ANÁLISIS DE RIESGOS

José Enrique López

Medidas de seguridad

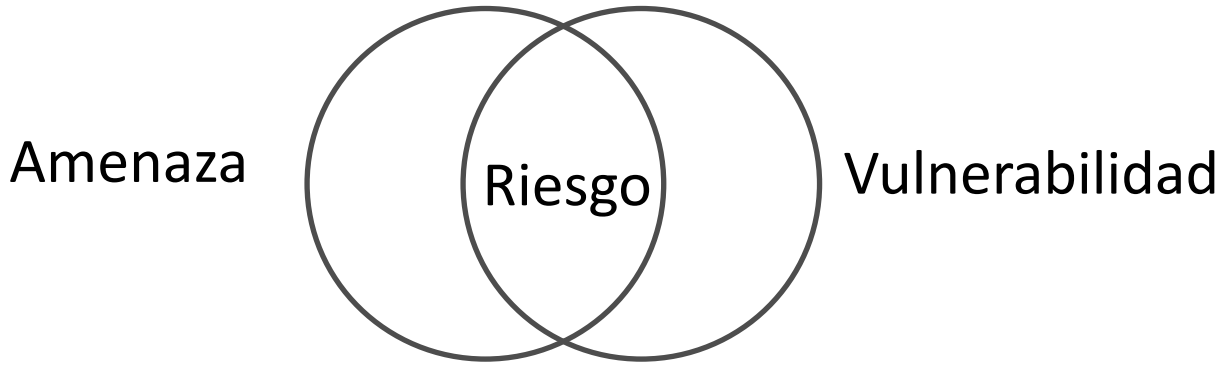
- ¿Qué queremos proteger?
  - Los recursos del sistema: hardware, software, datos,…
- ¿De qué nos queremos proteger?
  - De todos aquellas amenazas que puedan afectar a nuestros recursos
    - Personas: empleados, ex-empleados, curiosos, hackers, crakers, terroristas …
    - Amenazas Lógicas: software defectuoso, herramientas de seguridad, puertas traseras, bombas lógicas, canales ocultos, virus, troyanos, …
    - Siniestros y catástrofes naturales
- ¿Cómo nos podemos proteger?
  - Análisis de amenazas
  - Evaluación de (posibles) pérdidas y su probabilidad
  - Definición de una política de seguridad
  - Implementación de la política: Prevención, Detección, Recuperación y Formación

Contramedidas que forman parte de una política

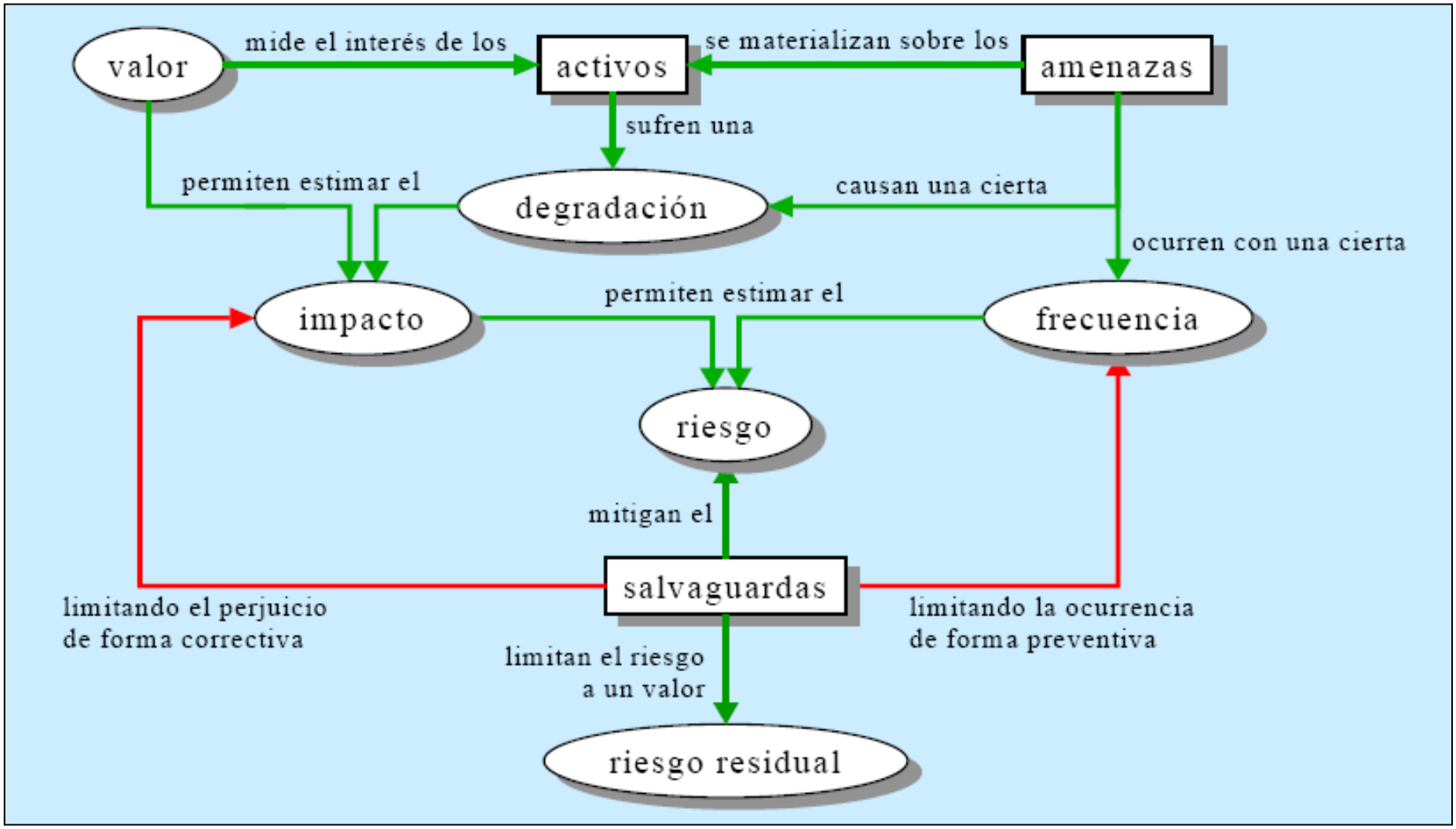
- Política segura de contraseñas:
  - Longitud y complejidad mínimos
  - Cambio regular
- Control de la adquisición y actualización del software.
- Cifrado. Proporciona confidencialidad, autenticidad e integridad
- Actuaciones en el nivel de arquitectura: Redes privadas virtuales
- Gestión de incidentes: detección de ataques, históricos, control de integridad
- Acciones administrativas: identificación de responsables de seguridad, política de sanciones, políticas de privacidad, definición de buenas prácticas de uso
- Formación

Riesgos

- **Riesgo**: probabilidad de que una amenaza explote una vulnerabilidad sobre un activo o grupo de activos y por tanto cause un daño a la organización



Riesgos


valor
mide el interés de los
activos
se materializan sobre los
amenazas
sufren una
permiten estimar el
degradación
causan una cierta
ocurren con una cierta
impacto
permiten estimar el
frecuencia
riesgo
mitigan el
salvaguardas
limitando el perjuicio
de forma correctiva
limitando la ocurrencia
de forma preventiva
limitan el riesgo
a un valor
riesgo residual

Análisis de riesgos

- Es una aproximación sistemática para determinar el nivel y calidad de las medidas de seguridad de una organización
  - Identificación de amenazas y puntos críticos
  - Directamente relacionado con el análisis coste beneficio
  - El análisis es diferente para cada organización

- Los pasos a seguir en la evaluación de riesgos
  - Identificación de los activos y elementos valiosos de red de la organización
  - Valoración de los activos clasificándolos por su criticidad
  - Estudio de las amenazas y las vulnerabilidades
    - Compromiso de la información
    - Pérdida de la integridad de los datos
    - No disponibilidad de recursos
  - Evaluación analítica de los riesgos

Análisis de riesgos

- Existen diferentes metodologías para realizar el análisis de riesgos
  - Cuantitativas, emplean datos empíricos y estadísticas probadas
  - Cualitativas, emplean una evaluación intuitiva y por la experiencia
  - Combinadas

- Independientemente de la metodología, el objetivo es la cuantificación de las pérdidas y probabilidad de que se produzcan, de forma que tengan sentido y convenzan al personal que decide en cuestión de riesgos

- Existen múltiples métodos ya que no existen estándares de ningún tipo para realizar el análisis y el cálculo de riesgos

- En la actualidad se emplean herramientas software que de una forma intuitiva presentan datos de la evaluación de riesgo

Análisis de riesgos

ACTIVO	DESCRIPCIÓN
Hardware	Estaciones de trabajo, ordenadores personales, impresoras, switches, routers, cortafuegos, módems, servidores de terminales, servidores de acceso remoto, servidores de red, servidores de Internet
Software	Código fuente y código objeto de programas, utilidades, programas de diagnóstico, sistemas operativos, programas de comunicaciones, Números de serie
Datos	Datos almacenados on-line y archivados off-line, copias de seguridad, ficheros de log y de registros, bases de datos, datos en tránsito sobre diferentes medios de transmisión y soporte
Personal	Usuarios, Administradores y personal de mantenimiento de hardware
Documentación	Programas, evaluaciones internas de software y hardware, Procedimientos de operación y administración de los sistemas

Análisis de riesgos

TIPOS DE DATOS	CLASIFICACIÓN	CRITICIDAD
Resultados de análisis clínicos	Investigación	Alta
Tendencias de mercado	Investigación	Baja
Patentes pendientes	Propietarios	Alta
Memorias corporativas	Administrativos	Baja
Directorio de empleados	Administrativos	Baja
Datos de nuevos productos	Propietarios	Media
Secretos comerciales	Propietarios	Alta
Datos adquiridos	Financieros	Alta
Salarios de los empleados	Financieros	Media

Análisis de riesgos

AMENAZA	DESCRIPCIÓN
Compromiso de la Información	➢ Cualquier información transferida electrónicamente puede ser robada ➢ Las consecuencias pueden variar de mínimas hasta catastróficas ➢ Debe crearse una lista con la información más valiosa para la organización ➢ La política de seguridad deberá reflejar el lugar y la forma de almacenar la información sensible ➢ Indicar quien tiene acceso
Pérdida de la integridad de los datos	➢ Puede causar problemas de confianza en una organización ➢ Costes elevados en analizar y determinar los datos comprometidos ➢ La integridad puede comprometerse a través de las copias de seguridad, almacenamiento de las mismas, acceso físico a datos y al almacenamiento ➢ Pérdida de datos por catástrofes naturales, no es posible recuperación ➢ La política de seguridad debe indicar como proteger la integridad
No disponibilidad de los recursos	➢ Suele afectar a los recursos de red ➢ Si los recursos críticos no son accesibles, pérdidas millonarias ➢ Hay que evaluar los costes en que se incurre si los sistemas están fuera de servicio durante un cierto tiempo ➢ Pueden ser causas naturales o ataques del tipo DoS ➢ La política fijará temas de fiabilidad, redundancia y diseño de red

Análisis de riesgos

ACTIVOS	TASACIÓN				AMENAZAS	POSIBILIDAD DE OCURRENCIA DE AMENAZAS	VULNERABILIDADES	POSIBILIDADES DE SER LAS VULNERABILIDADES EXPLO. TADAS POR LAS AMENAZAS	VALORES DE ACTIVOS EN RIESGO	POSIBILIDADES DE OCURRENCIA DE AMENAZAS	TOTAL
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL							

Análisis de riesgos

Probabilidad Amenaza
1: Poco probable
2: Probabilidad media
3: Alta probabilidad

Pérdida Estimada
1: Pérdida bajo coste
2: Pérdida coste medio
3: Pérdida crítica

Riesgo

R = PA x PE

Prob. Amenaza	Pérdida estimada	Riesgo
1	1	1-> RIESGO BAJO
1	2	2-> RIESGO BAJO
1	3	3-> RIESGO MODERADO
2	1	2-> RIESGO BAJO
2	2	4-> RIESGO MODERADO
2	3	6-> RIESGO ELEVADO
3	1	3-> RIESGO MODERADO
3	2	6-> RIESGO ELEVADO
3	3	9-> RIESGO ELEVADO

Análisis de riesgos

Análisis de riesgos. Análisis coste-beneficio

- Realizado el análisis de riesgo, se conoce cuales son los riesgos más elevados, y que se estima se producirán con una mayor probabilidad

- Es necesario conocer
  - Coste de las pérdidas en caso de producirse
  - Coste estimado de la prevención

- El proceso para determinar si una inversión para prevenir un riesgo es necesaria, se puede estimar de forma prácticamente inmediata
  - La comparación entre diferentes riesgos establecerá una prioridad

- Ejemplos de análisis coste-beneficio:
  - SAI en un entorno en que no se producen muchas caídas de red eléctrica
  - Pérdida del password de un administrador en una entidad financiera