# Guía Examen Final

Esta guía, no incluye todo lo que puede venir en el examen, y no todo lo que incluye estará en el examen.
Es solo una referencia de los temas, y de las posibles preguntas y ejercicios que estarán en el examen Final

## TEORÍA:

Da la definición de:

Disponibilidad
Autorización
Autentificación
Riesgo
Vulnerabilidad
IPv4 e IPv6
Cifrado
Certificados
Firmas digital
Encriptación
Cifrado
Huella
Hash
Llaves Simetricas y Asimetricas
Llaves Públicas y Privadas
MD5
SHA-1,SHA-256, SHA-512
CRC32
Base64
DRP
DLP
Base58
Cadena de Bloques

¿Qué son las curvas de Fallas?
¿Por qué fallan los componentes mecánicos?
¿Por qué fallan los componentes electrónicos?
¿Qué se puede hacer para mejorar la disponibilidad?

¿Por qué se debe de probar el software y menciona 4 pruebas importantes?

Menciona 3 mecanismos para proteger una base de datos

¿Para qué sirven las pruebas de penetración de Aplicaciones?
¿Qué es un análisis de vulnerabilidades?

¿Que es un CVE y menciona 3 ejemplos explicados?
¿Que es un CVSS y explicarlo con un ejemplo?
¿Que es Mitre ATT&CK?

Menciona 4 tipos de ataques a las seguridad
¿Para que se utilizan diccionarios en los ataques?
¿En qué consiste el Diseño, Planeamiento, Implantación y Desarrollo De Una Ciberdefensa?
¿Que es un análisis de vulnerabilidades y como se solucionan las vulnerabilidades encontradas?

¿Para qué se utiliza Wazuh?
¿Qué información proporciona Wazuh?
¿Que son los Controles CIS?
¿Cuales son las funciones especificas de los controles CIS?
¿Qúe activos protegen los controles CIS?
Explica con tus palabras la utilidad del CIS

¿Qué es el NIST?
¿Qué es el marco de ciberseguridad del NIST?
Explica con tus palabras como ayuda el marco de Ciberseguridad del Nist

¿Qué es OWASP?
¿Cuáles son las principales causas de inseguridad según el OWASP?
¿Cómo se usa la metodología OWASP?

Menciona cual es la estrategia 3-2-1 de los Respaldos
¿Por qué son importantes los respaldos para la ciberseguridad?
¿Qué tipos de respaldos existen?

¿Qué son las políticas y los controles de la prevención de pérdida de datos (DLP)?
¿Por qué es importante el DLP para la ciberseguridad?
¿Por qué es importante conocer las iniciativas y reglamentación de seguridad de cada país para considerar un DLP?

¿Para qué se utiliza el Blockchain?
Menciona 3 usos del blockchain.
Explica el proceso para agregar un nuevo bloque a una cadena de Blockchain
Explica el proceso validar una cadena de Blockchain

## Práctica:

Escribe una aplicación que genere un par de llaves pública y privada. De cada llave, codificalas usando Base64 y guardalas en 2 archivos, publica.txt y privada.txt

Escribe una aplicación que te pregunte un texto, y te genere una clave simétrica para AES. Y esa clave se almacene en un archivo llamado Clave.txt

Escribe una aplicación que pongas que tipo de redundancia tienes, el valor de disponibilidad de cada sistema y te calcule la disponibilidad total (En % y en días, horas y minutos) y la NO disponibilidad (En % y en días, horas y minutos)

Escribe una aplicación que te permita:

a) Encriptar con tu llave privada
b) Encriptar con una llave pública
c) Encriptar con tu llave privada primero y después con una llave pública

Escribe una aplicación que te permita:

d) Desencriptar con tu llave privada
e) Desencriptar con una llave pública
f) Desencriptar con tu llave privada primero y después con una llave pública

Escribe una aplicación que por cada movimiento de dinero, te genera 2 bloques:
El primero, de donde se toma el dinero y cual es el saldo inicial y final de esa cuenta.
El segundo bloque, a donde se deposita el dinero, y cual es el saldo inicial y final de esa cuenta.
Cada bloque además de los campos anteriores, incluya el correo del que realizó el movimiento, la fecha y hora y el lugar de donde se originó la transacción (Codificados en Base58)
Estos 2 bloques se deben agregar a una cadena ya existente.
Validar que siempre el blockchain tenga un número impar de bloques (El génesis y 2*n)

Escribe un esquema de validación por cada inciso de acceso a una base de datos de Derby

a) Qué la contraseña sea el usuario, pero escrito con mayúsculas, ejem: Lorenzo, LORENZO
b) Qué la contraseña sea el usuario, pero escrito al revés, ejem: Lorenzo, ozneroL
c) Qué la contraseña sea el MD5 del usuario Lorenzo, a96e8f71351fbe70573b70189c0dd2bb
d) Qué la contraseña sea el SHA256 del usuario Lorenzo, 114b25448d0a392be6f3f78d7f0f1f46fcb301244088ad2a229b685604606ff6
e) Qué la contraseña sea igual a el Base64, del usuario+espacio+fecha+espacio+basedatos Ejem: Si me voy a conectar a la bd: Examen con el usuario Lorenzo el 1/mayo/2023 sería: Lorenzo, TG9yZW56byAxL21heW8vMjAyMyBFeGFtZW4=

Escribe una aplicación, que digas:

a) Tamaño actual e incremento diario en %
b) Qué tipos de respaldos quieres, cada cuantos días y te genere un plan detallado para respaldar y para recuperar la información.