SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

Antonio Villalón Huerta

toni@shutdown.es

Octubre, 2007

Contenidos

- Introducción.
- Seguridad del entorno.
- Seguridad del sistema.
- Seguridad de la red.
- Gestión de la seguridad.
- Otros aspectos de la seguridad.
- Conclusiones.

INTRODUCCIÓN

- Introducción. ⇐
- Seguridad del entorno.
- Seguridad del sistema.
- Seguridad de la red.
- Gestión de la seguridad.
- Otros aspectos de la seguridad.
- Conclusiones.

Introducción

- Presentación y objetivos.
- ¿Qué es seguridad?
- ¿Qué queremos proteger?
- ¿De qué lo queremos proteger?
- ¿Cómo lo podemos proteger?

En este curso...

- Analizaremos los peligros a los que se exponen nuestros recursos.

  ⇒ *Hackers*, virus, catástrofes...

- Conoceremos las salvaguardas que podemos aplicar.

  ⇒ Cortafuegos, IDSes, *backups*...

- Aprenderemos a gestionar nuestra seguridad.

  ⇒ MAGERIT, ISO 2700X, LOPD...

En este curso **NO**...

- Nos centraremos únicamente en aspectos técnicos.

  ⇒ Los problemas suelen ser siempre organizativos, rara vez técnicos.

- Aprenderemos a utilizar en profundidad herramientas de seguridad.

  ⇒ Podemos consultar otra documentación.

- Jugaremos a ser 'hackers'.

  ⇒ ¡Intrusismo ≠ Seguridad!

OBJETIVO: Ser capaces de determinar los riesgos que afectan a nuestros recursos, conocer las posibles salvaguardas, y poder implantarlas y gestionarlas.

¡NO EXISTE LA SEGURIDAD ABSOLUTA!

Seguridad: Característica que indica que un sistema está libre de todo peligro, daño o riesgo.

$$\Downarrow$$

Demasiada rigidez

$$\Downarrow$$

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

Introducción → ¿Qué es seguridad?

Seguridad (fiabilidad) es la suma de...

- **Confidencialidad:** Los objetos sólo pueden ser accedidos por actores autorizados y de una forma controlada.

+

- **Integridad:** Los objetos sólo pueden ser modificados por actores autorizados.

+

- **Disponibilidad:** Los objetos han de permanecer accesibles a los actores autorizados.

Adicionalmente...

- **No repudio:** Un actor no puede negar lo que ha dicho.

Introducción → ¿Qué es seguridad?

- En función del tipo de entorno y sus necesidades, se prioriza uno u otro aspecto.
- ¡No son incompatibles!
- Estado ideal: equilibrio correcto.

Introducción → ¿Qué queremos proteger?

Protegemos **activos** (recursos que forman parte del sistema):

- **Fungibles:** Elementos que se consumen con el uso (poco importantes).
- **Hardware:** Elementos físicos.
- **Software:** Programas lógicos.
- **Datos:** Información manejada por el hardware y el software (prioritario).
- **Otros:** Personas, infraestructuras...

Introducción → ¿Qué queremos proteger?

Los **datos** son habitualmente el activo 'informático' más preciado en cualquier organización:

- Los fungibles son baratos y fáciles de reponer.
- El hardware es caro, pero fácil de reponer.
- El software puede ser caro o barato, pero también fácil de reponer.
- ...

Introducción → ¿Qué queremos proteger?

Pero si se **destruye/roba/modifica** la información...

- Dificultad (¿imposibilidad?) para reponerla.
- Daños incalculables.
- Pérdidas millonarias.
- ...

Pregunta: ¿Qué preferiríamos destruir, nuestra nueva máquina Sun Fire 15K recién adquirida (> 1.5M€), o toda nuestra información?

Introducción → ¿De qué lo queremos proteger?

- Los **activos** presentan **vulnerabilidades** (debilidades de cualquier tipo que comprometen su seguridad).
- Por definición existen **amenazas** (escenarios en los que un evento o acción, deliberada o no, compromete la seguridad de un activo).
- Si un sistema presenta una vulnerabilidad y existe una amenaza, aparece un **riesgo** asociado (probabilidad de que el evento se materialice).
- Cuando el riesgo se materializa, la medida del daño causado se denomina **impacto**.
- A las medidas que eliminen la vulnerabilidad o la amenaza, o disminuyan el riesgo o impacto asociados, se les denomina **defensas**, **salvaguardas**, **controles**...

Introducción → ¿De qué lo queremos proteger?

Los datos son el recurso más importante a proteger.
¿Qué amenazas existen contra los mismos?

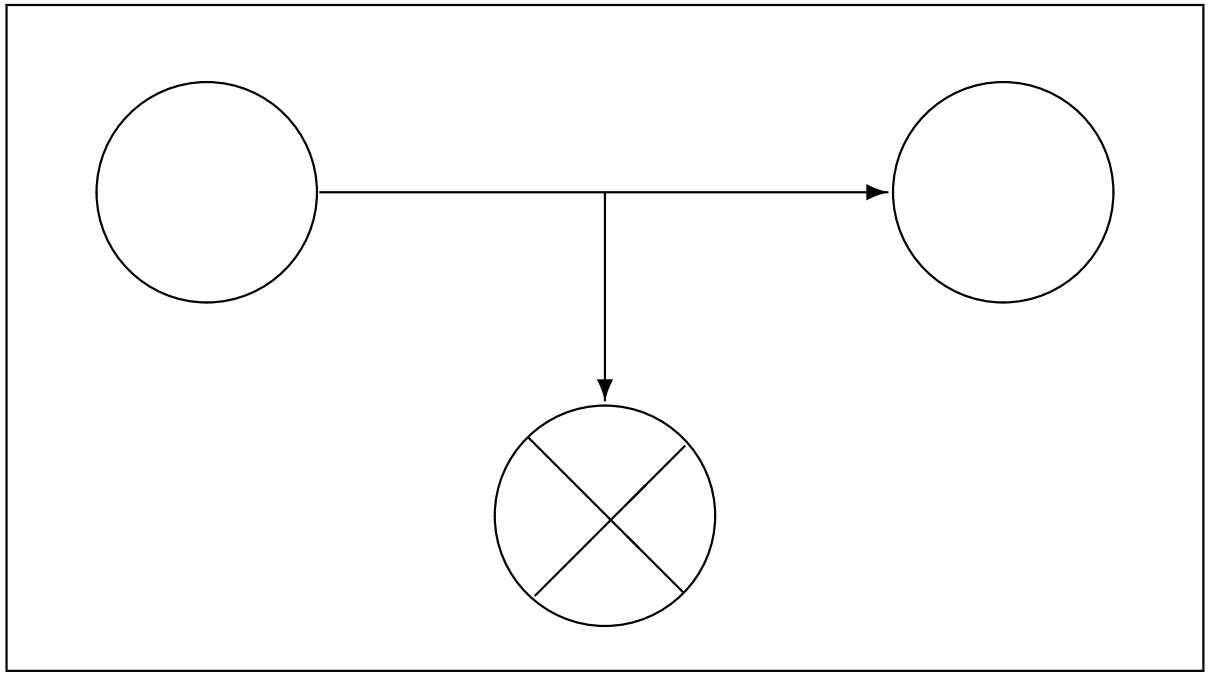
- Interceptación.
- Modificación.
- Interrupción.
- Fabricación.

Introducción → ¿De qué lo queremos proteger?

Flujo normal de comunicación entre emisor y receptor

- Confidencialidad: Nadie no autorizado accede a la información.
- Integridad: Los datos enviados no se modifican en el camino.
- Disponibilidad: La recepción es correcta.

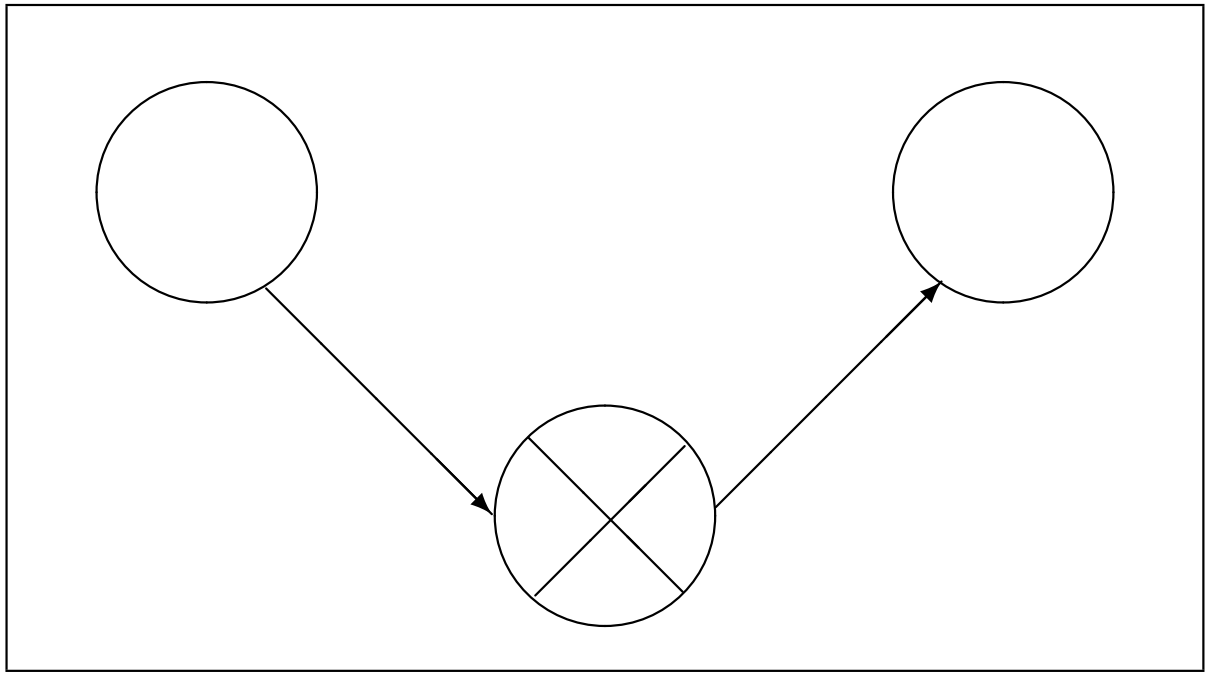
Introducción → ¿De qué lo queremos proteger?



Interceptación

- Confidencialidad.
- Integridad.
- Disponibilidad

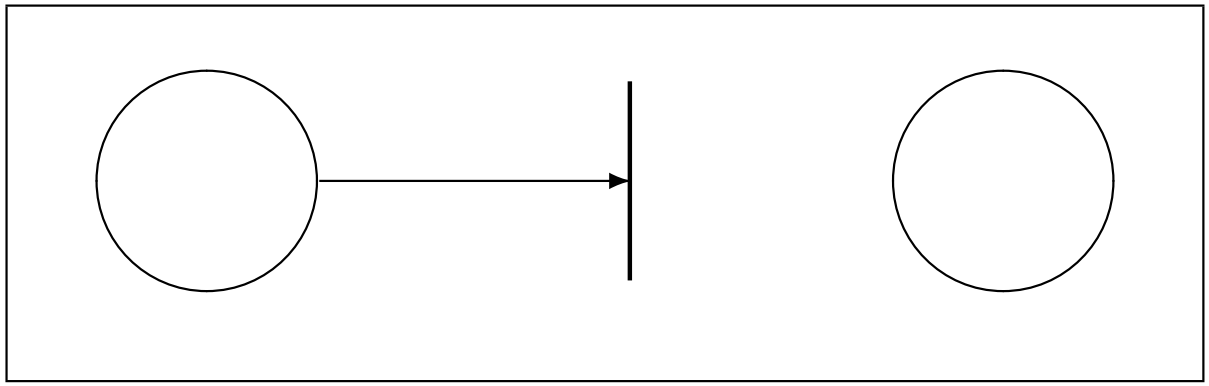
Introducción → ¿De qué lo queremos proteger?



Modificación

- Confidencialidad.
- Integridad.
- Disponibilidad.

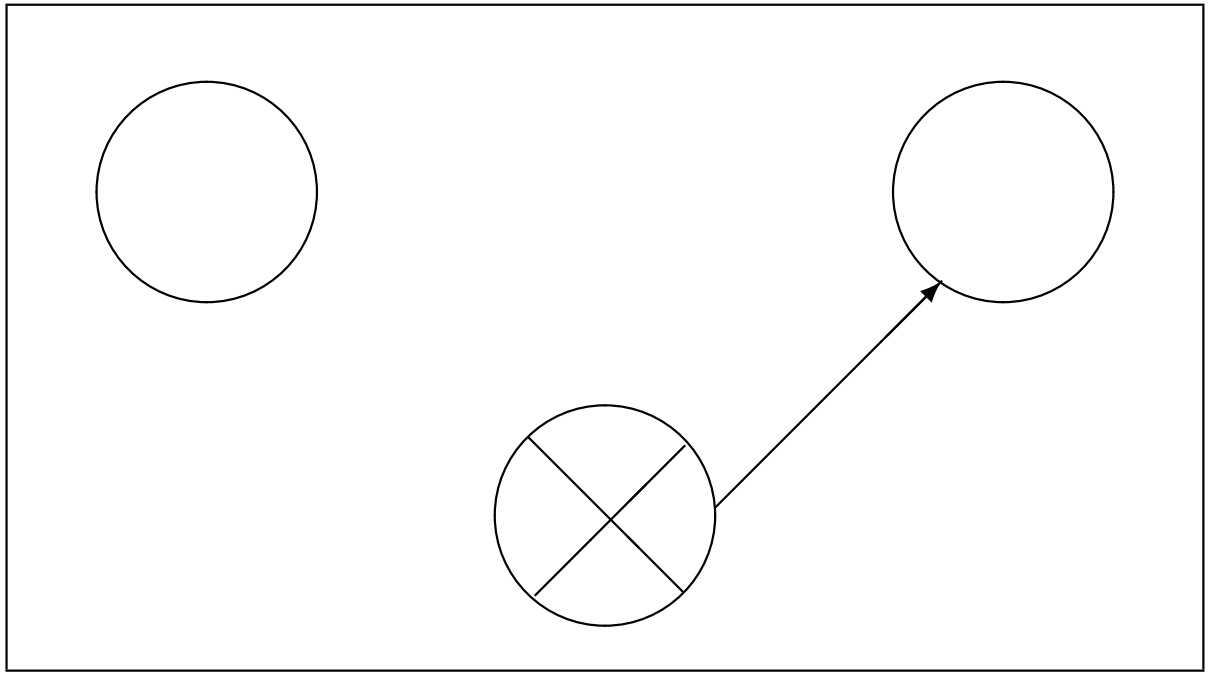
Introducción → ¿De qué lo queremos proteger?



Interrupción

- Confidencialidad.
- Integridad.
- Disponibilidad.

Introducción → ¿De qué lo queremos proteger?



Fabricación

- Confidencialidad.
- Integridad.
- Disponibilidad.
- ¿Otros problemas?

Introducción → ¿De qué lo queremos proteger?

¿Quién materializa estas amenazas?

- Personas

  Usuarios, ex–empleados, piratas, terroristas...

- Fauna

  Caballos de Troya, virus, gusanos...

- Medio

  Cortes de luz, catástrofes naturales...

Introducción → ¿Cómo nos podemos proteger?

- Primera línea de defensa: **política de seguridad**: documento sencillo que define las directrices organizativas en materia de seguridad.
- La política se suele dividir/apoyar en normativas que cubren áreas más específicas.
- Confusión en las denominaciones.
- Hasta ahora no proporcionamos seguridad 'directa': todo es papel.
- La política o las normativas se implantan mediante **mecanismos de seguridad**.

De esta forma...

Política de Seguridad

⇓

Normativas

⇓

Implantación

⇓

Mecanismos de seguridad

Veremos ejemplos en el último capítulo.

Mecanismos de seguridad

- **Prevención.**

  Evitan desviaciones con respecto a la política de seguridad.

- **Detección.**

  Detectan dichas desviaciones si estas se producen.

- **Recuperación.**

  Recuperan el funcionamiento correcto tras una desviación.

SEGURIDAD DEL ENTORNO

- Introducción.
- Seguridad del entorno. ⇐
- Seguridad del sistema.
- Seguridad de la red.
- Gestión de la seguridad.
- Otros aspectos de la seguridad.
- Conclusiones.

Seguridad del entorno

- **Introducción.**
- **Amenazas del entorno.**
  - Físicas.
  - Operacionales.
- **Contramedidas:**
  - **Prevención.**
    - Ante amenazas físicas.
    - Ante amenazas operacionales.
  - **Detección.**
    - De vulnerabilidades físicas.
    - De vulnerabilidades operacionales.
  - **Recuperación.**
    - Planes de contingencia.

Por el simple hecho de existir en un entorno, los activos ya están expuestos a amenazas:

- Terremoto que destruya completamente los SSII.
- Error operacional que borre copias de seguridad.
- Secuestro o extorsión de un administrador.
- *Alien* que abduce una máquina.
- Café derramado sobre un monitor.
- ...

Seguridad del entorno → Introducción

La seguridad del entorno de operaciones se divide en dos grandes áreas:

- Seguridad **física**.

  Aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas contra las amenazas a los recursos y la información confidencial.

- Seguridad **operacional**.

  Aplicación de procedimientos que garanticen la seguridad de las operaciones en el SI y del personal que las realiza.

Seguridad del entorno → Introducción

La seguridad del entorno...

- A veces demasiado ensalzada (auditoría clásica).
- A veces demasiado descuidada (nuevos 'auditores').
- Algunas amenazas son de bajo riesgo en nuestro entorno...
- ...¡pero no todas!

Seguridad del entorno → Amenazas

Amenazas físicas:

- Acceso físico.
- Radiaciones electromagnéticas.
- Desastres naturales.
  - Terremotos.
  - Tormentas eléctricas.
  - Inundaciones y humedad.
- Desastres del entorno.
  - Electricidad.
  - Ruido eléctrico.
  - Incendios y humo.
  - Temperaturas extremas.

Seguridad del entorno → Amenazas

Acceso físico

- Riesgo considerable (en nuestro entorno), suficiente para tenerlo en cuenta.
- Impacto muy alto.
- En ocasiones se descuida su seguridad (ejemplo: tomas de red 'libres').
- ¡Si existe acceso físico a un recurso, no existe seguridad!

Radiaciones electromagnéticas

- Cualquier aparato eléctrico emite radiaciones.
- Con el equipo adecuado, estas radiaciones se pueden capturar y reproducir.

  Un atacante puede 'escuchar' los datos que circulan por un cable telefónico.
- Algo casi restringido al entorno militar (TEMPEST)...
- ...aunque hoy en día parece resurgir (redes *wireless*, comunicaciones vía satélite, infrarrojos...).

Seguridad del entorno → Amenazas

Desastres naturales

- Riesgo reducido en nuestro entorno:
  - Zona sísmicamente poco activa.
  - Medio urbano (abundancia de pararrayos, zonas no inundables...).
  - ...
- Impacto muy alto.
- Si se materializaran, hablaríamos de **desastre** (no sólo por los SSII).

Seguridad del entorno → Amenazas

Personalizando...

- ¿Hay riesgo de un terremoto en mi entorno? (Sur de la CV)
- ¿Conozco el historial de inundaciones de los últimos años? (Zona de La Ribera)
- ¿Están ubicadas las instalaciones sobre un antiguo cauce o barranco?
- ¿Tengo alguna protección frente a las tormentas con aparato eléctrico?
- ...

Seguridad del entorno → Amenazas

Desastres del entorno

- Riesgo considerable.
- Impacto medio/alto.
- Suelen existir salvaguardas aceptables en cualquier entorno.
- Problema: ¿Comprobamos periódicamente que las salvaguardas son correctas y funcionan adecuadamente?
  - ¿Cuánto tiempo hace que no verifico el SAI?
  - ¿Cada cuantos meses realizo un simulacro de incendio?
  - ¿Realmente está **prohibido** fumar en la sala de servidores?
  - ...

Seguridad del entorno → Amenazas

Amenazas operacionales:

- Ingeniería social.
- *Shoulder surfing.*
- Basureo.
- Actos delictivos.

Seguridad del entorno → Amenazas

Ingeniería social

- Manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
- El atacante aprovecha la buena voluntad o el desconocimiento de un usuario o de un administrador.
- Ataque de alto impacto, riesgo medio, y sobre todo fácil y seguro para el atacante.
- **PELIGRO**: El atacante no es casual.

Las personas suelen ser el punto más débil en la seguridad de cualquier organización

Seguridad del entorno → Amenazas

Shoulder Surfing

- Acceso a información confidencial simplemente 'paseando'.
- Claves tecleadas, papeles encima de la mesa...
- Riesgo bajo, pero impacto potencialmente alto.
- Ataque 'discreto', casi imposible de detectar.

Basureo

- Obtención de información dejada en o alrededor de un sistema de información tras la realización de un trabajo.
- Incluye basureo 'real' (en cubos de basura).
- El riesgo es bajo, pero el impacto puede ser enorme.
- Ejemplo: últimos casos de acceso a datos de carácter personal.

Seguridad del entorno → Amenazas

Actos delictivos

- Secuestro, amenaza, extorsión...
- Riesgo bajo (en nuestro entorno), impacto muy alto.
- **IMPORTANTE**: Notificación y denuncia.

Seguridad del entorno → Contramedidas

Controles de acceso y presencia:

- Controles de acceso biométricos.
- Cámaras de seguridad.
- Sensores de movimiento.
- Llaves, cerraduras...

Una vez abrimos una puerta... ¿cuándo se cierra?

Seguridad del entorno → Contramedidas

TEMPEST

- No es obligatorio en entornos civiles.
- Para minimizar el riesgo de captura...
  - Distancia (perímetro de seguridad).
  - Confusión (contaminar el espectro).
  - Equipamiento dedicado: circuitos de fuente eliminada, jaulas de Faraday...
- Recordemos que el riesgo en nuestro entorno es **mínimo**...

Seguridad del entorno → Contramedidas

Ante desastres naturales...

- Edificios antiterremoto.
- Planes de evacuación.
- Aislamiento eléctrico correcto.
- Sismógrafos.
- Sensores de humedad.
- ...

¡Muchas veces es imposible predecir un desastre!

Seguridad del entorno → Contramedidas

Ante desastres del entorno...

- Planes de evacuación.
- Simulacros.
- Ubicación correcta de los sistemas.
- Aire acondicionado, control de temperatura...

Seguridad del entorno → Contramedidas

Ante problemas operacionales...

- Formación.
- Concienciación.

  ⇒ Cada persona es vital para la seguridad global.
- Procedimientos operativos correctos.

  ⇒ Auditorías de cumplimiento.
- Más formación.

Planes de contingencia

- DEFINICIÓN: Análisis pormenorizado de las áreas que componen nuestra organización y que define una política de recuperación ante un desastre.
- OBJETIVO: Garantizar la continuidad del servicio en el menor plazo de tiempo posible.
- En la práctica es imposible la perfección.

Seguridad del entorno → Contramedidas

La implementación del plan suele ser **muy cara**:

- Equipos de respaldo, que durante el funcionamiento normal de la organización suelen permanecer inactivos.
- Infraestructura adicional: edificios separados, redes de comunicaciones entre ellos, canales seguros...
- Personal disponible en caso de necesidad.
- ...

Seguridad del entorno → Contramedidas

No obstante, el plan de contingencias es **vital**:

- Las organizaciones dependen cada vez más de sus activos informáticos.
- Consecuencias **fatales** si se pierden determinados activos.
- El plan proporciona conocimiento de las debilidades.
- Aunque el plan sea caro, su inexistencia puede resultar mucho más cara: imagen, clientes, ingresos, credibilidad...

Seguridad del entorno → Contramedidas

Consideraciones del plan de contingencias

- ¿Ante qué amenazas debo definir plan de contingencia?
  ⇒ Mayores riesgos.
- Deben contemplar **todos** los aspectos para llegar a ofrecer servicio ante un desastre.
- Plan de emergencia + Plan de recuperación.
- Simulaciones periódicas.

¿Cuánto tiempo podría permitirme **ahora** permanecer con mis sistemas parados?

SEGURIDAD DEL SISTEMA

- Introducción.
- Seguridad del entorno.
- Seguridad del sistema. ⇐
- Seguridad de la red.
- Gestión de la seguridad.
- Otros aspectos de la seguridad.
- Conclusiones.

Seguridad del sistema

- **Introducción.**
- **Amenazas internas.**
  - Fauna.
  - Usuarios
  - Programación insegura.

Seguridad del sistema

- **Contramedidas:**
  - Prevención.
    - Sistemas antivirus.
    - Controles de acceso.
    - Autenticación de usuarios.
    - Almacenamiento seguro.
  - Detección.
    - Registros de auditoría.
    - Detección de intrusos.
  - Recuperación.
    - Copias de seguridad.
    - Sistemas de respaldo.

Seguridad del sistema → Introducción

- Amenazas a un sistema y salvaguardas que podemos aplicar.
- Aspectos mayoritariamente **locales**, aunque su origen pueda ser remoto.
- Habitualmente, la última barrera de protección ante la materialización de una amenaza.
- Salvaguardas altamente sofisticadas y efectivas, pero poco aplicadas.

La seguridad a nivel de *host* es factible, aunque en muchas ocasiones se descuida:

- Elevado número de máquinas a cargo de un grupo reducido de administradores.
- Sistemas heterogéneos.
- Elementos críticos que no pueden detener su servicio.
- Sistemas *'out of the box'* inseguros, pero funcionales.
- ...

Seguridad del sistema → Introducción

Actualmente, casi cualquier sistema tiene la capacidad y las herramientas de prevención, detección y recuperación necesarias para garantizar los niveles mínimos de seguridad.

Somos nosotros los que no sabemos, queremos o podemos aplicar estas medidas.

Seguridad del sistema → Amenazas

Existen dos grandes grupos de amenazas al sistema:

- Las relativas a usuarios que tratan de violar la seguridad.

  ⇒ Escalada de privilegios, usurpación de identidad, accesos no autorizados...

- Las relativas a programas con el mismo objetivo: *malware*.

  ⇒ Conejos, gusanos, virus, caballos de Troya, *backdoors*...

Virus

- Secuencia de código que se inserta en un fichero ejecutable, de forma que al ejecutar el programa también se ejecuta el virus.
- La ejecución implica generalmente la copia del código viral.
- Es necesaria la existencia de un huésped.
- Especialmente críticos en plataformas Windows, aunque no son exlusivos de este entorno.

  Primeros virus (70s) sobre Univac 1108 e IBM 360.

Gusanos

- Programa capaz de viajar por sí mismo a través de una red para realizar cualquier tipo de actividad una vez alcanzado un recurso.
- El mayor incidente de seguridad de la historia de Internet fue causado por un gusano (Morris Worm, 1988).
- En los últimos años han vuelto a proliferar, especialmente sobre plataformas Windows (Outlook, Internet Information Server...).

Conejos

- Programas que se reproducen de forma exponencial sin ninguna actividad concreta.
- Negación de servicio por consumo excesivo de recursos (procesador, memoria, disco...).
- Es posible limitar su impacto configurando correctamente el núcleo de cualquier sistema operativo.

Caballos de Troya

- Misma idea que el caballo de Troya (Homero, *La Odisea*).
- Programa que aparentemente realiza una función útil para quien lo ejecuta, pero en realidad realiza una tarea oculta que el usuario desconoce.
- No son tan habituales como los virus, pero tampoco son extraños.
- Variante: Mula de Troya.
- Detección simple, pero no practicada: uso de funciones resumen.

Bombas lógicas

- Malware que se activa bajo ciertas condiciones.
- Funciones de activación: tiempo, existencia de ficheros o procesos, número de ejecuciones...
- Peligrosidad: pueden permanecer activas durante mucho tiempo sin hacer nada perjudicial, lo que puede complicar su detección.

Puertas traseras

- Mecanismo para circunvalar mecanismos de autenticación.
- Frecuentemente utilizado por programadores durante el desarrollo de aplicaciones.
- Aceptable en esta fase, pero extremadamente peligroso tras la implantación del sistema.
- ¿Siempre es un olvido eliminar las puertas traseras?

Superzapping

- Procedimientos o herramientas que evitan ciertos controles del sistema operativo, para ser utilizadas en caso de necesidad extrema.
- `'superzap'`: Antigua herramienta de emergencia para realizar tareas administrativas.
- **No** es una puerta trasera, ya que todo el mundo conoce su existencia.
- Vulnerabilidad grave: alto riesgo y alto impacto.

Técnicas salami

- Desvío de pequeñas cantidades de recursos de una gran fuente.
- Especialmente críticos en bancos o en entornos que manejen datos económicos (por ejemplo, sueldos).
- *Round down*, redondeo hacia abajo, es el caso más habitual.

Programación insegura

- Aspecto casi inevitable de la programación imperativa (especialmente en desarrollos complejos).
- Todos los lenguajes introducen riesgos (C, Java, Perl...).
- Alto riesgo en partes críticas del sistema: núcleo y ejecutables *setuidados*.

Programación segura

- Existen llamadas al sistema a evitar siempre.
- Máxima restricción en los privilegios del programa.
- Especial atención a factores externos:
  - Capturar todas las señales.
  - Verificación de datos introducidos por el usuario.
- ...

Problemática derivada de los usuarios

- Usuarios legítimos que tratan de acceder a objetos o realizar acciones a las que no están autorizados.
- Atacantes externos que suplantan la identidad de un usuario legítimo.

Si un atacante externo consigue penetrar nuestro sistema, ha recorrido el 80% del camino hasta conseguir un control total de un recurso

¿A quién nos enfrentamos? Ex–empleados

- Por algún motivo desean perjudicarnos.
- Amplio conocimiento del entorno.
- Atacantes no casuales: su objetivo somos nosotros, no nuestro vecino.

Seguridad del sistema → Amenazas

¿A quién nos enfrentamos? Piratas (*¿hackers?*)

- Casi siempre casuales.
- Casi siempre fáciles de detener.
- Casi siempre sin actitud 'agresiva'.
- Casi siempre suelen buscar cierto prestigio en la comunidad *underground* como único objetivo.
- **. . . ¿CASI SIEMPRE?**

Seguridad del sistema → Amenazas

¿A quién nos enfrentamos? Terroristas

- Su objetivo es causar daño (p.e. *Information Warfare*).
- Amplios conocimientos.
- Herramientas y ataques sofisticados.
- No son atacantes casuales.
- **MUY PELIGROSOS**
- Raros en nuestro entorno.

¿A quién nos enfrentamos? Intrusos remunerados

- Su objetivo suele ser el robo de información.
- Amplios conocimientos.
- Herramientas y ataques sofisticados.
- No son atacantes casuales.
- **MUY PELIGROSOS**
- Raros en nuestro entorno.

¿A quién nos enfrentamos? Personal interno

- Nombre propio: *insiders*.
- Amplios conocimientos del entorno.
- No necesariamente con mala intención.
- Más comunes de lo que podemos pensar.

  $\Rightarrow$ Más del 80% de las pérdidas generadas por problemas de seguridad son causadas por el personal interno.

Seguridad del sistema → Amenazas

¿Cómo lo consiguen?

- 'Adivinación' de contraseñas.
- Explotación de vulnerabilidades en los programas.
- Aprovechamiento de errores operacionales.
- ...

¿Qué hacer para evitarlo, detectarlo y corregirlo?

- Multitud de salvaguardas y controles del sistema. Vamos a verlos...

Sistemas antivirus

- Analizan (bajo demanda o de forma contínua) los ficheros que se almacenan en disco o se ejecutan (en local y en remoto).
- Amplio espectro de productos.
- Base de datos de patrones víricos.

El mejor antivirus es la prevención

Seguridad del sistema → Contramedidas

Sistemas antivirus personales

- Se ejecutan en la estación de trabajo de cada usuario.
- Última salvaguarda antes de la contaminación.
- Problemas de usabilidad (rapidez, conflictos con otro software...).

  ⇒Muchos usuarios lo desinstalan.
- IMPORTANTE: Adopción de antivirus corporativo.

Sistemas antivirus SMTP

- Se instalan en la pasarela de correo corporativa (donde se recibe el *e–mail* de los usuarios).
- Detecta y elimina virus recibidos a través del correo.
- No dejamos la seguridad en manos de los usuarios.
- El correo electrónico **no** es el único medio de contaminación (navegación *web*, unidades extraíbles...).

Filtrado de contenidos

- No son estrictamente un antivirus.
- Se integran con los sistemas cortafuegos.
- Todo el tráfico *web* de los usuarios ha de pasar por el filtro.
- Evitan que contenidos 'perjudiciales' lleguen al usuario final cuando navega.
- ¿Qué es 'perjudicial'? ¿Quién lo decide?

Controles de acceso

- Mecanismos para determinar qué actores tienen acceso a qué objetos y de qué forma.
- Dos grandes familias:
  - DAC (*Discretionary Access Control*).
  - MAC (*Mandatory Access Control*)

Control de acceso discreccional

- El propietario de un objeto controla el acceso al mismo.
- Enfoque habitual de la mayor parte de operativos (p.e. Unix y sus permisos `rwx`).
- No aceptable en entornos de alta seguridad.
- Estándar POSIX.1

Control de acceso obligatorio

- La protección de un objeto no es determinada por el propietario del mismo.
- Se asocian etiquetas (TOP SECRET, SECRET, CONFIDENTIAL...) a la información.
- Caso particular: RBAC (*Role Based Access Control*).
  - Define roles para los perfiles de acceso al sistema.
  - Estándar del NIST.
- Aplicable en sistemas operativos *'trusted'*.
- Estándar POSIX.6

Autenticación de usuarios

- Autenticar: Verificar que un actor es quien dice ser.
- Usuario se identifica ante el sistema (p.e. *login*).
- El sistema lo autentica (p.e. *password*).
- Esquemas de autenticación de todo tipo: buenos y malos, caros y baratos...

Propiedades cualitativas del esquema de autenticación

- Fiable.

  Baja probabilidad de fallo. Resistencia ante ataques.

- Factible.

  Adecuado al entorno, por ejemplo económicamente.

- Aceptable.

  Los usuarios han de estar *relativamente* de acuerdo en utilizarlo.

Propiedades cuantitativas del esquema de autenticación

- Tasa de falso rechazo (FRR, *False Rejection Rate*).
  Probabilidad de rechazo de un usuario legítimo.
- Tasa de falsa aceptación (FAR, *False Acceptation Rate*).
  Probabilidad de aceptación de un usuario ilegítimo.
- Interesa minimizar ambas:
  - FRR alta → Poca disponibilidad. Descontento de los usuarios.
  - FAR alta → Poca integridad y confidencialidad.

Tipos de autenticación

- Basada en algo conocido (p.e. claves).
- Basada en algo poseido (p.e. tarjetas inteligentes).
- Basada en características físicas (biometría).

Autenticación por algo conocido

- Esquema más barato y fácil de implantar ⇒ El más usado.
- Alto grado de aceptación: es 'lo normal'.
- *A priori* el menos fiable.
  - Las claves se olvidan.
  - Las claves se pierden.
  - Las claves se roban.
  - ...

Ejemplo: nombre de usuario + contraseña (Unix)

- Cada usuario identificado unívocamente por un nombre.
- Claves almacenadas en el sistema, cifradas.
- Usuario teclea su nombre y contraseña, sistema la cifra y compara con la registrada. Si es positivo: acceso permitido.
- Problemas y soluciones: *shadow password*, *aging password*...

Autenticación por algo poseido

- Esquema de precio intermedio.
- Muy utilizado para control de acceso y presencia física.
- Alto grado de aceptación por los usuarios.
- En ocasiones muy vulnerable.

Ejemplo: tarjetas inteligentes

- Dispositivo del tamaño de un tarjeta de crédito, con capacidad de almacenamiento y *antitampering*.
- Lectura mediante elementos *hardware* dedicados ⇒ Caro.
- Frecuentemente complementado con otros modelos (p.e. clave).
- Amigable y fácil de usar, pero también de robar, perder...
- Con fotografía, también usadas como cipol (*badge*).

Autenticación biométrica

- Esquema más caro, difícil de implantar, y en principio más robusto.

  ⇒ Subversión del sistema con dedos de gelatina

- Control de acceso físico en entornos de alta seguridad.
- Cada vez más popularizado.
- Tras el *boom* inicial, ahora se aplica más 'relajadamente'.
- En ocasiones, baja aceptación entre los usuarios.
- PROBLEMA: Mi clave la puedo cambiar, pero una parte de mi cuerpo **no**.

Proceso de autenticación

- **Captura:** Lectura de los datos presentados.
- **Extracción:** Determinación de características relevantes.
- **Comparación:** De las mismas con las almacenadas en BBDD.
- **Decisión:** ¿El usuario es quien dice ser?

Aproximaciones habituales

- Verificación de voz.
- Verificación de escritura.
- Verificación de huellas.
- Verificación de patrones oculares.
  - Vasculatura retinal.
  - Iris.
- Verificación de geometría de la mano.

Problemas de aceptación

- Reconocimiento de huellas: asociado a criminales.
- Reconocimiento ocular:
  - 'Miedo' a mirar por un visor.
  - Determinación de enfermedades, drogas...
- En general, temor a autenticarse con una parte del cuerpo. Si me amenazan, puedo decir mi clave, puedo dar mi tarjeta inteligente, pero... ¿me cortarán el dedo?
- Tranquilos. El lector no acepta miembros muertos... ¿verdad?

Seguridad del sistema → Contramedidas

Un esquema robusto...

- Combina diferentes aproximaciones.
- AND lógico (**nunca** OR).
- Ejemplo: Cajeros automáticos ($$$), PIN + tarjeta.
  ⇒ Incluso existen cajeros con reconocimiento ocular.

Seguridad del sistema → Contramedidas

Almacenamiento seguro: sistemas de ficheros

- FS proporciona primer nivel de protección: DAC.
- Generalmente basado en ACLs (Unix, Windows...).
- Cada objeto tiene un propietario; el resto de actores tiene un acceso definido por el mismo (p.e. lectura, escritura, modificación...).

¿Qué sucede si alguien nos roba un soporte físico?

Almacenamiento seguro: cifrado

- Aplicaciones de cifra.
- Sistemas de ficheros cifrados.
- Sistemas de ficheros esteganográficos.
- Copias cifradas.

Almacenamiento seguro: aplicaciones de cifra

- Generalmente basadas en algoritmos de cifrado simétrico.
- El proceso de cifrado y descifrado puede ser lento (p.e. archivos grandes).
- Gestión habitualmente incómoda.
- Ejemplos: PGP, `crypt`...

Almacenamiento seguro: FS cifrados

- Algoritmos de cifra simétrica.
- Todo el almacenamiento se realiza por defecto cifrado.
- Se busca compaginar seguridad y transparencia.
- Problema: mucha información cifrada ⇒ Ataques.
- Ejemplos: CFS, TCFS (nivel de *kernel*)...

Almacenamiento seguro: FS esteganográficos

- Sistemas de cifra: toda la seguridad reside en la clave.
- PROBLEMA: ¿Y si un atacante la adivina o me obliga a revelarla?
- SOLUCIÓN: No puedo ocultar la existencia de información cifrada, pero sí su cantidad.
- Negación creíble: atacante no puede determinar si una clave proporciona acceso a toda la información o solo a una parte.
- Ejemplos: StegFS.

Almacenamiento seguro: copias cifradas

- La seguridad de las copias debe ser equivalente a la de los datos 'originales'.
- Problemas incluso legales: LOPD.
- Almacenamiento y recuperación lentas.
- ¡Debo garantizar que puedo recuperar en casos extremos!
- Ejemplos: Tivoli Storage Manager (TSM).

Almacenamiento seguro: borrado

- ¿`undelete`?
- Habitualmente es posible recuperar ficheros borrados.
  $\Rightarrow$ ¡Incluso después de sobreescribir varias veces!
- Algoritmos de borrado seguro (lentos).
- Empresas especializadas en recuperación extrema (caras).

Debemos asegurarnos de que realmente eliminamos la información que queremos borrar.

Registros de auditoría

Cualquier sistema operativo guarda información (*logs*) de las actividades que se llevan a cabo sobre el mismo:

- Seguridad ⇐
- Contabilidad.
- Parametrización.
- Solución de problemas.
- ...

Ejemplo: `syslogd` (Unix)

- Configuración sencilla y efectiva.
- Registro en texto plano:
  - Eventos: `/var/log/syslog`.
  - Mensajes: `/var/adm/messages`.
  - Aplicaciones: ...
- Interfaz con aplicaciones (p.e. `logger`).

Accounting

- Monitorización exhaustiva: registro de todos los programas ejecutados.
- Almaceno mucha cantidad de información.
  - Amplio consumo de recursos.
  - Herramientas para reducir o interpretar *logs*.
  - Dificultad de análisis.
  - ...
- En principio, innecesario en nuestro entorno.

Registros clásico vs. alta seguridad

- Modelo clásico: registro tras la ejecución del proceso.
- Alta seguridad: registro de cada acceso o intento de acceso a un objeto, cambio de estado del objeto o del actor, y cambio del sistema global.
- Identificador de auditoría (*Audit ID*).

  Asignado a cada grupo de procesos ejecutados y registrado junto a cada llamada al sistema.
- Elevado consumo de recursos (CPU, memoria, disco...).

Detección de intrusos

- Aspecto **prioritario** en un esquema de seguridad.
- Habitualmente, detección de intrusos basada en red.
- Hablaremos con detalle en el capítulo siguiente.
- **IDEA**: Detectar actividades 'sospechosas' en un sistema antes de que puedan comprometer su seguridad.

Detección en el sistema

Tres grandes familias de IDSes:

- Verificadores de integridad del sistema, SIV (*System Integrity Verifiers*).
- Monitores de registros, LFM (*Log File Monitors*).
- Sistemas de decepción (*Honeypots*).

Verificadores de integridad

- Monitorizan objetos para detectar modificaciones no deseadas.
- Basados en funciones resumen.
- Ejemplos: TripWire, Solaris ASET...

Monitores de registros

- Monitorizan *logs* en busca de patrones que puedan denotar una intrusión.
- ¿Cuáles son estos patrones?
- Ejemplos: Swatch, Logcheck...

Sistemas de decepción

- Simulación de vulnerabilidades.
- ¿De qué nos sirve simular una vulnerabilidad que no tenemos?
- Ejemplos: PortSentry, *'Sonria a la cámara oculta'*...

Seguridad del sistema → Contramedidas

Copias de seguridad

- Con frecuencia, la única tabla de salvación de nuestros datos.
- Su seguridad se suele descuidar (verificación, protección...).
- Aspecto crítico en la mayoría de entornos.
- **¡No existe la política universal!**

Si ahora mismo pierdo mis datos, ¿hasta que punto podría recuperarlos?

Estrategias de *backup*

- Copia completa (Nivel 0)

  Copia de todo un sistema o partición, reseteando bit de archivo.

- Copia incremental o progresiva

  Se guardan archivos modificados desde la última copia (completa o progresiva), reseteando bit de archivo.

- Copia diferencial

  Se guardan archivos modificados desde la última copia sin resetear bit de archivo.

Niveles de *backup*

- Nivel 0: copia completa.
- Nivel N: ficheros modificados desde la última copia de nivel N-1.
- En la práctica, el nivel máximo es el 2.

Copias completas

- Técnicamente sencillas de realizar.
- Gran consumo de recursos (tiempo, dispositivos...).
- En ocasiones, restauración costosa (pero sencilla).
- Recomendables de forma periódica y antes de grandes cambios.

Copias incrementales

- Más rápidas que las completas.
- Muy frecuentes en organizaciones medias o grandes.
  $\Rightarrow$ Muchos datos para una completa diaria.
- Recomendables al menos cada dos días.
- Restauración costosa (varios juegos de cintas).

Copias diferenciales

- También frecuentes en organizaciones medias o grandes.
- Pueden llegar a ser más lentas que las incrementales.
- Restauración eficiente.
- Misma información, registrada varias veces.

Plan de copias

- ¿Qué ficheros copiar?
- ¿Cuándo copiarlos?
- ¿Cuál es su frecuencia de cambio?
- ¿Quién es el responsable de la copia?
- ¿Cuál es el tiempo de recuperación máximo permitido?
- ¿Dónde almacenar las copias? ¿Dónde recuperarlas?

Rara vez se puede garantizar una recuperación del 100% de los datos

Ejemplo de planificación

Lunes: Nivel 0. Resto de dias: Nivel 1 (diferencial).

- Estrategia típica.
- Periódicamente realizo copia completa ⇐ Recomendable.
- Dos juegos de cintas para restauración completa.
- Si datos cambian mucho, la última diferencial se puede asemejar en volumen a la completa.
- Puedo perder un día de trabajo. ¿Aceptable?

Algunas consideraciones...

- ¿Cuánta información puedo perder en cada momento?
- Misma seguridad (p.e. LOPD) para copias que para datos en sistema.
- ¿Dónde almaceno los dispositivos?
- ¿Etiqueto los dispositivos?
- ¿Verifico las copias?

Sistemas de respaldo

- **OBJETIVO:** Garantizar la disponibilidad ante cualquier evento.
- Replicación de información.
- Replicación de sistemas y elementos de comunicaciones.
- ¿'Replicación'?
- Recursos (servidores, elementos de comunicaciones...) alejados de los originales.

Si ahora mi cortafuegos se para y no arranca, ¿cuánto tardo en recuperarme?

Puntos únicos de fallo

- Elementos cuya degradación total o parcial afecta a todo el entorno.
- Denominados SPFs (*Single Points of Failure*).
- Especial atención a su seguridad, desde todos los puntos de vista.
- Debemos **eliminarlos**, o reducir el impacto de un posible fallo.
  ⇒ Redundancia, sistemas tolerantes a fallos...

Ejemplo habitual: cortafuegos

- Todo el tráfico de la red pasa por él.
- Si deja de funcionar obtengo segmentos aislados entre sí.
- Eliminación: cortafuegos en HA, balanceo de carga...
- Reducción del riesgo: cortafuegos replicados, procedimientos de *bypass*...

SEGURIDAD DE LA RED

- Introducción.
- Seguridad del entorno.
- Seguridad del sistema.
- Seguridad de la red. ⇐
- Gestión de la seguridad.
- Otros aspectos de la seguridad.
- Conclusiones.

Seguridad de la red

- **Introducción.**
- **Amenazas remotas.**
  - Introducción: servicios de red.
  - Piratas informáticos.
  - Ataques.
- **Contramedidas:**
  - Prevención.
    - Seguridad perimetral.
    - Comunicaciones cifradas.
  - Detección.
    - Sistemas de detección de intrusos.

- Sin sentido hace años.
- Actualmente, necesaria en casi todos los entornos:
  ⇒ Los sistemas aislados son cada vez menos comunes.
- Excepciones típicas: bancos, *hosts*...
- La mayor parte de amenazas son remotas.
  ⇒ ¡Esto no significa que el atacante lo sea!

¿Alguien de nosotros trabaja en un entorno sin amenazas remotas?

La red introduce grandes avances, pero también muchas amenazas:

- Compartición de conocimientos entre piratas.
- Un atacante no tiene que llegar físicamente a nuestro entorno para causarnos problemas.
- La complejidad en las aplicaciones las hace más vulnerables.
- 'Aldea global': todos conocemos los problemas de todos.

Sistema de red

- *Software* que posibilita la conexión entre sistemas.
- Dos grandes partes:
  - *Kernel*: Tareas de bajo nivel (pila TCP/IP, controladores de interfaces, tablas de rutado...).
  - Aplicación: Programas y ficheros para configuración de parámetros de red desde espacio de usuario.
- Introduce vulnerabilidades y riesgo: somos potenciales objetivos remotos.

Servicios de red

- Las redes se crean para intercambiar información entre los sistemas que están conectados a ellas.
- Un sistema intercambia la información que alberga mediante **servicios** ofrecidos al 'exterior'.

  SMTP, HTTP, FTP...
- Cada servicio ofrecido es una puerta de entrada a nuestra información.
- Cada uno de ellos introduce nuevas vulnerabilidades: lo sirve un programa en muchos casos complejo y con graves problemas.

Nuestros servicios

- La 'puerta de entrada' no siempre es legítima.
- Debemos reducir su número al máximo.
  ⇒ Servicios innecesarios.
- Asegurar los servicios que no podamos eliminar.
  ⇒ Servicios de alto riesgo.

Consideraciones en MIS sistemas

- ¿Qué servicios estoy ofreciendo?

  ```
  netstat -an |grep -i listen
  ```

- ¿Por qué los ofrezco? ¿Son realmente necesarios?
- ¿A quién se los ofrezco?

  Cortafuegos, *wrappers*...
- ¿Qué programa los ofrece? ¿Es vulnerable?

  Apache, Internet Information Server, ProFTPD, Oracle...

Piratas informáticos

- Ya hemos hablado de ellos: clasificación.
- *Hackers*, *crackers*, *phreakers*...
- El factor 'simpatía'.
- El factor 'eso sólo pasa en el cine'.
- ¿Genios informáticos? **NO**, sólo delincuentes.

Motivos de un pirata

- Satisfacción personal.
- Caso particular de 'satisfacción': vandalismo.
- *Status* social en la comunidad *underground*.
- Venganza.
- Dinero (o 'especias').
- ...

Grupos Tigre

- Piratas contratados por el propietario de los activos con el objeto de determinar su nivel de vulnerabilidad.
- $\neq$ Intrusismo remunerado.
- Denominación comercial: *hacking ético*.
- 'Auditoras' que presumen de contar con los mejores piratas.
- Rechazado por todos los expertos en seguridad.

¿Quién contrata a un pirata para que analice sus vulnerabilidades?

YO NO.

Ataques

- 'Escaneos' de puertos.
- *Spoofing*.
- Negaciones de servicio.
- Interceptación.
- Análisis de vulnerabilidades.

'Escaneos' de puertos

- Determinación del estado de todos o algunos puertos en uno o varios sistemas remotos.
- Ataques poco 'agresivos'.
- Quizás simple curiosidad...
- ...pero puede ser el principio de un ataque más serio.

Clasificación de los escaneos

- En función del objetivo elegido:
  - Barridos horizontales (Un puerto, varias máquinas).
  - Barridos verticales (Varios puertos, una máquina).
- En función de la técnica empleada:
  - *Open*: Protocolo *Three–Way Handshake* .
  - *Half–Open*: No finaliza el protocolo.
  - *Stealth*: Viola el protocolo.

Estado de los puertos

- Tres posibles estados de un puerto:
  - Abierto.
  - Cerrado (o filtrado mediante *Reject*).
  - Filtrado (mediante *Drop*).
- Podemos determinar el estado mediante un simple `telnet`.
- Herramienta habitual: `nmap`.

¿Cómo protegerme?

- **No** puedo evitar el escaneo.
- Puedo minimizar sus resultados:
  - NAT (*Network Address Translation*).
  - *Proxies*.
  - Filtrado: *Drop* vs. *Reject*.
  - IDS + AR.
  - ...
- Hablaremos de las técnicas en el apartado siguiente.

Spoofing

- Creación de tramas TCP utilizando suplantando la dirección origen.
- Aprovecha relaciones de confianza entre máquinas.
- Entran en juego tres sistemas: atacante, atacado y suplantado.
- Ataque 'ciego': el pirata no ve las respuestas de su objetivo.

Escenario

- Dos sistemas (A y B) mantienen relación de confianza por IP.
- Atacante (C) deja 'fuera de juego' a B.
- C simula *three–way handshake* con A.
- Si tiene éxito, C envía orden a A sin esperar respuesta.
- Orden: permitirá conexión 'normal'.

Dificultades

- Evitar que el sistema suplantado intervenga en el *three–way handshake*.

  ⇒ Negación de servicio.

- Generación de números de secuencia TCP/IP.

  ⇒ Números aleatorios que cada máquina genera en su primera trama de la conexión.

- Superación del ataque ciego.

Negaciones de servicio

- Degradación total o parcial de un recurso, rebajando su nivel de disponibilidad.
- Denominadas **DoS** (*Denial of Service*).
- Existen negaciones locales (p.e. conejos), pero generalmente son remotas.
- Ataque muy habitual entre piratas novatos: *'nukes'*.
- Ejemplos: `teardrop`, `winnuke`, `smbnuke`...

Interceptación

- Captura de datos en tránsito o en proceso por parte de usuarios no autorizados.
- Realizado mediante herramientas *software* o mediante *hardware* dedicado.
- Ataque completamente **pasivo** ⇒ Peligrosidad.
- El más habitual: *sniffing*

Modelos habituales de interceptación

- *TTYSnooping*: Captura lógica de sesiones locales (en terminal, TTY).
- *KeyLogging*: Registro de datos introducidos por teclado.
- *Sniffing*: Captura de tramas que circulan por la red local.
  $\Rightarrow$ El más habitual.
- ...

Sniffing

- *Hardware*: *Sniffers* de alta impedancia.
- *Software*: Un atacante con privilegio total en el sistema pone su tarjeta en modo promiscuo.

  ⇒ Problema: ¡Windows 9x! (una vez más ;)
- Redes de difusión: Todos ven las tramas de todos.
- Resultado: captura de toda la información en tránsito.
- Ejemplos de capturadores: `dsniff`, `TCPDump`, `SniffIt`...

¿Qué hacer?

- Arquitecturas de red seguras.
  ¿Switches?
- Cableado en vacio.
- Redes punto a punto.
- ...
- **CIFRADO**, cifrado y más cifrado.

Análisis de vulnerabilidades

- Análisis de las vulnerabilidades remotas de un sistema operativo y sus aplicaciones.
- Ayuda al responsable de seguridad a determinar el nivel de riesgo de algunos de sus recursos.
- Realizado durante auditorías de seguridad...
- ...pero también durante ataques.
- Herramientas automáticas + análisis manual.

Analizadores

- Pueden analizar un servicio o subsistema concreto, o bien realizar un análisis completo.
- Extremadamente útiles en las manos adecuadas pero muy peligrosos en las de un pirata.
- Generalmente herramientas de uso público.

  ⇒ Si no las empleamos nosotros, un pirata lo hará.
- Su uso periódico debería considerarse **prioritario**.
- Ejemplos: *Nessus*, *ISS Internet Scanner*, *WMap*...

Seguridad perimetral

- **IDEA**: Definición de un perímetro lógico que aisla entre sí dos o más zonas en función de sus requisitos de seguridad.
- Al menos dos zonas: interna (confiable) y externa (insegura).
- En nuestro entorno, recomendables más zonas aisladas mediante sistemas cortafuegos:
  - DMZ externa.
  - DMZ interna.
  - Ofimática.
  - Servidores internos.
  - ...

Cortafuegos

- Sistema o grupo de sistemas que implanta una política de control de acceso entre diferentes redes o segmentos.
- Generalmente, sistema operativo **especialmente asegurado** (*firewall software*) o *appliance* dedicada (*hardware*).
- Al menos dos zonas:
  - Espacio protegido: perímetro de seguridad.
  - Espacio exterior: zona de riesgo.

Cortafuegos: definiciones

- **Bastión:** Punto de contacto entre dos o más redes.

  ⇒ Especialmente crítico por estar conectado a una zona de riesgo.

- **Choke:** Elemento que implanta el filtrado de paquetes.

- **Proxy:** Programa que controla el acceso a una cierta aplicación entre diferentes redes.

Arquitecturas de cortafuegos: filtrado de paquetes

- Modelo más antiguo y sencillo.
- Bloqueo o permito el tránsito de tramas en función de algunas de sus características:
  - Direcciones origen y destino.
  - Puertos origen y destino.
  - Interfaces de entrada y salida.
  - Protocolo.
  - ...
- Implantado en un *router* o en un servidor mediante ACLs.

Arquitecturas de cortafuegos: *multi–homed host*

- Sistema con dos o más tarjetas de red conectadas a diferentes segmentos.
- *Proxy* por cada servicio que pase por el cortafuegos.
- Diferentes zonas 'no se ven' entre sí, sólo al *firewall*.
- Entrada/salida: conexión al *firewall* o vía *proxy*.
- Incómodo para el usuario ⇒ Poco utilizado.

Arquitecturas de cortafuegos: *screened host*

- *Choke* que filtra tráfico.
- Bastión con servidores *proxy*.
- Entrada/salida: directa (ACLs) o vía *proxy*.
- ¡Dos puntos únicos de fallo!

Arquitecturas de cortafuegos: *screened subnet*

- Arquitectura más utilizada en la actualidad.
- Define DMZ (zona desmilitarizada, *De–militarized zone*): segmento donde ubicar el bastión y otros elementos.
- Al menos dos *chokes* (suelen coincidir en un único sistema).
- Entrada/salida: directa (ACLs) o vía *proxy*.

Cortafuegos: problemática asociada

- Falsa sensación de seguridad.
- Sólo detecta ataques que pasen por el cortafuegos.
  ¿Y si un usuario instala un módem?
- Trabaja a niveles bajos: deja pasar mucho tráfico dañino.
- Implantación compleja ⇒ Errores.
- Punto único de fallo en nuestra red.

Comunicaciones cifradas

- Utilización de mecanismos de cifra para eliminar (minimizar) el impacto de la interceptación de las comunicaciones:
  - Protocolos cifrados.
  - Túneles de cifrado.
  - Redes privadas virtuales.
- Debemos considerarlas **obligatorias** para datos críticos.

¿Cuántas claves circulan cada día en claro por mi red?

Protocolos cifrados

- Mayoría de protocolos: en texto claro.
- Debo tratar de sustituirlos por equivalentes cifrados.
  $\Rightarrow$ SSH vs. *telnet*, `rlogin`, `rsh`...
- ¿Es siempre posible?

Túneles de cifrado

- No siempre puedo utilizar (o existen) equivalentes cifrados.
- Solución: túnel de cifra por el que pasa un protocolo en texto claro.
- Ejemplos: túneles SSH, STUNNEL (SSL)...

Redes privadas virtuales

- Mecanismo que permite utilizar redes de propósito general para transmitir datos de forma segura.
- Mucho más barato que soluciones dedicadas.
- Integrado con algunos productos cortafuegos y SSOO.
- ¡No necesariamente caro!

Redes privadas virtuales: conceptos

- VPN = Cliente + Pasarela.
- *Tunneling:* Encapsulación de tramas dentro de otras proporcionando confidencialidad (sólo son visibles las direcciones de los puntos VPN).
- Diferentes protocolos que implementan VPNs, en ocasiones incompatibles entre sí.

Redes privadas virtuales: uso

- Conexión cliente remoto a LAN.

  ⇒ Cliente VPN remoto (p.e. portátil) conecta a pasarela corporativa.

- Conexión entre LANs remotas.

  ⇒ Extensión del concepto anterior: en lugar de cliente, conexión de red completa.

- Acceso controlado en LAN.

  ⇒ Aprovecho beneficios de VPN en mi red.

Protocolos VPN: PPTP

- *Point–to–Point Tunneling Protocol.*
- Desarrollado por diferentes compañías.
- Soporte a protocolos no IP (p.e. PPP).
- Integrado en muchos productos (p.e. Microsoft Windows).
- No proporciona estándar de cifrado y autenticación.
  $\Rightarrow$ Productos compatibles PPTP e incompatibles entre sí.

Protocolos VPN: L2TP

- *Layer 2 Tunneling Protocol* (nivel de enlace OSI).
- Basado en protocolo L2F (*Layer 2 Forwarding*), mejorado con algunas características de PPTP.
- Implementado principalmente en productos Cisco.
- Como PPTP, soporta clientes no IP, pero no define estándar de cifrado.
- Adicionalmente, soporta VPNs no basadas en Internet: *Frame Relay*, ATM...

Protocolos VPN: IPSec

- *IP Security.*
- Colección de protocolos usados como solución VPN completa o como simples esquemas de cifra.
- Extensión de IP para incluir ciertos servicios de seguridad (no sólo VPNs).
- Trabaja a nivel 3 OSI (Red).

Redes privadas virtuales: beneficios

- Integridad: Uso de resúmenes antes de emitir y después de recibir información.
- Confidencialidad: Uso de algoritmos simétricos de cifra (3DES, RC4...).
- Autenticación: Uso de algoritmos de clave pública (RSA, Diffie–Hellman...).
- Transparencia: Establecida la VPN, el usuario trabaja de forma normal, como si estuviera dentro de la red donde se ubica la pasarela.
- Precio: Mecanismo mucho más barato que otras soluciones.

Redes privadas virtuales: desventajas

- Muchas veces mecanismos complejos de implantar y gestionar.
- Disponibilidad y rendimiento dependiente de factores externos a la organización.
- Estándares inmaduros: incompatibilidad entre fabricantes (PPTP, IPSec...).

Sistemas de detección de intrusos

- Intrusión: Conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad de un recurso.
  - No sólo penetraciones contra un sistema.
- Detección de intrusos: Análisis automático de parámetros que modelan la actividad de un entorno con el propósito de detectar e identificar intrusiones.

Clasificación de los IDSes

- En función de dónde provienen sus datos:
  - IDSes basados en máquina (HIDS, *Host–based IDS*).
  - IDSes basados en red (NIDS, *Network–based IDS*).
- En función de la técnica utilizada:
  - Detección de anomalías (*Anomaly detection*).
  - Detección de usos indebidos (*Misuse detection*).
- En función de su modo de funcionamiento:
  - Periódicamente o 'pasivos'.
  - En tiempo real o 'activos'.

Seguridad de la red → Contramedidas

Habitualmente...

- *Network–based IDS*, NIDS (vs. *Host–based IDS*, HIDS).
- Detección de usos indebidos (vs. detección de anomalías).
- Detección distribuida.

Algunos ejemplos: SNORT

- `http://www.snort.org/`
- NIDS, *misuse detection* (sistema experto), tiempo real...
- Sistema abierto: muchas herramientas de terceros, incluida AR.

¡Libre (GNU)!

Algunos ejemplos: RealSecure

- Internet Security Systems, Inc. (`http://www.iss.net/`).
- NIDS, *misuse detection* (sistema experto), tiempo real...
- Generación de informes 'escalada'.
- Incorpora respuesta automática.

Algunos ejemplos: PHF

- Sistema de decepción (*honeypot*) simple.
- Emula vulnerabilidad BID #629 en el CGI `phf` (1996), que permite ejecución remota.
- Proporciona información falsa (pero creíble) al atacante, mientras registra sus actividades.
- Fichero único en PERL: efectivo, fácil de instalar y gestionar.

Seguridad de la red → Contramedidas

¿Son necesarios? SÍ

- Los sistemas cortafuegos no son mágicos.
- Proporcionan conocimiento del entorno.
- Alertas ante actividades sospechosas.
- Registro adicional de incidentes. . . ¿Pruebas judiciales?
- . . .

Seguridad de la red → Contramedidas

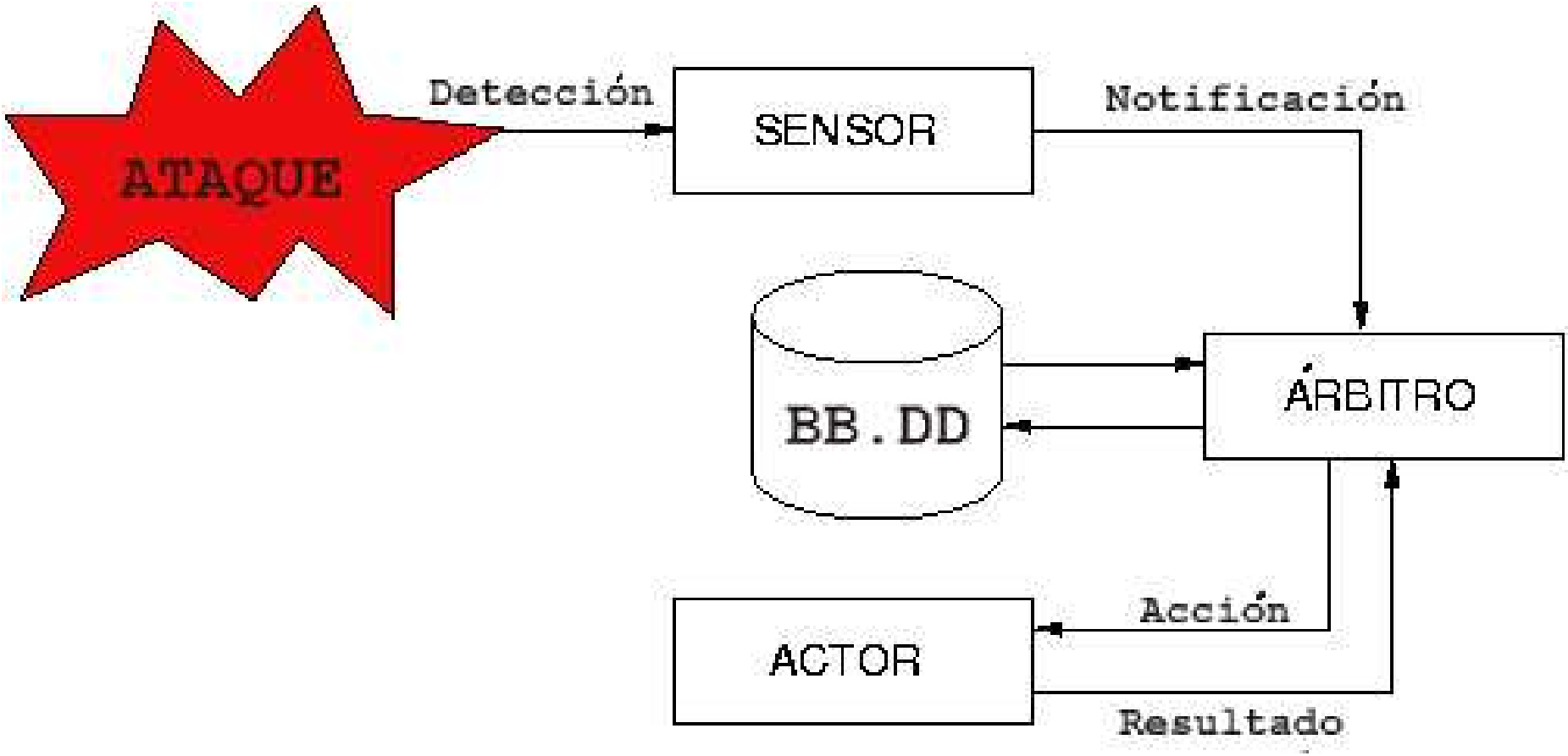
¿Son suficientes? NO

- Normalmente, sólo detectan ataques conocidos.
- Es posible (y a veces fácil) engañarlos.
- ¡IMPORTANTE!: Mecanismos de seguridad **pasivos**.
- ...

IDSes: Respuesta automática

- AR: Conjunto de acciones que se ejecutan sin intervención humana al detectar un evento, generalmente con el objetivo de salvaguardar la integridad, disponibilidad o confidencialidad de un determinado recurso.
- Transformación del IDS en mecanismo **activo**.
- ¿Por qué responder ante un ataque muchas veces conocido?

Esquema de funcionamiento



Tipos de respuesta

- Registro
- Bloqueo
- Ataque
- Recuperación
- Decepción

Riesgos de la AR

- **Negación de Servicio**
- ¿Cómo minimizar el riesgo?
  - Limitación de respuestas por u.t.
  - Actores protegidos.
  - Ponderación de ataques.

GESTIÓN DE LA SEGURIDAD

- Introducción.
- Seguridad del entorno.
- Seguridad del sistema.
- Seguridad de la red.
- Gestión de la seguridad. ⇐
- Otros aspectos de la seguridad.
- Conclusiones.

Gestión de la seguridad

- Introducción.
- Análisis de riesgos y amenazas.
- Políticas de seguridad.
- Seguridad en la organización.
- Normativas de seguridad.
  - UNE 71501.
  - ISO 27002.
  - ISO 27001.
  - ISO/IEC 15408.

Gestión de la seguridad → Introducción

- **Gestionar** es llevar a cabo las diligencias necesarias para lograr un determinado fin.

  ⇒ La gestión de la seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización.

- Consideraciones:
  - Los problemas de seguridad no son únicamente de índole tecnológica.
  - Los riesgos no se eliminan. . . se gestionan.
  - La seguridad no es un producto, es un **proceso**.

Gestión de la seguridad → Introducción

Es necesario **gestionar** la seguridad de la información:

- Garantizar la confidencialidad, integridad y disponibilidad de sus activos es crítico para cualquier organización.
- Las nuevas tecnologías introducen nuevas amenazas.
- La dependencia creciente de los recursos de TI aumenta los impactos.
- No siempre podemos eliminar los riesgos.
- ...

Gestión de la seguridad → Análisis de riesgos y amenazas

- Proceso necesario para responder a tres cuestiones sobre nuestra seguridad:
  - ¿Qué queremos proteger?
  - ¿De qué lo queremos proteger?
  - ¿Cómo lo queremos proteger?
- Dos aproximaciones: cuantitativa y cualitativa

Análisis cuantitativo

- Dos parámetros fundamentales:
  - Probabilidad de que produzca cierta pérdida (riesgo).
  - Estimación del coste si la pérdida ocurre (impacto).
- Su producto: Coste anual estimado (EAC, *Estimated Annual Cost*).
- Determino el coste de implantar cierta salvaguarda para prevenir la pérdida.

  $\Rightarrow$ Si el coste es menor que EAC, debo implantarla.
- Análisis de riesgos caro y complejo.

Análisis cualitativo

- Más sencillo e intuitivo que el anterior: no aplico fórmulas ni pesos exactos.
- Determino amenazas, vulnerabidades, riesgos e impactos de forma aproximada (p.e. 'alto', 'medio', 'bajo').
- Con estos datos obtengo indicador cualitativo del nivel de riesgo asociado a cada activo.
- Aplico salvaguardas en función de mis resultados.

Resultados del análisis

- Riesgo calculado: resultado del análisis de riesgos.
- Umbral de riesgo: parámetro definido por la política corporativa.
- Riesgo residual: $R_r = U - R_c$
- Si el riesgo residual es positivo (riesgo calculado menor que el umbral), hablo de riesgo asumible. $\Rightarrow$ ¡$\neq$ asumido!
- Si es negativo ($R_c > U$) he de reducir el riesgo.

Gestión de la seguridad → Análisis de riesgos y amenazas

MAGERIT

- Metodología de Análisis y GEstión de Riesgos de los sistemas de Información de las AdminisTraciones públicas.
- Aproximación cualitativa y genérica.
- Cuatro etapas:
  - Planificación.
  - Análisis de riesgos.
  - Gestión de riesgos.
  - Aplicación de salvaguardas.
- http://www.map.es/csi/

Gestión de la seguridad → Políticas

- Conjunto de requisitos definidos por los responsables directos o indirectos de un sistema de información que indica en términos generales qué está y qué no está permitido en cuanto a seguridad se refiere durante la operación habitual del sistema.
- Dos aproximaciones:
  - Prohibitiva: todo lo que no esté explícitamente permitido está prohibido (recomendable).
  - Permisiva: todo lo que no esté explícitamente prohibido está permitido.
- Términos generales ⇒ He de concretar en normativas o políticas de aplicación específica.

Gráficamente...

Gestión de la seguridad → Organización

Políticas de aplicación específica

- Seguridad organizativa.
- Clasificación y control de activos.
- Seguridad del personal.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Controles de acceso.
- Desarrollo y mantenimiento de sistemas.
- Gestión de incidentes.
- Gestión de continuidad de negocio.
- Requisitos legales.

Gestión de la seguridad → Organización

El Área de Seguridad...

- ...define normativas y vela por su implantación.
  ⇒ Trabajo más normativo que técnico.
- ...formada por profesionales cualificados e interesados.
  ⇒ El problema del personal 'reciclado'.
- ...independizada de otras áreas pero integrada con ellas.
- ...debe ser respaldada desde la dirección, al más alto nivel.

Outsourcing

- Externalización de la gestión de seguridad de los SSII.
- Cada día más practicado, sobre todo en la empresa privada.
- La seguridad no es un fin, sólo una herramienta más al servicio de un determinado negocio.
- Recomendable si la organización está alejada del mundo de las tecnologías.

Outsourcing: Ventajas

- Permite al contratista centrarse en sus líneas de negocio.
- Gestión realizada por personal *a priori* muy especializado.
- El contratado dispone de más recursos técnicos de seguridad que el contratista.
- Habitualmente reduce riesgos y costes.

Outsourcing: Inconvenientes

- Dejamos nuestra seguridad en manos de desconocidos.
- Exceso de 'despreocupación'.

  ⇒ No es recomendable desentenderse por completo de la gestión de seguridad.
- Seguridad 'en serie'.
- En ocasiones, simplemente falta de profesionalidad.

UNE 71501 (ISO/IEC TR 13335)

- Conocida como GMITS (*Guidelines for the Management of IT Security*).
- Guía para la gestión de la seguridad de T.I.
- Facilita la comprensión de la seguridad de las T.I. y proporciona orientaciones sobre su gestión.
- Dirigido a los responsables de seguridad de T.I.
- **No certificable** (TR).

UNE 71501: Objetivos

- Definir y describir los conceptos relacionados con la gestión de la seguridad de T.I.
- Identificar las relaciones entre la gestión de la seguridad de las T.I. y la gestión de las T.I. en general.
- Presentar varios modelos para explicar la seguridad de las T.I.
- Proporcionar orientación sobre la gestión de seguridad de las T.I. y la elección de salvaguardas.

UNE 71501: Estructura

Tres partes diferenciadas:

- UNE 71501-1: Conceptos y modelos para la seguridad de TI.
  ⇒ Visión general y conceptos fundamentales.
- UNE 71501-2: Gestión y planificación para la seguridad de TI.
  ⇒ Relaciones entre los aspectos de gestión de la seguridad.
- UNE 71501-3: Técnicas para la gestión de la seguridad de TI.
  ⇒ Técnicas de seguridad aplicables en el ciclo de vida de un proyecto.

ISO 13335 define partes adicionales, no traducidas hasta el momento.

Gestión de la seguridad → Normativas

Utilizaremos UNE 71501 para identificar y gestionar todos los aspectos de la seguridad de las T.I.:

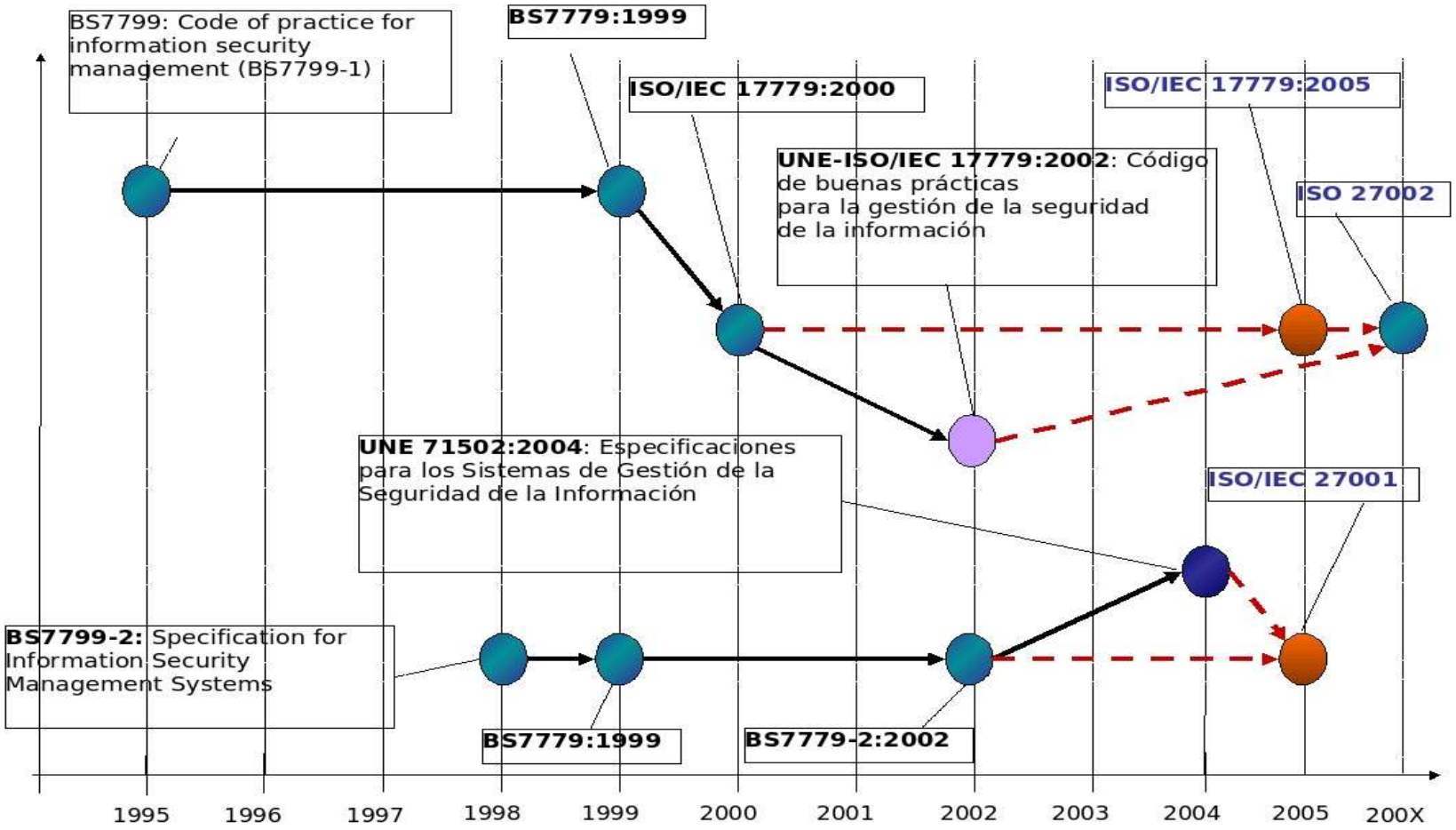
- Conocimiento de los aspectos básicos de la seguridad.
- Relaciones entre dichos aspectos y con el resto de las T.I.
- Necesidades de seguridad organizativas.
- Selección de salvaguardas.
- Control y seguimiento de su implantación.
- ...

Gestión de la seguridad → Normativas

ISO 27002

- Código de buenas prácticas para la gestión de seguridad de los SS.II.
- Proporciona una base común para desarrollar estándares y gestión práctica de la seguridad: lo que *deberíamos* hacer.
- Dirigido a los responsables de iniciar, implantar o mantener la seguridad en una organización.
- Quizás una norma 'técnica', pero no tecnológica.
  $\Rightarrow$ SSII (ISO 27002) vs. TI (ISO 13335)

ISO 27002: Historia



Gestión de la seguridad → Normativas

ISO 27002 define once dominios de control:

- Política de seguridad.
- Organización de la Seguridad de la Información.
- Gestión de activos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Gestión de continuidad de negocio.
- Cumplimiento (legal, técnico...).

Gestión de la seguridad → Normativas

Utilizaremos ISO 27002 para desarrollar estándares de seguridad organizativa y gestión práctica de la misma:

- Construcción de la infraestructura de seguridad.
- Definición de políticas.
- Selección y gestión de controles.
- ...

ISO 27001

- Especificaciones para los sistemas de gestión de la seguridad de la información (SGSI).
- Basada en BS 7799 – II: guía de auditoría basada en requisitos.
- Aparecen la **auditoría** y el **control:**

  ⇒ Norma certificable y auditable.

ISO 27001: SGSI

- Estructura organizativa, procedimientos, procesos y recursos necesarios para implantar la gestión de la seguridad de la información.
- Herramienta para la Dirección para cumplir políticas y objetivos de seguridad.
- Proporciona mecanismos para la salvaguarda de los activos conforme a la política de seguridad.

ISO 27001: Etapas del SGSI

- Marco general.

  ⇒ Establecimiento de controles, documentación, registros...

- Implantación.

  ⇒ Implantación y eficacia de los controles.

- Explotación.

  ⇒ Gestión de recursos, competencias...

- Revisión.

  ⇒ Auditoría y control.

- Mejora.

  ⇒ Mejora contínua y acciones preventivas y correctivas.

Gestión de la seguridad → Normativas

Utilizaremos ISO 27001 para establecer, implantar, documentar y evaluar un SGSI de acuerdo con ISO 27002:

- Especificación de los requisitos de los controles de seguridad.
- Control de registros.
- Implantación, explotación y revisión del SGSI.
- Auditoría.
- Mejora contínua de nuestro SGSI.
- ...

ISO/IEC 15408

- Adaptación ISO de los Criterios Comunes (*Common Criteria for Information Technology Security Evaluation*).
- Utilizado para evaluar la seguridad (IT) de un determinado producto o sistema, total o parcialmente.

  ⇒ Aplicaciones, redes, sistemas operativos, *chips*...
- **TOE** *(Target Of Evaluation)*: parte del producto o sistema que es objeto de evaluación.

ISO/IEC 15408: Estructura

- Tres partes diferenciadas:
  1. Introducción y modelo general.
  2. Requisitos funcionales de seguridad.
     Definen el comportamiento de seguridad deseado del TOE ante diferentes amenazas.
  3. Requisitos de aseguramiento.
     Definen las propiedades del TOE que proporcionan la confianza en su seguridad.

ISO 15408: requisitos funcionales

- FAU. Auditabilidad de la seguridad.
- FCO. Comunicaciones.
- FCS. Soporte criptográfico.
- FDP. Protección de datos de usuarios.
- FIA. Identificación y autenticación.
- FMT. Gestión de seguridad.
- FPR. Privacidad.
- FPT. Protección de las funciones de seguridad.
- FRU. Utilización de recursos.
- FTA. Acceso al TOE.
- FTP. Canales de comunicación fiables.

ISO 15408: requisitos de aseguramiento

- Gestión de configuraciones.
- Entrega y operación.
- Desarrollo de producto.
- Documentación del producto.
- Soporte durante el ciclo de vida.
- Pruebas de conformidad.
- Análisis de vulnerabilidades.

Gestión de la seguridad → Normativas

ISO 15408 proporciona una escala de evaluación de aseguramiento formada por **siete niveles EAL** *(Evaluation Assurance Levels)*:

- EAL1. Funcionalmente probado.
- EAL2. Estructuralmente probado.
- EAL3. Metodológicamente probado y comprobado.
- EAL4. Metodológicamente diseñado, probado y revisado.
- EAL5. Diseñado y probado semiformalmente.
- EAL6. Diseño verificado y probado semiformalmente.
- EAL7. Diseño verificado y probado formalmente.

OTROS ASPECTOS

- Introducción.
- Seguridad del entorno.
- Seguridad del sistema.
- Seguridad de la red.
- Gestión de la seguridad.
- Otros aspectos de la seguridad. ⇐
- Conclusiones.

Otros aspectos de la seguridad

- Criptología.
- Herramientas de seguridad.
- Aspectos legales.

Introducción

- **Ciencia** que trata los problemas teóricos relacionados con la seguridad en el intercambio de mensajes en clave entre un emisor y un receptor a través de un canal de comunicaciones.
- Tan antigua como nuestra civilización.
- Dos ramas:
  - Criptografía: estudia el diseño de criptosistemas.
  - Criptoanálisis: estudia la rotura de criptosistemas.

Historia de la criptografía

Tres grandes periodos:

- Hasta 1949: criptografía precientífica ('arte').
  ⇒ *Scytale*, cifrado Caesar, cifrado Vigènere, Enigma...
- 1949–1976: criptografía científica (base matemática).
  ⇒ *Lucifer*, DES...
- Desde 1976: criptografía de clave pública.
  ⇒ RSA, ElGamal, DSA...

Criptosistemas

Cuaterna de elementos $\{\mathcal{A}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$:

- Alfabeto $\mathcal{A}$.
- Espacio de claves $\mathcal{K}$.
- Transformaciones de cifrado $\mathcal{E} : \mathcal{A} \rightarrow \mathcal{A}$.
  $\Rightarrow \mathcal{E}(k, a) = c$
- Transformaciones de descifrado $\mathcal{D} : \mathcal{A} \rightarrow \mathcal{A}$.
  $\Rightarrow \mathcal{D}(k', c) = a$

Funcionamiento de un criptosistema

1. Emisor emite texto en claro.
2. Cifrador lo cifra utilizando una clave de cifrado, creando un criptograma.
3. Criptograma llega al descifrador a través de un cierto canal.
4. Descifrador convierte el texto cifrado en texto claro, apoyándose en una clave de descifrado.
5. Receptor lee texto claro que coincide con el emitido.

Cifrado simétrico

- También denominado de clave secreta, privada o única.
- Clave de descifrado puede ser calculada en función de la de cifrado y viceversa (generalmente, ambas son idénticas).
- Seguridad del criptosistema: secreto de la clave.
  $\Rightarrow$ ¿Cómo la transmito?
- Clave de cifrado y descifrado entre cada dos usuarios del criptosistema: $\frac{N(N-1)}{2}$ claves para N usuarios.
  $\Rightarrow$ Impracticable en SSII.
- Ejemplos: Caesar, Vigènere, DES...

Cifrado asimétrico

- También denominado de clave pública.
- Claves de cifrado (pública) y descifrado (privada) diferentes.
- No son independientes, pero es imposible determinar la clave privada únicamente conociendo la pública.
- Cualquiera puede cifrar con mi clave pública, pero sólo yo puedo descifrar (con mi clave secreta).
- Cualquiera puede verificar la autenticidad de mi mensaje (no repudio).
- Lento para cifrado de comunicaciones.
- Ejemplos: RSA, ElGamal...

Funciones resumen

- *Hash Functions.*
- Proyecciones de un conjunto (generalmente de muchos o infinitos elementos) sobre otro de tamaño fijo y más pequeño que el anterior:

  $$H : A \rightarrow B$$

- Ejemplo:

$$H(x) = \begin{cases} 0 & x \leq 0 \\ 1 & x > 0 \end{cases}$$

- No todas las funciones resumen son interesantes en criptología: han de cumplir ciertas propiedades.

Propiedades de las funciones resumen en criptología

- Entrada puede ser de tamaño indeterminado.
- Salida de tamaño fijo, varios órdenes de magnitud más pequeño que la entrada.
- Dado x, calcular $H(x)$ es computacionalmente barato.
- $H(x)$ es de un solo sentido (*One–Way Hash Function*).
  $\nexists\, H^{-1}(x)$ o su cálculo es computacionalmente difícil.
- $H(x)$ no presenta colisiones.
  $x \neq y \rightarrow H(x) \neq H(y)$

Ejemplo: MD5 (*Message Digest 5*).

Firma digital

- Basada en criptografía de clave pública.
- Misma idea que firma 'tradicional': no repudio.
- Adicionalmente: confidencialidad (cifrado) e integridad (resumen).
- Ejemplos: PGP, GPG...
  - Firmo con mi clave privada.
  - Cifro con la clave pública del receptor.
- Problema: ¿cómo doy a conocer mi clave pública?

Certificados digitales

- Fichero que contiene información identificativa junto a la clave pública de un usuario (estándar X.509):
  - Nombre de CA (emisor del certificado).
  - Nombre del propietario.
  - Clave pública del propietario.
  - ...
- Firmado por un 'notario' (*Trusted Third Party*) que autentica sujetos y emite y gestiona certificados (CA, *Certification Authority*).
- Nos 'fiamos' del notario.

Criptoanálisis

- Ciencia 'complementaria' (no opuesta) a la criptografía.
- **Muy compleja.**
- Estudia como romper los criptosistemas.
- Ventaja para el analista: los usuarios son el punto más débil de un criptosistema.

Criptoanálisis: condiciones del peor caso

1. El criptoanalista tiene acceso completo al algoritmo de cifra.
   Principio de Kerckhoffs: La seguridad del cifrado reside exclusivamente en el secreto de la clave, no en el mecanismo de cifrado.
2. El criptoanalista tiene una cantidad considerable de texto cifrado.
3. El criptoanalista conoce el equivalente en claro de parte de ese criptograma.

Criptoanálisis: ataques

- Ataque exhaustivo o de fuerza bruta: pruebo todas las posibles claves.
- Ataque sólo al criptograma: conozco algoritmo de cifra y tengo acceso al texto cifrado.
- Ataque de texto en claro conocido: se cumplen condiciones del peor caso.
- Ataque de texto en claro escogido: además del peor caso, puedo cifrar cantidad indeterminada de texto en claro.
- Ataque de texto cifrado escogido: puedo obtener texto en claro correspondiente a criptogramas de mi elección.

Esteganografía

- Ciencia que estudia los procedimientos encaminados a ocultar la existencia de un mensaje en lugar de su contenido.
- No sustituye al cifrado convencional: lo **complementa**.
- Ejemplos 'tradicionales': tinta invisible, micropunto...
- Ejemplos digitales: ocultación en imágenes, audio o video.
- Auge tras el 11-S.

Herramientas de seguridad

- SSH.
- Nessus.
- WMAP.
- Nikto.
- SNORT.
- Crack.
- Titan.

SSH

- *Secure Shell*: Protocolo diseñado para proporcionar comunicaciones seguras a través de redes no fiables.
- Aporta autenticación por claves pública/privada, cifrado...
- Dos variantes: comercial (http://www.ssh.com/) y libre (http://www.openssh.org/).
- Versiones de cliente y servidor para diferentes entornos, incluyendo Unix, Windows y dispositivos móviles...

Suite SSH

SSH proporciona emulación de terminal, transferencia segura de ficheros y redirección cifrada de puertos. Tres grandes aplicaciones:

- `ssh`: Sesión remota con un *host* (sustituyendo a `telnet`, `rsh`, `rlogin`...)
- `scp`: Transferencia segura de archivos (sustituyendo a `rcp`).
- `sftp`: Transferencia segura de archivos mediante interfaz similar a FTP (sustituyendo a `ftp`).

¡Todas las comunicaciones se realizan a través de un único puerto!

Nessus

- Analizador remoto de vulnerabilidades.
- Arquitectura cliente–servidor.
- Actualización periódica (y automatizable) de *plugins*.
- NASL (*Nessus Attack Scripting Language*): lenguaje propio para *plugins* (también en C).
- Genera informes en diferentes formatos (HTML, TXT, XML...).
- http://www.nessus.org/

WMAP

- Analizador de vulnerabilidades en servidores *web*.
- Herramienta englobada dentro del proyecto OSSTMM.
- Bases de datos de objetivos (directorios, archivos...) en inglés y castellano.
- Alternativa popular: Nikto.
- http://www.osstmm.org/tid.htm

SNORT

- Sistema de detección de intrusos basado en red.
- Funciona sobre Unix o Windows, sin consumir grandes recursos.
- Sencillo de instalar, configurar y gestionar.
- Base de datos de patrones actualizada frecuentemente.
- Muchas herramientas de terceros (AR, BBDD...).
- http://www.snort.org/

Crack

- *Crackeador* clásico de contraseñas Unix.
- Funciona sobre este sistema operativo.
- ¡También hay adivinadores para otros entornos!
  Ejemplo: L0phtCrack para Windows NT.
- Recomendable: complementarlo con más diccionarios.
- http://www.users.dircon.co.uk/~crypto/

Titan

- Analizador de vulnerabilidades a nivel local.
- Informa de configuraciones o gestión incorrecta de la máquina.
- Originalmente para Solaris; también funciona sobre Linux y FreeBSD.
- http://www.fish.com/titan/

Aspectos legales

- Ley Orgánica de Protección de Datos.
- Reglamento de Medidas de Seguridad.

Otros aspectos → Legales

LOPD

- Ley Orgánica 15/1999 de 13 de Diciembre, de Protección de Datos de Carácter Personal.
- **Ley Orgánica**: derivada inmediatamente de la Constitución de un estado y que contribuye a su más perfecta ejecución y observancia.

  $\Rightarrow$ Derecho fundamental.
- Deroga y amplia la antigua LORTAD.
- Establece el derecho de cada ciudadano a controlar datos relativos a su propia persona.

LOPD: Conceptos fundamentales (I)

Datos de carácter personal

Información concerniente a personas físicas indentificadas o identificables.

- Conciernen únicamente a personas físicas (no jurídicas).
- Proporcionan información sobre la persona a la que se refieren.
- Asociación entre la información proporcionada y el interesado.

LOPD: Conceptos fundamentales (II)

Fichero de datos personales

Conjunto organizado de datos de carácter personal cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

- 'Organizado': Ordenación tal que permita el acceso a los mismos en función de algún criterio lógico.
- No tiene por qué estar automatizado (aplica también a archivos físicos, a partir de 2007).
- No tiene por qué constituir un fichero único: datos **susceptibles** de ser incorporados a un fichero.

LOPD: Conceptos fundamentales (III)

Tratamiento de datos

Operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

- Ampliación LORTAD: . . . automatizado **o no**.

¿Alguien aquí **no** realiza tratamiento de datos?

LOPD: Infracciones leves

- No rectificar o cancelar datos personales a petición del interesado.
- Desatender a la APD (p.e. no inscribiendo el fichero).
- Recopilar datos personales sin informar de sus derechos al interesado.
- No cumplir el deber de secreto (nivel básico).
- ...

LOPD: Infracciones graves

- Creación de ficheros o recogida de datos con fines distintos a su objeto legítimo.
- No informar al afectado de los datos que de él disponemos.
- Mantenimiento sin condiciones de seguridad exigidas.
- Obstruir una inspección de la APD.
- No cumplir el deber de secreto (nivel medio).
- ...

Otros aspectos → Legales

LOPD: Infracciones muy graves

- Recogida de datos de forma engañosa y fraudulenta.
- Recogida y tratamiento de datos de nivel alto sin consentimiento expreso del afectado.
- Cesión de datos.
- No atender sistemáticamente los derechos del interesado (notificación, cancelación...).
- No cumplir el deber de secreto (nivel alto).
- ...

LOPD: Sanciones

- Infracciones leves: De 601,01 € a 60.101,21 €.
- Infracciones graves: De 60.101,21 € a 300.506,05 €.
- Infracciones muy graves: De 300.506,05 € a 601.012,10 €.

Reglamento de Medidas de Seguridad

- Real Decreto 994/99 de 11 de junio.
- Establece medidas técnicas y organizativas para garantizar la seguridad de los SSII donde existan datos de carácter personal.
- Define tres niveles de seguridad:
  - BÁSICO: Por defecto.
  - MEDIO: Infracciones administrativas, penales, de Hacienda Pública, servicios financieros o de evaluación de personalidad.
  - ALTO: Ideología, religión, creencias, origen racial, salud, vida sexual o fines policiales.

Otros aspectos → Legales

RMS: Nivel básico

- Documento de seguridad.
- Funciones y obligaciones del personal definidas y documentadas.
- Registro, notificación y gestión de incidencias.
- Control de accesos y relación de usuarios autorizados.
- Soportes: identificables, inventariados, salida y almacenamiento controlados...
- Copias al menos semanalmente.

RMS: Nivel medio

- Nivel básico + ...
- Identificación del responsable de seguridad en Documento de Seguridad.
  - Designado por el responsable del fichero.
  - Controla y coordina las medidas de seguridad definidas.
- Auditoría interna o externa al menos cada dos años.
- Identificación unívoca e inequívoca de usuarios.
- Gestión de soportes: registro de E/S, destrucción de datos...
- Registro de incidencias más exhaustivo.

Otros aspectos → Legales

RMS: Nivel alto

- Nivel medio + ...
- Control de accesos exhaustivo.
- Conservación de registros de acceso: dos años.
- Distribución de soportes cifrada.
- Transmisión cifrada (si se realiza a través de redes de terceros).
- Copias y sistemas de respaldo físicamente separados de los originales.

RMS: Implantación de medidas

- Se ha cumplido el plazo para todos los niveles.
- Si técnicamente no es posible: plazo de tres años.
  $\Rightarrow$ ¡Verano de 2003 para nivel alto!
- Incumplimiento: multas de hasta 100 Mptas (ficheros de titularidad privada) o sanciones administrativas (titularidad pública).
- Director de la APD puede ordenar la cesación del tratamiento y la cancelación de ficheros si no se cumple el Reglamento.

CONCLUSIONES

- Introducción.
- Seguridad del entorno.
- Seguridad del sistema.
- Seguridad de la red.
- Gestión de la seguridad.
- Otros aspectos de la seguridad.
- Conclusiones. ⇐

Conclusiones

- La información y los sistemas que la tratan son activos muy valiosos sobre los que existen **amenazas**, por lo que debemos protegerlos.
- Asociado a cada amenaza existe un **riesgo** (probabilidad de que la amenaza se materialice) y un **impacto** (daño que causa la materialización).
- Para minimizar o eliminar el riesgo y el impacto aplicamos **salvaguardas**, controles, etc. de todo tipo.

  $\Rightarrow$ No únicamente técnicos.

Conclusiones

- Seguridad = Confidencialidad + Integridad + Disponibilidad.
- La seguridad es una propiedad dinámica: el que hoy seamos seguros no implica que mañana lo sigamos siendo.

  $\Rightarrow$ Se suele decir que la seguridad es un **proceso**, no un producto.
- El objetivo marcado siempre debe ser mejorar nuestra seguridad: caminar hacia delante, nunca hacia atrás.

¡La seguridad total no existe!

Conclusiones

Seguridad del entorno

- Sobre un sistema de información, simplemente por estar en un momento y lugar determinados, existen amenazas.
- Los problemas de seguridad físicos se agravan con la introducción del factor humano.
- Debo garantizar que puedo responder de forma adecuada ante problemas en el entorno a diferentes niveles, desde los más simples a los más catastróficos.

  $\Rightarrow$ ¡Riesgo vs. coste!
- Estos aspectos frecuentemente se descuidan, pero no podemos hacerlo para hablar de seguridad global.

Conclusiones

Seguridad del sistema

- Todos los sistemas son *a priori* vulnerables desde un punto de vista lógico.
- Siempre (¿casi?) disponemos de las herramientas para garantizar un nivel aceptable de seguridad, pero en ocasiones no de los recursos (humanos, económicos, materiales...) suficientes para lograrlo.
- Debo tratar de garantizar un equilibrio entre funcionalidad, seguridad...y costes.

Conclusiones

Seguridad de la red

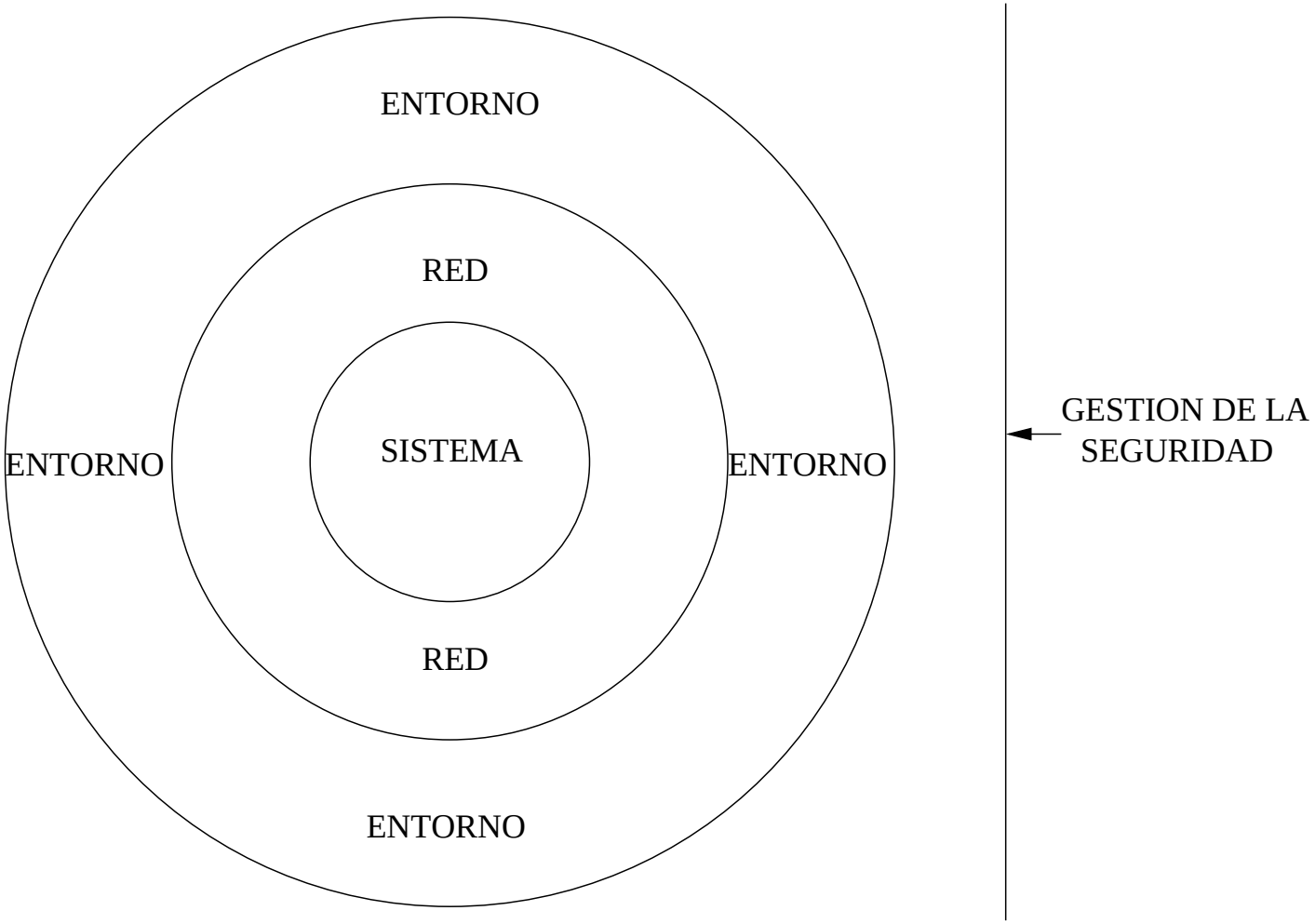
- Las redes introducen innegables avances en un entorno de trabajo, pero también numerosos problemas.
- Hoy en día es raro el entorno en el que no existen redes de todo tipo y tecnología.
- Muchas de las amenazas sobre un sistema de información vienen a través de una red: debo detectarlas y, sobre todo, detenerlas.

Gestión de la seguridad

- La seguridad debe ser gestionada y medida de forma adecuada, mejorando contínuamente los niveles alcanzados.
- Una gestión normalizada me ayuda a mejorar (y a compararme con otros).

Conclusiones

Podemos contemplar una visión concéntrica de la seguridad:



¡¡Muchas gracias a todos!!

Antonio Villalón Huerta
toni@shutdown.es