **aplicaciones y datos se encuentren operativos para los usuarios autorizados en todo momento y sin interrupciones**, **carácter crítico**.
  - **M**antener sistemas funcionando 24 horas, 7 días, 365 días a salvo de interrupciones. El mayor nivel acepta 5 minutos de inactividad al año, disponibilidad de 5 nueves: 99,999%.
  - Ejemplo de AD: Centros de procesamiento de datos (CPD).

SEGURIDAD Y ALTA DISPONIBILIDAD

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

- **Autenticación**: verificación de la identidad de un usuario, aporta algún modo que permita verificar que es quien dice ser (credencial: usuario o *login* + contraseña o *password)*.
- **No repudio** o **irrenunciabilidad**: permite probar la participación de las partes en una comunicación. Existen dos posibilidades:
  - **No repudio en origen**: el emisor no puede negar el envío. 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. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.2 FIABILIDAD, CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

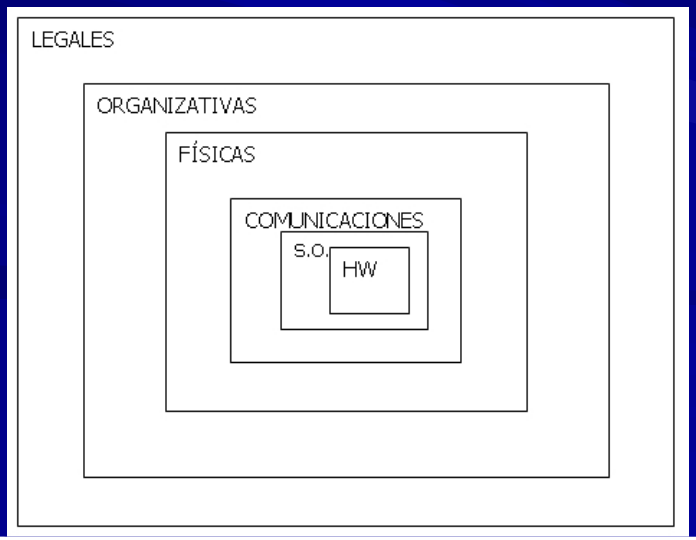
- 1º Disponibilidad de servicio. Sin ese parámetro no se pueden sustentar los otros.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.3 ELEMENTOS VULNERABLES EN EL SISTEMA INFORMÁTICO:

HARDWARE, SOFTWARE Y DATOS

- Seguridad → **problema integral.**
- Los problemas no aislados → la seguridad del sistema = punto más débil.
- Datos: principal elemento a proteger



SEGURIDAD Y ALTA DISPONIBILIDAD

1.4 AMENAZAS

- Personas:
  - Personal de una organización.
  - Hacker: White / Grey / Black (cracker)
    - Newbie / wanabber / script-kiddie / luser.
- Físicas o ambientales:
  - Robos, incendio, inundación, terremoto, cortes de suministro eléctrico, interferencias electromagnéticas, etc.
- Lógicas o de software:
  - Malware (virus, gusano, troyano,etc), rootkit, rogueware, backdoor, sw bacteria, canal cubierto, etc.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.4 AMENAZAS

- Técnicas de ataque:
  - Malware
  - Ingeniería social / Scam / Phishing
  - Botnet
  - Dos / DDos
  - Spam
  - Sniffing
  - Spoofing / Pharming
  - Password cracking / Shoulder surfing

SEGURIDAD Y ALTA DISPONIBILIDAD

1.5 PROTECCIÓN

- Auditoría: Análisis de amenazas y riesgos potenciales → Adoptar medidas de seguridad.
- **Requisitos de auditoría y sistemas de gestión de seguridad**: estándar **ISO 27001**.
- **Fases de auditoría**:
  - Enumeración de sistemas operativos, servicios, aplicaciones, topologías y protocolos de red.
  - Detección, comprobación y evaluación de vulnerabilidades.
  - Medidas específicas de corrección.
  - Recomendaciones sobre implantación de medidas preventivas.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.5 PROTECCIÓN

- Tipos **de auditoría**:
  - Interna, perimetral, test de intrusión, de código de aplicaciones, análisis forense.
- Ejemplo prácticos:
  - Auditoría wireless
  - Auditoría de acceso a sistemas operativos
  - Auditoría de acceso a datos y aplicaciones seguras.
  - Auditoría de versiones inseguras de aplicaciones y sistema operativo.

SEGURIDAD Y ALTA DISPONIBILIDAD

1.5 PROTECCIÓN

- Medidas de seguridad:
  - Recurso a proteger:
    - Seguridad física
    - Seguridad lógica
  - Momento de ponerlas en marcha:
    - Activas o preventivas: Seguridad lógica → acceso a sistemas, permisos de usuario, antimalware, criptografía, etc.
    - Pasivas o correctivas: copias de seguridad, sistemas de alimentación ininterrumpida, etc.

SEGURIDAD Y ALTA DISPONIBILIDAD

DIRECCIONES DE INTERÉS

- *INTECO* - Instituto Nacional de Tecnologías de la Comunicación:
  - www.inteco.es
- Blog y repositorio de blogs de seguridad informática de INTECO:
  - http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad
- Hispasec Sistemas: Seguridad y Tecnologías de información. Noticias diarias y resúmenes anuales de noticias de actualidad sobre seguridad informática:
  - www.hispasec.com
- Informes sobre vulnerabilidades en aplicaciones y sistemas operativos, se puede buscar información sobre las versiones de los productos de distintos fabricantes, e incluso descargar exploits de verificación.
  - www.securityfocus.com.
- Guía completa de seguridad informática
  - http://www.rediris.es/cert/doc/unixsec/unixsec.html
- Web de seguridad informática de la empresa de tecnologías de información (IT) IDG.
  - www.idg.es
- Blog de seguridad informática de la empresa Trend Micro con noticias actuales:
  - http://blog.trendmicro.es

SEGURIDAD Y ALTA DISPONIBILIDAD

DIRECCIONES DE INTERÉS

- Portal de ISO 27001 en español:
  - www.iso27000.es
- Blog sobre auditoría y seguridad informática ISO 27001:
  - http://sgsi-iso27001.blogspot.com
- Sitio web sobre seguridad informática de GNU/Linux, de Criptonomicón, un servicio ofrecido libremente desde el Instituto de Física Aplicada del CSIC:
  - http://www.iec.csic.es/CRIPTonOMICon/linux/
- Blog de la empresa de máxima seguridad S21SEC
  - http://blog.s21sec.com/
- Blogs sobre seguridad informática. Para estar a la última en novedades sobre vulnerabilidades y ataques.
  - http://www.opensecurity.es/
  - http://www.bloginformatico.com/etiqueta/seguridad-informatica
- Blog de análisis de aplicaciones de seguridad informática:
  - http://lestathijackthis.wordpress.com/
- TESIS completa sobre Seguridad informática.
  - http://www.segu-info.com.ar/tesis/

SEGURIDAD Y ALTA DISPONIBILIDAD

SOFTWARE

- **Rootkit Hunter**: Analizador de rootkit para sistemas GNU/Linux:
  - www.rootkit.nl/
- **VirusTotal**: analizador online de archivos potencialmente malware:
  - www.virustotal.com
- **NESSUS:** Aplicación que detecta vulnerabilidades tanto para sistemas y aplicaciones de Windows como GNU/Linux. En su última versión Nessus4, funciona como servidor web.
  - www.nessus.org.
- **Microsoft Baseline Security Analyzer (MBSA)**: analizador del el estado de seguridad según las recomendaciones de seguridad de Microsoft, ofrece orientación de soluciones específicas. Sirve para detectar los **errores más comunes de configuración de seguridad y actualizaciones de seguridad** que falten.
  - http://technet.microsoft.com/es-es/security/cc184924
- **NMAP**: programa de código abierto que sirve para efectuar rastreo de puertos.
  - http://www.insecure.org/nmap/
- **Microsoft Update**: para ver las últimas actualizaciones del sistema operativo Windows en caso de tenerlo instalado en nuestro equipo. Podremos hacerlo entrando con Internet Explorer 5 o superior en:
  - http://www.update.microsoft.com/
- Comprueba el estado de actualización de tus aplicaciones, con un análisis desde la web de **Secunia** y su inspector online:
  - http://secunia.com/vulnerability_scanning/online/?lang=es
- Analizador del nivel de fortaleza en tus contraseñas:
  - http://www.microsoft.com/latam/protect/yourself/password/checker.mspx

SEGURIDAD Y ALTA DISPONIBILIDAD

DIRECCIONES DE INTERÉS

- **Mantenerse siempre informado y al día es la primera y mejor recomendación en materia de seguridad informática.**
  - **Origen y evolución del eFraude**
  - http://www.securitybydefault.com/2010/01/origen-y-evolucion-del-efraude.html
  - **Los peligros más comunes para los usuarios de Internet los encontramos en las denominadas redes sociales, ya que son actualmente de las webs más usadas. Para ello se propone analizar la siguiente noticia "Cinco nuevas estafas en Facebook y Twitter".**
  - Fuente:http://www.csospain.es/Cinco-nuevas-estafas-en-Facebook-y-Twitter/seccion-alertas/articulo-196360