# Evaluación de Riesgos
# Tema 1

## Que se considera riesgo informático

**José-Andrés Barbero Calzada**

# Esquema

1. Introducción
2. Definiciones
    1. Riesgo
    2. Amenaza
    3. Vulnerabilidad
    4. Activo
    5. Impacto
    6. Salvaguarda o control
    7. Análisis y Evaluación de riesgos
    8. Valoración y Gestión de riesgos
    9. Riesgo residual
3. Análisis de riesgos – Modelo de Gestión
4. El ciclo de Deming
    1. Plan (Planificar)
    2. Do (Hacer)
    3. Check (Verficar)
    4. Act (Actuar)

La SOCIEDAD es cada vez más DEPENDIENTE de los SISTEMAS Y SERVICIOS DE INFORMACIÓN y cada vez más VULNERABLE a las AMENAZAS existentes.

# ¿Por qué aumentan las amenazas?

**Algunas Causas**

- Crecimiento exponencial de las Redes y Usuarios Interconectados
- Profusión de las BD On-Line
- Inmadurez de las Nuevas Tecnologías
- Alta disponibilidad de Herramientas Automatizadas de Ataques
- Nuevas Técnicas de Ataque Distribuido (Ej:DDoS)
- Técnicas de Ingeniería Social

# Son causadas generalmente por:

El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (por desinterés, falta de información o a propósito).

Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o *Script boy*, viruxer, etc.).

Un siniestro (robo, incendio, inundación): una mala manipulación o una malintención derivan a la pérdida del material o de los archivos.

El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática.

# Amenaza / Threat

- **Amenaza** (según ISO/IEC 13335-1:2004)**:** causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
- Las amenazas siempre existen y son aquellas acciones que pueden ocasionar consecuencias negativas en la operativa habitual.
  - Físicas: ej. Inundación, terremoto, acceso físico a un edificio
  - Lógicas: ej. Intento de acceso inadecuado a una BBDD.

***Leonardo Sena y Simón Mario Tenzer***

# Vulnerabilidad / Vulnerability

- **Vulnerabilidad:** (Inglés: Vulnerability). Debilidad en la seguridad de la información de una orga nización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debi lidad de un ac tivo o c onjunto de activos que puede ser explotado por una amenaza.
- Las amenazas siempre están presentes pero sin la identificación de una vulnerabilidad no podrán ocasionar ningún impacto

***Leonardo Sena y Simón Mario Tenzer***

Ejemplos de vulnerabilidades: Antivirus desactualizado, versiones antiguas de software, puertos abiertos en firewalls, bugs del software, etc.

# Activo / Asset

- **Activo:** (Inglés: Asset). En relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la o rganización. Según [ISO/IEC 13335-1:2004]: Cualquier co sa que tiene valor para la organización.
- Ejemplos de activos: datos, hardware, software, servicios , documentos, edificios, recursos humanos.

***Leonardo Sena y Simón Mario Tenzer***

# Riesgo / Risk

- Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

# Riesgo / Risk

- **Riesgo:** eventualidad que imposibilit a el cumplimiento de un objetivo
- **Risk** is the possibility of suffering loss
- **Riesgo** (según RAE): Contingencia o proximidad de un daño.
- **Riesgo tecnológico** (según ISO-Guías para la gestión de la seguridad TI/TER 13335-1, 1996).: La pro babilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos , generándole pérdida o daños
- **Riesgo**: (Inglés: Risk). Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de informació n. Según [ISO Guía 73:2002] : combinación de la probabilidad de un evento y sus consecuencias.

# Impacto / Impact

- **Impacto:** (Inglés: Impact). El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros

- Ejemplos de impactos: pérdida económica, perdida de reputación, implicaciones legales, pérdida de confianza, reducción de la eficiencia, pérdida de oportunidades de negocio, perdida de vidas humanas, afectación del medio ambiente, etc.

# Análisis y Evaluación de Riesgos

- **Análisis de riesgos** (Inglés: Risk analysis). Según [ISO/IEC Guía 73:2002]: Uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Evaluación de riesgos**: (Inglés: Risk evaluation). Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

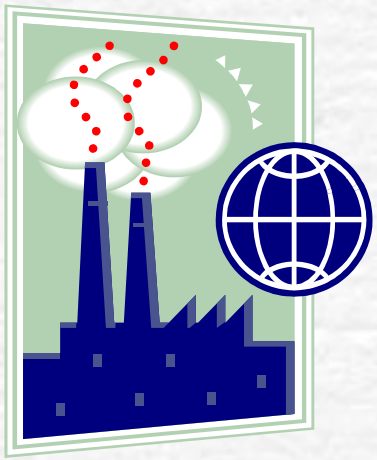
# Valoración y Gestión de Riesgos

- **Valoración de riesgos** (Inglés: Risk assessment). Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

- **Gestión de riesgos**: (Inglés: Risk management). Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

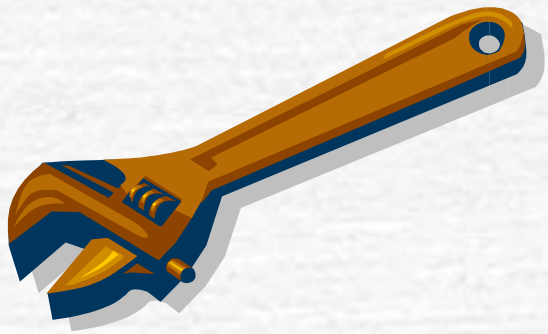
# Alcance / Scope

- **Alcance:** (Inglés: Scope). Ámbito de la organización que queda sometido al SGSI. Debe incluir la identificación clara de las dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.



# Salvaguarda o control / Safeguard

- **Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida).



# Riesgo residual / Residual Risk

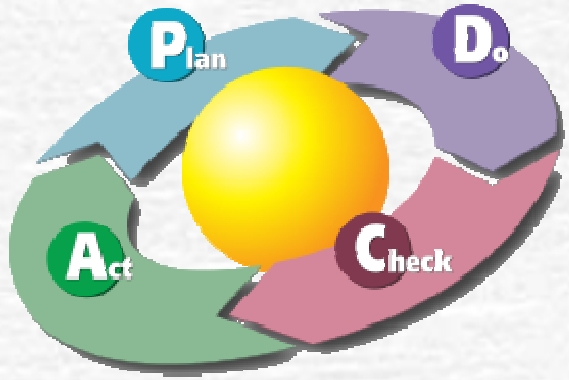
- **Riesgo residual:** (Inglés: Residual Risk). Según [ISO/IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

# Análisis de riesgos – Modelo de Gestión

# El círculo de DEMING

- El ciclo PDCA, también conocido como "Círculo de Deming o circulo de Gabo" (de Edwards Deming 1900-1993), es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. También se denomina espiral de mejora continua. Es muy utilizado por los SGC.
- Las siglas PDCA son el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Palabras clave:
Circulo, rueda o ciclo de Deming, proceso de mejora contínua, PDCA.




***http://es.wikipedia.org***

# PLAN (Planificar)

- Establecer los objetivos y procesos necesarios para obtener los resultados de acuerdo con el resultado esperado. Al tomar como foco el resultado esperado, difiere de otras técnicas en las que el logro o la precisión de la especificación es también parte de la mejora.
- 1.-Identificar proceso que se quiere mejorar 2.-Recopilar datos para profundizar en el conocimiento del proceso 3.-Análisis e interpretación de los datos 4.-Establecer los objetivos de mejora 5.-Detallar las especificaciones de los resultados esperados 6.-Definir los procesos necesarios para conseguir estos objetivos, verificando las especificaciones

***http://es.wikipedia.org***

# DO (Hacer)

- Implementar los nuevos procesos. Si es posible, en una pequeña escala.

***http://es.wikipedia.org***

# CHECK (Verificar)

- Pasado un periodo de tiempo previsto de antemano, volver a recopilar datos de control y analizarlos, comparándolos con los objetivos y especificaciones iniciales, para evaluar si se ha producido la mejora

- Monitorea la Implementación y Evalúa el plan de ejecución documentando las conclusiones.

***http://es.wikipedia.org***

# ACT (Actuar)

- Documentar el ciclo

- En base a las conclusiones del paso anterior elegir una opción:
  - Si se han detectado errores parciales en el paso anterior, realizar un nuevo ciclo PDCA con nuevas mejoras.
  - Si no se han detectado errores relevantes, aplicar a gran escala las modificaciones de los procesos
  - Si se han detectado errores insalvables, abandonar las modificaciones de los procesos
  - Ofrece una Retro-alimentación y/o mejora en la Planificación.

***http://es.wikipedia.org***