**UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS**

UNIVERSIDAD DEL PERÚ, DECANA DE AMÉRICA



**SGI - Documento de Análisis de Riesgos**

**Curso:** Gestión de Configuración de Software

**Integrantes (Grupo N° 5):**

* Balarezo Ramos, Luis Jesús
* Durand Caracuzma, Marlon Milko
* Del Aguila Febres, Brayan Tadeo
* Balceda Delgado, Mariana Alejandra
* Canecillas Contreras, Juan Mariano
* Soller Barnechea, Carlos Javier
* Huarhua Piñas, Edson Sebastian
* Justiniano Quispe, Diego André

# 

## ***ÍNDICE***

[**ÍNDICE 2**](#_icp6r59c7idf)

[**Análisis de riesgos del proyecto**](#_i58on9lso2ef) “[**Sistema de Gestión de Incidencias” 3**](#_icw5yx110z10)

[**1. Identificación de riesgos 3**](#_eucv17745upc)

[**2. Análisis de riesgos 3**](#_offbrflvq6gl)

[2.1 Evaluación de la probabilidad de ocurrencia 3](#_ulqn4eyegc)

[2.2 Evaluación de la gravedad de las consecuencias 4](#_bm514e8v7k2g)

[2.3 Evaluación del impacto en el proyecto 4](#_afr1qdppz1sk)

[2.4 Priorización de los riesgos 5](#_g63g9w1vremx)

[**3. Plan de mitigación 5**](#_c9otqb5kfb78)

[**4. Plan de contingencia 6**](#_tgihae1xg8oo)

[**5. Seguimiento y control 6**](#_5bun31kh6ssm)

**6**[**. Conclusiones y Recomendaciones**](#_1163qravwb1j) **6**

## 

# Análisis de riesgos del proyecto “Sistema de Gestión de Incidencias”

El análisis de riesgos es una parte crítica del desarrollo de cualquier sistema, incluyendo el Sistema de Gestión de Incidencias. Identificar y analizar los riesgos potenciales puede ayudar a minimizar los efectos negativos en el proyecto y en los usuarios del sistema. En este proceso, se deben considerar los posibles problemas y fallas que podrían surgir, y tomar medidas para mitigarlos o prepararse para ellos. El análisis de riesgos se divide en varias etapas, como la identificación de los riesgos, el análisis y evaluación de su probabilidad y gravedad, la priorización de los riesgos, la elaboración de un plan de mitigación y un plan de contingencia, y finalmente el seguimiento y control del sistema para asegurarse de que esté funcionando de manera efectiva y segura. En este contexto, es importante resaltar que las conclusiones y recomendaciones resultantes del análisis de riesgos pueden ser de gran ayuda para mejorar y fortalecer el Sistema de Gestión de Incidencias.

## 1. Identificación de riesgos

| **Número** | **Riesgo** | **Descripción** | **Área de impacto** |
| --- | --- | --- | --- |
| 1 | Pérdida de datos | Pérdida de información almacenada en el sistema debido a fallas técnicas, errores humanos, catástrofes naturales u otros eventos | Técnico y usuario |
| 2 | Ataque de hackers | Acceso no autorizado a la información del sistema por parte de hackers, crackers u otros delincuentes informáticos | Técnico y legal |
| 3 | Incumplimiento de regulaciones de privacidad de datos | Incumplimiento de leyes y regulaciones de privacidad de datos, lo que podría resultar en multas, sanciones o daños a la reputación de la organización | Legal y financiero |
| 4 | Fallo en la interfaz de usuario | Problemas con la usabilidad, accesibilidad y/o diseño de la interfaz del usuario, lo que podría llevar a la frustración del usuario y una menor adopción del sistema | Usuario y financiero |
| 5 | Fallo en el rendimiento del sistema | El sistema no cumple con las expectativas de rendimiento en términos de velocidad, capacidad, disponibilidad o eficiencia, lo que podría resultar en una pérdida de productividad y rentabilidad | Técnico y financiero |
| 6 | Retrasos en el desarrollo | Retrasos en la entrega del proyecto debido a problemas de gestión de proyectos, cambios en los requisitos, problemas técnicos u otros problemas | Financiero y legal |
| 7 | Falta de comunicación entre el equipo | Comunicación insuficiente o ineficaz entre los miembros del equipo, lo que podría llevar a errores, malentendidos y retrasos | Técnico y financiero |

## 

## 2. Análisis de riesgos

### 2.1 Evaluación de la probabilidad de ocurrencia

| **Número** | **Riesgo** | **Probabilidad** |
| --- | --- | --- |
| 1 | Pérdida de datos | La probabilidad de pérdida de datos puede ser alta si no se implementan medidas de seguridad adecuadas, como copias de seguridad regulares y controles de acceso. |
| 2 | Ataque de hackers | La probabilidad de un ataque de hackers puede ser alta si el sistema no se asegura adecuadamente, como no tener actualizaciones de seguridad regulares y la falta de controles de acceso adecuados. |
| 3 | Incumplimiento de regulaciones de privacidad de datos | La probabilidad de incumplimiento de regulaciones puede ser alta si no se implementan medidas de seguridad adecuadas, como la falta de una política clara de privacidad de datos y controles de acceso inadecuados. |
| 4 | Fallo en la interfaz de usuario | La probabilidad de fallo en la interfaz de usuario puede ser alta si no se realizan pruebas adecuadas y se toman en cuenta los comentarios de los usuarios. |
| 5 | Fallo en el rendimiento del sistema | La probabilidad de fallo en el rendimiento del sistema puede ser alta si no se realizan pruebas adecuadas y no se monitorea el sistema regularmente. |
| 6 | Retrasos en el desarrollo | La probabilidad de retrasos en el desarrollo puede ser alta si no se planifica adecuadamente y no se establecen objetivos claros. |
| 7 | Falta de comunicación entre el equipo | La probabilidad de falta de comunicación puede ser alta si no se establecen canales claros de comunicación y no se fomenta la comunicación efectiva entre los miembros del equipo. |

### La probabilidad se ha evaluado en función de la posibilidad de que ocurra el riesgo. En este caso, se ha utilizado una escala de baja, media y alta para indicar el nivel de riesgo. Estas probabilidades se han determinado a partir de la experiencia y la opinión de expertos en la materia.

### 2.2 Evaluación de la gravedad de las consecuencias

| **Número** | **Riesgo** | **Gravedad** |
| --- | --- | --- |
| 1 | Pérdida de datos | La pérdida de datos puede tener consecuencias catastróficas, como la imposibilidad de resolver problemas importantes y la pérdida de privacidad, lo que puede llevar a posibles responsabilidades legales. |
| 2 | Ataque de hackers | Un ataque de hackers puede resultar en la exposición y posible robo de datos confidenciales y la interrupción del sistema, erosionando la confianza del cliente y potencialmente dañando la reputación de la empresa. |
| 3 | Incumplimiento de regulaciones de privacidad de datos | El incumplimiento de regulaciones puede resultar en posibles responsabilidades legales, sanciones y la pérdida de la confianza del cliente, lo que puede afectar la reputación de la empresa. |
| 4 | Fallo en la interfaz de usuario | Un fallo en la interfaz puede resultar en la incapacidad del usuario para informar correctamente una incidencia, lo que puede llevar a una solución incorrecta o la no resolución del problema. |
| 5 | Fallo en el rendimiento del sistema | Un fallo en el rendimiento del sistema puede llevar a la interrupción de la gestión de incidencias, lo que puede resultar en una solución tardía o la no resolución del problema. |
| 6 | Retrasos en el desarrollo | Los retrasos pueden afectar la fecha de lanzamiento del sistema, lo que puede llevar a una pérdida de oportunidades de negocio y una posible pérdida de ingresos. |
| 7 | Falta de comunicación entre el equipo | La falta de comunicación puede llevar a la duplicación de trabajo y a una solución tardía o incorrecta de la incidencia, lo que puede afectar la satisfacción del cliente y la reputación de la empresa. |

### La gravedad se ha evaluado en función del impacto que tendría cada riesgo en el proyecto y en la organización. En este caso, se ha utilizado una escala de baja, media y alta para indicar el nivel de gravedad. Estas evaluaciones se han realizado en función de la experiencia y la opinión de expertos en la materia.

### 2.3 Evaluación del impacto en el proyecto

| **Número** | **Riesgo** | **Impacto** |
| --- | --- | --- |
| 1 | Pérdida de datos | Si se produce una pérdida de datos importante, podría llevar a la imposibilidad de completar el proyecto y a la necesidad de comenzar de nuevo desde cero. Además, puede haber impactos financieros importantes, especialmente si se pierden datos de clientes o de la empresa. |
| 2 | Ataque de hackers | Un ataque de hackers puede tener consecuencias graves, como la exposición de información confidencial, la pérdida de datos importantes o el acceso no autorizado a sistemas críticos. También puede dañar la reputación de la empresa y llevar a la pérdida de clientes o de ingresos. |
| 3 | Incumplimiento de regulaciones de privacidad de datos | El incumplimiento de las regulaciones de privacidad de datos puede tener consecuencias legales y financieras importantes. Podría llevar a multas, acciones legales, daños a la reputación y la pérdida de clientes. |
| 4 | Fallo en la interfaz de usuario | Un fallo en la interfaz de usuario puede llevar a una experiencia de usuario insatisfactoria y a la pérdida de clientes. También puede requerir tiempo y recursos adicionales para corregir el problema. |
| 5 | Fallo en el rendimiento del sistema | Un fallo en el rendimiento del sistema puede llevar a la imposibilidad de completar el proyecto y a la necesidad de comenzar de nuevo desde cero. También puede afectar la productividad y la eficiencia de los empleados y llevar a la pérdida de clientes o de ingresos. |
| 6 | Retrasos en el desarrollo | Los retrasos en el desarrollo pueden llevar a la pérdida de tiempo y recursos, así como a la posibilidad de no cumplir con los plazos y presupuestos establecidos. También pueden afectar la calidad del proyecto y la satisfacción del cliente. |
| 7 | Falta de comunicación entre el equipo | La falta de comunicación entre el equipo puede llevar a malentendidos, errores y conflictos. También puede afectar la productividad y la eficiencia de los empleados y llevar a la pérdida de tiempo y recursos. |

### 

### 2.4 Priorización de los riesgos

| **Número** | **Riesgo** | **Probabilidad** | **Gravedad** | **Impacto** | **Prioridad** |
| --- | --- | --- | --- | --- | --- |
| 1 | Pérdida de datos | Alta | Alta | Alta | Alta |
| 2 | Ataque de hackers | Media | Alta | Alta | Alta |
| 3 | Incumplimiento de regulaciones de privacidad de datos | Baja | Alta | Alta | Media |
| 4 | Fallo en la interfaz de usuario | Media | Media | Media | Baja |
| 5 | Fallo en el rendimiento del sistema | Alta | Media | Alta | Alta |
| 6 | Retrasos en el desarrollo | Alta | Media | Media | Alta |
| 7 | Falta de comunicación entre el equipo | Media | Baja | Media | Baja |

## 3. Plan de mitigación

| **Número** | **Riesgo** | **Estrategia de mitigación** | **Responsable** | **Plazo límite** |
| --- | --- | --- | --- | --- |
| **1** | Pérdida de datos | Implementación de backups regulares y almacenamiento en un lugar seguro | Analista Sr. / Programador Back-End | 3 días |
| **2** | Ataque de hackers | Implementación de medidas de seguridad adicionales, como autenticación de dos factores y cifrado de datos | Arquitecto de Software / Programador Back-End | 4 días |
| **3** | Incumplimiento de regulaciones de privacidad de datos | Revisión y cumplimiento de las regulaciones pertinentes, como GDPR y CCPA | Analista Sr. / Diseñador UI UX | 2 días |
| **4** | Fallo en la interfaz de usuario | Pruebas exhaustivas de UI y UX antes del lanzamiento, incluyendo pruebas de usuario beta | QA / Diseñador UI UX | 3 días |
| **5** | Fallo en el rendimiento del sistema | Pruebas de carga y ajuste de hardware y software para garantizar la escalabilidad y el rendimiento adecuado | Arquitecto de Software / Programador Back-End | 2 días |
| **6** | Retrasos en el desarrollo | Establecimiento de plazos claros y realistas y seguimiento regular del progreso del equipo | Jefe de Proyecto / Analista Sr. | 2 días |
| **7** | Falta de comunicación entre el equipo | Establecimiento de reuniones regulares y comunicación clara de los roles y responsabilidades de cada miembro del equipo | Jefe de Proyecto / Analista Sr. | 1 día |

## 

## 4. Plan de contingencia

| **Número** | **Riesgo** | **Estrategia de contingencia** | **Responsable** | **Plazo límite** |
| --- | --- | --- | --- | --- |
| 1 | Pérdida de datos | Establecer un plan de copias de seguridad regulares y asegurar que los datos estén respaldados en un lugar seguro. | Programador Back-End | 3 días |
| 2 | Ataque de hackers | Implementar medidas de seguridad adecuadas, como la instalación de software de seguridad y la realización de pruebas de penetración regulares. | Analista Senior / DBA | 2 días |
| 3 | Incumplimiento de regulaciones de privacidad de datos | Establecer políticas claras de privacidad de datos y asegurarse de que se implementen medidas de seguridad adecuadas para proteger los datos de los usuarios. | Jefe de Proyecto / Analista Sr. | 1 día |
| 4 | Fallo en la interfaz de usuario | Realizar pruebas exhaustivas y obtener comentarios de los usuarios para mejorar la interfaz de usuario. | QA | 3 días |
| 5 | Fallo en el rendimiento del sistema | Monitorear regularmente el sistema y establecer planes de acción para abordar los problemas de rendimiento. | Jefe de Proyecto / Analista Sr. | 1 día |
| 6 | Retrasos en el desarrollo | Establecer objetivos claros y plazos realistas, y planificar con anticipación para minimizar los retrasos. | Diseñador UI UX / Arquitecto de Software | 2 días |
| 7 | Falta de comunicación entre el equipo | Establecer canales claros de comunicación y fomentar la comunicación efectiva entre los miembros del equipo mediante reuniones regulares y herramientas de colaboración en línea. | Analista Sr. | 3 días |

## 

## 

## 

## 

## 5. Seguimiento y control

| **Número** | **Riesgo** | **Plan de seguimiento** | **Fecha de revisión** |
| --- | --- | --- | --- |
| 1 | Falta de personal en el equipo de desarrollo | Monitorear el avance del proyecto y el desempeño del equipo. Si se identifican retrasos significativos o sobrecarga de trabajo, se debe considerar la contratación de personal adicional. | 2 días |
| 2 | Vulnerabilidades de seguridad en el sistema | Realizar pruebas de seguridad regulares y monitorear los registros del sistema en busca de actividad sospechosa. Actualizar y mantener los mecanismos de seguridad implementados. | 4 días |
| 3 | Fallos en el hardware o software de los servidores | Establecer un plan de mantenimiento preventivo y de respaldo regular. Implementar redundancias en los servidores y monitorear constantemente su funcionamiento. | 3 días |
| 4 | Problemas en la usabilidad del sistema | Realizar pruebas de usabilidad con usuarios y solicitar retroalimentación. Realizar mejoras en la interfaz de usuario y en la experiencia de usuario según la retroalimentación recibida. | 3 días |

## 6. Conclusiones y Recomendaciones

**Conclusiones:**

* El análisis de riesgos es una herramienta clave para identificar y evaluar los riesgos potenciales que pueden afectar el éxito del proyecto del Sistema de Gestión de Incidencias.
* La evaluación de la probabilidad de ocurrencia y la gravedad de las consecuencias son factores clave para determinar la prioridad de los riesgos y asignar recursos para su mitigación.
* El plan de mitigación y el plan de contingencia son fundamentales para minimizar el impacto de los riesgos y mantener el proyecto en marcha en caso de que se presenten problemas.

**Recomendaciones:**

* Se debe asignar un responsable para cada riesgo y asegurarse de que tengan los recursos y la autoridad necesarios para implementar las estrategias de mitigación y contingencia correspondientes.
* Es recomendable realizar evaluaciones periódicas de riesgos para detectar nuevos riesgos y actualizar la estrategia de mitigación y contingencia según sea necesario.
* Se debe fomentar una cultura de gestión de riesgos en el equipo del proyecto, para que todos estén conscientes de los riesgos potenciales y sepan cómo actuar en caso de que se presenten.