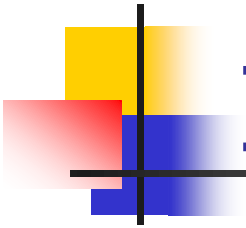
Bloque I
Criptografía

Introducción a la Seguridad en Redes

Seguridad en Redes de Comunicaciones

María Dolores Cano Baños

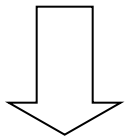


Introducción

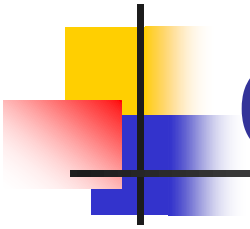
- Antes de 1988
  - redes propietarias más o menos aisladas
- En 1988
  - Robert T. Morris, ataque con gusano *worm*
- Después de 1988
  - DARPA crea el CERT, extendido a varios paises
- Situación actual: gran número de redes, convergencia de tecnologías, Internet,...
- ¿Se requieren expertos en seguridad?

Qué es Seguridad

- Definición: característica de cualquier sistema, telemático o no, que indica si ese sistema está libre de todo peligro, daño o riesgo, y que es en cierta manera infalible.



- Fiabilidad: probabilidad de que un sistema se comporte tal y como se espera de él.



Qué es Seguridad

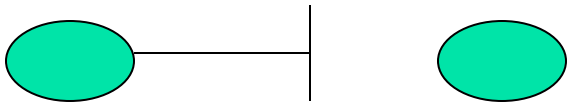
- Confidencialidad
  - criptografía
- Integridad
  - criptografía, algoritmos hash, etc.
- Disponibilidad
  - cortafuegos, detectores de intrusismo, ...
- Autenticación, no repudio y control de acceso.

Vulnerabilidad y Amenazas

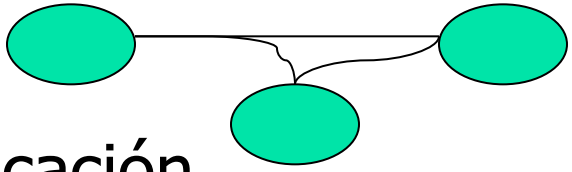
- **Vulnerabilidad**: es un punto débil de la red de comunicaciones o de sus equipos.
- **Amenaza**: cualquier circunstancia o evento que potencialmente puede causar un daño a una organizaciám mediante la exposición, modificación o destrucción de información o mediante la denegación de servicios críticos.
- **Ataque**: poner en práctica una amenaza aprovechando las vulnerabilidades del sistema o red de comunicaciones
- A proteger: software, hardware y datos.

Tipos de Amenazas

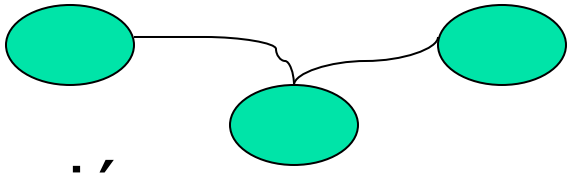
- Interrupción



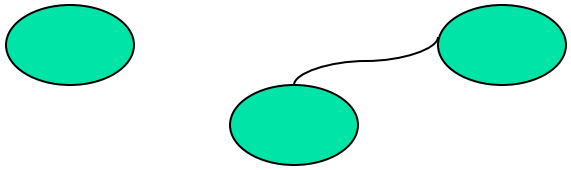
- Interceptación

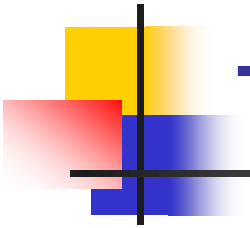


- Modificación



- Generación



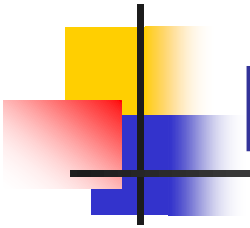


Tipos de Ataques

- Ataques pasivos o activos
- Ataques activos
  - suplantación
  - réplica
  - alteración
  - denegación de servicio

Procedencia de las Amenazas

- Personas
  - Piratas
  - Ing. social, shoulder surfing, basureo
- Programas o amenazas lógicas
  - Softw. Incorrecto (bugs), herramientas de seguridad, puertas traseras, bombas lógicas, canales cubiertos, virus, gusanos, caballos de troya, programas conejo/bacterias, técnicas salami.
- Catástrofes naturales
  - terremotos, inundaciones, ...

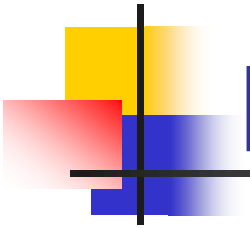


Métodos de Defensa

- Análisis de amenazas, pérdidas originadas y probabilidad de ocurrencia => política de seguridad:
  - Defina responsabilidades y reglas (evitar o minimizar)
- Mecanismos de seguridad: de prevención, de detección y de recuperación.
  - Mecanismos de prevención: autenticación/ identificación, control de acceso, separación, seguridad en las comunicaciones.

Métodos de Defensa

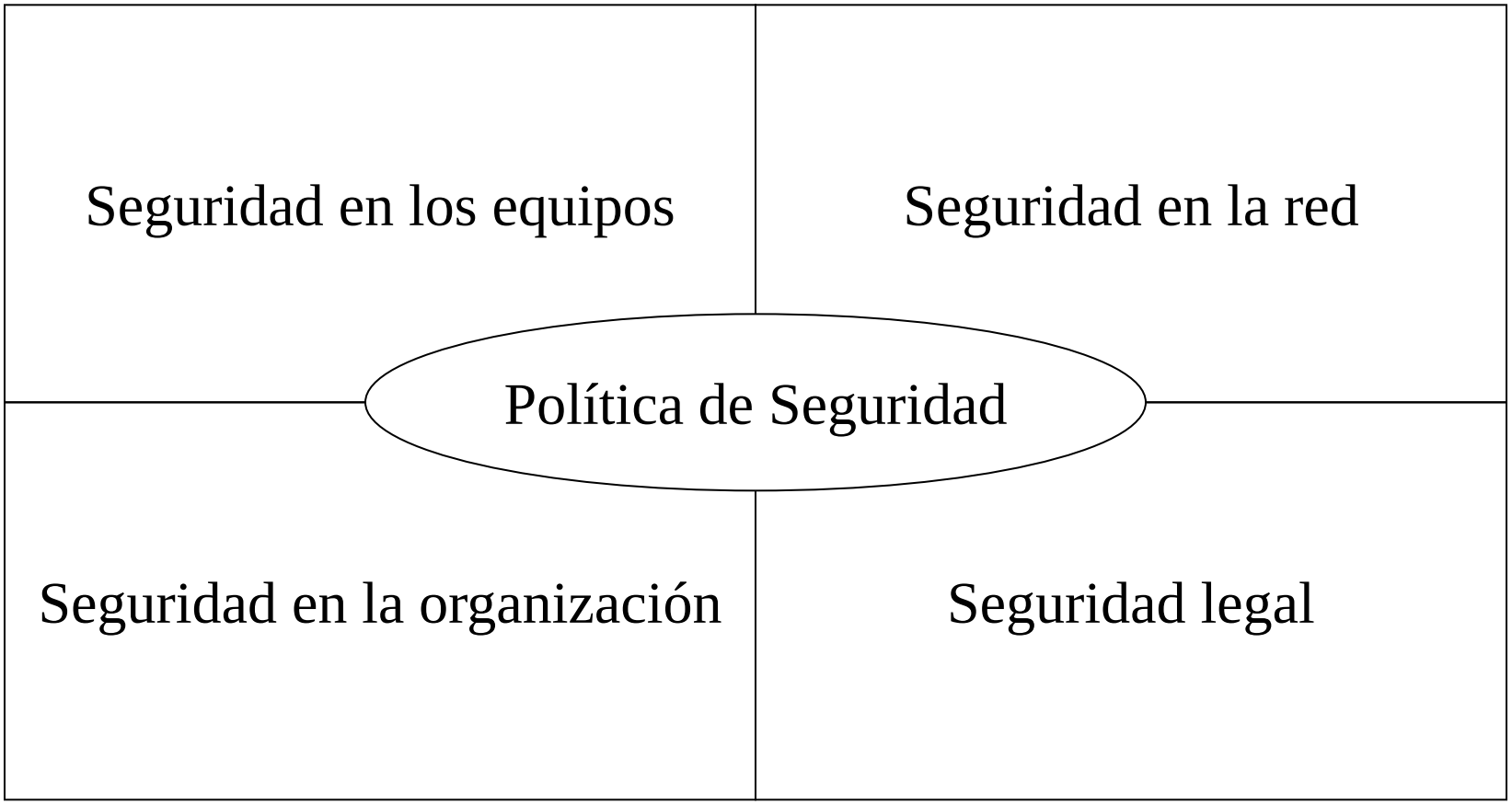
- Protección del hardware:
  - Acceso físico
    - Prevención: autenticacion, cerrar puertas, proteger cableado, tarjetas electrónicas de acceso, ...
    - Detección: cámaras de vigilancia, alarmas, ...
  - Desastres naturales
    - Prevención: terremotos -> equipos en superficies bajas, usar fijaciones; inundaciones o humedad -> detectores de agua, equipos a cierta elevación,...
  - Desastres del entorno
    - Prevención: electricidad -> uso de SAI, apagar equipos ante riesgo de tormenta eléctrica, ...; incendio -> no fumar cerca de equipos, extintores automáticos, ...

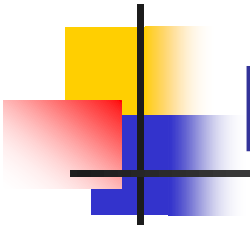


Métodos de Defensa

- Protección de datos
  - Interceptación
    - Prevención: no segmentos de red de fácil acceso, aplicaciones de cifrado, hardware de cifrado (DES), ...
  - Pérdidas de información
    - Prevención: copias de seguridad/respaldo

Política de Seguridad





Política de Seguridad

- Política de Seguridad
  - Conjunto de requisitos definidos por los responsables del sistema indicando qué está y qué no está permitido.
  - RFC 2196
    - Política de Seguridad no debe ser una entelequia
    - Guía de compra de hw/sw, política de privacidad, de acceso, de responsabilidad, de autenticación, de disponibilidad, de mantenimiento, de comunicación de violaciones, e información de apoyo.

Política de Seguridad

- Seguridad local
- Seguridad en red
  - Controles de acceso eficiente y proteger información.
- Seguridad en la organización
- Seguridad legal