# Título

**Plan de Gestión**

**de Riesgos**

***[Proyecto ERP para pymes]***

***Fecha: [29/08/2024]***

# Tabla de contenido

[**Título 1**](#_heading=h.gjdgxs)

[**Tabla de contenido 2**](#_heading=h.30j0zll)

[**Escala de probabilidad**](#_heading=h.3rdcrjn) **3**

[**Escala de impacto**](#_heading=h.z337ya) **4**

[**Matriz de Probabilidad e Impacto**](#_heading=h.3as4poj) **5**

[**Riesgos Gestionados por Proyecto**](#_heading=h.49x2ik5) **6**

[**Gestión de riesgos**](#_heading=h.147n2zr) **7**

# 

# Escala de probabilidad

|  |  |  |  |
| --- | --- | --- | --- |
| Escala | Clasificación | Descripción | Frecuencia |
| 5 | Cierto | El riesgo es altamente probable de ocurrir. Se espera que ocurra en la mayoría de las situaciones en que se encuentre presente. | Más de 1 vez por semana |
| 4 | Probable | El riesgo es probable de ocurrir en reiteradas ocasiones en el corto plazo. | Más de 1 vez al mes  Hasta 1 vez por semana |
| 3 | Posible | El riesgo tiene una probabilidad moderada de ocurrir en el mediano plazo. | Más de 1 vez en un proyecto, hasta 1 vez al mes |
| 2 | Improbable | El riesgo es poco probable de ocurrir, pero aún existe una posibilidad. | Hasta 1 vez en un proyecto |
| 1 | Excepcional | El riesgo es altamente improbable de ocurrir, sólo en circunstancias excepcionales o como resultado de una combinación de eventos inusuales. | Hasta 1 vez entre todos los proyectos |

# Escala de impacto

|  |  |  |
| --- | --- | --- |
| Escala | Clasificación | Descripción |
| 5 | Mayor | El riesgo tiene un impacto devastador en el proyecto. Podría causar la interrupción total del proyecto o resultados negativos. |
| 4 | Alto | El riesgo tiene un impacto crítico en el proyecto. Podría causar retrasos significativos, sobrecostos importantes o problemas que afecten gravemente la calidad del proyecto. |
| 3 | Moderado | El riesgo tiene un impacto moderado en el proyecto. Podría causar desviaciones en el cronograma, el presupuesto u otros aspectos del proyecto, pero aún podría ser manejado con ajustes y medidas correctivas. |
| 2 | Menor | El riesgo tiene un impacto relativamente bajo en el proyecto. Podría causar efectos menores en el progreso del proyecto y podría ser manejado sin mayores dificultades. |
| 1 | Insignificante | El riesgo tiene un impacto mínimo en el proyecto. Su ocurrencia no tendría efectos significativos en el desarrollo del proyecto o en sus resultados finales. |

# Matriz de Probabilidad e Impacto

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Impacto  Probabilidad | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 |
| 2 | 2 | 4 | 6 | 8 | 10 |
| 3 | 3 | 6 | 9 | 12 | 15 |
| 4 | 4 | 8 | 12 | 16 | 20 |
| 5 | 5 | 10 | 15 | 20 | 25 |

## 

## **Riesgos Gestionados**

1. No alcanzar a implementar la solución en el tiempo definido
2. Realizar estimaciones de tiempo inexactas
3. No considerar tiempo para pruebas y correcciones
4. No considerar eventos imprevistos
5. No encontrar personal calificado
6. Tener costos inesperados que sobrepasen el presupuesto
7. Ocurre un retraso en la configuración que afecta el cronograma
8. El sistema no soporta alta carga de usuarios
9. Datos incorrectos registrados en el sistema
10. Pérdida de datos por fallas en la nube
11. Dificultad en la adopción del nuevo sistema por los empleados
12. Fallos en la integración con sistemas existentes
13. Brechas de seguridad en el sistema

# 

# Gestión de riesgos

**1.- No alcanzar a implementar la solución en el tiempo definido:**

* **Probabilidad:** 3 (Posible)
* **Impacto:** 5 (Mayor)
* **Vulnerabilidad:** Falta de experiencia definiendo tiempos en proyectos similares
* **Amenaza:** Cambios frecuentes en los requisitos del proyecto durante el desarrollo
* **Mitigación:** Establecer una planificación que considere un ritmo de trabajo capaz de cumplir con los tiempos estimados y con un pequeño tiempo de mitigación en caso de imprevistos
* **Costo de Mitigación:** 4,5 UF

**2.- Realizar estimaciones de tiempo inexactas**

* **Probabilidad:** 3 (Posible)
* **Impacto:** 4 (Alto)
* **Vulnerabilidad:** Falta de experiencia definiendo tiempos en proyectos similares
* **Amenaza:** Cambios frecuentes en los requisitos del proyecto
* **Mitigación:** Realizar reuniones periódicas de seguimiento con los directivos para asegurar la correcta interpretación de los requerimientos.
* **Costo de Mitigación:** 4,5 UF

**3.- No considerar tiempo para pruebas y correcciones**

* **Probabilidad:** 3 (Posible)
* **Impacto:** 4 (Alto)
* **Vulnerabilidad:** Enfoque excesivo en algunas fases del proyecto, dejando de lado otras
* **Amenaza:** Retrasos imprevistos en algunas fases del proyecto
* **Mitigación:** Incluir tiempo de pruebas en el cronograma.
* **Costo de Mitigación:** 4,5 UF

**4.- No considerar eventos imprevistos**

* **Probabilidad:** 3 (Posible)
* **Impacto:** 4 (Alto)
* **Vulnerabilidad:** Planificación rígida sin márgenes de cambios
* **Amenaza:** Eventos inesperados como fallas técnicas
* **Mitigación:** Crear un plan de contingencia para eventos imprevistos.
* **Costo de Mitigación:** 4,5 UF

**5.- No encontrar personal calificado**

* **Probabilidad:** 3 (Posible)
* **Impacto:** 4 (Alto)
* **Vulnerabilidad:** Tener pocas maneras y estrategias para buscar personal calificado
* **Amenaza:** Mercado laboral limitado
* **Mitigación:** Realizar un proceso de selección exhaustivo y buscar en múltiples plataformas de empleo.
* **Costo de Mitigación:** 4,5 UF

**6.- Tener costos inesperados que sobrepasen el presupuesto**

* **Probabilidad:** 3 (Posible)
* **Impacto:** 4 (Alto)
* **Vulnerabilidad:** Falta de experiencia estimando costos en proyectos similares
* **Amenaza:** Presupuesto insuficiente
* **Mitigación:** Incluir una reserva de contingencia en el presupuesto.
* **Costo de Mitigación:** 4,5 UF

**7.- Ocurre un retraso en la configuración que afecta el cronograma**

* **Probabilidad:** 3
* **Impacto:** 4
* **Vulnerabilidad:** No considerar eventos imprevistos
* **Amenaza:** Interrupciones en las operaciones del colegio que impidan la continuidad de la instalación
* **Mitigación:** Mantener un margen de holgura que permita que en caso de que se atrase una tarea no afecte todo el cronograma
* **Costo de Mitigación:** 4,5 UF

**8..-El sistema no soporta alta carga de usuarios**

* **Probabilidad**: 3 (Posible)
* **Impacto**: 4 (Mayor)
* **Vulnerabilidad**: Falta de pruebas de estrés en entornos de producción
* **Amenaza**: Sobrecarga del sistema durante picos de uso
* **Mitigación**: Realizar pruebas de carga y optimizar el rendimiento del sistema para soportar alta concurrencia
* **Costo de Mitigación**: 5 UF

**9.- Datos incorrectos registrados en el sistema**

* **Probabilidad**: 3 (Posible)
* **Impacto**: 5 (Mayor)
* **Vulnerabilidad**: Falta de validación en la entrada de datos
* **Amenaza**: Errores en la información que afectan la toma de decisiones
* **Mitigación**: Implementar validación automática en campos clave para asegurar la precisión de los datos ingresados
* **Costo de Mitigación:**: 4 UF

**10. -Pérdida de datos por fallas en la nube**

* **Probabilidad**: 2 (Poco probable)
* **Impacto**: 5 (Catastrófico)
* **Vulnerabilidad**: Dependencia en un solo proveedor de servicios en la nube
* **Amenaza**: Caídas o fallas en la infraestructura del proveedor
* **Mitigación**: Implementar respaldos automáticos y redundancia en la nube con proveedores alternativos
* **Costo de Mitigación**: 6 UF

**11.-Dificultad en la adopción del nuevo sistema por los empleados**

* **Probabilidad**: 4 (Probable)
* **Impacto**: 4 (Mayor)
* **Vulnerabilidad**: Resistencia al cambio y curva de aprendizaje elevada
* **Amenaza**: Baja productividad y errores operativos
* **Mitigación**: Ofrecer capacitación intensiva y soporte continuo durante el periodo de transición
* **Costo de Mitigación**: 3 UF

**12.- Fallos en la integración con sistemas existentes**

* **Probabilidad**: 3 (Posible)
* **Impacto**: 4 (Mayor)
* **Vulnerabilidad**: Incompatibilidades técnicas entre el nuevo sistema y los sistemas existentes
* **Amenaza**: Pérdida de datos o inconsistencias en la operación
* **Mitigación**: Realizar pruebas de integración exhaustivas y ajustes técnicos antes del despliegue completo
* **Costo de Mitigación**: 5 UF

**13.- Brechas de seguridad en el sistema**

* **Probabilidad**: 2 (Poco probable)
* **Impacto**: 5 (Catastrófico)
* **Vulnerabilidad**: Configuración de seguridad inadecuada
* **Amenaza**: Ataques cibernéticos que comprometen datos sensibles
* **Mitigación**: Implementar cifrado, autenticación de múltiples factores y revisiones de seguridad periódicas
* **Costo de Mitigación**: 7 UF

## 

## Riesgos más importantes y/o a destacar

**1. Datos incorrectos registrados en el sistema**

* **Descripción**: Se registran datos de usuarios y clientes en el sistema de gestión.
* **Riesgo**: Registro de datos incorrectos (correos electrónicos, nombres mal escritos).
* **Vulnerabilidad**: Falta de validación en la entrada de datos.
* **Amenaza**: Información incorrecta que afecta la toma de decisiones y la comunicación con clientes.
* **Tipo de Plan**: Mitigación.
* **Mitigación**: Implementar validación automática en campos clave para asegurar la precisión de los datos ingresados.
* **Contingencia**: Contactar a los clientes para corregir los datos incorrectos y ajustar cualquier error en las recompensas.
* **Probabilidad: 3**
* **Impacto: 5**
* **Calificación Total: 15**

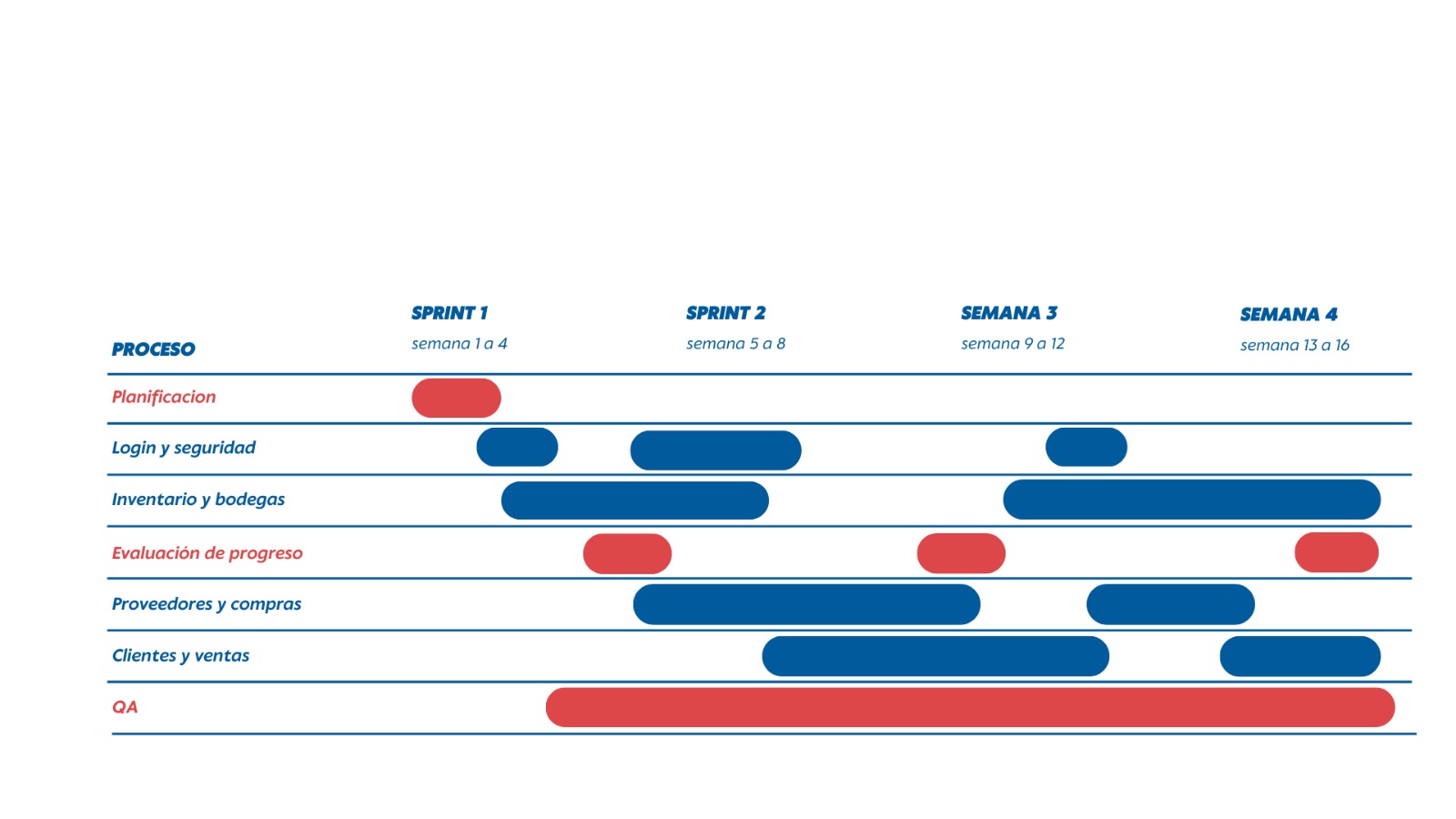
**2. Fallos en la integración con sistemas existentes**

* **Descripción**: Integración del nuevo sistema con sistemas preexistentes de la Pyme.
* **Riesgo**: Fallas en la integración que resultan en pérdida de datos o duplicación.
* **Vulnerabilidad**: Incompatibilidades técnicas entre el nuevo sistema y los sistemas existentes.
* **Amenaza**: Pérdida de datos o inconsistencias en la operación.
* **Tipo de Plan**: Mitigación.
* **Mitigación**: Realizar pruebas de integración exhaustivas y ajustes técnicos antes del despliegue completo.
* **Contingencia**: Desarrollar scripts de corrección y herramientas de limpieza de datos para solucionar problemas rápidamente.
* **Probabilidad: 3**
* **Impacto: 4**
* **Calificación Total: 12**

**3. Brechas de seguridad en el sistema**

* **Descripción**: Asegurar la protección de los datos almacenados en la nube.
* **Riesgo**: Brechas de seguridad que comprometan datos sensibles.
* **Vulnerabilidad**: Configuración de seguridad inadecuada.
* **Amenaza**: Ataques cibernéticos que resulten en robo o pérdida de datos.
* **Tipo de Plan**: Mitigación.
* **Mitigación**: Implementar cifrado de datos, autenticación de múltiples factores y auditorías regulares de seguridad.
* **Contingencia**: Desarrollar un plan de respuesta a incidentes que incluya notificación a clientes y recuperación de datos.
* **Probabilidad: 2**
* **Impacto: 5**
* **Calificación Total: 10**

# Cronograma



# 

# Monitoreo y control

Administración de Riesgos a lo Largo del Tiempo:

**Monitoreo Continuo:**

* Establecer reuniones periódicas de seguimiento para evaluar el estado de cada riesgo identificado. Revisar si las probabilidades o impactos han cambiado y ajustar las estrategias de mitigación en consecuencia.

**Actualización del Plan de Riesgos:**

* A medida que el proyecto avanza, es posible que surjan nuevos riesgos o que algunos riesgos previamente identificados cambien en severidad. Es fundamental actualizar el plan de riesgos regularmente para reflejar el entorno actual del proyecto.

**Asignación de Responsabilidades:**

* Designar responsables específicos para cada riesgo, asegurando que haya una persona o equipo encargado de monitorear y ejecutar las acciones de mitigación y contingencia.

**Capacitación y Concientización:**

* Proporcionar capacitación continua al equipo sobre la importancia de la gestión de riesgos y cómo identificar posibles riesgos emergentes en sus áreas de trabajo.

**Evaluación de la Eficacia:**

* Al final de cada fase del proyecto, realizar una evaluación de la efectividad de las medidas de mitigación implementadas. Esto permitirá ajustar las estrategias futuras basadas en las lecciones aprendidas.

# Reflexión

La gestión de riesgos en un proyecto de desarrollo de software es un aspecto crucial para asegurar su éxito. Cada riesgo identificado representa una posible barrera que puede impactar negativamente el proyecto si no se aborda de manera adecuada. La clave está en anticipar estas barreras y desarrollar estrategias efectivas para mitigarlas, de manera que minimicemos su impacto en el cronograma, los costos y la calidad del producto final.

En este proyecto específico, los riesgos van desde errores en la gestión del tiempo hasta problemas técnicos en la integración y la seguridad del sistema. El hecho de que muchos de estos riesgos estén relacionados con la planificación y la precisión de las estimaciones subraya la importancia de una gestión proactiva y bien estructurada.