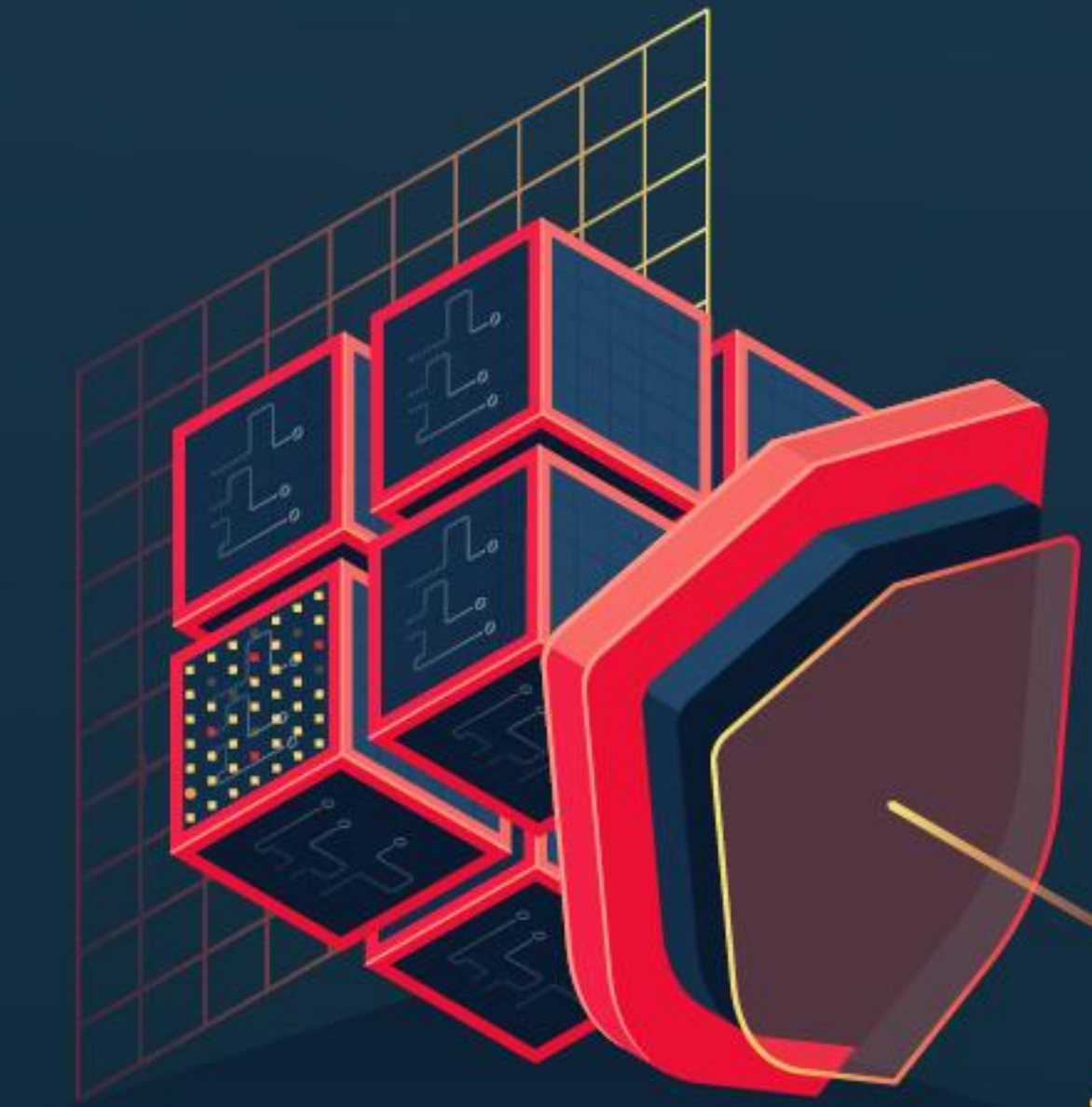


UNIVERSIDAD INTERNACIONAL SEK ECUADOR

FUNDAMENTOS DE CIBERSEGURIDAD

Ing. José Luis Medina

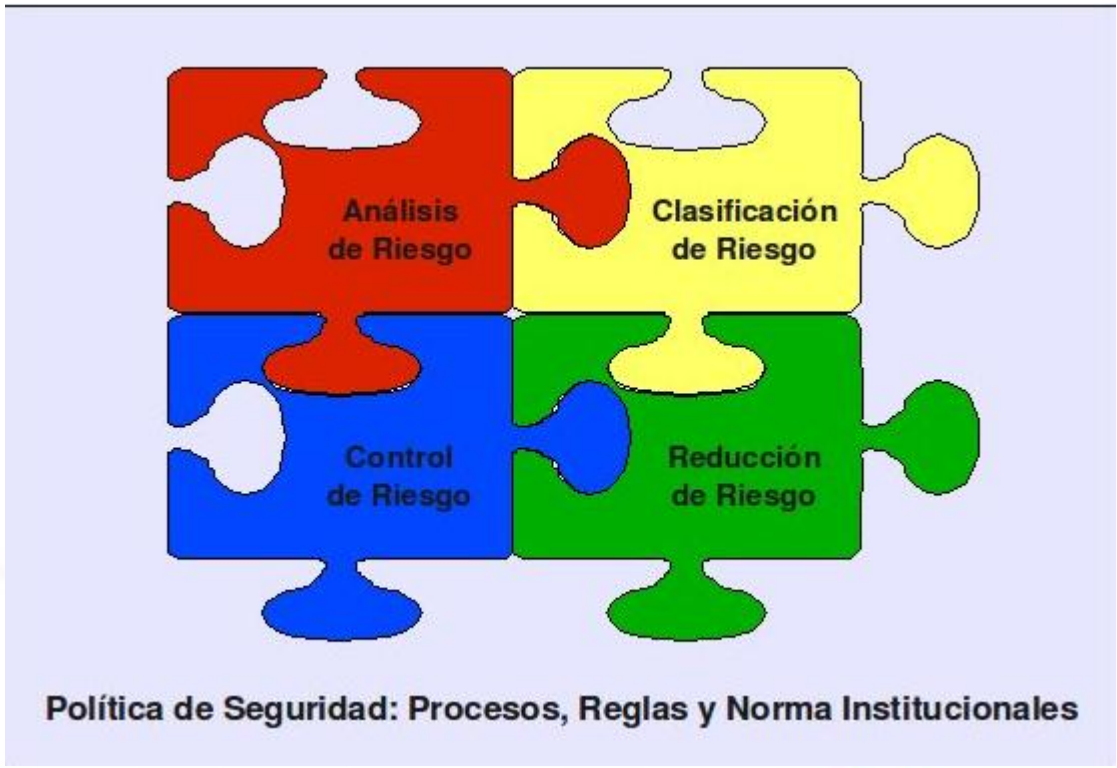
Dominios de la Ciberseguridad

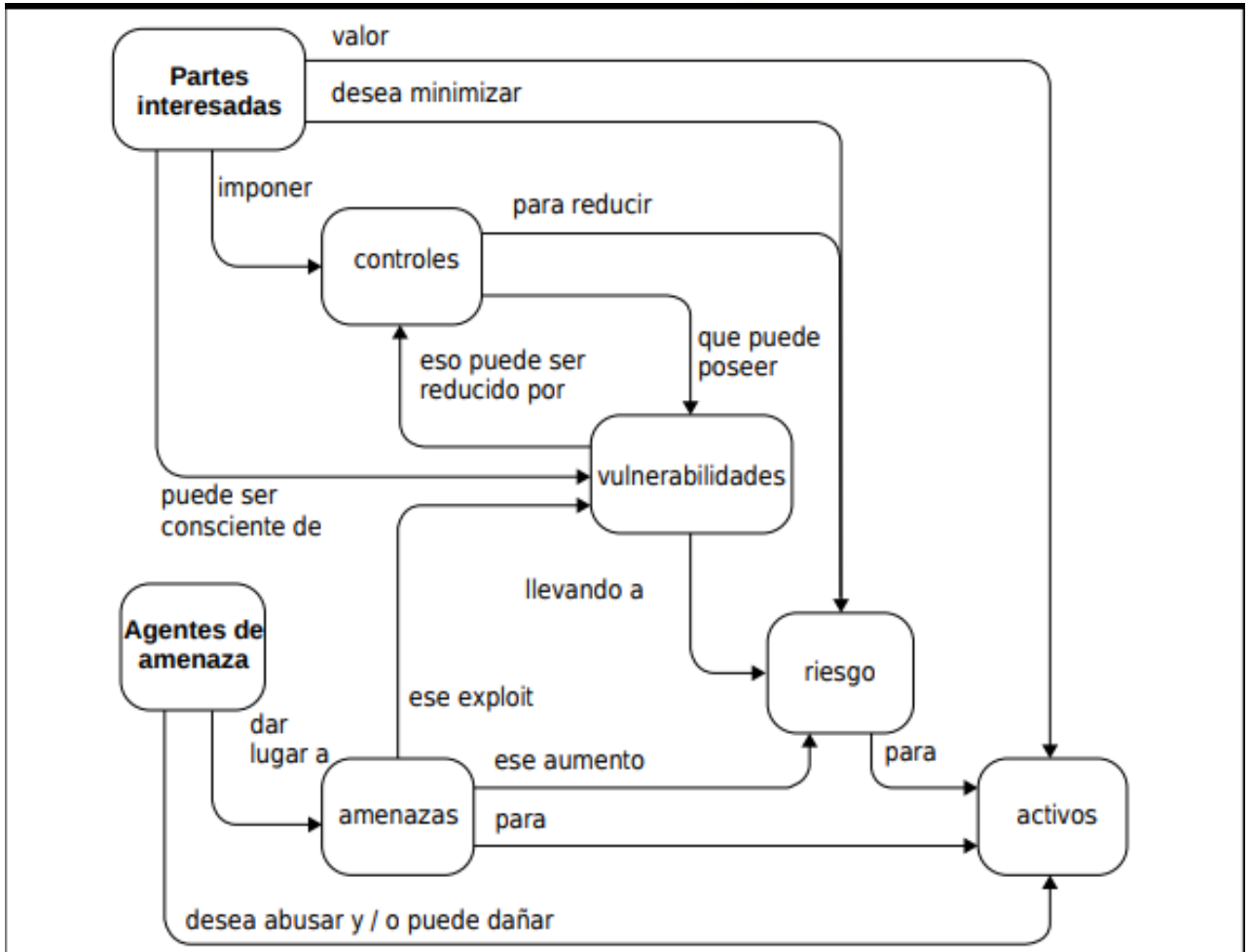
Ciberseguridad

- Si la ciberseguridad se define como la **protección** de los **activos de información**, abordando las **amenazas** a la información **procesada**, **almacenada** y **transportada** por sistemas de información interconectados
- Entonces, es importante conocer algunas definiciones:

- ***Activos***
- Un activo es todo lo que necesita ser protegido
- Esto puede ser:
  - Información digital, por ejemplo: registros médicos, registros bancarios, información académica en el caso de instituciones educativas
  - Sistemas de cómputo por ejemplo: Infraestructuras computacionales, infraestructuras críticas
  - Servicios de Tecnología por ejemplo: WebSites, Portales

- ***Riesgo***
- Un riesgo es la probabilidad de que una amenaza pueda aprovechar una vulnerabilidad para ser explotada y de esta manera causar daño o afectación a un servicio
- Es Pensar sobre la pérdida de información, por ejemplo: pérdida de data en un sistema de backups





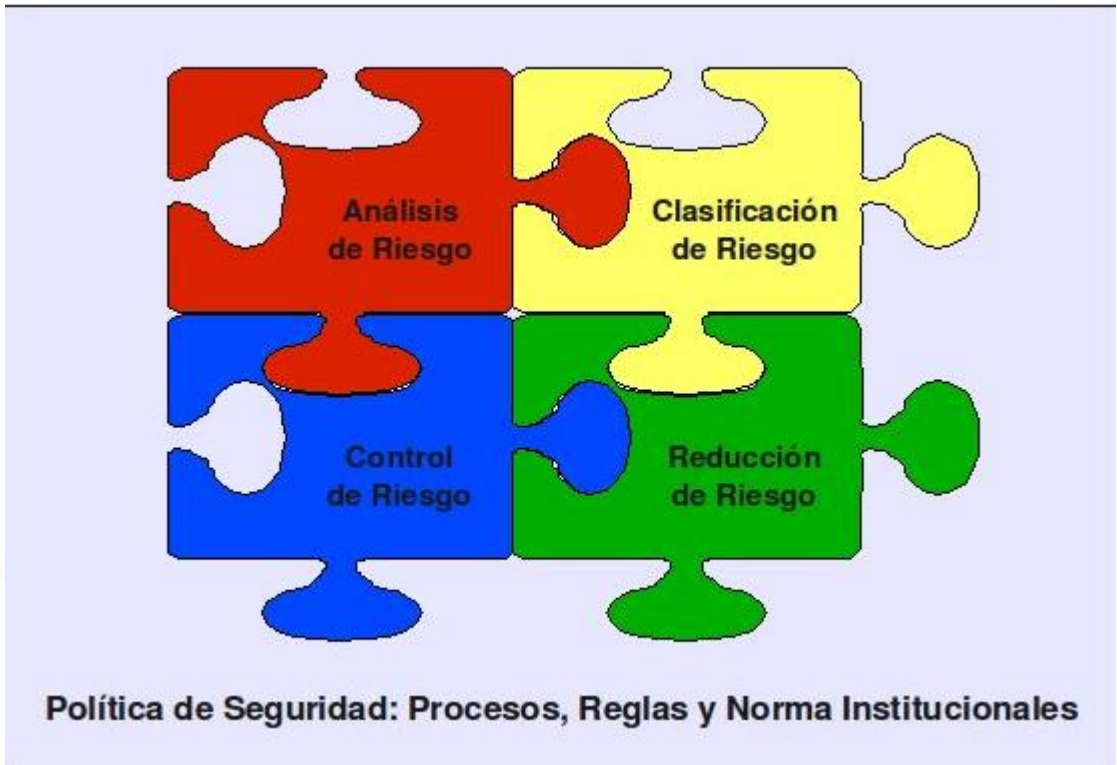
Fuente: Organización internacional de normalización, *ISO/IEC 27032:2012: Information technology—Security techniques—Guidelines for cybersecurity*, Suiza, 2012

- El riesgo se mitiga a través de controles o salvaguardas
- **Riesgo Inherente** es un nivel de riesgo que se considera sin haber tomado en cuenta las medidas a ejecutar
- **Riesgo residual** es un nivel de riesgo aún cuando se hayan ejecutado medidas para mitigar el mismo

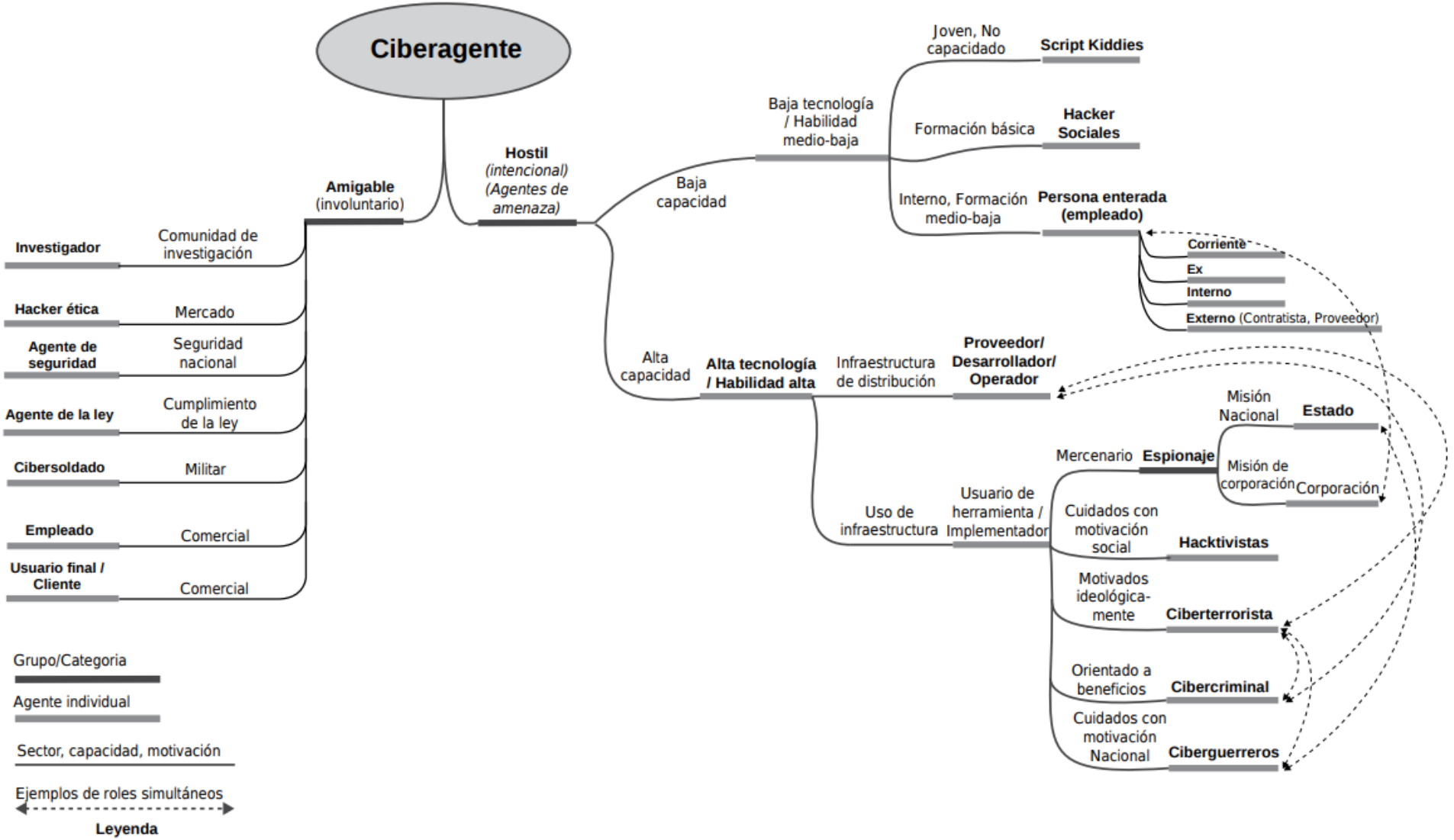
Gestión de Riesgos

- La gestión de riesgos es el **proceso** continuo de **identificación**, **evaluación** y **responder** al **riesgo**. Para administrar el riesgo, las organizaciones deben **comprender** la **probabilidad** de que ocurra un **evento** y el **impacto** resultante. Con esta información, las organizaciones pueden determinar el nivel aceptable de riesgo para la prestación de servicios y pueden expresar esto como su tolerancia al riesgo.
- Con una comprensión de la tolerancia al riesgo, las organizaciones pueden priorizar las actividades de ciberseguridad, permitiendo a las organizaciones tomar decisiones informadas sobre los gastos de esta

- La implementación de programas de **gestión de riesgos** ofrece a las organizaciones la capacidad de **cuantificar** y comunicar los ajustes a sus programas de seguridad cibernética. Las organizaciones pueden optar por manejar el riesgo de diferentes maneras, incluida la mitigación, la transferencia, la prevención o la aceptación del riesgo, según el impacto potencial en la prestación de los servicios críticos



- ***Amenaza***
- Una amenaza es cualquier violación potencial que puede causar daño o afectación a un activo
- Esto podría ser:
  - Alguien con ganas de hacer daño
  - Un servicio de tecnología inseguro
  - Errores humanos por desconocimiento de un sistema o servicio
- Un agente de amenaza es cualquier persona o cualquier cosa que puede causar daño o afectación a un activo
  - Hackers
  - Hacktivistas
  - Alguna entidad no maliciosa pero por error causa afectación a un servicio por ejemplo (un choque contra un poste de luz)



Fuente: Marinos, Louis, A. Belmonte, E. Rekleitis, "ENISA Threat Landscape 2015," ENISA, Enero 2016, Grecia

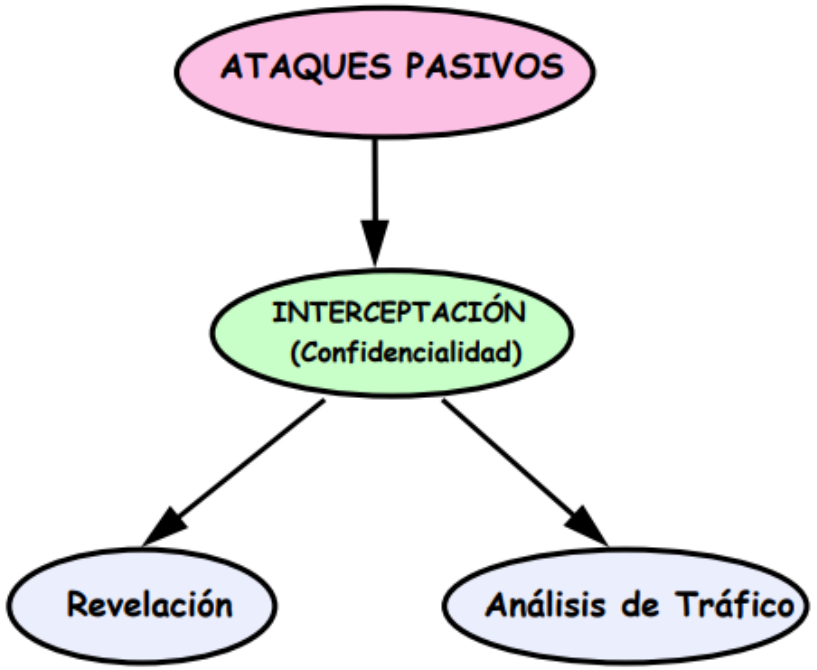
- *Vulnerabilidad*
- Una vulnerabilidad es una **falla** o **debilidad** en el diseño o implementación de un **activo** que un agente de amenaza o simplemente una amenaza podría ser aprovechada para causar afectación
- Estas pueden ser:
  - Incorrecta configuración en la implementación de un servicio
  - Puertos abiertos permitidos no necesarios
  - Implementación de un código pobre, vulnerable

```
you = new person();
me = new person();
if(you.profession() == programmer)
{
   while(1)
   {
      you.fix(myComputer);
      me.screw(myComputer);
   }
}
```

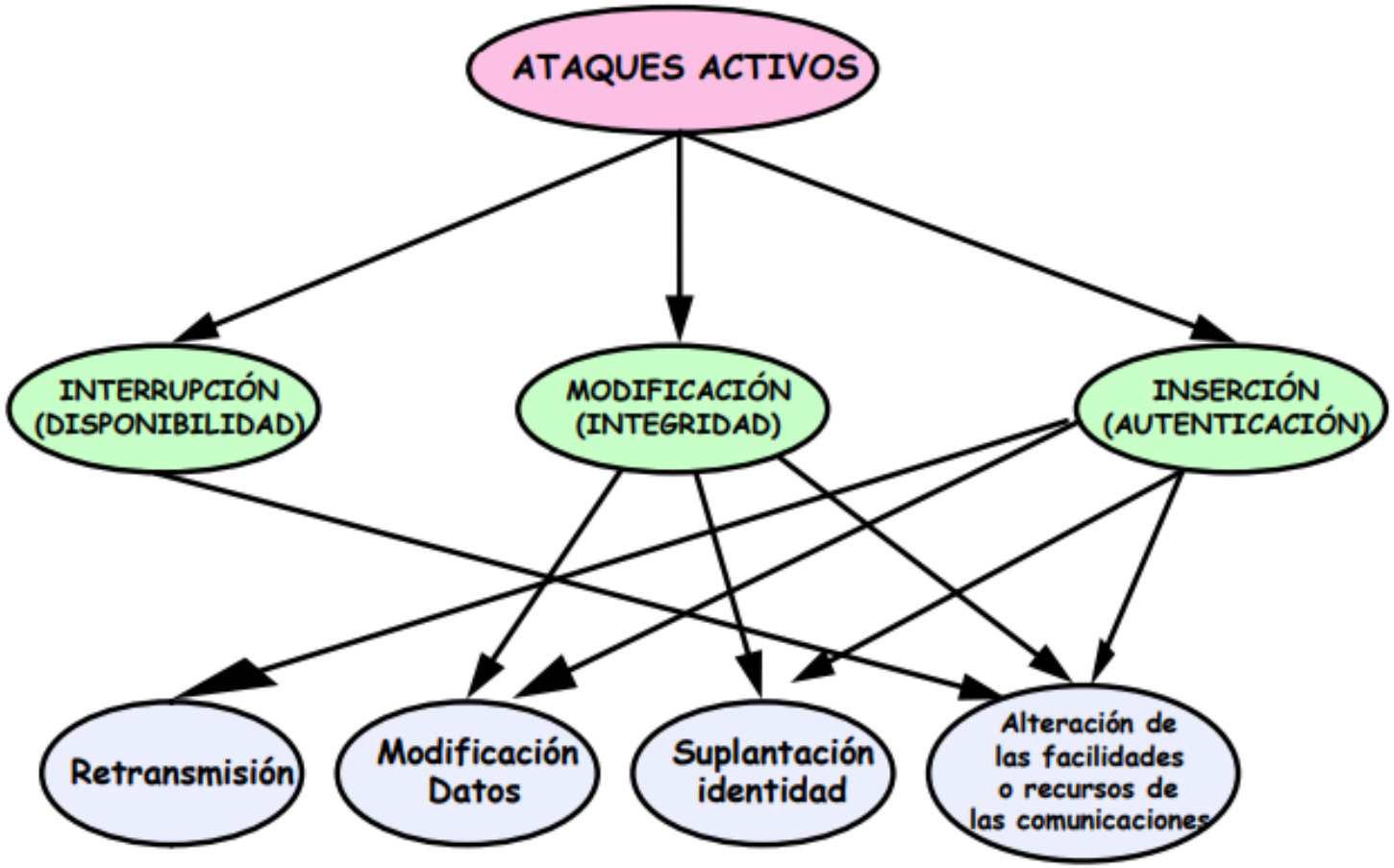
- ***Exploit***
- Un exploit es cualquier programa o conjunto de herramientas que son intencionalmente usadas para aprovechar cualquier vulnerabilidad de un activo
- Estas pueden ser:
  - Herramientas de Hacking, metasploit, ophcrack

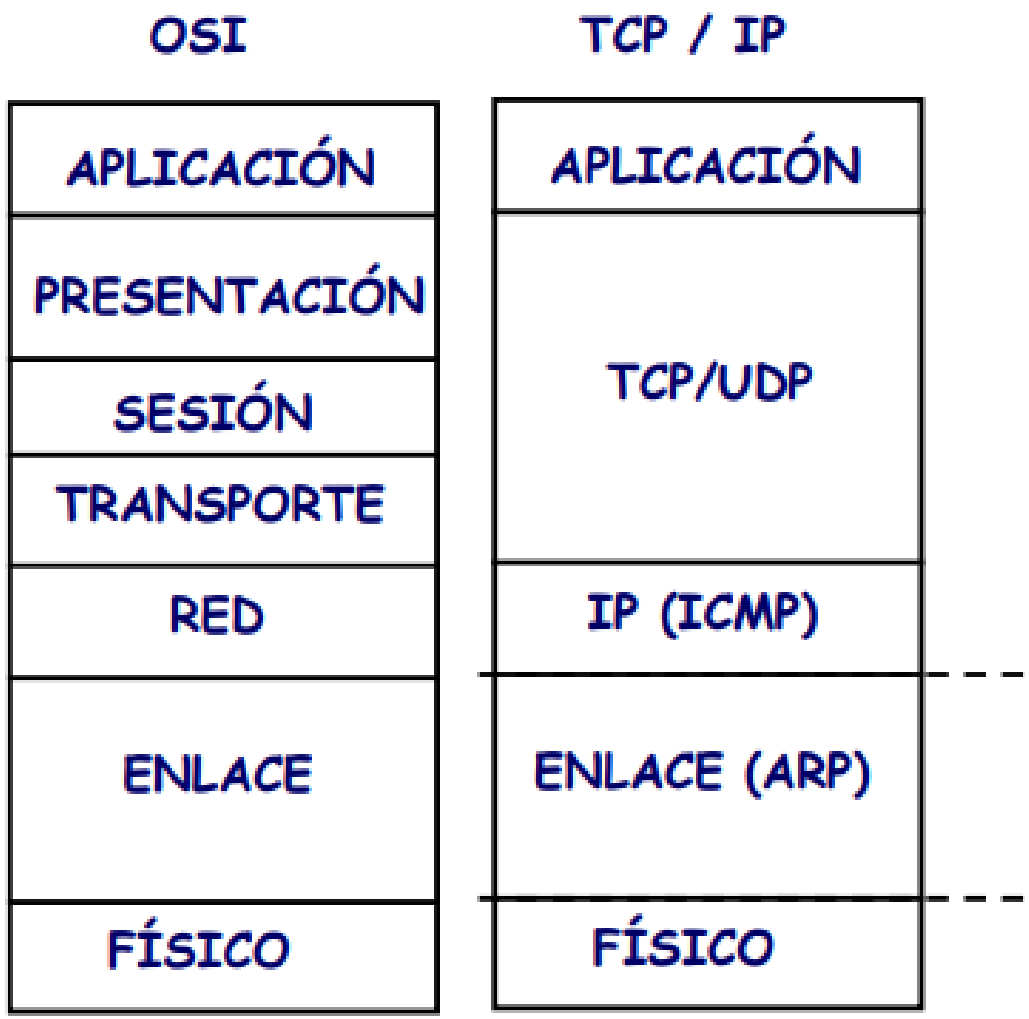
- ***Ataque***
- Un ataque es un evento intencional o no intencional que intenta causar daño o afectación a un servicio
- Un ataque es un asalto a un sistema de seguridad, desde una amenaza inteligente para evadir servcicios de seguridad y violar políticas de un sistema
- Un ataque también podría ser cualquier acción que comprometa la seguridad de información que pertenece a una organización
- ***Se puede decir que es la materialización de una amenaza***

- Dentro de los tipos de ataques:
- ***Pasivo.-*** el objetivo es obtener información que está siendo transmitida, son difíciles de detectar, sin embargo, es posible evitar este tipo de ataques
- Un ataque pasivo puede ser:
  - Liberación del contenido de mensajes
  - Análisis de tráfico



- Un ataque **Activo** es: implican alguna modificación del flujo de datos o la creación de flujos de datos falsos
- Se pueden subdividir en 3 categorias:
  - Interrupción de Servicios
  - Modificación de datos
  - Inserción (autenticación)





ATAQUES DHCP

ATAQUES TCP/SYN

PING FLOOD

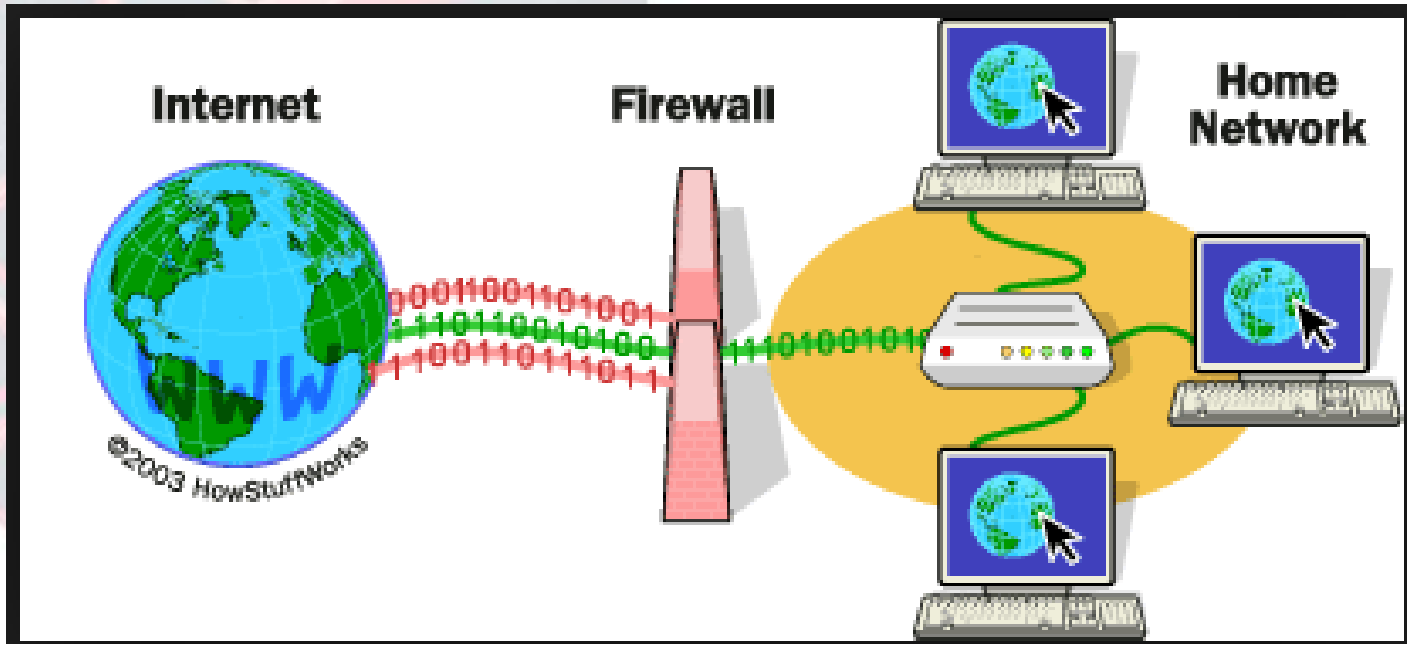
ARP SPOOFING

MAC FLOODING

MAC SPOOFING

Ataques en diferentes niveles

- ***Mitigación***
- Mitigación es cualquier herramienta o grupo de herramientas cuyo objetivo es reducir el riesgo de que se produzca un ataque
- Un firewall podría ser un ejemplo de una herramienta que reduce el riesgo de ataque a un activo al impedir intencionalmente la amenaza

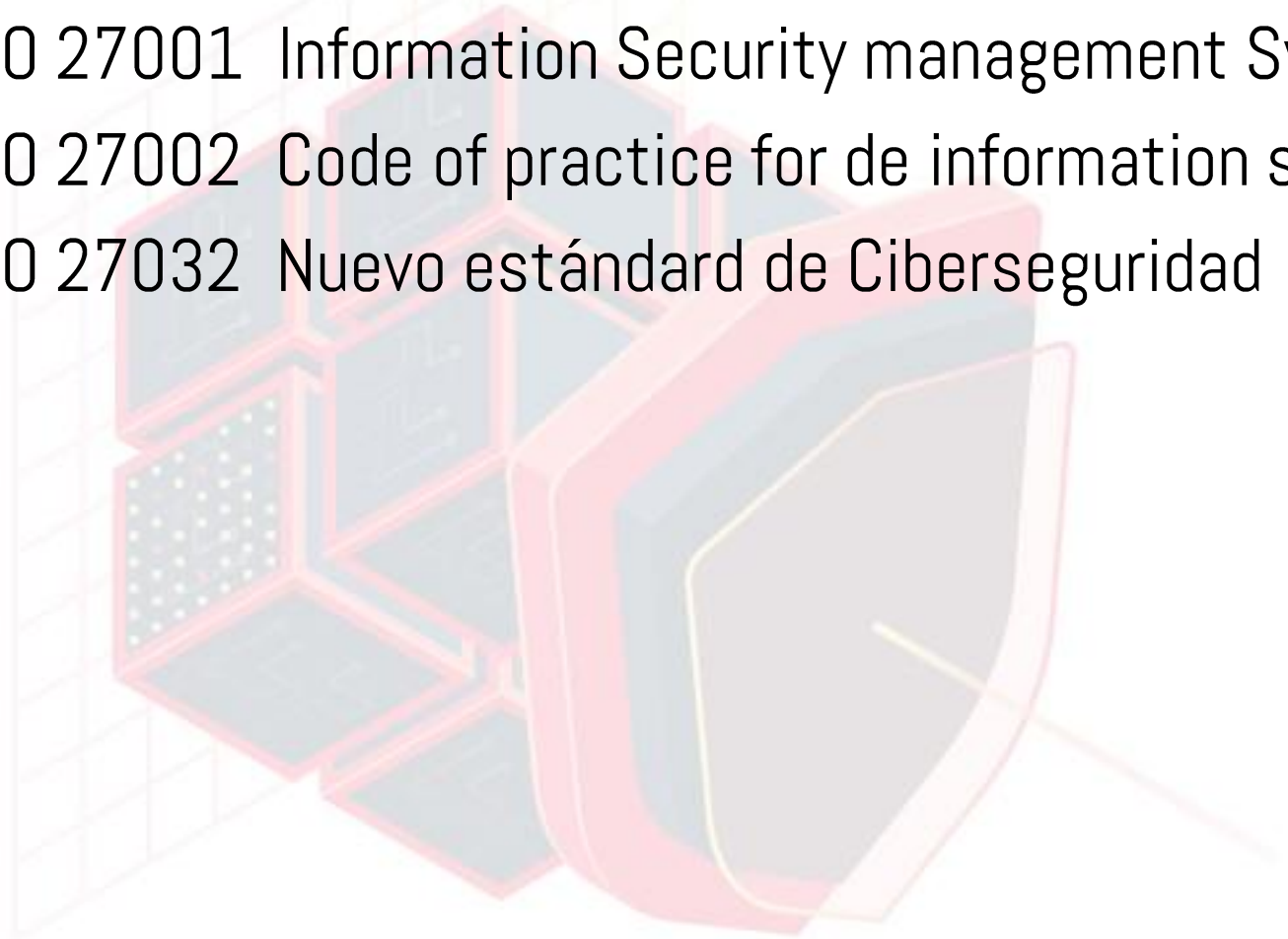


Security Frameworks

- Son entornos de trabajo estándares que pueden ser seguidos con el fin de mejorar y validar los procesos de seguridad
- Los Frameworks generalmente son probados y validados por mucha gente de la industria
- Un Framework puede ser pensado como una hoja de ruta a seguir ya que dependiendo del mismo puede indicar el punto en el que se encuentra y que falta por hacer

- ***NIST Framework (The National Institute for Standard s and Technology)***
- Mantiene publicaciones especiales que han sido estandars por muchos años
- Son muy fáciles de seguir y tiene diferentes niveles dependiendo el tipo de cumplimiento que se requiera
    - NIST Cybersecurity Framework
        - Aimed at protecting critical infrastructure
        - One of the best frameworks to follow and easy to adopt
    - NIST SP 800-53
        - Security and Privacy Controls for Federal Information Systems and Organizations
        - Broken down into security controls
        - Comprehensive
    - NIST SP 800-171
        - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
        - Much easier to follow than 800-53

- ***ISO 27001 – 27002 (The International Organization for Standardization)***
- Provee un entorno de trabajo donde se especifica los controles de seguridad
- ISO 27001 Information Security management Systems
- ISO 27002 Code of practice for de information security controls
- ISO 27032 Nuevo estándard de Ciberseguridad



- ***CIS Framework (Center for Information Security)***
- Este framework propone el uso de los 20 controles críticos a seguir como gestión de seguridad informática
- Diseñado para cubrir diferentes sectores de la industria
- Es el menos conocido en su adopción, sin embargo, hoy en día ya se está realizando la difusión de este framework

Bibliografía

- ISACA, Fundamentos de Ciberseguridad, Segunda Edición, 2017
- ESTRADA Corletti Alejendro, Ciberseguridad una estrategía informático / militar, Nov. 2017