Documentación del Proyecto: CyberSec Manager

1. Descripción General

El objetivo es desarrollar una plataforma web para una empresa de Ciberseguridad que permita la comercialización y gestión de servicios profesionales.

La aplicación servirá como:

1. **Escaparate Comercial (Pública):** Para captar clientes interesados en Formación, Consultoría (ISO27001, ENS, NIS2), Auditorías y servicios SOC.
2. **Portal de Cliente (Privada - Externa):** Donde los clientes acceden a sus documentos (políticas), ven el calendario de auditorías y reportan incidentes.
3. **Gestión de Operaciones (Privada - Interna):** Donde consultores, auditores y analistas SOC gestionan sus proyectos y tareas.

2. Requisitos Funcionales

Parte Pública (Frontend - Visitantes y Clientes)

- **Catálogo de Servicios:** Páginas informativas divididas en tres ramas:
    - *Gobernanza:* Implantación de normativas (ISO27001, ENS, NIS2).
    - *Defensa:* Servicios SOC y respuesta a incidentes.
    - *Auditoría:* Pentesting y auditorías de cumplimiento.
- **Solicitud de Presupuesto:** Formularios específicos según el servicio (ej: para formación, preguntar número de empleados).
- **Área de Cliente (Intranet):**
    - **Repositorio Documental:** Descarga de políticas y procedimientos generados por los consultores.
    - **Calendario de Proyectos:** Visualización de fechas de auditoría agendadas.
    - **Buzón SOC:** Formulario para reportar una incidencia de seguridad urgente.

Parte Privada (Backend - Staff)

- **Gestión de Proyectos:** Crear expedientes para clientes (ej: "Implantación ENS para Empresa X").

- **Gestión Documental:** Subida de archivos PDF/Docx (políticas, informes) asociados a un cliente específico.
- **Calendario de Auditorías:** Sistema para que los Auditores marquen fechas y los Consultores/Clientes las vean.
- **Ticketing SOC:** Listado de incidentes reportados, asignación a analistas y cambio de estado (Abierto -> En Análisis -> Resuelto).
- **Gestión de Usuarios (RBAC):** Asignación de permisos.

3. Roles de Usuario (RBAC)

El sistema contará con **5 roles** bien diferenciados (+ Invitado), cumpliendo el requisito académico:

1. **Invitado (Guest):**
    - Ve el catálogo público y solicita presupuestos.
2. **Cliente (User):**
    - Accede a su área privada.
    - Descarga sus políticas/informes.
    - Ve fechas de auditoría.
    - Abre tickets al SOC.
3. **Consultor (Staff Nivel 1):**
    - Gestiona proyectos de "Implantación de Normativa".
    - Sube documentación para el cliente.
    - Consulta el calendario para coordinarse con auditores.
4. **Auditor (Staff Nivel 2):**
    - Gestiona proyectos de "Auditoría".
    - Tiene permisos de escritura en el **Calendario** para fijar las fechas de auditoría.
    - Sube informes de resultados.
5. **Analista SOC (Staff Técnico):**
    - Acceso exclusivo al módulo de **Incidentes/Tickets**.
    - Recibe alertas y cierra incidencias de seguridad.
6. **Super-Administrador:**

    - Crea usuarios empleados, gestiona el catálogo de servicios y asigna roles.

4. Análisis de Datos (Estructura Base)

Aparte de la tabla user, necesitaremos estas entidades clave para que funcione:

- **Servicios:** Catálogo base (ej: "Consultoría ISO27001", "Pentesting Web").
- **Proyectos:** La contratación real. Relaciona Cliente + Servicio.
    - *Campos:* fecha_inicio, estado (Planificación, En curso, Finalizado).
- **Documentos:** Archivos entregables.
    - *Campos:* ruta_archivo, tipo (Política, Procedimiento, Informe), proyecto_id.
- **Eventos_Calendario:**
    - *Campos:* fecha, tipo (Auditoría Interna, Auditoría Certificación), proyecto_id, auditor_id.
- **Incidencias (Tickets SOC):**
    - *Campos:* titulo, severidad (Alta/Media/Baja), estado, cliente_id, analista_id.

5. Notas Técnicas para el Desarrollo (Yii2)

- **Calendario:** Se recomienda usar la extensión yii2-fullcalendar para mostrar las fechas de auditoría visualmente.
- **Subida de Archivos:** Utilizar la clase UploadedFile de Yii2 para que los consultores suban los PDFs de las normativas.
- **Seguridad:** Dado que es una web de ciberseguridad, intentad implementar buenas prácticas (ej: contraseñas fuertes obligatorias en el modelo User).