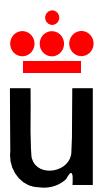
Introducción

GSYC

19 de enero de 2018



Universidad
Rey Juan Carlos

Seguridad en TIC

"**Proceso** para minimizar la vulnerabilidad de bienes y recursos telemáticos"

- Bien: algo de valor (datos, servicios, hardware, etc).
- Vulnerabilidad: debilidad que se puede explotar para violar un sistema o la información que contiene.

Seguridad en TIC

- La mayoría de los sistemas y protocolos que se usan no han sido diseñados pensando en la seguridad.
- Los usuarios no se preocupan de la seguridad (¿deberían? ¿pueden?).
- Sociedad de la Información: los ordenadores se usan para todo: los bienes que hay que proteger son muy "jugosos".
- No sólo hay fallos de seguridad técnicos, hay fallos humanos, relativos a la ingeniería social.
- Hay muchas motivaciones distintas para los ataques.
- 2010s: cyberwar.

Seguridad en TIC

Análisis coste/beneficio:

- Calcular el coste de la pérdida de un activo.
- Calcular la probabilidad de una pérdida.
- Calcular el coste de la prevención.
- Decidir con todo ello las medidas a tomar.

Procedimiento común en muchas ingenierías, pero es difícil evaluarlo en las TIC.¿Cuánto vale tu base de datos? Seguramente más que lo que piensas.

Conceptos básicos

- Confidencialidad (secreto): sólo los usuarios (humanos o programas) autorizados puede conocer la información.
- Integridad: sólo los usuarios autorizados pueden modificar los objetos (datos, programas, etc.).

Conceptos básicos

- Disponibilidad: los objetos deben estar operativos como se espera.
- Consistencia: el sistema debe comportarse correctamente, de la forma esperada.
- Autenticidad/autenticación: los objetos y los usuarios deben ser genuinos.

Conceptos básicos

- Control de acceso: mecanismos para determinar las operaciones que puede realizar un usuario sobre un objeto.
- Auditoría: posibilidad de saber conocer qué operaciones se han realizado sobre qué objetos, quién los ha realizado, etc.
- No repudio: un actor no puede negar su participación en la creación de un objeto o una comunicación.

Conceptos básicos

- Primer Principio de Kerckhoffs: el sistema, si no es teóricamente seguro, debe ser seguro en la práctica (i.e. *computacionalmente seguro*).
- Segundo Principio de Kerckhoffs: la seguridad no debe depender de que el método que seguimos se mantenga en secreto.
- Principio de mínimo privilegio: posible para usuarios (humanos y programas).
- Principio de mínima exposición: se deben desactivar los servicios y características que no se necesitan.

Conceptos básicos

- Hacker/Hacking: significa distintas cosas según el contexto. No es un término preciso. Se puede referir a:
  - Un buen programador, un buen técnico. Contexto técnico (TIC).
  - Alguien que se cuela en un sistema. Contexto más general, prensa, etc.

Conceptos básicos

- White Hat: atacante con motivación legítima, hacking ético. Tiene autorización para encontrar vulnerabilidades. Pentesting.
- Black Hat: atacante con motivación ilegítima, delincuente, vándalo, etc.
- Muchas veces, la frontera no está bien definida.

Buenas prácticas

- Restringir el acceso físico al hardware.
- Actualizar el software de forma periódica.
- Instalar software de terceros con precaución.
- Elegir de contraseñas apropiadas.

Buenas prácticas

- Controlar el acceso remoto al equipo por la red.
- Realizar un análisis periódico de la seguridad del equipo.
- Límitar el número de autenticaciones fallidas.
- Timeout adecuado para el cierre de sesiones por inactividad.

Buenas prácticas

- Mantener de copias de seguridad del sistema.
- Almacenamiento de copias de seguridad en un espacio físico diferente al de la copia original.
- Dedicar el tiempo necesario a la configuración correcta del sistema, antivirus, firewall, etc.
- Estudiar alternativas seguras para aplicaciones y protocolos (p. ej. FTP).

Buenas prácticas

- Usar cifrado en la comunicación y el almacenamiento de datos sensibles.
- Desconfiar de procedimientos no habituales (ingeniería social).
- Avisos legales en pantallas de login, constancia de que las normas han sido comunicadas y aceptadas etc.

Buenas prácticas

- Auditoria de la actividad de los usuarios.
- A la hora de retirar un disco duro, no es suficiente borrar los ficheros, hay que usar herramientas especializadas en borrar los datos para que no se puedan recuperar.

Jerga

Ojo, en el mundo de la seguridad TIC se usa mucha jerga específica y poco formal:

- Script kiddie, noob (newbie), lamer, elite (leet, l33t, 31337), H4X70R, luser (loser+user), spammer, 0day, pwned, defacement, reversing, pentesting, ...

Hay que estar al día

Fuentes de noticias:

- "Una al día": Newsletter, canal de Telegram
  `http://unaaldia.hispasec.com/`
- "Crypto-gram": Newsletter, blog
  `https://www.schneier.com/crypto-gram/`
- "RISKS": Newsletter
  `http://catless.ncl.ac.uk/Risks/`
- "Errata Security': Blog
  `http://blog.erratasec.com/`
- Twitter, reddit (r/netsec), etc...