CAPITULO 3
Gestión de Riesgos
Metodologías de Análisis y Evaluación de Riesgos

Jenny Torres, PhD.

Metodologías de Análisis y Evaluación de Riesgos

Definiciones

- **Riesgo:**
  - Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
  - El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.
- **Análisis de riesgos:**
  - Es el proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.
  - Sabiendo lo que podría pasar, hay que tomar decisiones.
- **Tratamiento de riesgos:**
  - Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

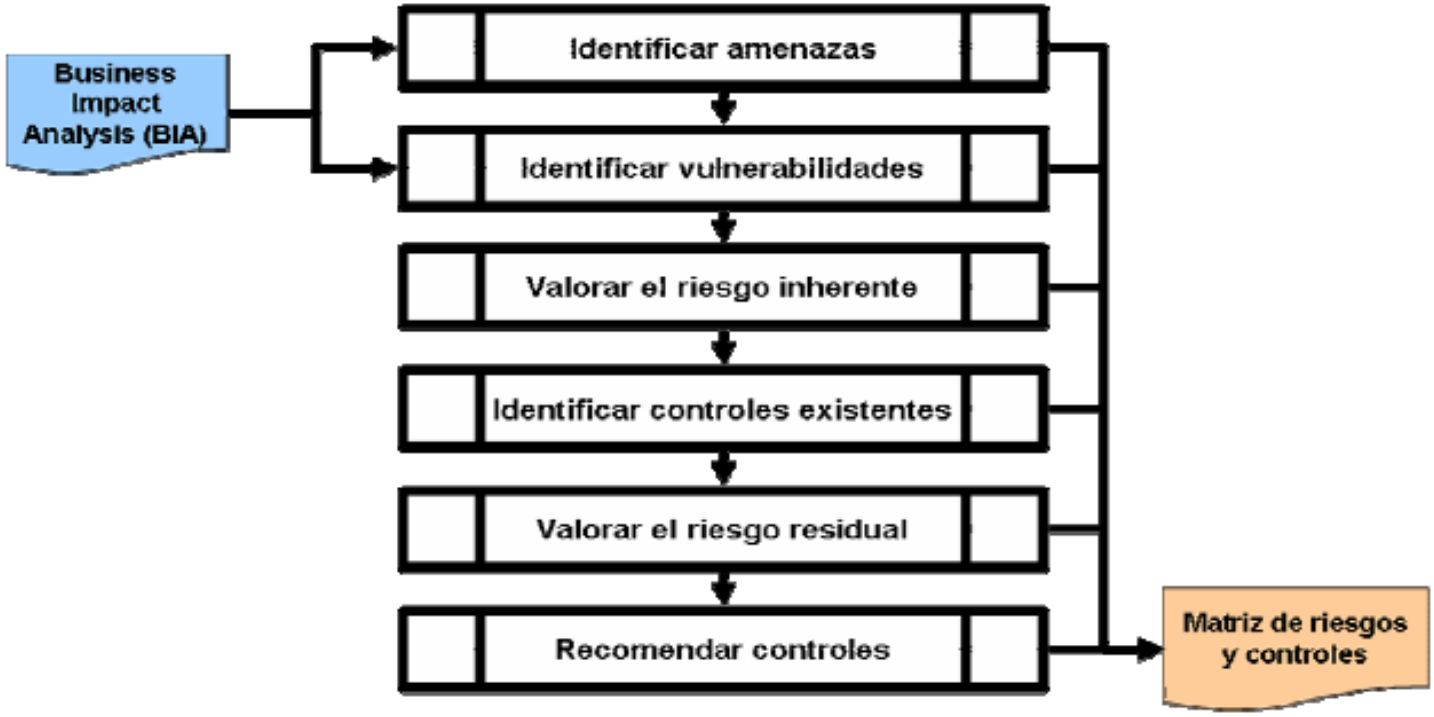
Metodologías de Análisis y Evaluación de Riesgos

Consecuencias

- La falta de una gestión del riesgo en cualquier entidad puede tener como consecuencia:
  - Pérdida de tiempo
  - Pérdida de productividad
  - Pérdida de información confidencial
  - Pérdida de clientes
  - Pérdida de imagen
  - Pérdida de ingresos por beneficios
  - Pérdida de ingresos por ventas y cobros
  - Pérdida de ingresos por producción
  - Pérdida de competitividad en el mercado
  - Pérdida de credibilidad en el sector

Metodologías de Análisis y Evaluación de Riesgos

Gestión del Riesgo



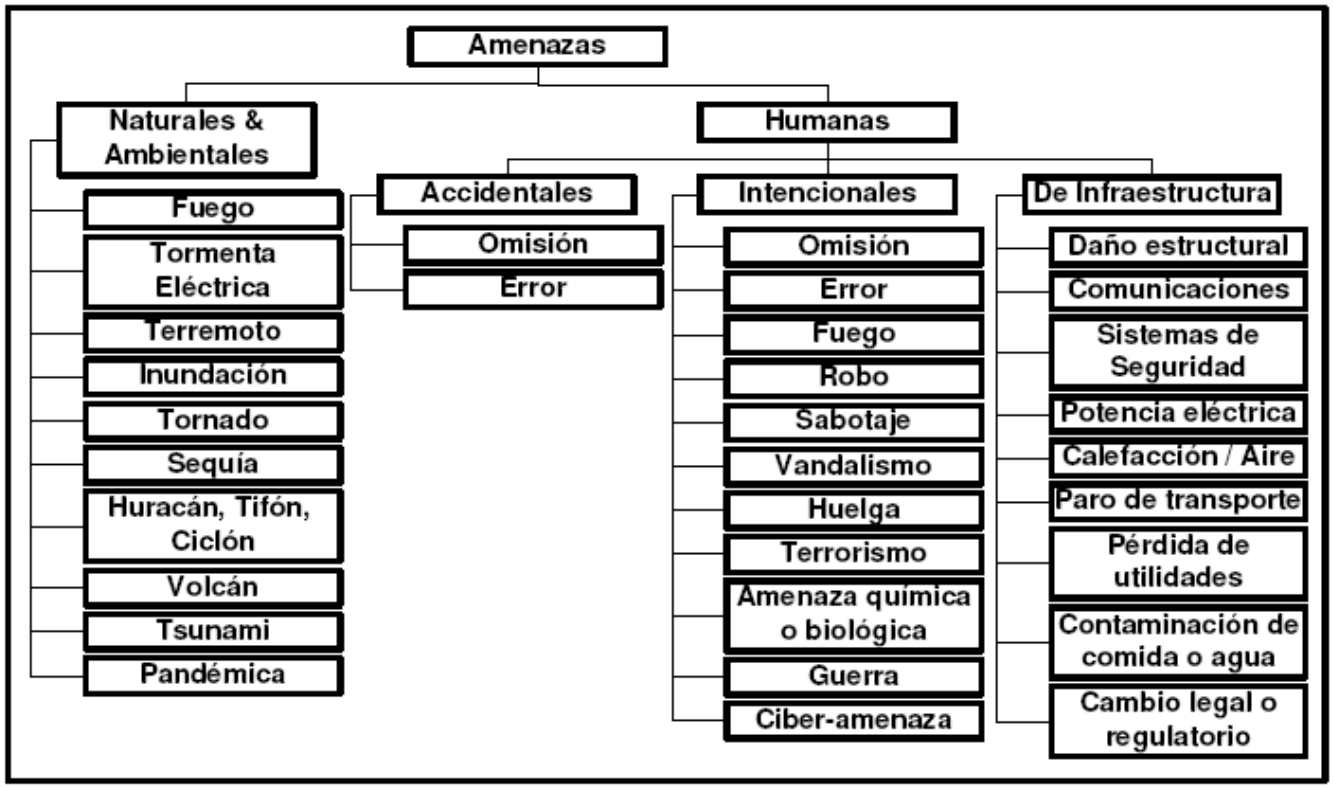
Metodologías de Análisis y Evaluación de Riesgos

Identificación de amenazas

- Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por la frecuencia estimada de ocurrencia y la estimación de daño (degradación) que causarían sobre los activos.
- Tareas:
  - Identificación de las amenazas
  - Valoración de las amenazas
- Clasificación
  - Amenazas Naturales & Ambientales
  - Amenazas Humanas (internas, externas, estructuradas, no estructuradas)
  - Amenazas tecnológicas

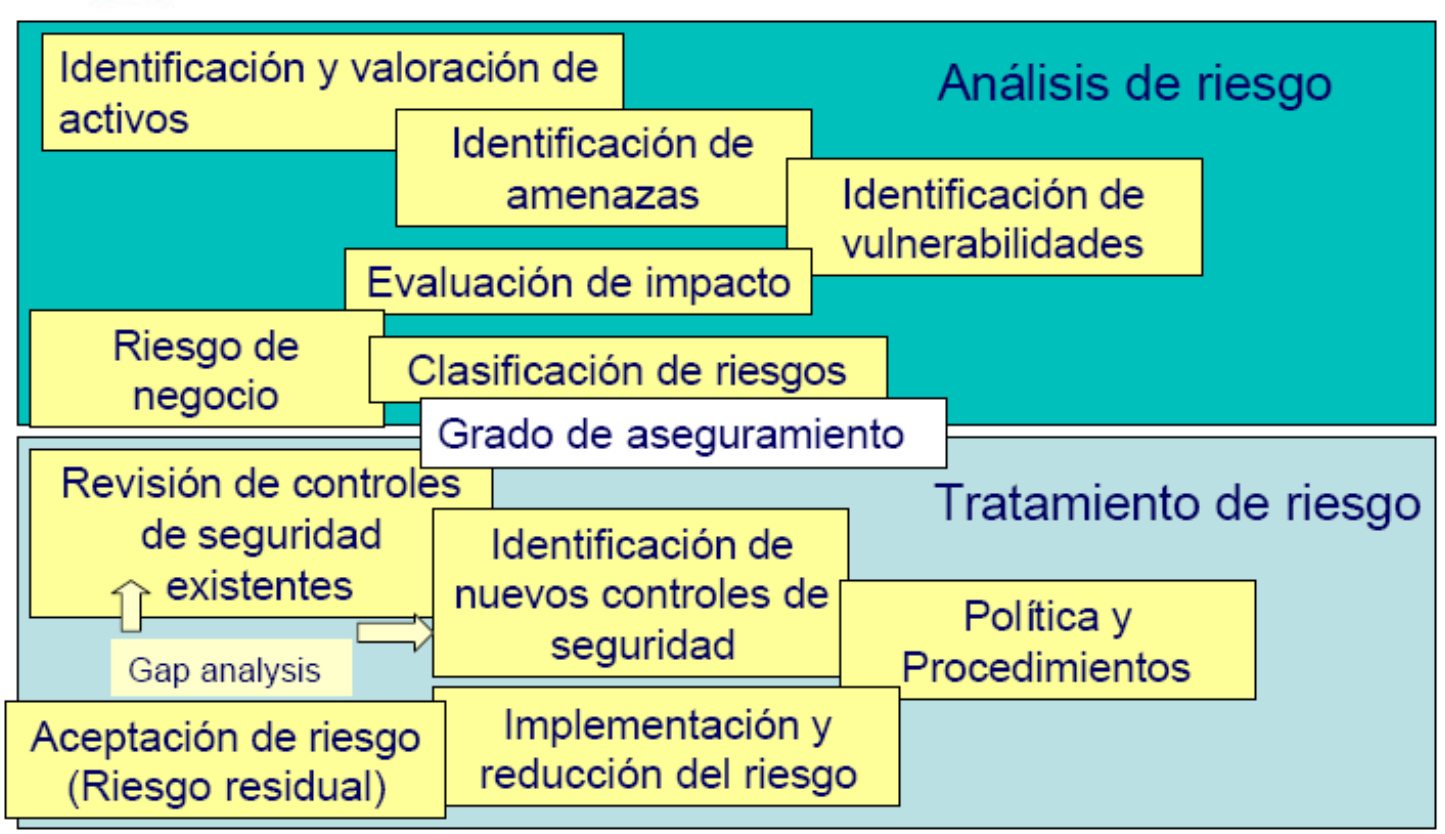
Metodologías de Análisis y Evaluación de Riesgos

Amenazas



Metodologías de Análisis y Evaluación de Riesgos

Gestión del Riesgo



Metodologías de Análisis y Evaluación de Riesgos

Metodologías

- **OCTAVE**
  - Evalúa amenazas y vulnerabilidades de los recursos tecnológicos y operacionales importantes de una organización
- **CURE**
  - Evalúa las áreas que tendrán mayor impacto con el uso de software exclusivamente.
- **MAGERIT**
  - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Metodologías de Análisis y Evaluación de Riesgos

Metodologías

- **ISO/IEC 27005 Risk Management standard 31/07/2008**
  - Fase de análisis de riesgos:
    - Determinación de activos
    - Determinación de amenazas
    - Estimación de impactos
    - Estimación de vulnerabilidad de las amenazas sobre los activos
  - Cálculo del nivel de riesgo.
    - Fase de tratamiento de riesgos:
    - Determinación de los criterios de aceptación del riesgo
    - Determinación de las medidas de seguridad necesarias
    - Estimación del nivel de riesgo residual

Metodologías de Análisis y Evaluación de Riesgos

Análisis de Riesgo

- La base de toda buena política de Seguridad es sin excepciones, un muy buen Análisis de riesgo.
- Este análisis de riesgo es el fundamento en el cual se establecen las normas de protección
- Determina:
  - Qué se necesita proteger
  - De quien protegerlo
  - Cómo protegerlo
- Los riesgos se clasifican por el nivel de importancia y por el impacto de la pérdida.

Metodologías de Análisis y Evaluación de Riesgos

Análisis de Riesgo

- Las tareas de análisis y gestión de riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.
- El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento.
- La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.
- Un análisis de riesgos no es una tarea menor que realiza cualquiera en sus ratos libres. Es una tarea mayor que requiere esfuerzo y coordinación. Por tanto debe ser planificada y justificada.
- Un análisis de riesgos es recomendable en cualquier Organización que dependa de los sistemas de información y comunicaciones para el cumplimiento de su misión.

Metodologías de Análisis y Evaluación de Riesgos

Metodología base del Análisis de Riesgo

- Definición de la Matriz de Impacto
- Definición de la Probabilidad de ocurrencia
- Definición de la Matriz de riesgos
- Identificación de Activos informáticos
- Identificación de amenazas
- Identificación de Medidas de seguridad
- Identificación de Oportunidades
- Acciones correctivas

Metodologías de Análisis y Evaluación de Riesgos

Estimación del Riesgo

- Esta actividad procesa todos los datos recopilados en las actividades anteriores para:
  - realizar un informe del estado de riesgo: estimación de impacto y riesgo
  - realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas
- Tareas:
  - Estimación del impacto
  - Estimación del riesgo
  - Interpretación de los resultados
- La metodología de evaluación de riesgos de seguridad de la información está basada en una consideración sistemática de los siguientes puntos:
  - Impacto potencial de una falla de seguridad
  - Probabilidad de ocurrencia de dicha falla

Metodologías de Análisis y Evaluación de Riesgos

Estimación del Riesgo

- **Riesgo Bruto**
  - Corresponde al impacto y probabilidad de ocurrencia de una amenaza en un supuesto dónde no existen ni controles ni medidas de seguridad implementadas.
  - Este análisis permite identificar el riesgo en su máxima expresión.
- **Riesgo Residual**
  - Corresponde al impacto y probabilidad de ocurrencia de una amenaza en donde existen controles y medidas de seguridad implementadas.

RIESGO = IMPACTO * PROBABILIDAD DE OCURRENCIA

Metodologías de Análisis y Evaluación de Riesgos

Matriz de impacto

- Está compuesta por el tipo de impactos que puede recibir en ciertos aspectos que son tenidos en cuenta:
  - Resultados
  - Clientes
  - Operaciones
  - Regulaciones
  - Reputación
- La matriz de impacto se obtiene en base a información provista por la empresa.

Metodologías de Análisis y Evaluación de Riesgos

Matriz de impacto

Clasificación del nivel	Descripción	Valores
Alto	Grandes consecuencias sobre el orden económico y financiero	9-10
Significativo	Efectos Significativos	7-8
Moderado	Efectos moderados, pero significativo	4-5-6
Menor	Consecuencias menores Pero significativas	2-3
Insignificante	Consecuencias insignificantes	1

Metodologías de Análisis y Evaluación de Riesgos

Matriz de impacto

Categoría	Impacto en resultados	Impacto en clientes	Impacto en Operaciones	Impacto regulatorio	Impacto en Reputación
Insignificante	Entre $0 a $0.01 millones	Sin reclamo de clientes	Sin impacto en las operaciones	El incumplimiento regulatorio no genera sanciones	Sin impacto en el valor o reputación de la marca
Menor	Entre $0,01 y $0,25 millones	Los reclamos de los clientes son aislados	Impacto menor en operaciones; no percibido por el cliente. Las consecuencias pueden ser absorbidas dentro de las operaciones normales	El incumplimiento regulatorio genera sanciones leves	Hay un impacto menor en la reputación y en el valor de la marca; difusión leve
Moderado	Entre$0,25 y $10 millones	Los reclamos de los clientes son importantes; hay pérdida menor de clientes	Impacto importante en operaciones, unidades de negocio sin servicio por hasta ocho horas, pudiera ser percibida por el cliente	El incumplimiento regulatorio genera sanciones que no afectan la capacidad de la organización para operar	Hay un impacto importante en el corto plazo en la reputación y en el valor de la marca; difusión masiva y corta
Significativo	Entre $10 a $100 millones	Los reclamos de los clientes son masivos; hay pérdida de cartera	Impacto mayor en operaciones que afecta seriamente la capacidad de la compañía para atender a sus clientes; hasta 48 horas sin servicio	El incumplimiento regulatorio resulta en sanciones que pudieran afectar la capacidad de la organización para operar	Hay una perdida mayor en la participación del mercado y en el valor de la marca, con publicidad adversa; las alianzas estratégicas están amenazadas
Catastrófico	Entre $100 a $1000 millones	Hay pérdida masiva de clientes; hay litigios contra las unidades de negocios	Impacto catastrófico en operaciones que afecta seriamente la capacidad de la compañía para continuar con el negocio; mas de 48 horas sin servicio	Suspensión de la autorización para operar	Hay una pérdida sustancial en la participación de mercado y en el valor de la marca y la reputación de la organización, con publicidad adversa prolongada; las alianzas estratégicas se desintegran

Metodologías de Análisis y Evaluación de Riesgos

Probabilidad de Ocurrencia

- Se calcula la probabilidad de ocurrencia de los posibles hechos
- Luego se orienta a tener una frecuencia anual de los mismos
- Se obtiene en base a la información provista por la empresa

Probabilidad	Descripción	Frecuencia anual
Muy Probable (5)	Se espera que ocurra en la mayoría de las circunstancias	1
Probable (4)	Se espera que ocurra en la menoría de las circunstancias	0.75
Posible (3)	Podría ocurrir algunas veces	0.5
Incierto (2)	No es muy probable que ocurra	0.25
Improbable (1)	Sólo podría ocurrir en casos excepcionales	0.1

Metodologías de Análisis y Evaluación de Riesgos

Matriz de Riesgos

- Está conformada por la matriz de ocurrencia y el impacto de un incidente.
- Luego se categorizan los riesgos en:
  - Riesgos extremos (mas de 10 millones)
  - Riesgos altos (hasta 10 millones)
  - Riesgos medios (hasta 0,25 millones)
  - Riesgos Bajos (hasta 0,01 millones)
- Se obtiene en base a la Matriz de Impacto y a la Matriz de Probabilidad de ocurrencia.

Metodologías de Análisis y Evaluación de Riesgos

Matriz de Riesgos

- Esta matriz sirve para determinar los activos de misión critica de la Empresa.
- Se debe determinar el riesgo a través del **Impacto** * la **Probabilidad** de Ocurrencia.

Ítem	Nombre del Recurso	Impacto (IM)	Probabilidad de Ocurrencia (PO)	Riesgo (IM*PO)

Metodologías de Análisis y Evaluación de Riesgos

Identificación de medidas de seguridad

- Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.
- Tareas
  - Identificación de las salvaguardas existentes
  - Valoración de las salvaguardas existentes
- Tienen como propósito:
  - Eliminar el riesgo
  - Reducir el riesgo
  - Aceptar el riesgo
  - Transferir el riesgo

Metodologías de Análisis y Evaluación de Riesgos

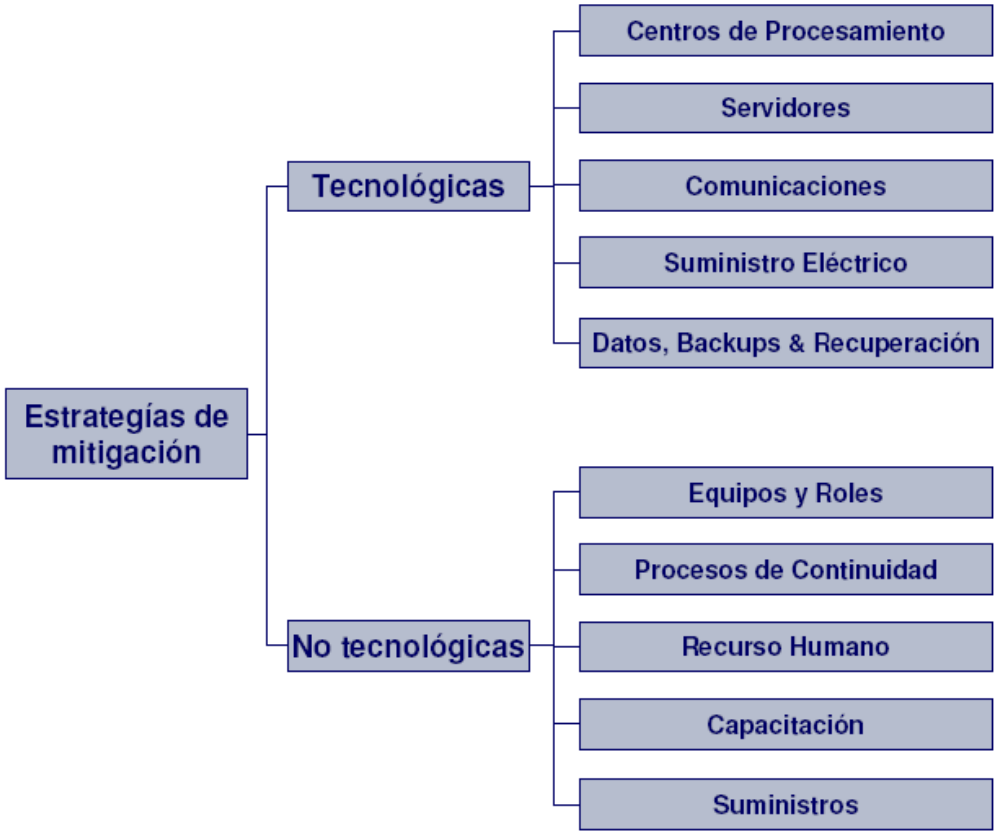
Identificación de medidas de seguridad

- Las cuatro respuestas básicas de la gestión de riesgos son las siguientes:

  - **Aceptar**: Admitir si el impacto del riesgo es mínimo o el costo para mitigarlo es mayor al costo del impacto del riesgo.
  - **Transferir**: Trasladar todo el riesgo a terceros para disminuir el riesgo en el proyecto.
  - **Mitigar**: Disminuir la probabilidad de que se produzca el riesgo al establecer acciones anticipadas para evitar que suceda.
  - **Evitar**: Contrarrestar los riesgos que van surgiendo mediante estrategias. Esto puede implicar cambios en el cronograma o el alcance del proyecto para eliminar la amenaza del riesgo.

Metodologías de Análisis y Evaluación de Riesgos

Estrategias de mitigación



Referencias

- ISO 27000, disponible en : http://www.iso27000.es
- Computer Emergency Response Team. Available at: http://www.cert.org
- Maiwald Eric, Fundamentos de Seguridad en Redes, McGrawHill, Segunda Edición, México 2005.
- Garfinkel Simson, Web Security, Privacy & Commerce.
- Tipos de delitos informáticos reconocidos por las Naciones Unidas. Disponible en http://tiny.uasnet.mx/prof/cln/der/silvia/tipos.htm