Actividad 5: Protocolo de Seguridad en el Desarrollo

El presente protocolo establece las mejores prácticas y medidas para garantizar un desarrollo seguro del MVP de EduTech IA, minimizando las vulnerabilidades en cada fase del ciclo de desarrollo. Se fundamenta en la incorporación de la seguridad desde el diseño, la aplicación de estándares reconocidos y la implementación de controles rigurosos en todas las etapas del proceso.

Requisitos y Evaluación de Riesgos

Se incorporan condiciones específicas de seguridad desde la etapa inicial de recolección de requisitos, definiendo claramente las necesidades de protección de la información. Para identificar posibles puntos vulnerables, se realiza una evaluación de riesgos utilizando metodologías como OWASP Threat Modeling. Este análisis permite detectar de forma anticipada los riesgos potenciales y definir medidas preventivas que aseguren la integridad y confidencialidad de los datos.

Medidas y Buenas Prácticas en el Ciclo de Desarrollo

La seguridad se integra de manera transversal en el desarrollo a través de los siguientes aspectos:

Seguridad desde el Diseño y Defensa en Profundidad:

Se implementa la seguridad en la fase de diseño, estableciendo mecanismos de autenticación, autorización, cifrado y manejo seguro de errores. La segregación de ambientes (desarrollo, pruebas y producción) ayuda a limitar la exposición de datos sensibles y a aislar incidentes potenciales.

Prácticas de Codificación Segura:

Se aplican las directrices de OWASP y patrones de diseño que evitan vulnerabilidades comunes. Se implementan medidas rigurosas para validar y sanitizar todas las entradas del usuario, asegurando que el código se desarrolle siguiendo las mejores prácticas en materia de seguridad.

Gestión de Dependencias y Revisión de Código:

Se mantiene actualizadas las librerías y frameworks utilizados, y se emplean herramientas para analizar vulnerabilidades en las dependencias. Además, se realizan revisiones de código y análisis estáticos de forma periódica para identificar y corregir posibles fallos de seguridad.

Pruebas de Seguridad Integradas:

Se llevan a cabo pruebas de penetración y escaneos automatizados, integrados en el proceso de integración y entrega continua, para detectar vulnerabilidades en etapas tempranas. La combinación de análisis estático y pruebas dinámicas contribuye a la robustez del sistema.

Configuración Segura y Supervisión:

Se aplican configuraciones seguras en servidores, contenedores y servicios, siguiendo el principio de “privilegio mínimo” y adoptando modelos de “confianza cero”. En la contenerización, se utilizan imágenes Docker simples y se realizan escaneos periódicos. Asimismo, se implementan controles sólidos de acceso, autenticación multifactorial y sistemas de monitoreo que permiten detectar y responder rápidamente a incidentes de seguridad.

Mantenimiento, Auditorías y Plan de Respuesta a Incidentes:

Se realizan actualizaciones y se aplican parches de seguridad de forma regular. Se llevan a cabo auditorías internas y externas para evaluar la efectividad de las medidas implementadas. Finalmente, se establece un plan de respuesta a incidentes que permite identificar, contener y resolver cualquier eventualidad de forma coordinada y eficaz.

Este protocolo, integrado en cada fase del ciclo de desarrollo del MVP, garantiza que el sistema se construya y opere bajo altos estándares de seguridad, minimizando riesgos y asegurando la protección integral de la información de los usuarios.