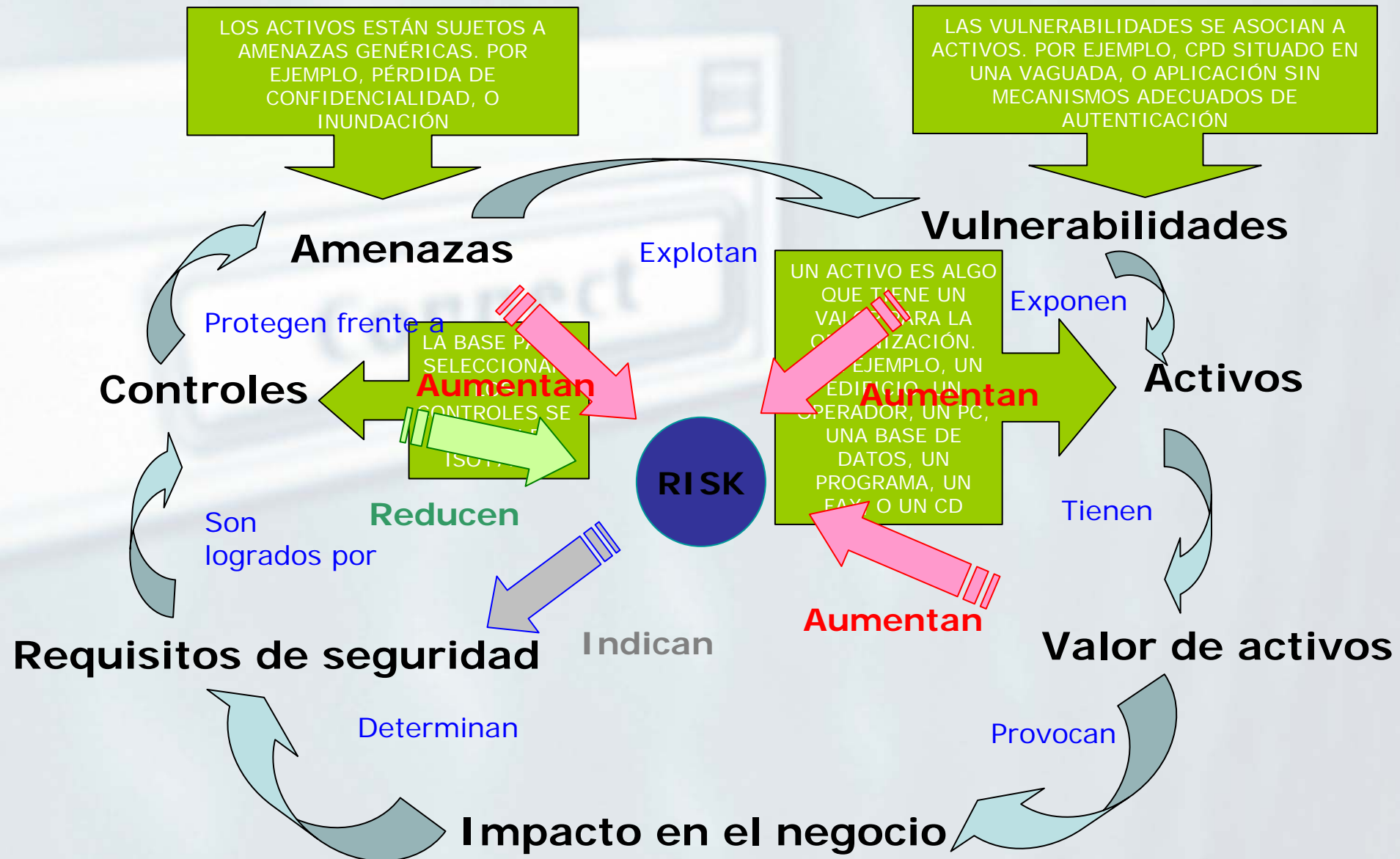


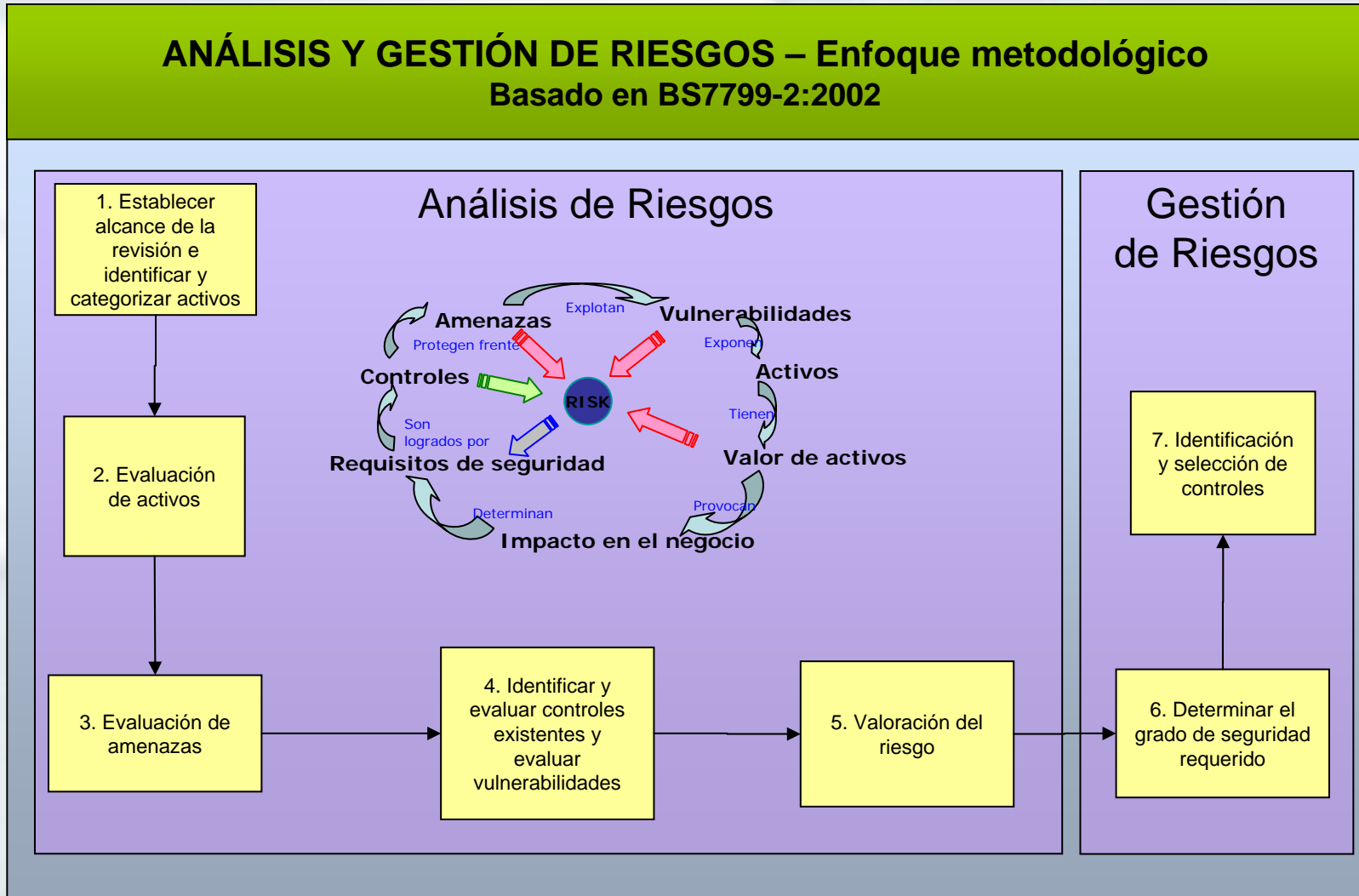


# **Análisis de Riesgos**

Barcelona, 15 de febrero de 2006



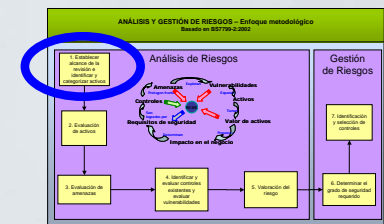
## ANÁLISIS Y GESTIÓN DE RIESGOS – Enfoque metodológico Basado en BS7799-2:2002



## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 1.- Establecer el alcance e identificar y categorizar activos

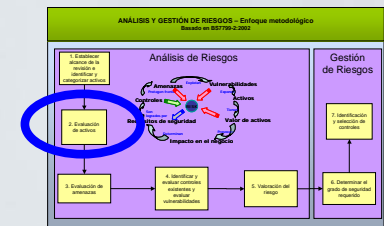
- ✓ Definir la extensión del análisis de riesgos
- ✓ Identificar los sistemas y personas involucrados en la revisión
- ✓ Identificar las actividades, funciones y responsabilidades
- ✓ Identificar para cada proceso revisado las entradas, salidas y recursos empleados
- ✓ Identificar los activos y asignar propietarios a los mismos
- ✓ Categorizar los activos involucrados en la revisión
  - ✓ Infraestructura
  - ✓ Personal
  - ✓ Hardware
  - ✓ Software
  - ✓ Comunicaciones
  - ✓ Documentos / Datos
  - ✓ Soportes



## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 2. Evaluar y establecer dependencias entre activos

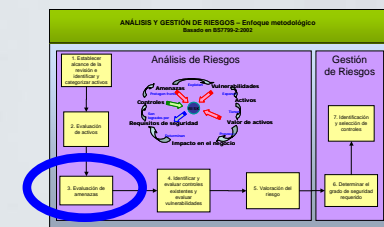
- ✓ Valorar los activos con respecto a la pérdida que supondría para el negocio si se comprometiera su integridad, disponibilidad o confidencialidad.  
La valoración se realizará cualitativamente según la escala: bajo, medio, alto, muy alto.
- ✓ Asignar un valor global al activo en función de las tres componentes valoradas.
- ✓ Contrastar las valoraciones con los propietarios de los activos.
- ✓ Homogeneizar las valoraciones finales.



## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 3. Evaluación de amenazas

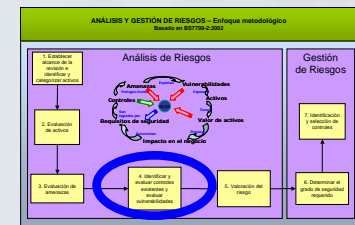
- ✓ Identificar las amenazas que podrían llegar a afectar a cada grupo de activos
- ✓ Valorar la probabilidad de ocurrencia de cada amenaza con respecto a cada uno de los activos con los que se encuentra relacionada en función de una escala cualitativa: baja, media, alta, muy alta.
- ✓ Contrastar las valoraciones con los propietarios de los activos o el personal relacionado con la naturaleza de la amenaza
- ✓ Homogeneizar las valoraciones finales



## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 4. Identificar y evaluar controles existentes y evaluar vulnerabilidades

- ✓ Identificar los controles existentes (en base al estándar ISO 17799) y el grado de implantación de los mismos con respecto cada activo en cuanto a:
  - ✓ Está implantado
  - ✓ Existe política
  - ✓ Existe procedimiento
  - ✓ Genera evidencia
  - ✓ Se encuentra automatizado
- ✓ Identificar las vulnerabilidades existentes para cada activo
- ✓ Valorar la cobertura de las vulnerabilidades por los controles identificados

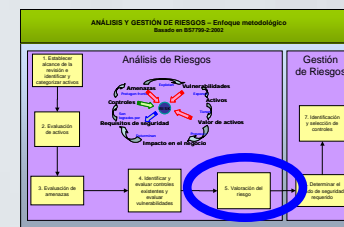




## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 5. Valoración del riesgo

- ✓ Valorar el impacto de cada riesgo resultante de la asociación de activos – amenazas – vulnerabilidades – controles en función de:
  - ✓ Valor del activo
  - ✓ Probabilidad de amenaza
  - ✓ Presencia de vulnerabilidades
  - ✓ Inexistencia de controles
- ✓ Priorizar y categorizar los riesgos en función del impacto calculado
- ✓ Contrastar los impactos resultantes con los propietarios de los procesos del alcance

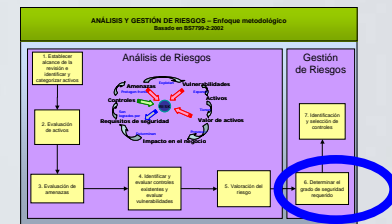




## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 6. Determinar el grado de seguridad requerido

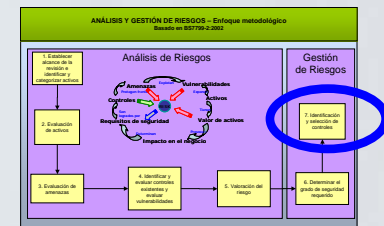
- ✓ Los responsables del proceso deben definir el nivel de riesgo mínimo a considerar y, para cada uno de los riesgos considerados las acciones que se quieren realizar sobre él:
  - ✓ Asumirlo
  - ✓ Evitarlo
  - ✓ Transferirlo
  - ✓ Mitigarlo
  - ✓ Definir el nivel de riesgo residual aceptable



## ANÁLISIS DE RIESGOS – Enfoque metodológico detallado

### 7. Identificación y selección de controles

- ✓ En función de la decisión tomada para cada riesgo y de la priorización de los riesgos identificar controles que cubran los objetivos marcados en base al estándar ISO 17799.
- ✓ Evaluar la diferencia entre el análisis de controles realizado y el grado de seguridad requerido
- ✓ Agrupar controles en proyectos que puedan ser estimados, priorizados y planificados.



# Deloitte.