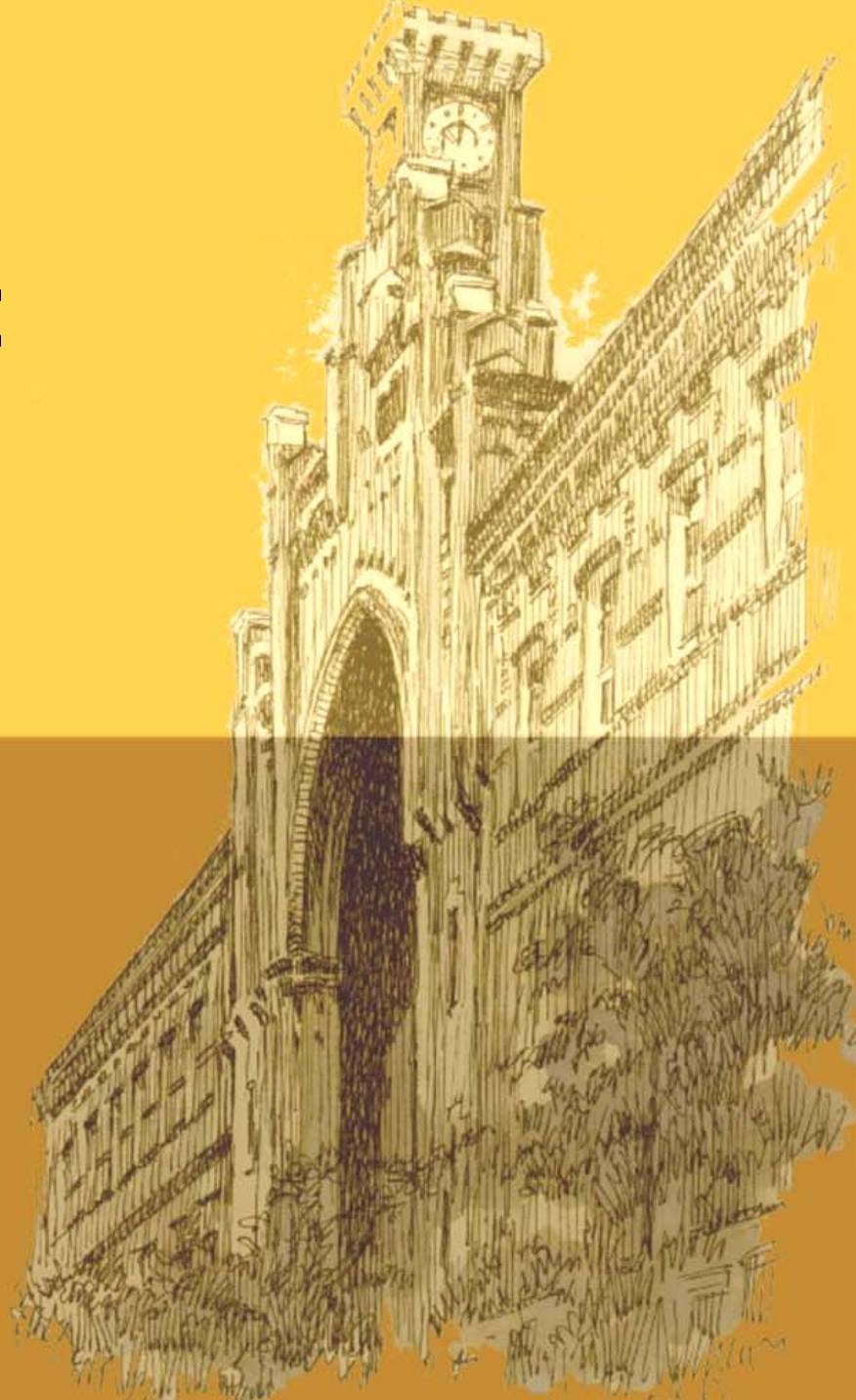
UNIVERSIDAD PONTIFICIA
ICAI ICADE
COMILLAS
MADRID

Seguridad Informática:

Capítulo 2: Análisis de Riesgos



Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2005-2006)

Javier Jarauta Sánchez
José María Sierra
Rafael Palacios Hielscher

Indice: Análisis de Riesgos

1. Identificación y valoración de activos
2. Identificación y valoración de las amenazas
3. Identificación de las medidas de seguridad existentes
4. Identificación y valoración de vulnerabilidades
5. Identificación de restricciones y objetivos de seguridad
6. Determinar medidas del riesgo
7. Determinar el impacto
8. Identificación y seleccionar las medidas de protección

Fase 1. Inventario Clasificación y valoración de Activos

Fase 1.1 : Inventario y clasificación de activos

- Físicos, edificios
- Equipos de soporte: climatización,
- Suministros varios
- Personal: propio y externo, función, perfil, formación
- Hardware: Mainframe, Servidores, PC, portátiles
- Software: S.O., aplicaciones comerciales y propias, herramientas de desarrollo y otros
- Equipos de comunicaciones: routers, modems
- Equipos y sistemas de back-up: discos, cintas, robot, cartuchos
- Información: bases de datos, ficheros
- Documentación: procedimientos operativos, manuales de los sistemas, planes de contingencia
- Confianza de los clientes
- Imagen de la organización
- Otros...

Fase 1.2: Valoración de activos

- El valor representa la importancia del activo en la organización
- No tiene por qué ser directamente económico (p.e. Imagen de la empresa)
- El método debe permitir valoración cualitativa (Alto, Medio, Bajo) y cuantitativa (en Meuros)
- El valor ha de tener en cuenta todo: su adquisición, desarrollo, mantenimiento, sustitución, credibilidad....

- Identificar y valorar los activos críticos

Tabla inventario de activos

- Clave: Código que lo identifique
- Activo: Nombre del activo
- Propietario:
- Administrador:
- Usuario (s):
- Confidencialidad: Alta, Media, Baja(actual / requerida)
- Integridad: Alta, Media, Baja(actual / requerida)
- Disponibilidad: Alta, Media, Baja(actual / requerida)
- Control de acceso: A, M, B (actual / requerida)
- Criticidad – Valoración: A, M, B – Valor estimado
- Observaciones:

Fase 2. Inventario Clasificación y valoración de Amenazas

Amenazas: definiciones y tipificación

- Activo: algo de valor al que afecta la amenaza
- Actor: quién o que puede violar los requisitos de seguridad
- Motivo: Accidental (desastres naturales, errores humanos, fallos en equipos) o Intencionado (solo a acciones humanas)
- Acceso: Cómo el actor accede al activo (físico, lógico (solo aplica a acciones humanas)
- Resultado: de la violación de los requisitos de seguridad de un activo (pérdida de confidencialidad, integridad –modificación-, disponibilidad -destrucción, pérdida, interrupción-)
- Impacto: efecto de una amenaza

Fase 2.1: Identificación de las amenazas

- 01. Desastres naturales (Tormentas, rayos, terremotos, inundaciones)
- 02. Estructurales (Incendios, inundaciones, humedad, cortes de electricidad, agua, refrigeración, comunicaciones)
- 03. Hardware (Fallo total o parcial de Servidores, Estaciones PC, portátiles)
- 04. Software (Errores en los SO, BD, software base, Web servers, aplicaciones, elementos de seguridad)
- 05. Red LAN y WAN (red interna, redes con delegaciones, sistemas de seguridad de las comunicaciones, redes públicas ajenas)

Fase 2.1: Identificación de las amenazas

- 06. Copias de seguridad (Fallos en elementos de copias, fallos en soportes cintas, discos, robot)
- 07. Información (Bases de datos, ficheros, manuales, procedimientos, planes de contingencia)
- 08. Personal (Errores y ataques de personal interno, externo, funciones, perfiles, formación)
- 09. Riesgos contra el patrimonio (Robo, pérdida no intencionada de activos)
- 10. Otros riesgos (Terrorismo, epidemias, confianza de los clientes, imagen de empresa, insolvencia de servicios externos, seguros, outsourcing...)

Fase 2.2: Valoración de las amenazas

- Establecer la importancia de la amenza
- Para cada amenaza hay que identificar:
  - El origen (qué o quién)
  - El blanco (elementos que pueden ser afectados)
- En una fase posterior del análisis se identificará:
  - La probabilidad de ocurrencia
  - El impacto y consecuencias de su ocurrencia
- Clasificación de su importancia en tres o cinco niveles
  - Alta, Media, Baja
  - Muy alta, Alta, Media, Baja, Muy baja

Fase 3. Identificación de las medidas de seguridad existentes

Fase 3.1: Identificación de las medidas de seguridad existentes

- Identificar las medidas de seguridad existentes
- Conocer su grado de efectividad
- Identificar a los activos que aplican
- Clasificación de las medidas existentes:
  - Medidas organizativas:
  - Medidas de seguridad física:
  - Medidas de seguridad lógica (tecnológicas)
  - Medidas legales
- Estimación de su criticidad y estado (bien, mejorable, malo)

Identificación de medidas existentes (I)

- Medidas organizativas:
  - Política de seguridad
  - Procedimientos, recomendaciones y normas
  - Formación y concienciación
- Seguridad física:
  - Acceso a edificios y salas de SI (Vigilancia,..)
  - Sistemas anti-intrusión (puertas blindadas, arcos detectores, control de accesos por llave, tarjeta...)
  - Sistemas anti-incendio y anti-inundación
  - Sistemas de alimentación eléctrica (general, baterías, generadores,...)
  - Aire acondicionado
  - Suministro de agua para refrigeración

Identificación de medidas existentes (II)

- Seguridad lógica
  - Integridad de los sistemas
  - Confidencialidad: cifrado en transmisión o almacenamiento, ...
  - Disponibilidad: redundancia,...
  - Identificación y autenticación de usuarios: estándar o fuerte,...
  - Auditorias: habilitación de logs y pistas

- Cumplimiento con la legislación:
  - Identificación de la legislación aplicable
  - Cumplimiento con LOPD, LSSI, otras

Fase 4. Identificación de vulnerabilidades

Fase 4.1: Identificación de vulnerabilidades

- Han de identificarse las vulnerabilidades generales para la organización
- Han de identificarse las vulnerabilidades específicas para cada activo o grupo de activos inventariados, especialmente los identificados como críticos
- Clasificar por categorías utilizando las mismas que las amenazas (01 a 10 categorías)
- Ha de evaluarse la importancia de la vulnerabilidad identificando si existe o no medida de protección frente a la misma, así como su eficacia
- Conviene ampliar el estudio con pruebas:
  - Test de intrusión (hacking ético) interno y externo
  - Ingeniería social

Fase 4.2: Valoración de vulnerabilidades

- Criterios de valoración en tres o cinco niveles
  - Alta, Media, Baja
  - Muy alta, Alta, Media, Baja, Muy baja
- Tabla de vulnerabilidades
  - Código:
  - Descripción:
  - Activo(s) a los que afecta
  - Impacto:
  - Valoración:
  - Recomendaciones

Fase 5. Identificación de restricciones y objetivos

Fase 5.1: Identificación de restricciones

- Afectan a las medidas de protección a implantar
- Restricciones de tiempo: que sea aceptable, limitar el tiempo máximo para un riesgo específico
- Restricciones financieras: el coste de las medidas no debe ser mayor que el de los activos que protegen
- Restricciones técnicas: mejor implantar medidas en la fase de diseño que en explotación. Si no existen medidas, implantar alguna compensatoria mediante procedimientos o de seguridad física
- Restricciones sociológicas: costumbres, cultura, mentalización, aceptación de la organización. Ante la negatividad, las medidas serán inoperativas
- Restricciones ambientales: superficie y espacio disponible, entorno, etc.
- Restricciones legales: informáticas y otras (edificios, laboral...) Suelen ser medidas impulsoras más que restricciones

Fase 5.2: Identificación de objetivos de seguridad

- Identificar lo que se espera del plan de seguridad de los Sistemas de Información
- Objetivos estratégicos definidos en la Política de seguridad
- Objetivos específicos cualitativos y cuantitativos referentes a un activo o grupo de activos
- Pueden definirse en relación a los servicios de Integridad, Confidencialidad y Disponibilidad
- Pueden identificarse fases limitando el alcance, teniendo en cuenta las restricciones identificadas

Fase 6. Determinación de la medida del riesgo

Fase 6: Determinar medidas del riesgo

- Es la probabilidad de que una amenaza ocurra
- Es la facilidad con que un ataque se implementa (Amenaza x Vulnerabilidad)
- Un riesgo resulta de la existencia de una amenaza explotando una vulnerabilidad
- Una amenaza sin vulnerabilidad no presenta riesgo, y una vulnerabilidad sin amenaza tampoco
- Si la combinación de amenaza y vulnerabilidad no produce impacto, tampoco han de implantarse las medidas de protección necesarias
- Un riesgo puede estar compuesto por varias amenazas

Determinar la medida del riesgo

- Existen tres medidas del riesgo a considerar:
  - 1. Inherente: medido sin tener en cuenta el efecto de las medidas de protección existentes
  - 2. Actual: medido teniendo en cuenta las medidas de protección existentes
  - 3. Residual: medido teniendo en cuenta las medidas de protección existentes, recomendadas y planificadas
- La diferencia entre 1, 2 y 3 es una medida de la efectividad de las medidas de protección

Determinación de las probabilidades

- Clasificación para amenazas naturales (4 niveles)
  - Alta (A): 1 ocurrencia cada año
  - Media (M): 1 ocurrencia cada 5 años
  - Baja (B): 1 ocurrencia cada 10 años
  - Muy baja (MB): 1 ocurrencia cada 20 años
- Clasificación para amenazas accidentales o intencionadas (5 niveles)
  - Extremadamente frecuente (EF) (60%)
  - Muy frecuente (MF) (20%)
  - Frecuente (F) (6%)
  - Frecuencia normal (FN) (2%)
  - Poco frecuente (PF) (0,6%)

Fase 7. Determinación del impacto

Fase 7: Determinar el impacto

- El impacto representa la consecuencia de la realización de un riesgo (parcial o total) en un sistema determinado o en la organización
- Es la medida de las pérdidas estimadas (económicas, de rendimiento, de imagen, etc.)
- La salvaguarda no ha de ser más cara que el impacto
- La valoración del impacto sirven para seleccionar las salvaguardas o medidas de protección, teniendo en cuenta los objetivos de seguridad y restricciones existentes
- Pueden utilizarse diferentes métricas, cualitativas o cuantitativas

Medidas del impacto

- Tipos de impacto
  - Daño: cuando un activo no puede usarse temporalmente
  - Destrucción: Cuando un activo queda destruido y no es reparable
  - Revelación: cuando se accede a un activo de forma no autorizada
  - Indisponibilidad: cuando el servicio informático no puede ofrecerse en un margen aceptable de tiempo
- Medidas Cualitativas:
  - Leve: tanto interno como públicamente
  - Moderado: interno, en la imagen pero sin sanciones
  - Grave: interno y público, con daño en la imagen y sanciones económicas

Fase 8. Identificación y selección de las medidas de protección

Fase 8: Identificación y seleccionar las medidas de protección

- Debe establecerse una lista de medidas de protección (salvaguardas) lo más amplia posible, sin ninguna restricción que se aplicarán posteriormente
- Se identificarán las medidas existentes, evaluando su mejora si fuese necesaria
- Seleccionar un conjunto de medidas equilibrado
- Ha de abarcar todas las areas:
  - Organización, procedimientos, documentación
  - Medidas físicas y lógicas
  - Hardware, Software, Comunicaciones
  - Personal

Identificación de medidas de protección

- Pueden ser medidas que:
  - Eviten o transfieran el riesgo: normalmente no se dan
  - Reduzcan la amenaza: son difíciles de implantar, sobre todo en sistemas existentes
  - Reduzcan la vulnerabilidad: son las más comunes y recomendadas (siempre existirá un nivel residual de riesgo)
  - Reduzcan el impacto: detectan el ataque y facilitan la recuperación. Son normalmente necesarias
- Además, las restricciones limitan normalmente la aplicación de las medidas

Selección de las medidas de protección

- Atendiendo a los objetivos de seguridad, restricciones y resultados del análisis de riesgos, se seleccionarán las medidas de protección a utilizar

- Se emitirán los siguientes documentos finales:
  - Análisis de riesgos
  - Recomendaciones de seguridad
  - Plan de proyectos de seguridad a implantar