1. **Propósito del Documento**

El propósito de este plan de contingencia es identificar y establecer medidas preventivas y de respuesta para los riesgos potenciales que podrían afectar el desarrollo y funcionamiento de la aplicación Featuring.

1. **Alcance del Plan de Contingencia**

Este documento abarca los riesgos relacionados con las funciones de la aplicación y sus medidas de mitigación y contingencia. Incluye aspectos de rendimiento, seguridad, privacidad y experiencia del usuario.

1. **Análisis de Riesgos y Medidas de Contingencia**

A continuación se presentan los riesgos identificados, su impacto, probabilidad, medidas de mitigación y de contingencia, así como el equipo responsable de cada riesgo:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | RIESGO | IMPACTO | PROBABILIDAD | ESTRATEGIA DE MITIGACIÓN | ESTRATEGIA DE CONTINGENCIA | RESPONSABLE |
| 1 | Fallo en la reproducción de contenido multimedia | Alto | Media | Optimizar el formato y calidad del contenido; realizar pruebas de rendimiento en múltiples dispositivos. | Ajustar formatos y reducir calidad de forma temporal; comunicar fallos a usuarios. | Equipo de desarrollo multimedia |
| 2 | Sobrecarga del servidor por alta demanda | Crítico | Alta | Configurar escalabilidad automática; optimizar uso de recursos y realizar pruebas de carga periódicas. | Activar servidores adicionales de respaldo; limitar accesos si es necesario. | Administrador de infraestructura |
| 3 | Acceso no autorizado a perfiles de usuario | Crítico | Media | Implementar autenticación multifactor y cifrado de datos sensibles; realizar auditorías de seguridad. | Desactivar accesos comprometidos; informar a usuarios y restablecer contraseñas. | Equipo de seguridad |
| 4 | Fallo en el sistema de notificaciones | Medio | Media | Realizar pruebas en el sistema de notificaciones; verificar integraciones con API de notificaciones push. | Crear sistema de respaldo de notificaciones por correo electrónico. | Equipo de desarrollo backend |
| 5 | Contenido inapropiado en la comunidad | Alto | Media | Implementar moderación automática con IA para detectar lenguaje ofensivo; activar reportes automáticos. | Revisar reportes manualmente; suspender temporalmente el contenido ofensivo. | Moderador de contenido |
| 6 | Interacciones inapropiadas entre usuarios | Alto | Media | Crear sistema de bloqueo y reportes entre usuarios; monitorear interacciones de alto riesgo. | Suspender cuentas problemáticas en casos extremos. | Moderador de comunidad |
| 7 | Problemas de privacidad en reportes y sanciones | Alto | Baja | Limitar el acceso a los reportes solo a personal autorizado; aplicar políticas estrictas de privacidad. | Revisar y ajustar los permisos de acceso; auditar cambios en los reportes. | Administrador de seguridad y privacidad |
| 8 | Mal rendimiento de la aplicación | Alto | Media | Optimizar el código y base de datos; realizar pruebas de rendimiento periódicas. | Notificar a los usuarios; implementar parches de emergencia para fallos críticos. | Equipo de desarrollo y QA |
| 9 | Desinformación o abuso en el sistema de reportes | Medio | Baja | Implementar validación de reportes; revisar manualmente reportes recurrentes o sospechosos para evitar falsos positivos. | Suspender temporalmente el sistema de reportes si hay abuso; realizar auditorías. | Moderador de reportes |
| 10 | Fallo en la funcionalidad de colaboración entre usuarios | Medio | Media | Realizar pruebas de compatibilidad y optimización en el intercambio de archivos y mensajes entre usuarios. | Desactivar temporalmente la funcionalidad; notificar a los usuarios afectados. | Equipo de desarrollo de funcionalidades sociales |

1. **Roles y Responsabilidades**

|  |  |
| --- | --- |
|  |  |
| Administrador de Proyecto | Coordinar el plan de contingencia y supervisar la implementación de acciones correctivas. |
| Equipo de Desarrollo | Implementar optimizaciones y correcciones en el sistema de reproducción, notificaciones, y colaboración. |
| Equipo de Seguridad | Gestionar y supervisar la seguridad de los datos y el acceso autorizado a perfiles de usuario. |
| Moderador de Contenido | Monitorear y moderar contenido inapropiado en la comunidad; revisar y actuar ante interacciones inapropiadas. |
| Administrador de Infraestructura | Garantizar la estabilidad y escalabilidad del servidor para soportar altos picos de tráfico. |
| Equipo de QA | Realizar pruebas de rendimiento y usabilidad; identificar problemas en fases tempranas del desarrollo. |

1. **Proceso de Evaluación de Riesgos**

Este plan se revisará y ajustará mensualmente para actualizar las estrategias de mitigación y contingencia en función de los cambios en el proyecto y el entorno tecnológico. Además, se realizarán revisiones después de cada incidente o problema crítico.

1. Mantenimiento y actualización del plan de contingencia

Este plan será revisado mensualmente para reflejar cualquier cambio en los riesgos o en el desarrollo de la aplicación.