Actividad 5: Desarrollo de un Protocolo de Seguridad en el Desarrollo

1. **Introducción**
   EduTechIA busca transformar la educación mediante una plataforma digital que personalice los cursos según las características de cada usuario. Para garantizar la seguridad del MVP, este protocolo establecerá medidas y mejorará las prácticas en cada fase del desarrollo, minimizando la vulnerabilidad y protegiendo los datos

2. **Fase de Planificación y Diseño**
   a. Análisis de Riesgos:
      - Identificación de Activos: Identificar los activos más vulnerables del sistema (datos de usuarios, algoritmos de IA, infraestructura, etc.).
      - Evaluación de Amenazas: Realizar un análisis de amenazas para identificar posibles ataques
      - Clasificación de Riesgos: Priorizar los riesgos según su impacto y probabilidad.

   b. Diseño Seguro
      - Diseñar el sistema para que cada componente tenga solo los permisos necesarios.
      - Seguridad por Defecto: Configurar todas las opciones de seguridad por defecto (ej: HTTPS, autenticación obligatoria).
      - Arquitectura de Confianza Cero (Zero Trust): Implementar un modelo donde ningún usuario o sistema sea confiable por defecto.
      - Protección de Datos Sensibles: Diseñar mecanismos para encriptar datos sensibles en reposo y en tránsito.

3. **Fase de Desarrollo**
   a. Prácticas de Codificación Segura
      - Uso de Librerías Seguras: Utilizar librerías y frameworks actualizados y con buena reputación en seguridad.
      - Manejo de Errores: Evitar revelar información sensible en mensajes de error.
   b. Revisiones de Código y Pruebas
      - Realizar revisiones de código para identificar vulnerabilidades y malas prácticas.
      - Realizar pruebas de penetración en etapas tempranas para identificar vulnerabilidades.

4. **Fase de Implementación**
   a. Configuración Segura del Entorno
      - Se asegurará la configuración de servidores y servicios (ej: deshabilitar servicios innecesarios, configurar firewalls)
      - Monitoreo y Logging: Implementar sistemas de monitoreo y logging para detectar actividades que sean sospechosas.
   b. Despliegue Seguro
      - CI/CD Seguro: Asegurar que el pipeline de CI/CD esté configurado de forma segura para impedir que se inserte código malicioso.

5. **Fase de Operación y Mantenimiento**
    a. Monitoreo Continuo
        - Deteccion y prevencion de intrusos (IDS, IPS)
        - Implementar un sistema de respuestas a incidentes, por si en caso de brecha actuar con rapidez.
    b. Actualizaciones y parches
        - Monitorear y aplicar parches de seguridad de una forma continua.
        - Mantener las dependencias del sistema siempre actualizadas.
6. **Conclusión**

    El protocolo descrito en los puntos anteriores aporta un marco robusto para garantizar un desarrollo seguro de la MVP de EduTechIA, con este protocolo de seguridad, la empresa puede reducir al mínimo la vulnerabilidad, proteger los datos de los usuarios y construir una plataforma segura y confiable.