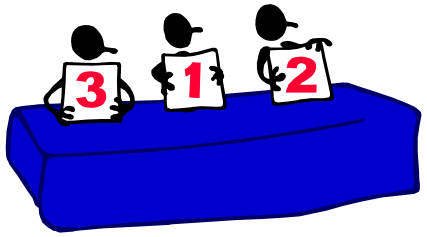
Objetivos

- Saber que es la Seguridad Informática
- Identificar aspectos que deben considerarse para el estudio de la Seguridad Informática
- Conocer método para la Gestión de Riesgo

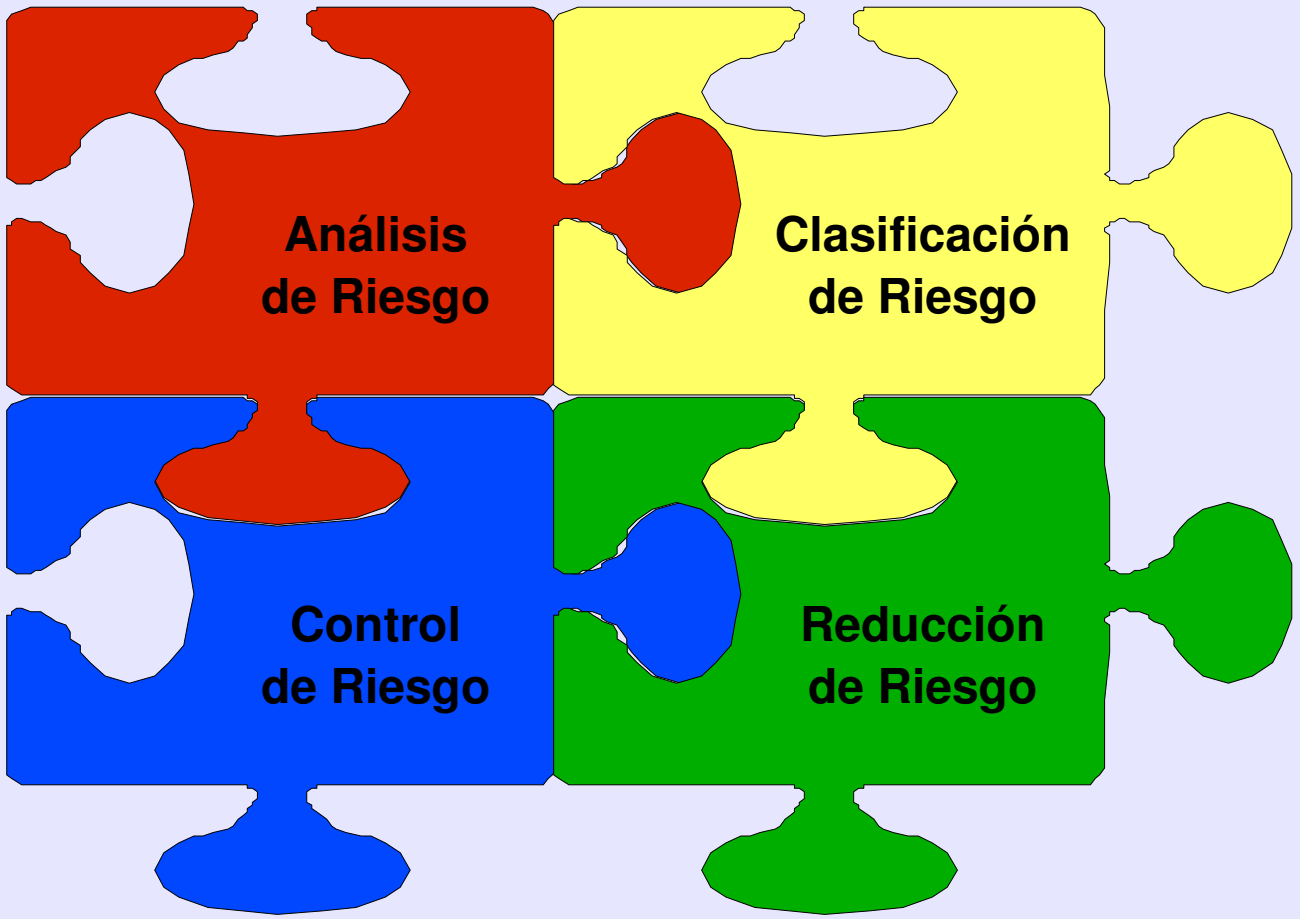
Definición de Seguridad Informática

- Garantizar condiciones y características de datos e información
  - Confidencialidad: Acceso autenticado y controlado
  - Integridad: Datos completos y non-modificados
  - Disponibilidad: Acceso garantizado

- Manejo del peligro
  - Conocerlo
  - Clasificarlo
  - Protegerse contra daños



Gestión de Riesgo



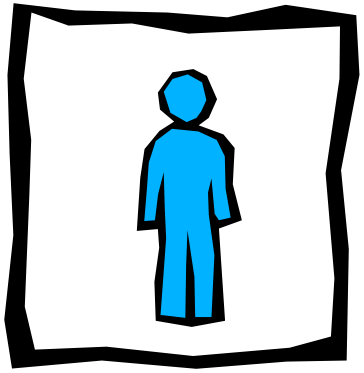
Política de Seguridad: Procesos, Reglas y Norma Institucionales

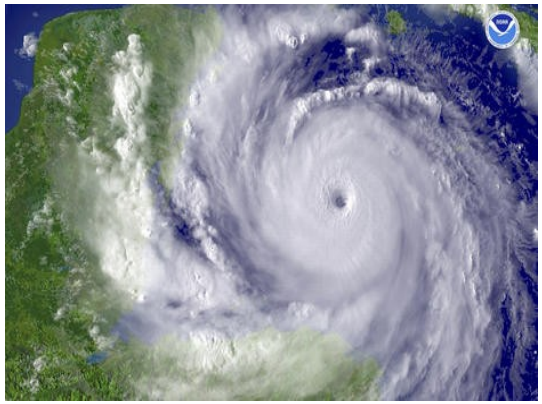
Seguridad Informática

Seguridad Informática

- **Seguridad de la información**
- **Protección de datos**

Seguridad de la Información





Seguridad de la información =
Protección contra **pérdida** y **modificación**

Motivación: Interés propio

Protección de Datos



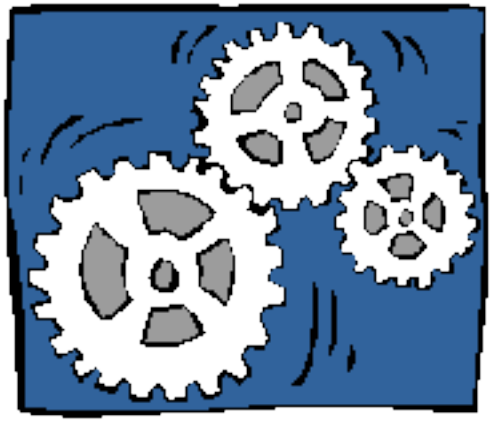

Protección de datos =
Protección de la **personalidad** y los **derechos personales** de los individuos, que salen en los datos, para evitar consecuencias negativas en contra de ellos.

Motivación: Obligación jurídica

Retos de la Seguridad

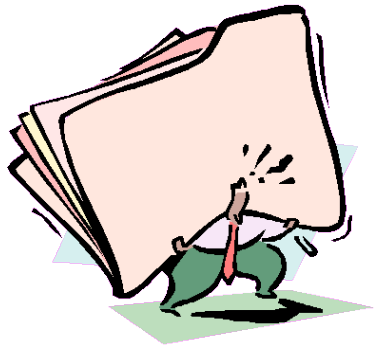
- No recibe atención adecuada
  - Costos
  - Ignorancia, falta de conocimiento
  - Negligencia del personal
  - Falta o no respetar de normas y reglas

- Proceso dinámico y permanente
  - Seguimiento de control y sanciones
  - Adaptar mediadas a cambios de entorno
  - Capacitación del personal
  - Documentación

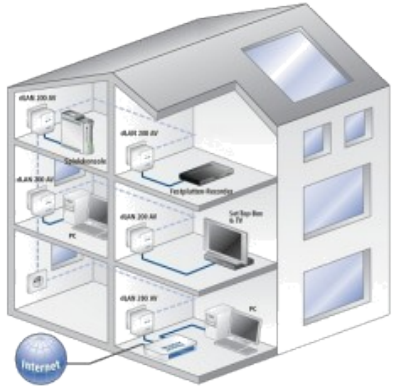


Elementos de Información

- Datos e información
  - Finanzas, RR.HH, Llamadas telefónicas, Correo electrónico, Base de Datos, Chateo, ...



- Sistemas e infraestructura
  - Edificio, Equipos de red, Computadoras, Portátiles, Memorias portátiles, Celulares, ...

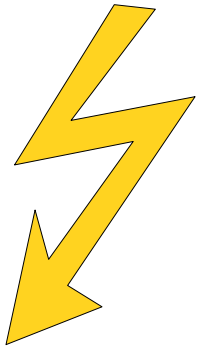


- Personal
  - Junta Directiva, Coordinación, Administración, Personal técnico, ...

Amenazas

- Criminalidad (común y política)
  - Allanamiento, Sabotaje, Robo / Hurto, Fraude, Espionaje, Virus, ...

- Sucesos de origen físico
  - Incendio, Inundación, Sismo, Polvo Sobrecarga eléctrica, Falta de corriente, ...



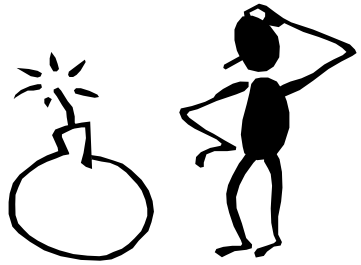
- Negligencia y decisiones institucionales
  - Falta de reglas, Falta de capacitación, No cifrar datos críticos, Mal manejo de contraseñas, ...

Vulnerabilidades

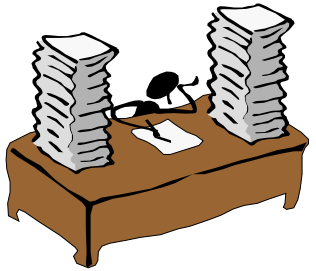
- Ambiental / Físicas
  - Desastres naturales, Ubicación, Capacitad técnica, Materiales...

- Económica
  - Escasez y mal manejo de recursos

- Socio-Educativa
  - Relaciones, Comportamientos, Métodos, Conductas...



- Institucional / Política
  - Procesos, Organización, Burocracia, Corrupción, Autonomía

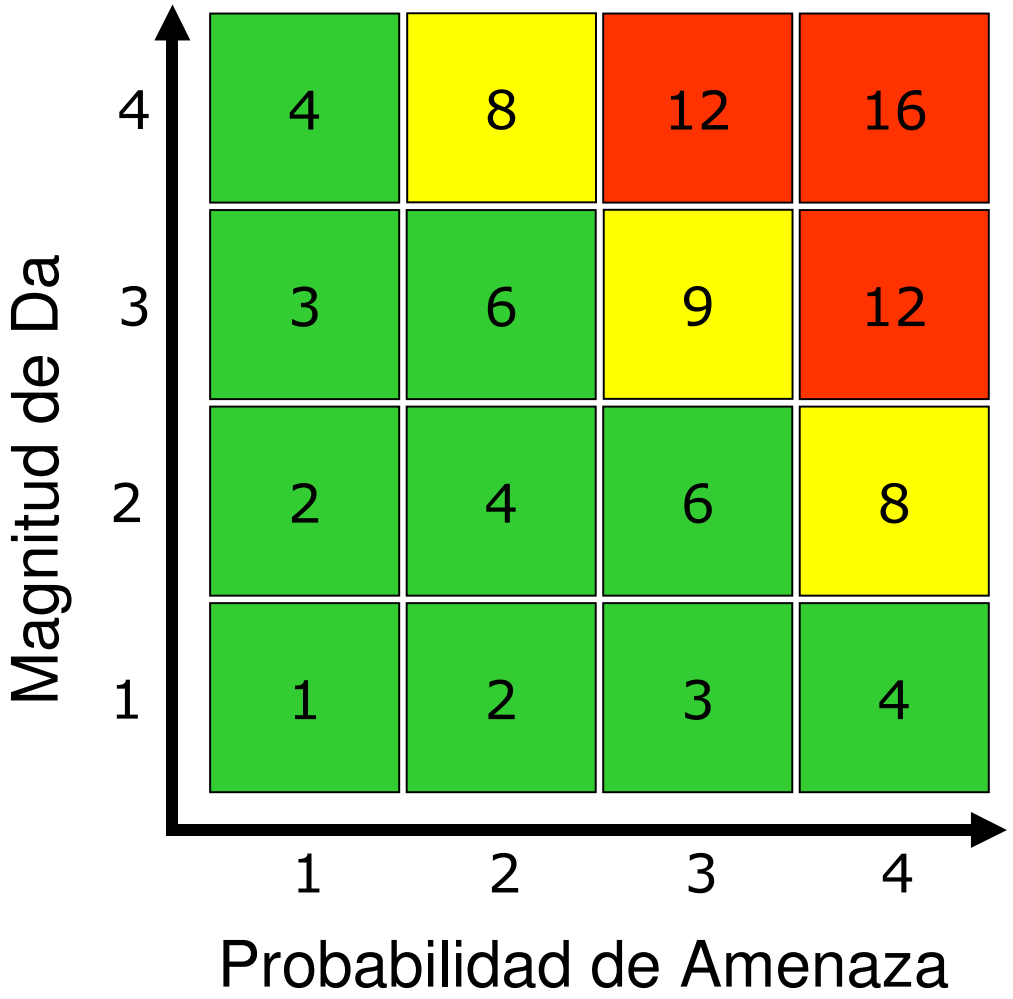


Clasificación y Flujo de Información

- Identificar tipo de datos e información y clasificarlo
  - Confidencial (acceso restringido: personal interno autorizado)
  - Privado (acceso restringido: personal interno)
  - Sensitivo (acceso controlado: personal interno, público externo con permiso)
  - Público
- Análisis de flujo de información
  - Observar cuáles instancias manejan que información
  - Identificar grupos externos que dependen o están interesados en la información
  - Determinar si se deben efectuar cambios en el manejo de la información

Análisis de Riesgo

Riesgo = Probabilidad de Amenaza * Magnitud de Daño



Alto Riesgo (12-16)

Medio Riesgo (8-9)

Bajo Riesgo (1-6)

Valores:
1 = Insignificante
2 = Baja
3 = Mediana
4 = Alta

¿Cómo valorar la Probabilidad de Amenaza?

- Consideraciones
  - Interés o la atracción por parte de individuos externos
  - Nivel de vulnerabilidad
  - Frecuencia en que ocurren los incidentes

- Valoración de probabilidad de amenaza
  - Baja: Existen condiciones que hacen muy lejana la posibilidad del ataque
  - Mediana: Existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en el largo plazo
  - Alta: Ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque

¿Cuándo hablamos de un Impacto?

- Se pierde la información/conocimiento
- Terceros tienen acceso a la información/conocimiento
- Información ha sido manipulada o está incompleta
- Información/conocimiento o persona no está disponible
- Cambio de legitimidad de la fuente de información

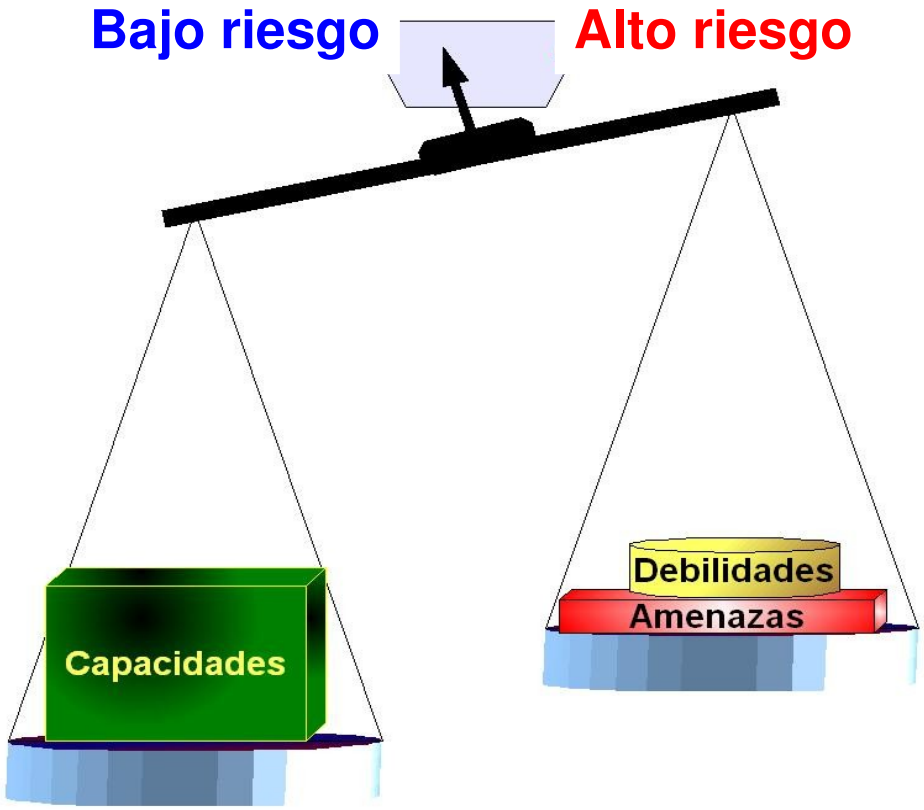
¿Cómo valorar la Magnitud de Daño?

- Consideración sobre las consecuencias de un impacto
  - ¿Quién sufrirá el daño?
  - Incumplimiento de confidencialidad (interna y externa)
  - Incumplimiento de obligación jurídicas / Contrato / Convenio
  - Costo de recuperación (imagen, emocional, recursos: tiempo, económico)

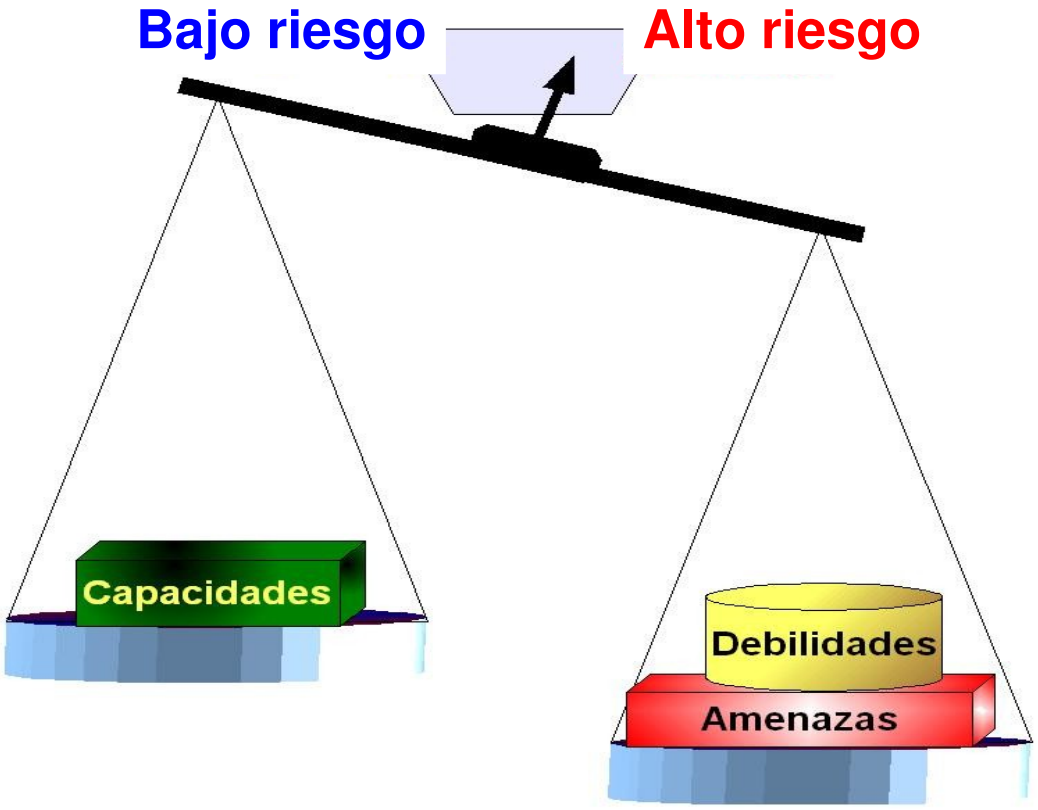
- Valoración de magnitud de daño
  - Bajo: Daño aislado, no perjudica ningún componentes de organización
  - Mediano: Provoca la desarticulación de un componente de organización. A largo plazo puede provocar desarticulación de organización
  - Alto: En corto plazo desmoviliza o desarticula a la organización

Clasificación de Riesgo

Seguro, pero exceso de atención



Inseguro, poca atención

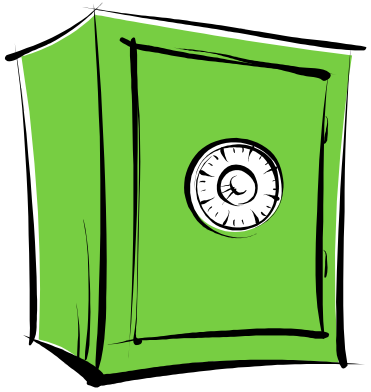


Riesgo restante

¡Nada es 100% seguro, siempre queda un riesgo restante!

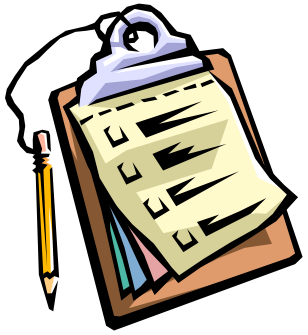
Reducción de Riesgo

- Medidas físicas y técnicas
  - Construcciones de edificio, Control de acceso, Planta eléctrica, Antivirus, Datos cifrados, Contraseñas inteligentes, ...



- Medidas personales
  - Contratación, Capacitación, Sensibilización, ...

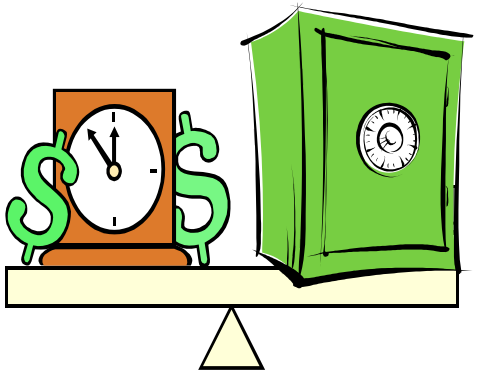
- Medidas organizativas
  - Normas y reglas, Seguimiento de control, Auditoría, ...



Medidas de Protección

- Medidas dependiendo del grado de riesgo
  - Medio riesgo: Medidas parciales para mitigar daño
  - Alto riesgo: Medidas exhaustivas para evitar daño

- Verificación de funcionalidad
  - Respaldado por coordinación
  - Esfuerzo adicional y costos vs. eficiencia
  - Evitar medidas pesadas o molestas



- Fundado en normas y reglas
  - Actividades, frecuencia y responsabilidades
  - Publicación