Conceptos de Ciberseguridad y Teoría

# Introducción

En el contexto actual, la ciberseguridad se ha convertido en una disciplina crítica debido a la creciente digitalización de sistemas y procesos. El objetivo de esta área es proteger los sistemas de información frente a amenazas y vulnerabilidades que pueden comprometer su confidencialidad, integridad y disponibilidad.

## Tipos de Ataques

Los ataques en ciberseguridad se pueden clasificar principalmente en dos tipos: pasivos y activos.  
- Los ataques pasivos buscan obtener información del sistema sin modificar su funcionamiento, como es el caso de la intercepción de datos.  
- Los ataques activos, por otro lado, implican la alteración directa de los sistemas para vulnerar su seguridad, como la inserción de malware.

## Superficies de Vulnerabilidad y Vectores de Ataque

El concepto de superficies de vulnerabilidad hace referencia a las áreas o puntos débiles de un sistema que pueden ser explotados por atacantes. Los vectores de ataque son los medios o caminos que utilizan los atacantes para acceder a estas vulnerabilidades.

# Criptografía y Criptoanálisis

La criptografía es la ciencia encargada de proteger la información mediante su cifrado, transformándola en un formato ilegible para usuarios no autorizados. Existen dos tipos principales de cifrado:  
- Cifrado simétrico: utiliza la misma clave para cifrar y descifrar la información.  
- Cifrado asimétrico: utiliza una clave pública para cifrar y una clave privada para descifrar.  
  
El criptoanálisis, por otro lado, es la disciplina que se encarga de encontrar vulnerabilidades en los métodos criptográficos, con el objetivo de descifrar la información sin conocer las claves.

# Generación de Claves Aleatorias

Un aspecto fundamental en la criptografía es la generación de claves seguras. Las claves deben ser lo más impredecibles posibles para evitar su deducción por parte de atacantes. Los generadores de números aleatorios basados en hardware son preferibles para crear claves verdaderamente aleatorias, mientras que los generadores de software producen claves pseudoaleatorias, menos seguras.