Curso de Master

DISEÑO DE APLICACIONES SEGURAS

- Profesores :
  - Unai Arronategui : unai@unizar.es, D. 1.02
  - Elvira Mayordomo: elvira@unizar.es, D 1.06
  - Fernando Tricas : ftricas@unizar.es, D 1.14

1. Introducción a la seguridad

Referencias

M. Bishop, *Computer Security: Art and Science*. Addison Wesley. 2003. ISBN 0-201-44099-7

- Sistemas operativos
- Bases de datos
- Redes de computadores
- Ingeniería software
- Sistemas distribuidos

Definiciones de Seguridad Informática

- Un sistema informático es seguro si su comportamiento es acorde con las especificaciones previstas para su utilización (dependability).
- Seguridad es el estado de bienestar de la información y las infraestructuras, en las cuales la posibilidad que puedan realizarse con éxito y sin detectarse, el robo, alteración y parada del flujo de información, se mantienen en niveles bajos o tolerables.

Servicios de seguridad

- Básicos :
  - *Confidencialidad* (Privacidad) :
    - Mecanismos de control de accesos : Criptografía, ...
    - Ley de protección de datos.
  - *Integridad: de datos o de origen (autentificación)*
    - Mecanismo de prevención : gestión modificaciones autorizadas
    - Mecanismos de detección
  - *Disponibilidad*
    - Ataques de denegación de servicio
- Adicionales : Consistencia, Control, Auditoría.

Riesgos : clasificación de Shirey

- 4 clases :
  - *Revelación* (disclosure) : Acceso no autorizado a información
  - *Engaño* (deception) : Admisión de datos falsos
  - *Perturbación* (disruption) : Interrupción o prevención de correcta operación
  - *Usurpación* : Control no autorizado de partes del sistema

Riesgos comunes (I)

- *Fisgoneo* (snooping): Captura no autorizada de información (forma pasiva de *revelación*).
  - Solución : Servicio de confidencialidad
- *Modificación* : cambio no autorizado de información (*engaño*, *perturbación*, *usurpación*).
  - Solución : servicio de integridad
- *Enmascaramiento* : una entidad hace pasarse por otra (*engaño*, *usurpación*).
  - Solución : servicio de integridad
  - Una forma permitida de *enmascaramiento* : *Delegación de Autoridad*.

Riesgos comunes (II)

- *Repudiación* : Falsa denegación de pertenencia a una entidad (*engaño*).
  - Solución : servicio de integridad
- *Denegación de recepción* (*engaño*)
  - Solución : servicio de integridad y disponibilidad
- *Denegación de servicio* : inhibición de servicio (*usurpación*, a menudo utilizado con *engaño*).
  - *Retardo* si es de corto plazo (caballos de troya).

    Solución : servicio de disponibilidad

Políticas y mecanismos

- *Pólitica* de seguridad: afirmaciones sobre lo que está y no está permitido.
  - Formalmente, provee descripción axiomática de estados seguros y no seguros.
  - Composición de políticas diferentes.
- *Mecanismos* de seguridad: métodos, herramientas o procedimientos para implementar una política de seguridad.
- *Objetivos de seguridad*
  - *Prevención*
  - *Detección*
  - *Recuperación*

Cimientos

- *Suposiciones* : Elementos que se *asume* cumplen su función y en base a los cuales se deriva...
- *Confianza*
  - Una política de seguridad debe describir correctamente los estados seguros del sistema, y de una forma lo más completa posible.
  - Elementos de confianza de mecanismos de seguridad :
    - Cada uno está diseñado para cubrir una o más partes de la política de seguridad.
    - La unión de todos ellos implementa todos los aspectos de la política de seguridad.
    - Están implementados correctamente.
    - Son instalados y administrados correctamente.

Nivel de seguridad

- *Especificación* de comportamientos deseables y no deseables del sistema.
- Análisis del *diseño* del hardware, software y otros elementos (humanos, físicos)
- Argumentos o pruebas de que la *implementación*, procedimientos operativos y de mantenimiento producirán el comportamiento especificado.

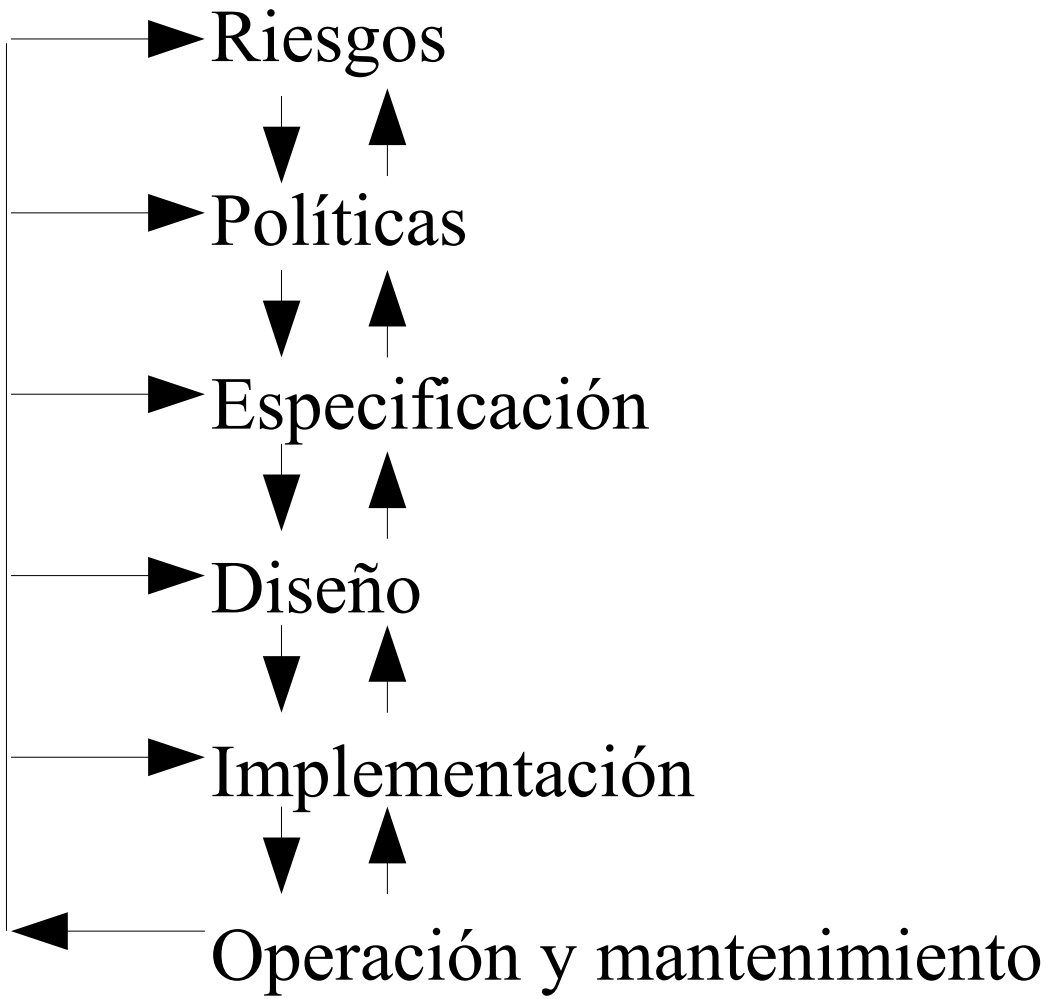
Aspectos operativos

- Análisis de riesgos
- Análisis de costes/beneficios
- Leyes y costumbres

Aspectos humanos

- Problemas organizacionales
  - Pérdidas en seguridad versus pérdidas sin seguridad
  - Responsabilidades, autoridades
  - Compartición con otras tareas
- Problemas humanos
  - Agentes externos, agentes internos
  - Personal no formado
  - Incorrecta utilización de mecanismos
  - Ingeniería social
  - Configuración de sistema incorrecta

En conjunto


Riesgos
Políticas
Especificación
Diseño
Implementación
Operación y mantenimiento