



**Anáhuac**  
Mayab

# **SEGURIDAD INFORMÁTICA Y ANÁLISIS FORENSE**

## **Assignment 3:**

Problemas

## **Docente:**

Guirao Aguilera Miguel Antonio

## **Alumno:**

Anibal Simeón Falcon Castro

## **Fecha de entrega:**

09/06/2025

## **Problema 1: Alice's Online Chess (AOC)**

### **¿Dónde (y por qué) es importante la confidencialidad para AOC y sus clientes?**

En el almacenamiento y transmisión de datos personales y de pago de los jugadores, así como en el canal de juego (movimientos, chat). Sin confidencialidad, un atacante podría robar credenciales, suplantar usuarios o conocer estrategias privadas.

### **¿Por qué es necesaria la integridad?**

Para asegurar que los movimientos y los resultados de las partidas no sean alterados en tránsito o en la base de datos. Sin integridad, un atacante podría falsear partidas, manipular rankings o hacer trampas.

### **¿Por qué es importante la disponibilidad?**

Porque los suscriptores pagan por acceso continuo a la plataforma. Un fallo prolongado o un ataque DDoS interrumpe el servicio, frustra a los usuarios y daña la reputación de AOC.

### **¿Dónde debería usarse criptografía en AOC?**

- En tránsito: TLS/HTTPS (y WebSocket cifrado) para login, envío de movimientos y chat.
- En reposo: Cifrado o hashing (con salt) de contraseñas y de los datos sensibles (historial de pagos, estadísticas).

### **¿Dónde debería usarse control de acceso en AOC?**

- Autenticación/Autorización: Validar suscripción activa antes de permitir login.
- Roles y permisos: Diferenciar jugador, moderador y administrador.
- Gestión de sesión: Tokens con expiración y posibilidad de revocación.

## **Problema 2: Métodos de Autenticación**

**Da un ejemplo de autenticación basada en “algo que eres” (biométrico).**

Reconocimiento de huella dactilar, escaneo de iris o reconocimiento facial.

**Da un ejemplo de autenticación basada en “algo que tienes” (posesión).**

Uso de un token hardware (p. ej. YubiKey) o tarjeta inteligente (smart-card) para acceder a la red corporativa.

**Da un ejemplo cotidiano de autenticación de dos factores e indica cuáles de los tres métodos usa.**

Iniciar sesión en Brightspace:

1. Algo que tienes: se envía un código a tu teléfono.
2. Algo que sabes: introduces el código recibido.
3. Algo que eres: proporcionas tu huella digital.