# **Avance del Proyecto – Ciberseguridad**

Profesor: Marcelo Pereira

# **Nombre del Grupo: Tecnicos y Asociados**

**Integrantes:**

**Federico Agustín Mosegui Suárez**

**Alex Renato González Benquet**

**Franco Emanuel Fagundez Ancel**

**Lucas Alejandro Vargas García**

**Sergio Daniel López Acosta**

**Logo del Grupo:**

****

**Objetivo:** Presentar el primer avance del proyecto en la asignatura Ciberseguridad, detallando cómo será protegido el sistema de tickets web, las amenazas identificadas, las medidas de prevención y la forma de actuar ante posibles incidentes.

## **1. Plataforma del sistema**

1. ¿Sobre qué plataforma/entorno funcionará el sistema de tickets (Windows, Linux, nube, etc.)?
2. ¿Qué lenguaje de programación o framework están usando (ej. PHP, JavaScript, etc.)?
3. ¿Qué base de datos utilizarán (MySQL, PostgreSQL, SQL Server, etc.)?
4. El sistema funciona en la plataforma Ubuntu Server 24.04
5. El lenguaje de programación utilizado en el proyecto es php 8.4, JavaScript y SQL como no lenguaje utilizamos CSS y HTML
6. Utilizamos la base de datos MySQL

## **2. Protección del sistema**

1. ¿Qué medidas aplicarán para proteger las contraseñas de los usuarios (hash, políticas de complejidad)?
2. ¿Cómo gestionarán los roles y permisos (ejemplo: admin, técnico, cliente)?
3. ¿Cómo evitarán accesos no autorizados al sistema?
4. ¿El sistema usará HTTPS? ¿Cómo lo implementarán?
5. Para proteger las contraseñas de los usuarios usaremos hash para automáticamente codificadar
6. Cada rol va a tener diferentes permisos los roles cliente y técnico no podrán hacer mucho en el sistema los Clientes pueden crear y editar tickets y productos, borrar los tickets en el caso de que ningún técnico este asociado a él todavía, podrá comunicarse con el técnico. El Técnico puede seleccionar con que tickets trabajar, actualizar su estado y comunicarse con los clientes. El admin puede ver el historial de acciones de toda la app y moderar técnicos y clientes
7. Protegiendo la base de datos de ataques de inyección de SQL

## **3. Seguridad en la infraestructura**

1. ¿Qué puertos y servicios necesita su sistema para funcionar?
2. ¿Cómo protegerán la base de datos de accesos externos indebidos?
3. Nuestro aplicación usa los puertos 8080, 433, 3306 y 22
4. Protegemos con un acceso restringido por farewell por el puerto 3306 para que la base de datos solo acepte conexiones desde la ip del servidor, no expondremos la base de datos a internet va a estar en una red privada sin acceso publico

## **4. Prevención de vulnerabilidades**

1. ¿Qué vulnerabilidades comunes pueden afectar a su sistema?
2. ¿Qué medidas tomarán para prevenirlas?
3. Ataque DDoS, inyección SQL, inserción de scripts maliciosos
4. 1-aumentar la capacidad del servidor  
   2-implementar tokens unicos en formularios para evitar ataques CSRF  
   3-gestion segura de sesiones  
   4-establecer tiempo de caducidad

## **5. Políticas de seguridad**

1. ¿Qué plan de copias de seguridad (backups) implementarán?
2. Implementaremos una copia física de los datos del servidor seguro que solo nosotros tendremos acceso