Seguridad Informática

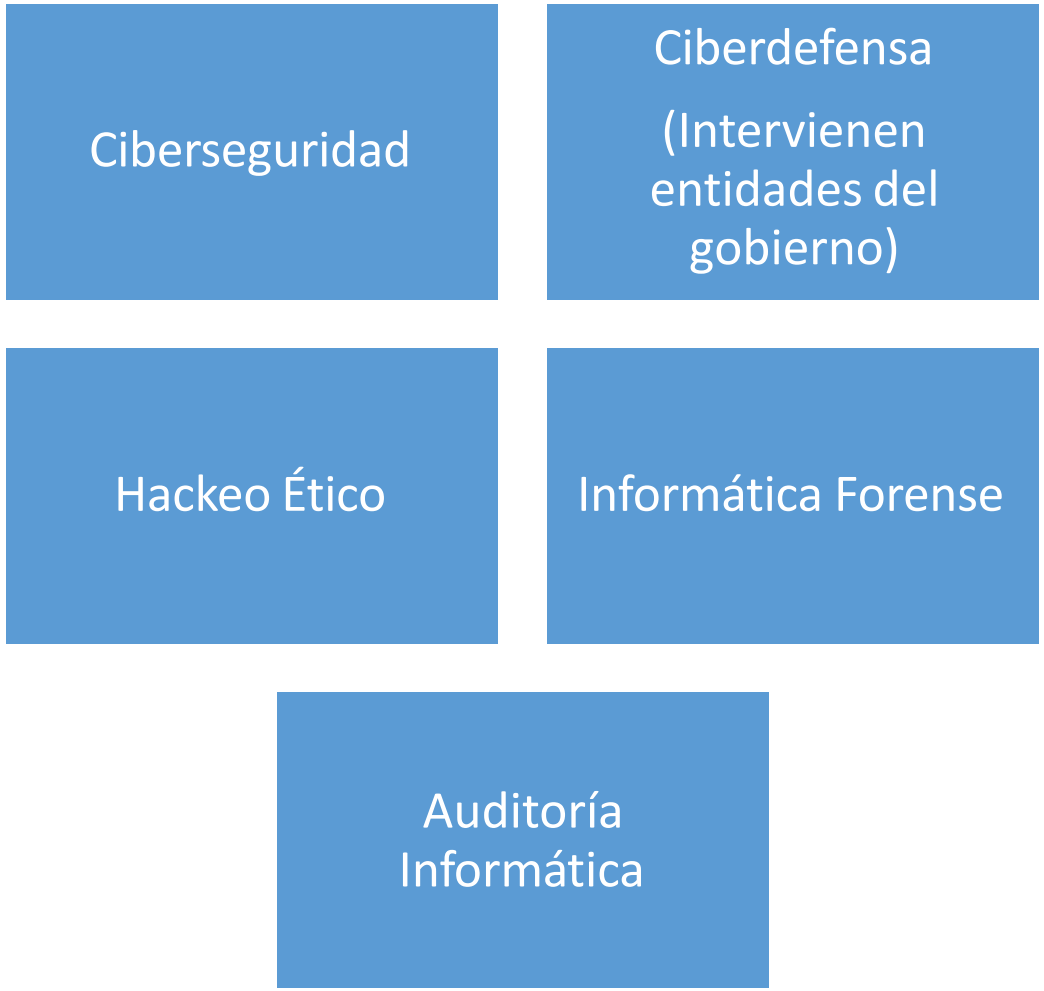
UNIDAD 1
Amenaza, Riesgo, Vulnerabilidad Impacto

Modalidad Virtual
Docente: Ing. Francisco Álvarez Solís, MSc.

UNIDAD 1

CIBERSEGURIDAD y CIBERDELINCUENCIA

Áreas de la Seguridad Informática



Término en español	Concepto
Ciberseguridad	**Medidas preventivas para proteger los sistemas de ataques externos.**
Hackeo Ético	**Pruebas a la ciberseguridad implementada en una empresa con el objetivo de detectar vulnerabilidades y corregirlas para evitar el acceso de personas no autorizadas a las redes o sistemas.** **Se requiere permiso de la institución.**
Informática Forense	Conjunto de técnicas para extraer la información de cualquier medio electrónico sin alterar su estado, lo que permite buscar datos ocultos, o dañados o hasta eliminados. El resultado del análisis de la información puede ser **prueba determinante en un proceso judicial. (Después de un delito o suceso)**
Auditoría Informática	**Evaluación de las medidas de seguridad para identificar y mitigar los posibles riesgos.**

Término en español	Concepto	Término en Inglés
Ciberdefensa	Conjunto de acciones de defensa activas pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al enemigo o a otras inteligencias en oposición.	*Cyber defence* *Cyber defense*
Ciberespacio	Se refiere a un entorno no físico creado por equipos de cómputo unidos para interoperar en una red. Ámbito virtual creado por medios informáticos.	*Cyberspace*
Informática Forense	El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o examen forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructuras tecnológicas que permiten identificar, preservar, analizar y presentar datos válidos dentro de un proceso legal.	*Cyber forensics*

Término en español	Concepto	Término en Inglés
Ciberdelincuencia	Actividades dirigidas contra sistemas informáticos de particulares, empresas o gobiernos con el objetivo de vulnerar la integridad, confidencialidad y disponibilidad de los datos que se almacenan o gestionan.	*Cybercrime*
Ciberterrorismo	Acción terrorista en el ciberespacio. Terrorismo: 1.Forma violenta de lucha política, mediante la cual se persigue la destrucción del orden establecido o la creación de un clima de terror e inseguridad susceptible de intimidar a los adversarios o a la población en general. 2. Sucesión de actos de violencia ejecutados para infundir terror.	*Cyber terrorism*
Ciberguerra	Conflicto en el Ciberespacio.	Cyberwar

Ciberdelincuencia

Ciberdelincuencia

Área que trata los delitos cometidos utilizando medios tecnológicos. Ejemplos de Delitos son:

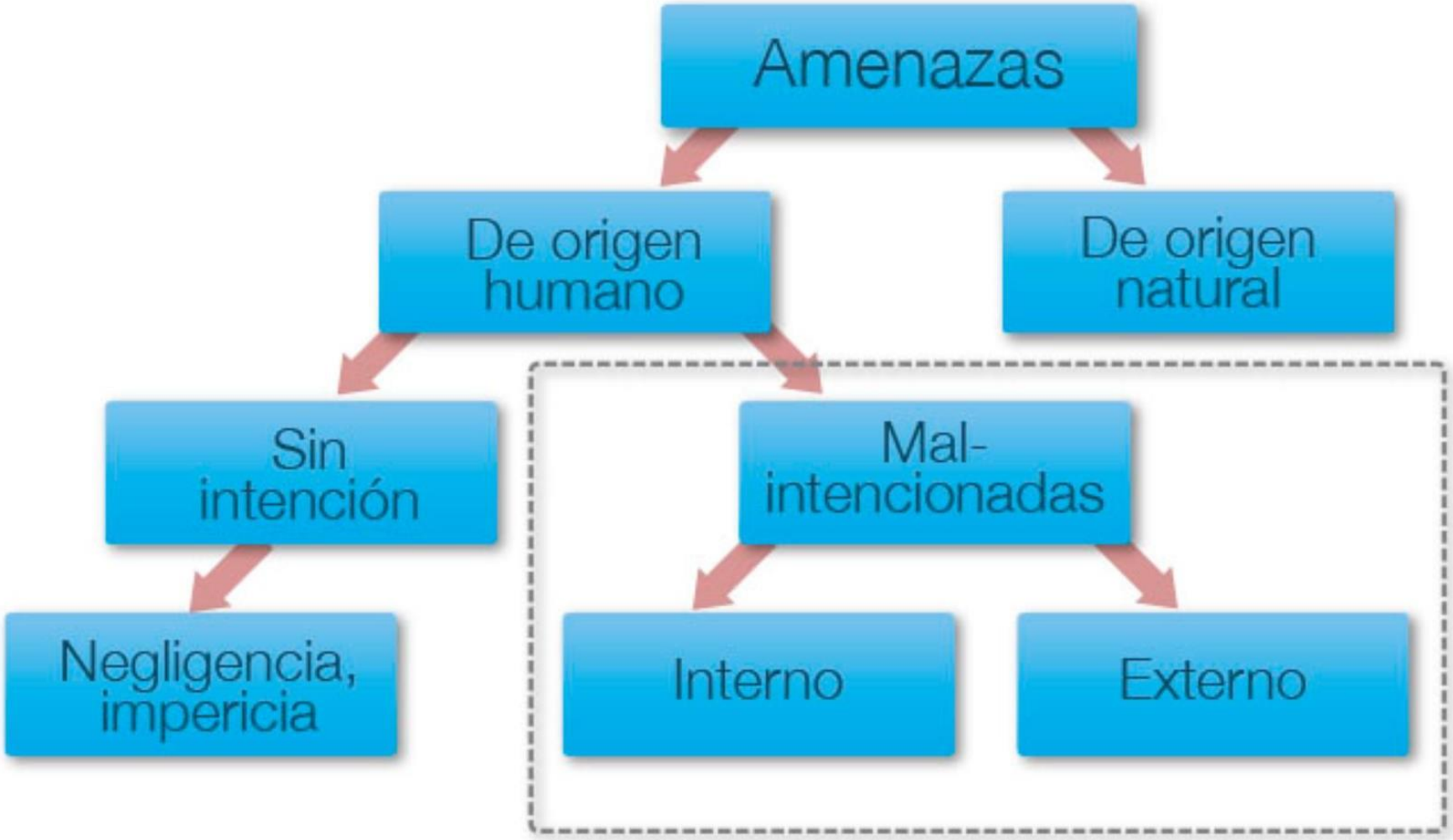
- Inyección SQL injection.
- Cross-Site Scripting (XSS).
- Intercepción.
- Ataques de contraseñas.
- Ataque DDoS.
- Robo de información

Conceptos Generales de Ciberdelincuencia

Término en Español	Ejemplo	Término en Inglés
Amenaza	Ladrones	Threat
Vulnerabilidad	Falta de Seguridad/Control de acceso.	Vulnerability
Riesgo	Probabilidad de que un robo ocurra.	Risk

Delincuente	Ladrones	Offender, thief, robber
Delito	Robo	Crime
Víctima	Personal del Banco/ Institución.	Victim, sufferer
Objeto del Delito	Dinero	Crime object
Impacto	Pérdida de ganancias, Inseguridad en los clientes	Impact

Amenazas


Amenazas
De origen humano
De origen natural
Sin intención
Mal-intencionadas
Negligencia, impericia
Interno
Externo

Tipos de Amenazas

Amenazas internas:

- Son más severas que todas aquellas que puedan venir del exterior ya que los usuarios conocen la red y saben cómo es su funcionamiento, tienen algún nivel de acceso a la red, los IPS y Firewalls son mecanismos no efectivos en amenazas internas

Amenazas externas:

- Se originan afuera de la red. Al no tener información certera de la red interna de la empresa, el atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla.
- Pueden ser evitadas desde el interior de la empresa si se tienen las medidas d seguridad correctas.

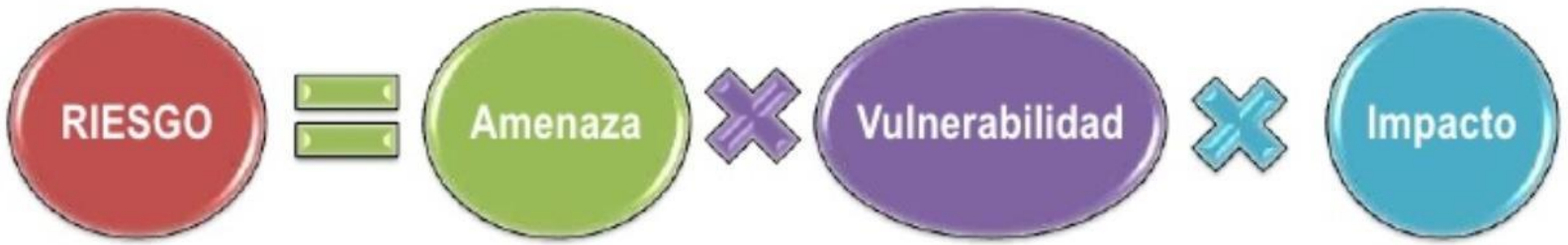
Vulnerabilidad

Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información.

Cualquier agente que pone en riesgo un sistema o lo hace susceptible ante ataques e intrusiones.

Riesgo

Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufra perjuicio o daño.



Tratamiento del Riesgo

Opciones de Tratamiento de Riesgos:

- **EVITAR**
- **TRANSFERIR**
- **MITIGAR**
- **ACEPTAR**

- **Evitar el Riesgo:** Se adoptan medidas con el propósito de prevenir la ocurrencia de eventos negativos.
- **Transferir el Riesgo:** Se adoptan medidas para transferir la probable pérdida a terceros (Seguros u otros instrumentos contractuales).
- **Mitigar el Riesgo:** Se adoptan acciones con la finalidad de reducir el impacto y/o la probabilidad (verificaciones, condiciones contractuales, supervisión, planes de contingencia entre otros).
- **Aceptar el Riesgo:** Se opta por aceptar el impacto y/o probabilidad del riesgo al encontrarse dentro del riesgo aceptado.

Intrusión

Acción de introducirse de forma indebida o ilegal en un sistema.

Explotación de Vulnerabilidades

Manipular las vulnerabilidades y crear un camino para realizar un ataque informático.

Se origina cuando a partir de la *vulnerabilidad* se crea una herramienta o script que automatiza la *explotación* de la *vulnerabilidad*

Ataque informático

Actividad que tiene como objetivo tomar el control, desestabilizar, dañar un sistema informático para robar, alterar o eliminar información.