NORMAS

Norma ISO 27001

A lo largo de este artículo veremos la diferencia que existe entre seguridad informática y seguridad de la información. La norma ISO 27001 nos posibilita conocer la seguridad de la información gracias a la implantación de un Sistema de Gestión de Seguridad de la Información.

Seguridad informática

La totalidad de los especialistas en seguridad basan sus conocimientos y experticias sobre el aspecto técnico tradicional de la seguridad, esto es en las áreas IT, aunque bastantes de ellos consideran las cuestiones propias como el nuevo aspecto en las comunicaciones y que hace que actualmente se hable de TIC.

Además de tener un enfoque técnico prácticamente, los especialistas únicamente se manejan con las vulnerabilidades y en parte con amenazas en forma de ataques, todo lo dicho no se considera suficiente para hablar de los riesgos correspondientes.

Estándares

Fundamentos de Seguridad Informática

Estándares

Los estándares de seguridad son una herramienta que apoya la gestión de la seguridad informática, ya que los ambientes cada vez más complejos requieren de modelos que

administren las tecnologías de manera integral, sin embargo, existen distintos modelos aplicables en la administración de la seguridad.

Trusted Computer Security Evaluation Criteria. TCSEC. [pdf]

Information Technology Security Evaluation Criteria. ITSEC. [pdf]

ISO 15408 Criterios Comunes (CC). [pág oficial] [pdf1] [pdf2][pdf3]

BS 7799 (Reino Unido).

ISO 17799. [pdf]

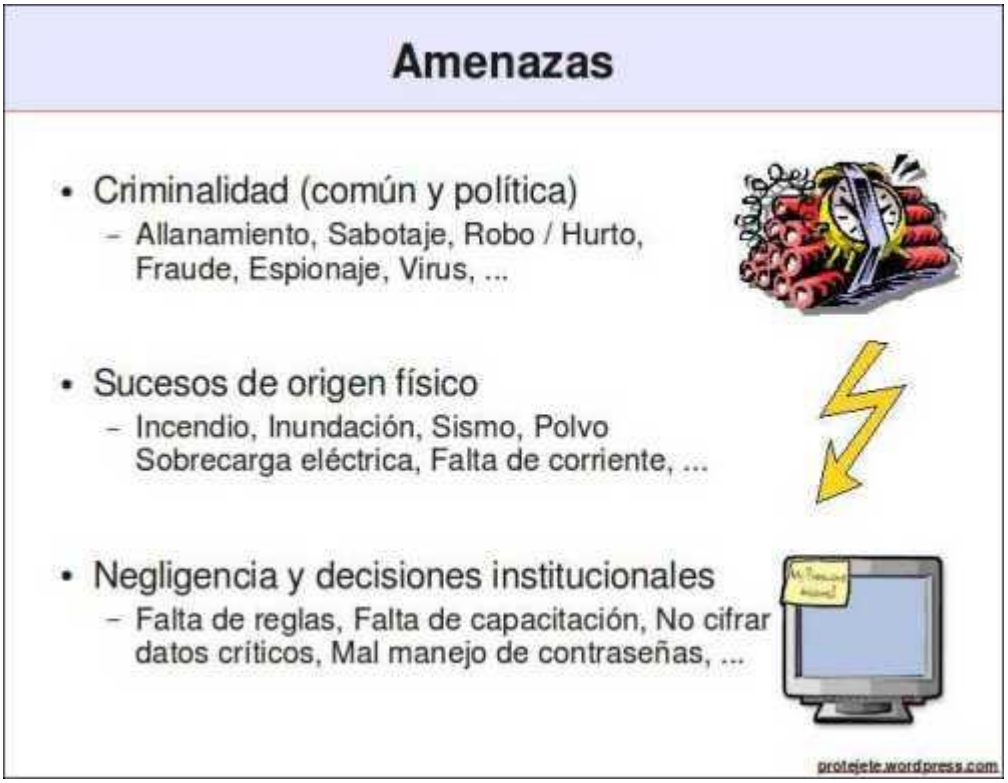
ISO 27000.

AMENAZAS DE LOS DATOS

Amenazas

Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la Seguridad Informática, los Elementos de Información. Debido a que la Seguridad Informática tiene como propósitos de garantizar

la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones.



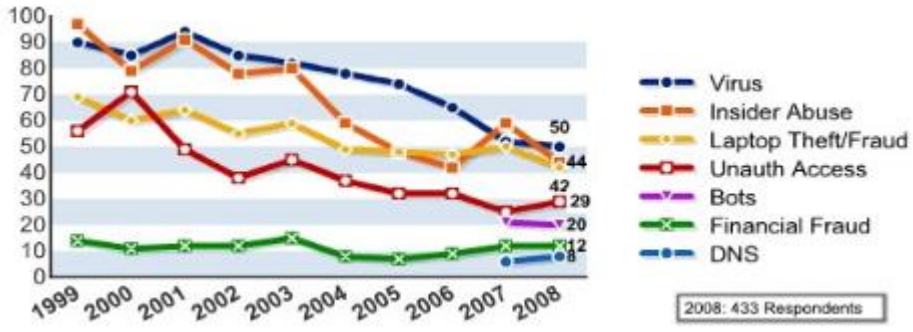
Desde el punto de vista de la entidad que maneja los datos, existen amenazas de origen externo como por ejemplo las agresiones técnicas, naturales o humanos, sino también amenazas de origen interno, como la negligencia del propio personal o las condiciones técnicas, procesos operativos internos (Nota: existen conceptos que defienden la opinión que amenazas siempre tienen carácter externo!)

Generalmente se distingue y divide tres grupos

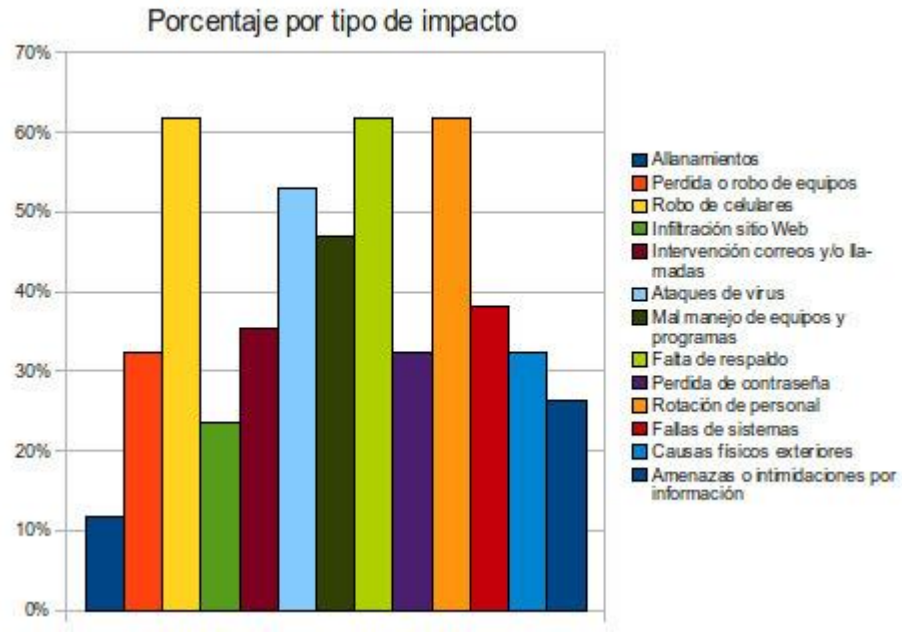
- **Criminalidad: son todas las acciones, causado por la intervención humana, que violan la ley y que están penadas por esta. Con criminalidad política se entiende todas las acciones dirigido desde el gobierno hacia la sociedad civil.**
- **Sucesos de origen físico: son todos los eventos naturales y técnicos, sino también eventos indirectamente causados por la intervención humana.**
- **Negligencia y decisiones institucionales: son todas las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.**

Existen amenazas que difícilmente se dejan eliminar (virus de computadora) y por eso es la tarea de la gestión de riesgo de preverlas, implementar medidas de protección para evitar o minimizar los daños en caso de que se realice una amenaza.

Para mostrar algunas de las amenazas más preocupantes, consultamos dos estadísticas, el primer grafo sale de la "Encuesta sobre Seguridad y Crimen de Computación – 2008" del Instituto de Seguridad de Computación (CSI por sus siglas en inglés) que base en 433 respuestas de diferentes entidades privadas y estatales en los EE.UU [6]



El segundo tiene su origen en una encuesta que se hizo en el año 2007, con 34 organizaciones sociales a nivel centroamericano



Ambos grafos, muestran el porcentaje de todos los encuestados que sufrieron ese tipo de ataque.

Como se observa, existen algunas similitudes respecto a las amenazas más preocupantes

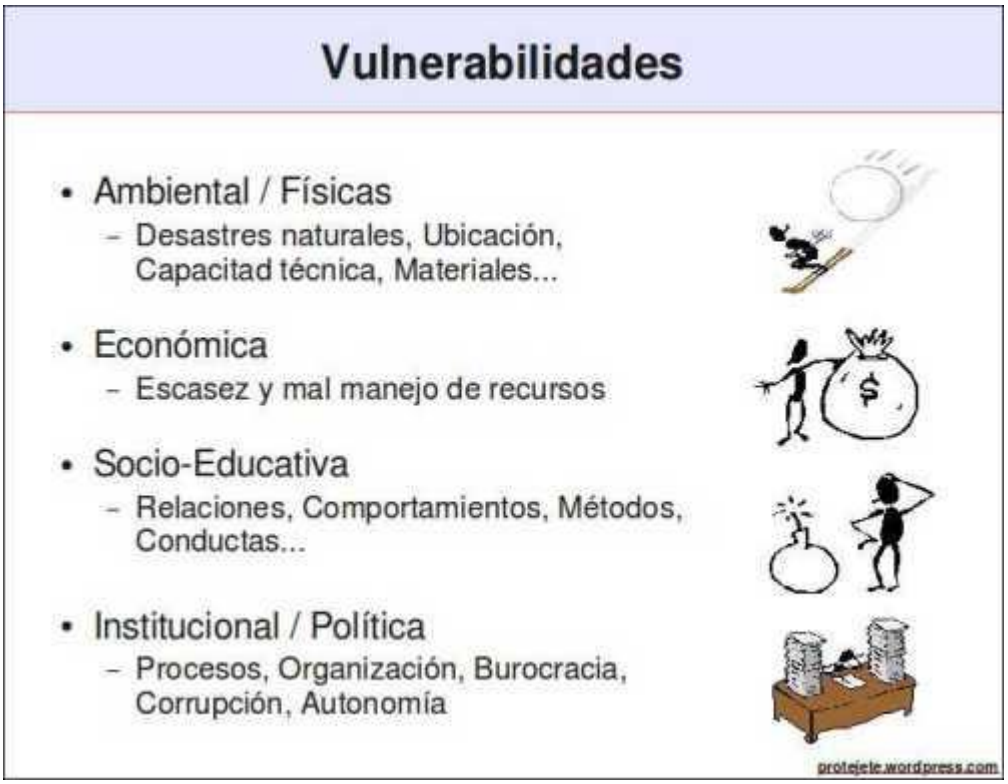
- **Ataques de virus (>50%)**
- **Robo de celulares, portátiles y otros equipos (>40%)**

Pero también existen otras amenazas que, aunque no aparezcan en ambas encuestas, son muy alarmantes y que se debe tomar en consideración

- **Falta de respaldo de datos**
- **Perdida de información por rotación, salida de personal**
- **Abuso de conocimientos internos (no consultado en encuesta de organizaciones sociales)**

- **Mal manejo de equipos y programas**
- **Acceso non-autorizado**
- **etc**

Vulnerabilidades



La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño [4].

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.

Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos

característicos: Ambiental, Física, Económica, Social, Educativo, Institucional y Políti ca [4].

En referencia al folleto ¡Pongámos las pilas! [5], se recomienda leer el capitulo "Algunas verdades incómodas", página 14 a 21, donde se aborda el tema de las amenazas y vulnerabilidades.