CAPITULO 3
Gestión de Riesgos
Vulnerabilidades y Amenazas en la Empresa

Jenny Torres, PhD.

Vulnerabilidades y Amenazas en la Empresa

Conceptos y Definiciones

- 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**.
- Los elementos de información son:
  - **Datos e Información:** finanzas, recurso humano, llamadas telefónicas, correo electrónico, base de datos, etc.
  - **Sistemas e Infraestructura**: edificio, equipos de red, computadores, celulares, equipos portátiles, etc.
  - **Personal:** personal directivo, administrativo, etc

Vulnerabilidades y Amenazas en la Empresa

Conceptos y Definiciones

- **Criminalidad**: acciones causadas por la intervención humana, que violan la ley y que están penadas por esta. **Allanamiento, sabotaje, robo, fraude, espionaje.**

- **Sucesos de origen físico**: eventos naturales y técnicos, y aquellos indirectamente causados por la intervención humana. **Incendio, inundación, sismo, sobrecarga eléctrica.**

- **Negligencia y decisiones institucionales**: acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Están directamente relacionado con el comportamiento humano. **Ausencia de normas, capacitación, mal manejo de contraseñas, no cifrar información.**

Vulnerabilidades y Amenazas en la Empresa

Conceptos y Definiciones

Los tipos de amenazas son:

- Externas
  - Agresiones técnicas
  - Agresiones naturales
  - Agresiones humanas

- Internas
  - Negligencia del personal
  - Condiciones técnicas
  - Procesos operativos internos

Vulnerabilidades y Amenazas en la Empresa

Conceptos y Definiciones

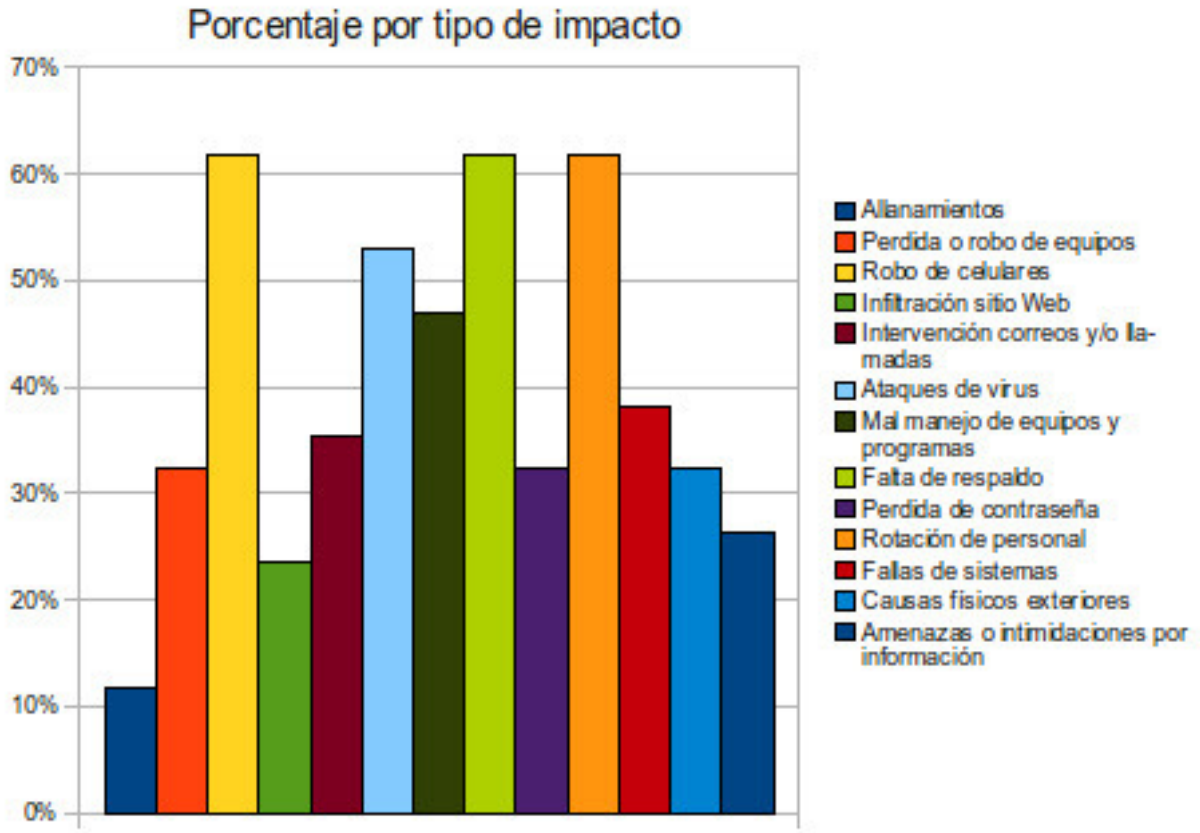
Los tipos de amenazas son:

- Externas
  - Agresiones técnicas
  - Agresiones naturales
  - Agresiones humanas

- Internas
  - Negligencia del personal
  - Condiciones técnicas
  - Procesos operativos internos

Vulnerabilidades y Amenazas en la Empresa

Conceptos y Definiciones



Vulnerabilidades y Amenazas en la Empresa

Conceptos y Definiciones

- La **Vulnerabilidad** es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.
- Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad ya que no se puede ocasionar un daño.
- Se pueden clasificar en
  - **Ambiental – Física:** desastres naturales, materiales, etc
  - **Económica**: mal manejo de recursos, etc.
  - **Social – Educativo**: comportamientos, métodos, conductas, etc
  - **Institucional - Política**: procesos, organización, autonomía, etc.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- **El malware es un software malicioso o software malintencionado** que tiene como objetivo **infiltrarse** o **dañar** una computadora o sistema de información sin el consentimiento de su propietario.
- **Los tipos de ataques son:**
  - **Virus:** Programas con capacidad de replicación. Es un malware que infecta a medida que se transmite.
  - **Gusanos:** Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos y son capaces de llevar esto a cabo sin intervención del usuario propagándose mediante el uso de Internet.
  - **Caballos de Troya:** Es un software malicioso que se presenta al usuario como un programa aparentemente legítimo e inofensivo pero al ejecutarlo ocasiona daños. Los troyanos pueden realizar diferentes tareas, pero, en la mayoría de los casos crean una puerta trasera (backdoor) que permite la administración remota un usuario no autorizado.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- El **virus informático** es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de USB o de la red de comunicación, causando diversos tipos de daños a los sistemas:
  - 12 de diciembre de 1987. El virus de Navidad, una tarjeta navideña digital enviada que causó un desbordamiento de datos en la red de IBM.
  - 10 de enero de 1988. El virus Jerusalén se ejecuta en una universidad hebrea y tiene como fecha límite el primer viernes 13 del año, como no pudieron pararlo se sufría una disminución de la velocidad cada viernes 13.
  - 20 de septiembre de 1988 en Fort Worth, Texas, Donald Gene un programador de 39 años será sometido a juicio el 11 de julio por cargos delictivos de que intencionadamente contaminó el sistema, por ser despedido, con un virus informático el año 85.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- Algunas de las operaciones que un **troyano** pueden llevar a cabo en el ordenador remoto son:
  - Utilizar la máquina como parte de una botnet (por ejemplo para realizar ataques de denegación de servicio o envío de spam).
  - Instalación de otros programas (incluyendo otros programas maliciosos).
  - Robo de información personal: información bancaria, contraseñas, códigos de seguridad.
  - Borrado, modificación o transferencia de archivos (descarga o subida).
  - Ejecutar o terminar procesos.
  - Apagar o reiniciar el equipo.
  - Monitorizar las pulsaciones del teclado.
  - Realizar capturas de pantalla.
  - Ocupar el espacio libre del disco duro con archivos inútiles.
  - Monitorización del sistema y seguimiento de las acciones del usuario.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

Exploit (explotar o aprovechar)

- Es una pieza de software, un fragmento de datos, o una secuencia de comandos con el fin de automatizar el aprovechamiento de un error, fallo o vulnerabilidad, con el objetivo de causar daños en los equipos.
- El fin del exploit puede ser violar las medidas de seguridad para poder acceder al mismo de forma no autorizada y emplearlo en beneficio propio o como origen de otros ataques a terceros.
- Los exploits pueden ser escritos empleando una diversidad de lenguajes de programación, aunque mayoritariamente se suele utilizar lenguaje C.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- Un **bug** es un error o un defecto en el software o hardware que hace que un programa funcione incorrectamente.
- Bug es español significa “insecto”.
- Según se dice, el primer bug de ordenador fué un insecto real, descubierto en 1945 en Harvard, una polilla atrapada en la calculadora Mark II hizo que la máquina entera se apagara.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

Spyware (Espía)

- Es todo aquel software utilizado con objeto de rastrear, identificar y perfilar las actividades de los usuarios sin su consentimiento.
- Suelen instalarse con alguna “utilidad” gratuita.
- Integrados en programas originales.
- Son discretos, no llaman la atención.
- Recopilan información del usuario.
- Páginas que visitan
- Horarios de conexión
- Servidores donde se conectan
- Software instalado
- Envían toda la información obtenida.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- Entre los programas espías “spyware” se pueden encontrar diversas familias:
  - **Cookies**: Permiten identificar las áreas de interés y los hábitos de utilización por parte de los usuarios.
  - **Adware**: Programas que instalen componentes en el ordenador para registrar la información personal del usuario.
  - **Monitores del Sistema**: Programas que capturan todo aquello que el usuario realiza en su ordenador almacenándolo cifrado o enviándolo automáticamente.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- **Spam**: Consiste en el envío masivo de mensajes electrónicos no solicitados.
- **Phishing**: Es un ataque de “ingeniería social” a través de e-mail o mensajería instantánea caracterizado por intentos fraudulentos de adquisición de información sensible mediante suplantación (spoofing)
- **Pharming** (Fraude): Es la explotación de una vulnerabilidad en servidores DNS que permite a un “hacker” usurpar un nombre de dominio y redirigir todo el tráfico web legítimo a otra ubicación.
- **Las máquinas "zombie"** (Crimen Telemático Organizado): Son computadoras comprometidas por algún tipo de “malware” al servicio de terceras personas para ejecutar actividades hostiles con el total desconocimiento del usuario del equipo.

Vulnerabilidades y Amenazas en la Empresa

Efectos del Malware en la Empresa

- **Botnet**: Es un término utilizado para una colección de robots (software) autónomos que pueden ser controlados remotamente por diversos medios con propósitos maliciosos.
- **Ataque DDOS (Distributed Denial Of Service Attack) o Ataque de Denegación de Servicio Distribuido:** ataque conjunto y coordinado entre varios equipos (que pueden ser cientos o decenas de miles) hacia un servidor víctima.
- **Juegos online:** se estima que el 54% de los archivos referidos a videojuegos en redes P2P, están troyanizados. Se analizaron 1000 muestras en sitios y en redes P2P de los 30 videojuegos más populares, y se constató que 528 contenían algún tipo de malware.
- **Páginas Web legitimas pero maliciosas:** Los visitantes se convierten en victimas sin conocimiento y pasan a formar parte de la red informática de los atacantes. Las redes sociales (My Space, Foto Blogs y Second Life, etc) se están convirtiendo en una moda peligrosa.

Referencias

- Micki Krause, Harold F. Tipton. "**Information Security Management Handbook".** *Auerbach Publications. Fifth Edition.* ISBN: 08493-1997-8.
- Simson Garfinkel with Gene Spafford. "**Web Security, Privacy & Comerse"**. O'Really. Second Edition. ISBN 0-596000-456.
- Eric Maiwald, "**Network Security, Abegineer´s Guide**". McGraw-Hill. 2nd. Ed. ISBN 222957-8.
- Christopher Hadnagy, **Ingeniería Social: El Arte Del Hacking Personal**, Anaya Multimedia, 2011 ISBN 9788441529656.