

Unidad 0 – Precurso

Módulo 5 Riesgos, Amenazas, Ataques y Vulnerabilidades

RIESGOS, AMENAZAS Y VULNERABILIDADES

¿Qué es un riesgo?

Es la **probabilidad** de que ocurra un hecho que **produzca** ciertos **efectos** junto con la magnitud del **impacto** que puedan causar.

Si el riesgo es negativo, se llama **riesgo** como tal.

Si el riesgo es positivo, se llama **oportunidad**.

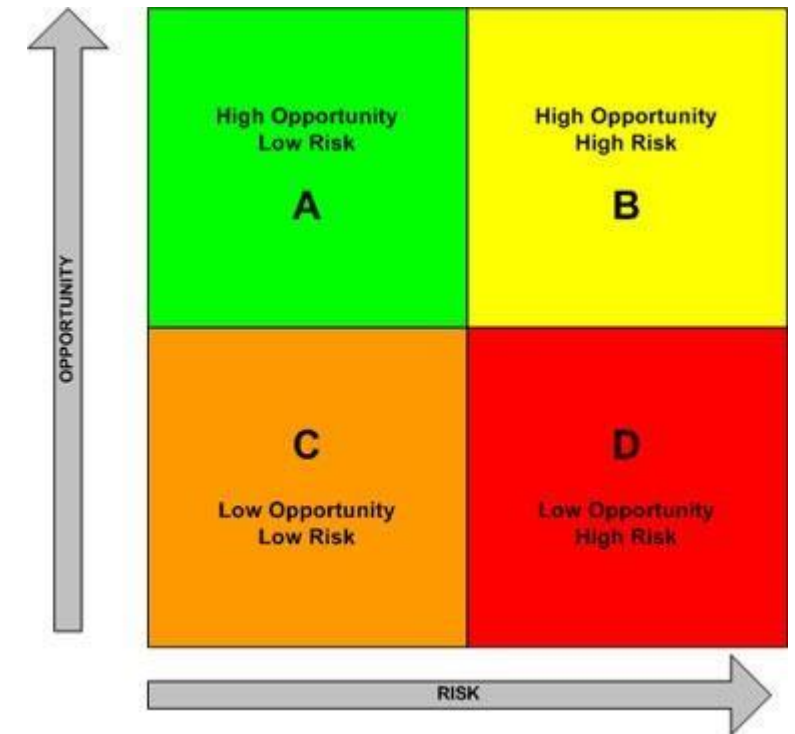
RIESGOS, AMENAZAS Y VULNERABILIDADES

¿Qué es un riesgo?

Es la **probabilidad** de que ocurra un hecho que **produzca** ciertos **efectos** junto con la magnitud del **impacto** que puedan causar.

Si el riesgo es negativo, se llama **riesgo** como tal.

Si el riesgo es positivo, se llama **oportunidad**.



RIESGOS, AMENAZAS Y VULNERABILIDADES

¿Qué es un riesgo?

Es la **probabilidad** de que ocurra un hecho que **produzca** ciertos **efectos** junto con la magnitud del **impacto** que puedan causar.

¿Qué es una amenaza?

Es la **materialización del riesgo** : Potencial ocurrencia de un hecho que puede darse en un lugar, duración e intensidad **determinadas**.

RIESGOS, AMENAZAS Y VULNERABILIDADES

¿Qué es un riesgo?

Es la **probabilidad** de que ocurra un hecho que **produzca** ciertos **efectos** junto con la magnitud del **impacto** que puedan causar.

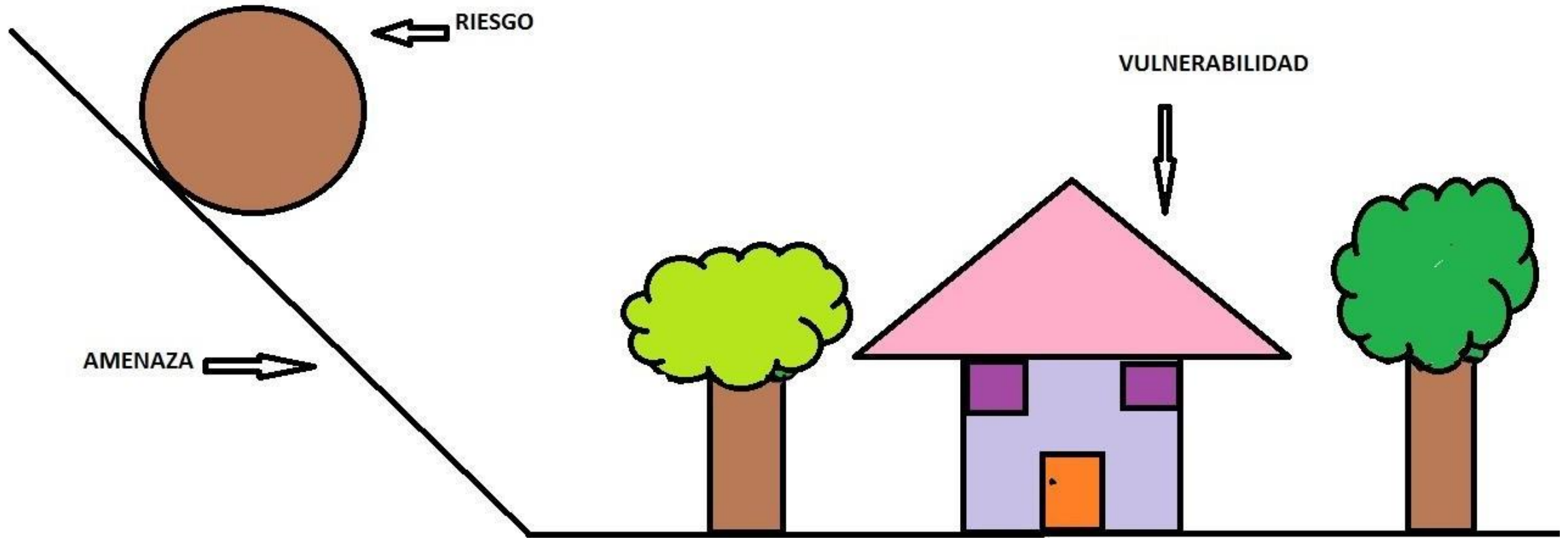
¿Qué es una amenaza?

Es la **materialización del riesgo** : Potencial ocurrencia de un hecho que puede darse en un lugar, duración e intensidad **determinadas**.

¿Qué es una vulnerabilidad?

Debilidad o ratio de exposición de un sujeto o sistema ante riesgos o amenazas.

RIESGOS, AMENAZAS Y VULNERABILIDADES



RIESGOS, AMENAZAS Y VULNERABILIDADES

¿Qué es un riesgo en seguridad informática?

Es la **probabilidad** de que se produzca un incidente de seguridad, materializándose una amenaza y causando pérdidas o daños.

¿Qué es una amenaza?

Es toda **acción** que aprovecha una **vulnerabilidad** para atentar contra la seguridad de un sistema de información.

¿Qué es una vulnerabilidad?

Es una **debilidad** o fallo en un sistema de información que pone en **riesgo** la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma

RIESGOS, AMENAZAS Y VULNERABILIDADES



ANALISIS DE RIESGOS



¿QUÉ HACER ANTE UN RIESGO?

- **Evitar** el riesgo : Eliminando su causa.
- **Mitigar** el riesgo o su probabilidad : Utilizando controles y monitorización.
- **Transferir** el riesgo : Compartirlo con terceros a través de seguros, contratos...
- **Aceptar** el riesgo : Se acepta su existencia y se monitoriza.

¿QUÉ HACER ANTE UN RIESGO?

EJERCICIO

Ejemplos de evitar, mitigar, transferir y aceptar un riesgo.

5 MINUTOS Y PUESTA EN COMUN

ORGANIZACIONES

MITRE :

<https://www.mitre.org>

NIST :

<https://nvd.nist.gov/>

FIRST :

<https://www.first.org/>

IDENTIFICACION DE VULNERABILIDADES

CVE (Common Vulnerabilities and Exposures)

Identificación de vulnerabilidades mediante :

- Número identificación (CVE-YYYY-NNNN)
- Descripción de la vulnerabilidad
- Referencia pública a la vulnerabilidad (paper o ejemplo)

<https://cve.mitre.org/>
<https://www.cvedetails.com/>

IDENTIFICACION DE VULNERABILIDADES

Otros sistemas de identificación de vulnerabilidades

- OSVDB (Deprecated) OCVDB-XXXX
- Android : A-XXXXXXXX
- Microsoft : MSXX-XXX
- ...

CVE ES EL MAS USADO INTERNACIONALMENTE

IDENTIFICACION DE VULNERABILIDADES

CWE (Common Weakness Enumeration)

Identificación de debilidades (más abstracto que CVE)

Por ejemplo : Tipos de ataques.

CWE-20 : Improper Input Validation

<https://cwe.mitre.org>

METRICAS DE RIESGOS

CVSS (Common Vulnerability Scoring System)

Traduce las características de una vulnerabilidad en una métrica numérica concreta indicando su severidad e importancia (impacto) :

Identificador

Impacto en Confidencialidad

Impacto en Integridad

Impacto en Disponibilidad

Complejidad de acceso

Autenticación

Acceso conseguido

<https://www.first.org/cvss/>

EXPLOTACION DE VULNERABILIDADES

EXPLOIT

Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en una aplicación o sistema, de forma que un atacante podría usarla en su beneficio.

Base de datos de exploits :

- <https://www.exploit-db.com>
- Paquete exploitdb en Kali

VULNERABILIDADES

EJERCICIO DE BUSQUEDA DE INFORMACION DE VULNERABILIDADES