

Ciberseguridad

Grado en Ingeniería Informática

M1 - Introducción a la ciberseguridad

Índice

- La seguridad como un proceso
- Amenazas y vulnerabilidades
- Gestión de riesgos
- Seguridad en el desarrollo
 - OWASP
 - ASVS

“La seguridad no es un producto,
es un proceso”

--Bruce Schneier

“La seguridad no es problema de
tecnología, sino de gente y de
administración”

--Kevin Mitnick

“La seguridad es como una **cadena**, y su nivel global es el del **más débil** de sus eslabones”

– ???

Seguridad de los sistemas IT



[REVIEWS](#)[NEWS](#)[VIDEO](#)[HOW TO](#)[SMART HOME](#)[CARS](#)[DEALS](#)[DOWNLOAD](#)

Total economic cost of insecure software: \$180 billion a year in the U.S

Software security is an oft overlooked area. A new book sheds some light on the topic.

Software



by **Dave Rosenberg**

June 26, 2008 8:09 PM PDT

@dr138

David Rice's book *Geekonomics: The Real Cost of Insecure Software* calls the software industry to account for its careless attitude toward security.

As [reported on Forbes.com](#): Rice blames the software industry for a litany of hidden costs, ranging from the infrastructure needed to fix hackable bugs in software to recent data breaches at the U.S. State Department and the Pentagon--even a Boeing 747 crash in 2005 that resulted from software glitches. All told, he places the total economic cost of security flaws in software at around \$180 billion a year.

Gestión de incidentes: GitLab



Lo metemos debajo de la alfombra...

- Si hay un problema, se ignora
- Ya se ha intentado muchas veces: es parte de lo que se llama ***Security through obscurity***, y NO funciona

Seguridad de los sistemas IT



Pérdida de portátiles



Pérdida de portátiles



Análisis y gestión de riesgos

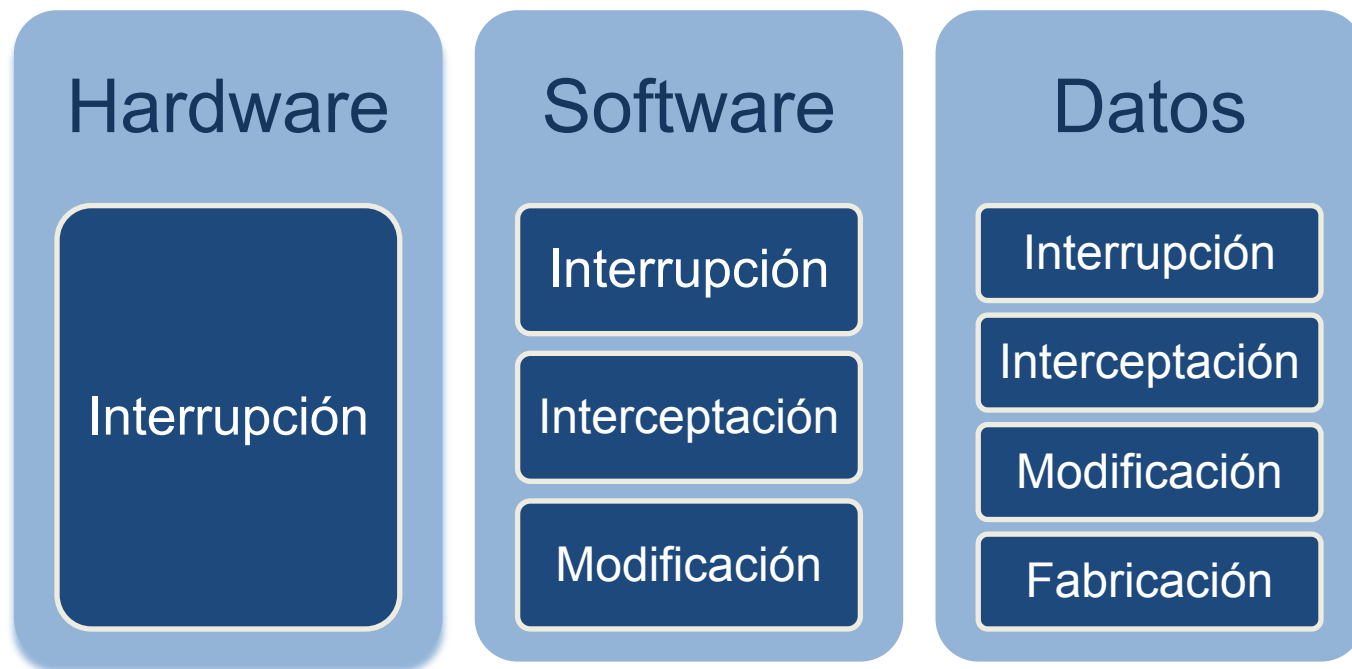
Definiciones

Amenazas y vulnerabilidades

Conceptos básicos

- **Amenaza:** Acción o conjunto de acciones que pueden ser dañinos para los activos de la organización
- **Vulnerabilidad:** Debilidad del sistema, o ausencia de salvaguarda, que permite que una amenaza sea explotada

Amenazas a una organización



Planos de actuación

- Objetivos **dispar**es, por lo que se debe actuar en distintos ámbitos:



Plano legal

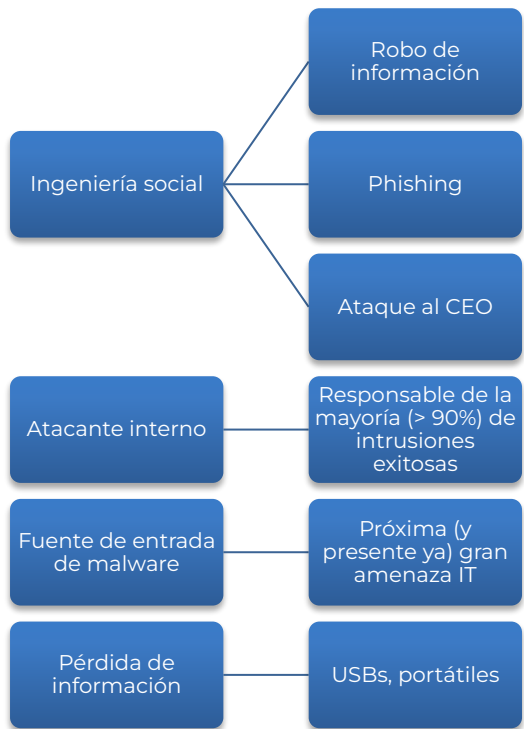
- Cada vez leyes más restrictivas en determinados sectores y para tratar determinados datos
- En nuestro país, destaca la LOPD, con fuertes multas para el incumplimiento de sus directivas sobre tratamientos de datos de carácter personal

Plano humano

- Formación y sensibilización de empleados y directivos hacia la necesidad de la seguridad.
- Definición de sus funciones y obligaciones, etc.

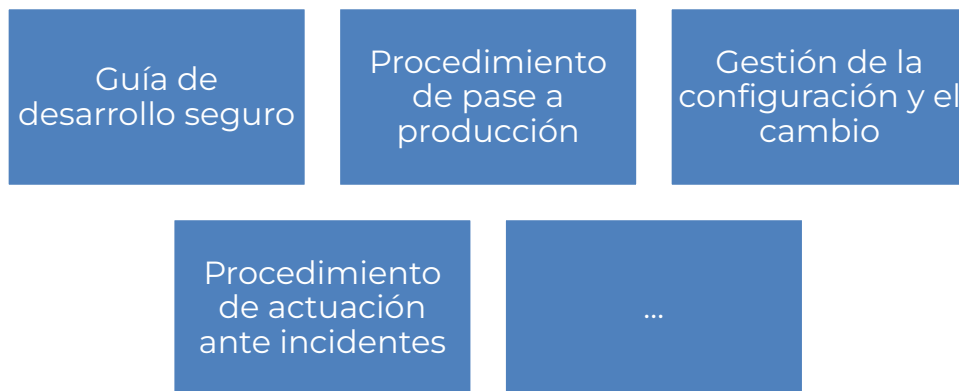
“La **formación** tiene la mejor relación coste/beneficio de la industria de la seguridad”

Plano humano



Plano organizativo

- Definición e implantación de **políticas de seguridad**, planes, normas, procedimientos y buenas prácticas de actuación.



Análisis y gestión de riesgos

Definiciones

Gestión del riesgo

Gestión y análisis de riesgos

- **Gestión de riesgos:** Proceso de identificación, evaluación y aplicación de los mecanismos que permiten reducir, mitigar y manejar los riesgos que afectan a los recursos de información de una organización
- **Análisis de riesgos:** Proceso utilizado para identificar los riesgos y evaluar su impacto, con el objetivo de determinar la estrategia más adecuada de reducción de riesgos.

Conceptos gestión de riesgos

- **Impacto o consecuencia** de la materialización de una amenaza sobre un activo aprovechando una vulnerabilidad
El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo, el 100% sería la pérdida total del activo.
- **Probabilidad:** es la posibilidad de ocurrencia de un hecho, suceso o acontecimiento.
Para estimar la frecuencia podemos basarnos en datos empíricos (datos objetivos) del histórico de la empresa, o en opiniones de expertos o del empresario (datos subjetivos).

Conceptos gestión de riesgos



Conceptos gestión de riesgos

- **Riesgo**: conceptualmente podríamos definirlo como:

$$\text{Riesgo} = \text{Impacto} * \text{Probabilidad}$$


- El riesgo se valora en términos de **coste**, derivado de los valores de los activos afectados:
 - Activo en estudio.
 - Daños personales
 - Pérdidas financieras, de imagen y reputación, etc.

Clasificación del impacto

| Rango Impacto | Descripción | Pérdidas financieras | Pérdida del activo(s) | Interrupción del servicio | Reputación e imagen | Disminución de rendimiento |
|---------------|----------------|-------------------------|-----------------------|---------------------------|------------------------|--|
| 5 | Catastrófico | > 6 % del presupuesto | Total | Mayor que un mes | Alta y muy extendida | > 50 % de variación en los indicadores |
| 4 | Desastroso | 6% del Presupuesto | Muy gran impacto | De una semana a un mes | Media y muy extendida | 25 - 50 % variación en los indicadores |
| 3 | Serio | 2% del presupuesto | Gran impacto | De un día a una semana | Media y poco extendida | 10 - 25% variación en los indicadores |
| 2 | Menor | 1% del presupuesto | Impacto menor | ½ día o 1 día | Baja y muy extendida | 5 - 10 % variación en los indicadores |
| 1 | Insignificante | < 0,5 % del presupuesto | Casi sin impacto | Menor de ½ día | Baja y poco extendida | Hasta el 5% variación en los indicadores |

Evaluación del impacto

| | | | | | | |
|----------------|---------|----------------|-------|-------|------------|--------------|
| Casi seguro | 5 | 5 | 10 | 15 | 20 | 25 |
| Muy probable | 4 | 4 | 8 | 12 | 16 | 20 |
| Posible | 3 | 3 | 6 | 9 | 12 | 15 |
| Improbable | 2 | 2 | 4 | 6 | 8 | 10 |
| Muy improbable | 1 | 1 | 2 | 3 | 4 | 5 |
| Probabilidad | X | 1 | 2 | 3 | 4 | 5 |
| | Impacto | Insignificante | Menor | Serio | Desastroso | Catastrófico |



Amenazas típicas a los activos IT

| # | AMENAZA | EJEMPLOS |
|---|---|--|
| 1 | Ataques a la propiedad intelectual | Copia ilegal de películas y música, sin respetar el copyright |
| 2 | Ataques vía software | Virus, gusanos, ataques de denegación de servicio |
| 3 | Ataques a la calidad de servicio (QoS, <i>quality of service</i>) | Cortes de electricidad, ataques al proveedor de servicio de Internet |
| 4 | Espionaje o intrusión | Acceso no autorizado y/o recolección de datos robados |
| 5 | Catástrofes naturales | Fuegos, inundaciones, terremotos, rayos |

Amenazas típicas a los activos IT

| # | AMENAZA | EJEMPLOS |
|----|--|--|
| 6 | Error humano | Accidentes, fallos de los empleados |
| 7 | Extorsión y/o secuestro de información | Criptovirus, extorsión bajo amenaza de publicar información comprometedor |
| 8 | Pérdidas de información | Pérdidas completas o parciales de información debido a un plan de <i>backup</i> inadecuado |
| 9 | Controles inadecuados | Falta de cortafuegos o sistemas de detección de intrusión, mala configuración de los mismos. |
| 10 | Sabotaje | Destrucción o robo físico de sistemas de información |

Amenazas típicas a los activos IT

| # | AMENAZA | EJEMPLOS |
|----|---------------------------|--|
| 11 | Fallos hardware | Fallos en el equipamiento hardware |
| 12 | Fallos software | Bugs, problemas de codificación o diseño |
| 13 | Obsolescencia tecnológica | Tecnologías o equipos anticuados |

Gestión de riesgos



Análisis de riesgo

Objetivo: averiguar el nivel de riesgo que la empresa está soportando.

Para ello, tradicionalmente las metodologías proponen que se realice un inventario de activos, se determinen las amenazas, las probabilidades de que ocurran y los posibles impactos

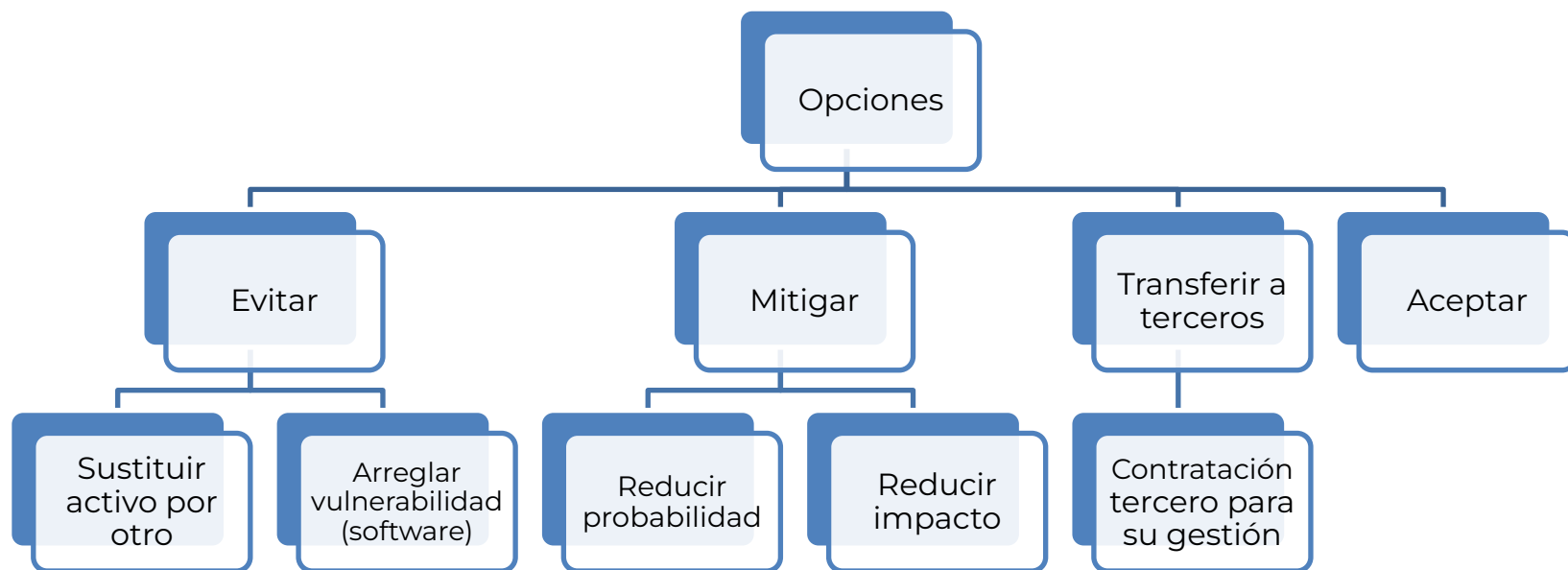
Tratamiento del riesgo

- Para aquellos riesgos cuyo nivel está por encima del umbral deseado la empresa debe decidir cuál es el mejor tratamiento que permita disminuirlos
- Esta decisión siempre ha de pasar un filtro económico donde el coste del tratamiento, o coste de protección, no supere el coste de riesgo disminuido

Coste de equilibrio



Tratamiento de riesgos



Tratamiento de riesgos

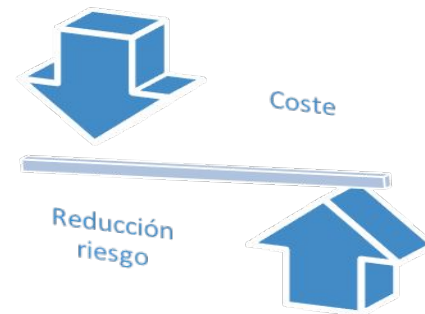


Roles

| Responsable de la información | Responsable del servicio | Analista de riesgos | Propietario del riesgo |
|---|---|---|--|
| <ul style="list-style-type: none">• Establece SUS propios requisitos de seguridad | <ul style="list-style-type: none">• Establece SUS propios requisitos de seguridad | <ul style="list-style-type: none">• Traslada los requisitos a medios técnicos• Selecciona y evalúa salvaguardas• Reporta el riesgo residual | <ul style="list-style-type: none">• Evalúa el riesgo en términos de negocio• Toma decisiones sobre el tratamiento del riesgo• Autoridad responsable de la gestión del riesgo |

Gestión de riesgos

- Análisis coste-beneficio salvaguardas:
 - Impacto de implantar
 - Impacto de no implantar
 - Estimación del coste de implantación
- Reglas:
 - Si la salvaguarda reduce el riesgo más de lo necesario ☐ **buscar alternativa más económica**
 - Si la salvaguarda cuesta más que la reducción de riesgo que proporciona ☐ **elegir otra**
 - Si la salvaguarda no reduce suficiente el riesgo ☐ **ampliar o cambiar**
 - Si la salvaguarda reduce riesgo y es efectiva en coste ☐ **aplicar**



Ejemplos de gestión de riesgos

- Cálculo del impacto, probabilidad
- Sucesos:
 - Alienígenas abducen a todo el Dpto. de Informática
 - Ladrón roba copias de seguridad
 - Godzilla arrasa la ciudad
 - Empleado descontento roba correos del presidente