(IFCT0310) ADMINISTRACIÓN DE BASES DE DATOS

- **Sistemas de almacenamiento** -

institución pau casals

Seguridad y protección de los datos (Conceptos clave)

Amenazas y riesgos:

a) DEFINICIONES CLAVE
b) PRINCIPIOS DE LA CIBERSEGURIDAD
c) COMPONENTES INVOLUCRADOS EN LA CIBERSEGURIDAD
d) SISTEMAS DE PROTECCIÓN COMO MEDIDA PARA AUMENTAR LA CIBERSEGURIDAD

Amenazas y riesgos: Definiciones

"La diferencia fundamental entre la amenaza y el riesgo es que la amenaza está relacionada con la probabilidad de que se manifieste un evento natural o un evento provocado, mientras que el riesgo está relacionado con la probabilidad de que se manifiesten ciertas consecuencias, las cuales están íntimamente relacionadas no sólo con el grado de exposición de los elementos sometidos sino con la vulnerabilidad que tienen dichos elementos a ser afectados por el evento." (Fournier, 1985)

Fournier, D. A. E. (1985, November). The quantification of seismic hazard for the purposes of risk assessment. In *International Conference on Reconstruction, Restauration and Urban Planning of Towns and Regions in Seismic Prone Areas, Skopje*.

Amenazas y riesgos: Definiciones

Riesgo:

"El Centro Criptológico Nacional define el riesgo como la posibilidad de que una amenaza se materialice aprovechando una vulnerabilidad y causando daño en un proceso o sistema."

CCN-CERT: Organismo del Estado Español adscrito al Centro Nacional de Inteligencia que se dedica a criptoanalizar y descifrar por procedimientos manuales, medios electrónicos y criptofonía, así como realizar investigaciones tecnológico-criptográficas y formar al personal especializado en criptología (Fuente: WIKIPEDIA)

Amenazas y riesgos: Definiciones

Contextualización de los términos en el ámbito de la seguridad informática:

- Riesgo/Amenaza de que el dispositivo móvil quede expuesto por tener activa la funcionalidad Bluetooth.
- Los virus representan una amenaza/riesgo para los equipos informáticos.
- Existe un riesgo/amenaza elevado de infectarse por un malware si no se instala un antivirus en el sistema operativo.
- El sistema está protegido ante un gran tipo de amenazas/riesgos.

Amenazas y riesgos: Definiciones

Contextualización de los términos en el ámbito de la seguridad informática:

- **Riesgo**/Amenaza de que el dispositivo móvil quede expuesto por tener activa la funcionalidad Bluetooth.
- Los virus representan una **amenaza**/riesgo para los equipos informáticos.
- Existe un **riesgo**/amenaza elevado de infectarse por un malware si no se instala un antivirus en el sistema operativo.
- El sistema está protegido ante un gran tipo de **amenazas**/riesgos.

Amenazas y riesgos: Definiciones

Seguridad y vulnerabilidad:

- La **seguridad** es la ausencia de riesgo. Se encarga de gestionar dicho riesgo y minimizarlo.
- La **vulnerabilidad** es el riesgo que una persona, sistema u objeto puede sufrir frente a peligros inminentes (amenazas). *El caso de las actualizaciones del sistema operativo.*

Amenazas y riesgos: Definiciones

¿Qué es la seguridad informática?

- "Disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad."

  Aguilera, P. (2011). Redes seguras (Seguridad informática). Madrid, España: Editex.

- "Conjunto de métodos y de varias herramientas para proteger el principal activo de una organización como lo es la información o los sistemas ante una eventual amenaza que se pueda suscitar."

  Aguirre, J. R. (2006). Libro electrónico de seguridad Informática y Criptografía. Madrid, España: Universidad Politécnica de Madrid.

Amenazas y riesgos: Definiciones

Seguridad FÍSICA vs. LÓGICA

- La **SEGURIDAD FÍSICA** está relacionada con amenazas como inundaciones, incendios, robos, etc. Su objetivo es la protección de los dispositivos involucrados con el sistema de información de la organización.
- La **SEGURIDAD LÓGICA** está relacionada con la protección de los datos, las aplicaciones que los gestionan y sistemas operativos que permiten su funcionamiento.

¿Habéis experimentado alguna situación en la que se haya visto comprometida la seguridad física o lógica de vuestro sistema de **información personal**?

Amenazas y riesgos: Definiciones

RESUMEN DE CONCEPTOS:

- Amenaza
- Riesgo
- Vulnerabilidad
- Seguridad:
  - Seguridad Informática
  - Seguridad Física
  - Seguridad Lógica

Principios de la ciberseguridad:

- Confidencialidad 
- Integridad 
- Disponibilidad 

Principios de la ciberseguridad:

CUESTION CLAVE:

¿Cómo podemos aumentar la seguridad de un sistema? La respuesta requiere abordar el problema desde diferentes perspectivas:

- Prevención del riesgo: Evitándolo o eliminándolo (Ejemplo)
- Mitigación del riesgo: Reduciéndolo de algún modo (Ejemplo)
- Transferencia del riesgo: Compartiéndolo con algún agente externo (Ejemplo)
- Aceptación del riesgo

Componentes involucrados en ciberseguridad:

COMPONENTES DE LA CIBERSEGURIDAD:

1.- Los **usuarios**: El eslabón más débil. Factor difícil de controlar.

¿Conocéis algún caso (cercano o de terceros) en el que el usuario pusiera en riesgo la seguridad de un sistema informático?

https://www.youtube.com/watch?v=c7wAz9w4urY

(Como el usuario puede ayudar con sus acciones mucho más que las propias políticas de seguridad)

Componentes involucrados en ciberseguridad:

COMPONENTES DE LA CIBERSEGURIDAD:

1.- Los **usuarios**:

https://www.youtube.com/watch?v=NPE7i8wuupk

(¿Nos vigilan?)

Componentes involucrados en ciberseguridad:

COMPONENTES DE LA CIBERSEGURIDAD:

2.- La **información:** Tener claro su estructura, formato, sistema de archivo, compatibilidad…

3.- La **infraestructura**

Sistemas de protección como medida para aumentar la ciberseguridad:

¿CÓMO PROTEJO A LOS USUARIOS?

Formación →

https://www.youtube.com/watch?v=Y6vO2HxrEPc

(Preparación del usuario)

Sistemas de protección como medida para aumentar la ciberseguridad:

¿CÓMO PROTEJO LA INFRAESTRUCTURA?

- Mediante la correcta configuración de los dispositivos de comunicación (no dejar el Bluetooth activo, protocolo WPA2 activo en el router…)
- Controles de acceso (biométrico o de patrón en el móvil…)
- Copia de seguridad del sistema…

¿Qué sistema de protección física tenéis para el dispositivo móvil (carcasa, funda, cristal templado…)?
¿Disponéis de un sistema de protección de sobretensiones o caídas?

Sistemas de protección como medida para aumentar la ciberseguridad:

¿CÓMO PROTEJO LA INFORMACIÓN?

- ¿Tenéis copia externa de vuestros contactos del teléfono (nube)?
- ¿Tenéis activo la copia de seguridad de las conversaciones de WHATSAPP?
- ¿Tenéis activo el almacenamiento automático de vuestras fotos en la nube?
- ¿Recordáis la contraseña de la cuenta de Google vinculada a tu dispositivo móvil?
- ¿Tenéis algún antivirus instalado en vuestro dispositivo móvil?
- ¿Cada cuánto tiempo soléis realizar copias de todos vuestros activos de información?
- ¿Hacéis copia completa del sistema o sólo de los datos?


institución pau casals