

## PLAN DE RIESGOS

Área de riesgo	Descripción de riesgo.	Probabilidad.	Impacto.	Estrategia de mitigación	Plan de contingencia	Responsable
<b>Errores de Software</b>	Errores en el código que afecten la funcionalidad de la aplicación	Media	Alto	Mantener un ciclo de pruebas continuas y actualizaciones periódicas.	Corregir los errores, realizar pruebas de emergencia y comunicar a los usuarios sobre las actualizaciones.	Desarrolladores
<b>Ataques Cibernéticos</b>	Vulnerabilidades que permitan acceso no autorizado a los datos de los usuarios	Alta	Alto	Implementar encriptación, autenticación de dos factores y monitoreo de seguridad continuo.	Activar el protocolo de respuesta a incidentes, cerrar acceso no autorizado, notificar a usuarios y analizar causas.	Equipo de seguridad informática
<b>Problemas de Compatibilidad</b>	La aplicación no es compatible con algunos dispositivos o sistemas operativos	Media	Medio	Diseñar y probar la aplicación para diferentes sistemas operativos y dispositivos..	Desarrollar una versión de emergencia para dispositivos incompatibles o proporcionar soporte técnico específico.	Desarrolladores
<b>Perdida de Datos</b>	Pérdida accidental de información de usuarios o progresos académicos	Baja	Alto	Realizar respaldos automáticos periódicos, contar con un sistema de recuperación de datos y capacitaciones para la administración segura de la base de datos.	Implementar mejoras en el sistema de respaldo y almacenamiento seguro.	Equipo de seguridad informática

<b>Sobrecostos</b>	Aumento en los costos de desarrollo que afecten el presupuesto	Media	Alto	Definir un presupuesto detallado y controlar los gastos regularmente.	Redefinir prioridades para ajustar el presupuesto, reducir gastos	Equipo completo.
<b>Privacidad</b>	Riesgo de exposición o mal uso de la información personal de los estudiantes	Alta	Alto	Implementar políticas estrictas de protección de datos y anonimizarían, limitar el acceso a la información y realizar auditorías de privacidad periódicas.	Activar el protocolo de respuesta en caso de exposición de datos, investigar la causa y realizar mejoras de seguridad.	Equipo de seguridad informática