La seguridad inicia con el Análisis de Riesgo

M. Farias-Elinos
Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Grupo de Seguridad de RedCUDI (Internet-2 México)
http://seguridad.internet2.ulsa.mx

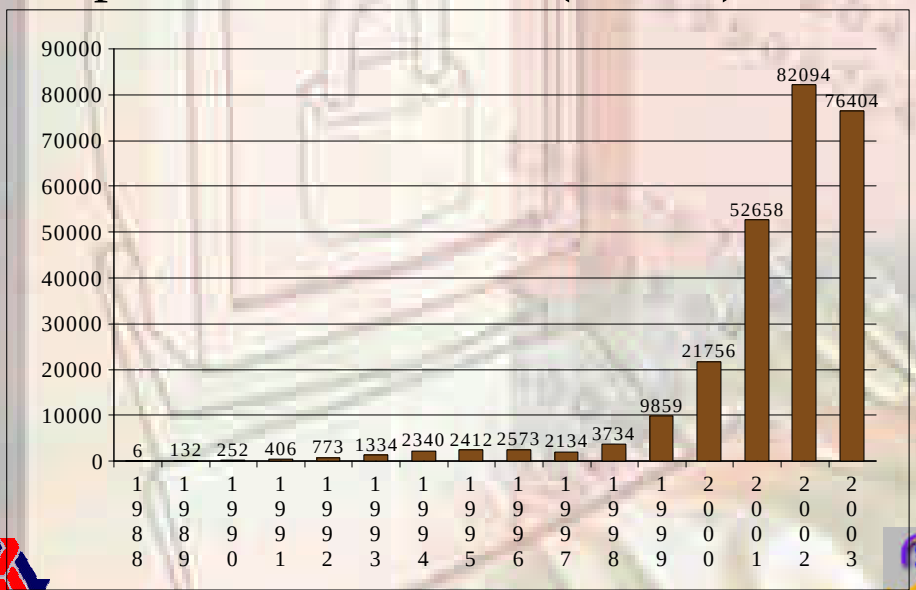
Contenido

- Problemática
- Definiciones
- Principios
- Analisis de riesgo
  - Objetivos
  - Beneficios
  - Elementos
  - Activos
  - Amenazas
  - Clasificaciones
- Conclusiones

Problemática

- Inexistencia o ineficiencia de los esquemas de seguridad informática
- Uso de herramientas tecnológicas sin un previo analisis de funcionalidad apropiados
- Creencia de ***Producto = Seguridad***

Reporte de incidentes (CERT)



Definiciones

- Riesgo
  - Posibilidad de sufrir una pérdida o daño
- Activo
  - Datos, software, hardware, infraestructura, personal, Información, etc.
- Seguridad informática
  - Todo aquello que se hace para reducir los riesgos a los activos.

Objetivo de la Seguridad Informática

- Preservar los activos de una organización y mantener la operabilidad de la organización basando en:
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - Privacidad
  - No-Repudio
  - Autenticidad
  - Control de Acceso

Principios de los participantes

- Conciencia de la necesidad de seguridad y de que se puede mejorar
- Todos son responsables de la seguridad
- Respuesta oportuna y cooperativa para prevenir, detectar y responder ante incidentes de seguridad
- Respeto a los intereses legítimos de otros
- La seguridad debe ser compatible con los valores de una sociedad democrática

Principios de los participantes

- Deberán ser una guía ante la presencia de una amenaza
- La seguridad debe de incorporase como un elemento escencial en los diseños
- Deberán realizar revisiones, actualizacion y modificaciones a los esquemas de seguridad, según las necesidades de la organización.

Análisis de riesgo

- Proceso por el cual se identifican las amenazas y vulnerabilidades de una organización
- Con el fin de generar controles que minimicen los efectos de los riesgos.
  - ISO 17799 (Information Technology -- Code of practice for information security management)

Objetivo del análisis de riesgo

- Tener la capacidad de:
  - Evaluar y manejar los riesgos de seguridad
  - Tomar las mejores decisiones en seguridad informática
  - Enfocar los esfuerzos en la protección de los activos

Beneficios del analisis de riesgo

- Asegurar la continuidad operacional de la organización
- Saber manejar las amenazas y riesgos críticos
- Mantener una estratégia de protección y de reducción de riesgos
- Justificar una mejora continua de la seguridad informática

Elementos de un análisis de riesgo

- Construir el perfil de las amenazas basado en los activos
  - Identificar los activos de la organización
  - Identificar las amenazas a los activos
  - Conocer las prácticas actuales de seguridad
  - Identificar las vulnerabilidades organizacionales
    - Recursos humanos, recursos técnicos, etc.
  - Identificar los requerimientos de seguridad de la organización

Elementos de un análisis de riesgo

- Indentificar las vulnerabilidades de la infraestructura
  - Detectar componentes claves
  - Detectar las vulnerabilidades de la tecnología utilizada

Elementos de un análisis de riesgo

- Desarrollo de planes y estratégias de seguridad
  - Riesgos para los activos críticos
  - Medidas de riesgos
  - Estratégias de protección
  - Planes para reducir los riesgos

Activos

- Servidores de información
  - Nominas, Servicios escolares, Contabilidad, Documentos, etc.
- Infraestructura de la red
  - Switches/hubs, ruteadores, cableado, etc.
- Servidores de Internet
  - e-mail, web, DNS, etc.

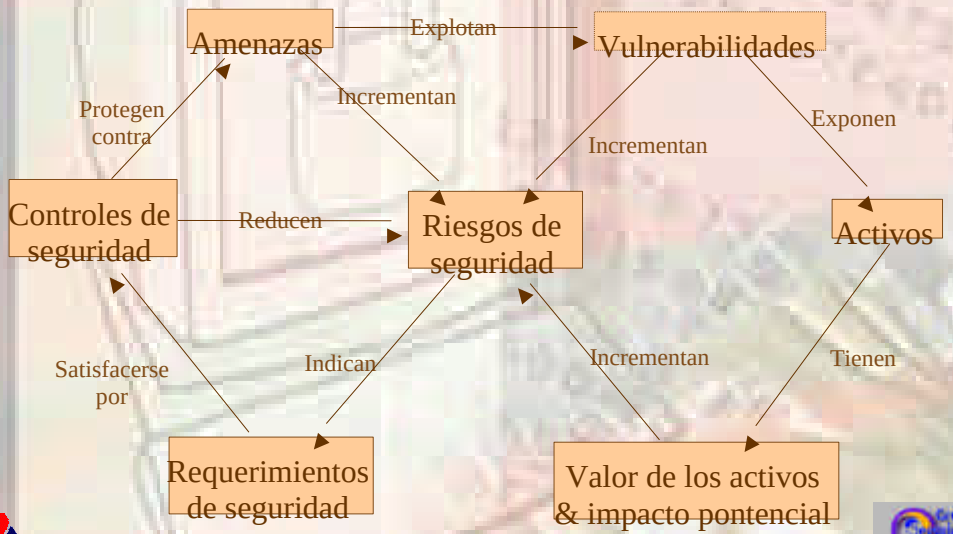
Amenazas

- Ambientales
  - Desastres naturales (terremotos, tormentas, etc.)
  - Condiciones ambientales (fallas del suministro eléctrico, contaminación, etc.)
- Deliberadas
  - Sabotaje, código malicioso, fraudes, etc.
- Accidentales
  - Errores de usuarios, errores de programación, fallas en los servicios de comunicación, etc.

Clasificaciones

- Riesgos
  - Muy Alto
  - Alto
  - Moderado
  - Bajo
- Consecuencias
  - Catastróficos
  - Mayores
  - Moderados
  - Menores
  - Insignificantes
- Probabilidad
  - Certeza
  - Probablemente
  - Moderado
  - Improbable
  - Raro

Relación de riesgos



Conclusiones

- La seguridad no es un producto
- La seguridad es un conjunto de planes y estratégias enfocadas a reducir los riesgos
- El Analisis de riesgo es la forma de conocer las vulnerabilidades de una organización, así como las amenazas que enfrenta.

Documentos

- ISO 17799 (Information Technology -- Code of practice for information security management)
- ISO 15335 (Information technology -- Guidelines for the management of IT Security)
- ISO 15408 (Information Technology -- Security techniques -- Evaluation criterial for IT security)

La seguridad inicia con el Análisis de Riesgo

M. Farias-Elinos
Lab. de Investigación y Desarrollo de Tecnología Avanzada (LIDETEA)
Grupo de Seguridad de RedCUDI (Internet-2 México)
http://seguridad.internet2.ulsa.mx