Seguridad en los Sistemas Informáticos
Tema 1: Introducción a la Seguridad

Grado en Ingeniería Informática

Departamento de Ingeniería Informática
Universidad de Cádiz

Curso 2024–2025

Índice

Definición de seguridad

Seguridad

Característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Fiabilidad

Probabilidad de que un sistema se comporte tal y como se espera de él.

Noticias de ciberseguridad (I)

TIEMPO DE LECTURA: **3 min.**

El acceso a la página del Servicio Público de Empleo Estatal (SEPE) no está disponible ni sus trabajadores pueden acceder al sistema interno. El **SEPE ha sufrido un ataque informático que ha paralizado los servicios** que presta a través de internet y también en las oficinas.

El hackeo ha paralizado la actividad en todo el territorio nacional. La Central Sindical Independiente de Funcionarios (CSIF) ha comunicado que **las 710 oficinas presenciales no pueden trabajar con normalidad** y que las 52 telemáticas tampoco pueden ofrecer su servicio.

De esta forma, ni los ordenadores de las oficinas ni los **dispositivos portátiles del personal que está teletrabajando** podría realizar las tareas habituales de su desempeño diario.

Figura: Un ciberataque bloquea la web del SEPE y paraliza también el servicio presencial

Noticias de ciberseguridad (II)

El ciberataque con el virus WannaCry se extiende a nivel mundial

BRUNO TOLEDANO | Madrid 12 MAY. 2017 | 21:02

117 Comentar →

Figura: El ciberataque con el virus WannaCry se extiende a nivel mundial

Noticias de ciberseguridad (III)

Un 'hackeo' a un tercero expone datos personales de un "número limitado" de clientes de Vodafone España

EP | NOTICIA | 22.11.2023 - 14:56H

- La compañía afirma que la incidencia ya ha sido resuelta e Incibe realiza recomendaciones de seguridad a los afectados.

Figura: Uno de los colaboradores de Vodafone sufre un ciberataque que expone DNI y números de cuentas bancarias

Noticias de ciberseguridad (IV)

Insomniac Games sufre un hackeo y amenazan a los autores de Marvel's Spider-Man 2 con revelar todos sus secretos

La compañía no ha confirmado el ataque, pero parece que los datos ya se han puesto a la venta en internet

Figura: Insomniac Games sufre un ataque de *ransomware*

Noticias de ciberseguridad (V)

Centro Criptológico Nacional (CCN):
`https://www.youtube.com/watch?v=BW-V9b-9sG8`

Dimensiones de la seguridad

Confidencialidad

Solo deben acceder a los objetos de un sistema los elementos autorizados.

Integridad

Los objetos solo pueden ser modificados por elementos autorizados, y de una manera controlada.

Disponibilidad

Los objetos del sistema deben permanecer accesibles a los elementos autorizados.

Tarea 1.1 - Primera parte

Aspectos de la seguridad

Dependiendo de la finalidad de un sistema, los responsables de su seguridad le deberían dar más prioridad a un aspecto u otro de los enumerados anteriormente:

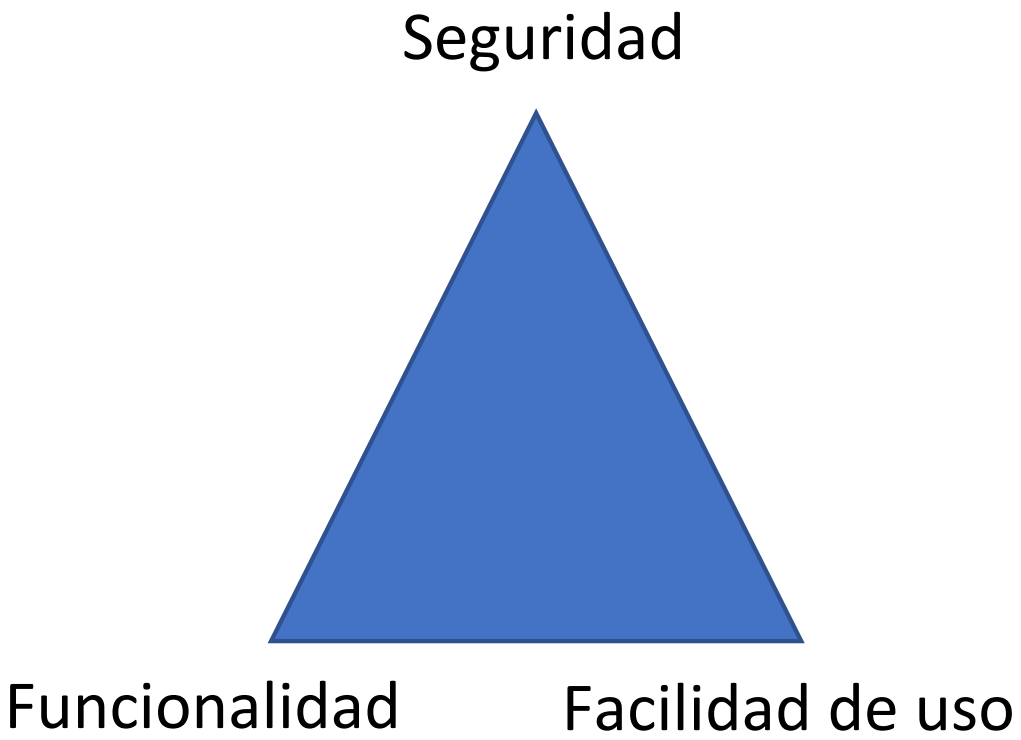
- Confidencialidad
- Integridad
- Disponibilidad

Priorización: según la situación

- ¿Cuál es más importante garantizar en un sistema militar?
- ¿Y en un sistema de un banco?
- ¿Y en un servidor de ficheros de prácticas en una universidad?

Razone sus respuestas.

Triángulo de seguridad



¿Qué queremos proteger?

Hardware

Ordenadores, periféricos, medios de almacenamiento externo.

Software

Sistema operativo, aplicaciones, etc.

Datos

- Almacenados en dispositivos de almacenamiento interno.
- Almacenados en dispositivos de almacenamiento externo.
- Los que se transmiten a través de la red.

Procedimientos

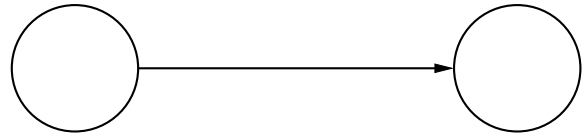
Cómo realiza la empresa las cosas.

Amenazas

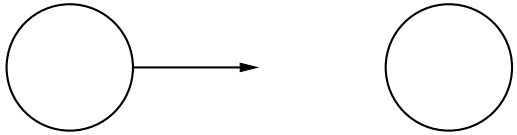
Tipos de amenazas

Interrupción	Hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
Interceptación	Un elemento no autorizado consigue acceder a un objeto del sistema.
Modificación	Un elemento no autorizado consigue modificar un objeto del sistema.
Fabricación	Un elemento no autorizado inserta objetos extraños en el sistema.

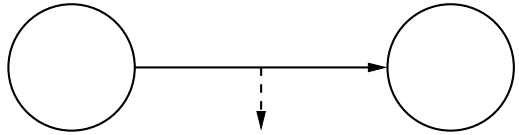
Amenazas



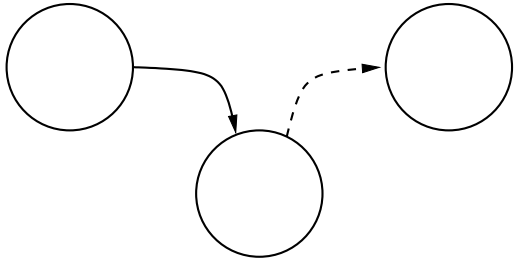
(a) Flujo normal



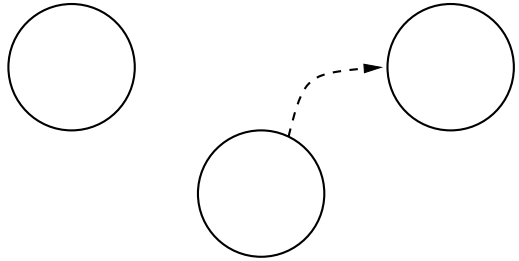
(b) Interrupción



(c) Interceptación



(d) Modificación



(e) Fabricación

Tarea 1.1 Segunda parte

Tipos de amenazas

Rellene la siguiente tabla con ejemplos de ataques a los diferentes elementos del sistema:

	Hardware	Software	Datos
Interrupción			
Interceptación			
Modificación			
Fabricación			

Relacione los tipos de amenazas con los diferentes aspectos de la seguridad.

	Confidencialidad	Integridad	Disponibilidad
Interrupción			
Interceptación			
Modificación			
Fabricación			

¿De dónde provienen las amenazas?

Personas

Tanto externas como internas a la organización.

Software

- Incorrecto: defectos de desbordamiento de *buffer*, ...
- Herramientas de seguridad
- Malicioso: Puertas traseras, virus, troyanos, ...

Catástrofes

Incendios, inundaciones, ...

Mecanismos de seguridad

¿Qué son?

Son las herramientas básicas para garantizar la protección de los sistemas de información.

Tipos

Prevención	Permiten aumentar la seguridad de un sistema durante el funcionamiento normal de este, previniendo la aparición de violaciones de la seguridad.
Detección	Permiten detectar violaciones de seguridad o intentos de violación.
Recuperación	Permiten devolver a un estado adecuado un sistema que ha sufrido un ataque de seguridad. Un *análisis forense* permite averiguar el alcance de la violación, las actividades efectuadas, la forma de entrada, etc.

Tarea 1.1 Tercera parte

Mecanismos de seguridad

Dé ejemplos de los diferentes tipos de mecanismos de seguridad:

Mecanismos	Ejemplos
Prevención	
Detección	
Recuperación	

Definiciones (I)

Política de seguridad

Es una declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran.

Plan de seguridad

Es un documento marco que establece una serie de líneas de actuación amplias. Las políticas de seguridad deben ser consistentes con las líneas establecidas en el plan.

Definiciones (II)

Procedimientos de seguridad

Las políticas de seguridad se implementan mediante procedimientos de seguridad. Estos describen cuáles son las actividades que se tienen que realizar en el sistema, en qué momento o lugar, quiénes son los responsables de su ejecución y cuáles son los controles aplicables para supervisar su correcta aplicación.

Distinción entre políticas y procedimientos de seguridad

Las políticas definen **qué** se debe proteger en el sistema, mientras que los procedimientos de seguridad describen **cómo** se debe conseguir dicha protección.

Política de seguridad (I)

Requisitos

- Debe definir claramente las responsabilidades exigidas al personal con acceso al sistema.
- Debe cumplir con las exigencias del entorno legal.
- Debe estar adaptada a las necesidades reales de cada organización.
- Debe ser revisada periódicamente para adaptarla a las nuevas exigencias de la organización y del entorno tecnológico y legal.
- Debe aplicar el principio de "Defensa en profundidad": definición e implantación de varios niveles o capas de seguridad.
- Asignación de privilegios mínimos.

Política de seguridad (II)

Colectivos implicados

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Personal del departamento de Informática y Comunicaciones.
- Miembros del equipo de Respuesta a Incidentes de Seguridad Informática, en caso de que este exista.
- Representantes de los usuarios que pueden verse afectados por las normas.
- Consultores externos expertos en seguridad informática.

Política de seguridad (III)

Información que debe contener

Cada documento que constituye una política de seguridad debe incluir la siguiente información:

- Título y codificación.
- Fecha de entrada en vigor.
- Fecha prevista de revisión o renovación.
- Ámbito de aplicación (a toda la organización o solo a un determinado departamento o unidad de negocio).
- Descripción detallada (redactada en términos claros y fácilmente comprensibles por todos los empleados) de los objetivos de seguridad.
- Persona responsable de la revisión y aprobación.
- Documento (o documentos) al que reemplaza o modifica.
- Otros documentos relacionados.

Política de seguridad (IV)

Información que debe contener (continuación)

En los procedimientos de seguridad será necesario especificar además otra información adicional:

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para verificar su correcta ejecución.

Políticas de seguridad específicas

Políticas específicas necesarias para una organización

- Política de seguridad física de las instalaciones, equipos y materiales
- Política de seguridad del personal
- Política de identificación y autenticación de usuarios
- Política de protección de la información (debe incluir una política de copias de seguridad)
- Política de protección de servidores y estaciones de trabajo
- Política de seguridad de las conexiones remotas
- Política de detección y respuesta ante incidentes de seguridad

Perímetro de seguridad

- Perímetro de red: *firewalls*, *proxies*, políticas de contraseñas...
- Seguridad física: vallas, cámaras de seguridad, cajas fuertes, guardias...

Defensa en profundidad

- Uso de varias capas de seguridad en una organización.
- Si se atraviesa el primer perímetro de seguridad, aún quedarán por atravesar otras capas.

Organismos de ciberseguridad (I)

- Agencia Española de Protección de Datos (AEPD). `https://www.aepd.es/`
- Agencia Estatal Boletín Oficial del Estado (BOE). `https://www.boe.es/`
- Centro Criptológico Nacional (CCN). `https://www.ccn.cni.es/`
- Centro Nacional para la Protección de Infraestructuras Críticas (CNPIC). `https://cnpic.interior.gob.es/`
- CERT Gubernamental Español (CCN-CERT). `https://www.ccn-cert.cni.es/`
- Computer Emergency Response Team (CERT). `https://www.cert.org/`

Organismos de ciberseguridad (II)

- Grupo de Delitos Telemáticos (GDT). `https://www.guardiacivil.es/es/institucional/Conocenos/especialidades/gdt/index.html`
- Instituto Nacional de Ciberseguridad (INCIBE). `https://www.incibe.es/`
- International Organization for Standardization (ISO). `https://www.iso.org`
- National Institute of Standards and Technology (NIST). `https://www.nist.gov/`
- National Security Agency (NSA). `https://www.nsa.gov/`

Competiciones de ciberseguridad (I)

¿Qué es un CTF?

Los CTF (*Capture The Flag*) son competiciones de ciberseguridad donde se trata de resolver algún tipo de problema de ciberseguridad con el objetivo de conseguir una cadena de texto a la que se le llama *flag*. Existen dos modalidades:

Attack-Defense En ella los participantes deben defender un servidor (parcheando vulnerabilidades del mismo) y atacar los del resto de participantes para conseguir sus *flags*.

Jeopardy Este tipo de competición es el más común. Se plantean retos relacionados con criptografía, ingeniería inversa, programación, análisis forense y explotación web, entre otras categorías.

Experiencia de CTF en la UCA: `https://hdl.handle.net/11705/JCIS/2022/017`

Competiciones de ciberseguridad (II)

Principales competiciones CTF

- **DEFCON**: Una de las conferencias de hacking más antiguas; su CTF es uno de los más respetados por la comunidad por su altísimo nivel.
- **Cybercamp**: Clasificatorio español para la selección nacional.
- **National Cyber League**: Competición multidisciplinar organizada por la Guardia Civil.
- **Google CTF**: Competición de CTF organizada por Google.
- **Pico CTF**: Competición orientada a personas que se están acercando al mundo de la ciberseguridad.

Competiciones de ciberseguridad (III)

Plataformas para aprender

- TryHackMe: Plataforma orientada a personas que están dando sus primeros pasos en el mundo de la ciberseguridad.
- **HackTheBox**: Plataforma pionera en la gamificación de la ciberseguridad, una de las más conocidas en el mundo de la ciberseguridad, centrada en seguridad ofensiva.
- **LetsDefend.io**: Plataforma centrada en el lado defensivo de la ciberseguridad.
- **MOBISEC**: Plataforma de CTF desarrollada por un profesor universitario para dar sus clases centradas en la seguridad de aplicaciones móviles.
- **CTFtime**: Liga mundial de competición donde se publican competiciones de CTF de manera semanal. Existe un *ranking* por el que equipos de todo el mundo compiten cada semana.