

## RIESGOS ASOCIADOS AL DESARROLLO DEL SOFTWARE

MARIANA HINCAPIÉ HENAO – 1017923583

NICOLAS FELIPE URIBE MENDEZ – 1003534021

NICOLAS CASTAÑEDA BETANCUR - 1020104128

INGENIERIA INFORMATICA

FEIBERT ALIRIO GUZMAN PEREZ

INGENIERIA DEL SOFTWARE 2

CORPORACIÓN UNIVERSITARIA UNILASALLISTA

CALDAS, ANTIOQUIA

Octubre 22 del 2024

# Introducción a los Riesgos en el Desarrollo de Software

En el contexto del desarrollo de software, un riesgo es cualquier evento o condición que puede afectar negativamente el éxito de un proyecto. Estos riesgos pueden surgir en diversas etapas del desarrollo y pueden impactar en el tiempo, costo y calidad del producto final.

## Tipos de Riesgos Para Considerar

### 1. Riesgos Tecnológicos

Estos riesgos se refieren a los problemas derivados de la tecnología utilizada en el desarrollo del software. Incluyen el uso de tecnologías obsoletas, dependencias de herramientas específicas que pueden no ser compatibles o fallos en el hardware y software que pueden interrumpir el trabajo.

- **Tecnologías obsoletas:** Utilizar tecnologías que están desactualizadas puede llevar a problemas de compatibilidad y limitaciones en las capacidades del software.
- **Dependencias de herramientas:** La dependencia de herramientas específicas, especialmente si no están bien soportadas o documentadas, puede causar retrasos y problemas técnicos.
- **Fallos de hardware/software:** Fallos en los equipos o en el software utilizado para el desarrollo pueden interrumpir el trabajo y causar pérdidas de datos.

### 2. Riesgos del Cliente

Estos riesgos están relacionados con la interacción con el cliente y sus expectativas. Pueden incluir cambios en los requisitos del cliente a mitad del proyecto, falta de comunicación clara con el cliente o expectativas no bien definidas que pueden llevar a un producto final que no cumpla con las necesidades del cliente.

- **Cambios en los requisitos:** Los cambios en los requisitos del cliente pueden causar retrabajo y desvíos significativos en el cronograma y el presupuesto.
- **Falta de comunicación:** Una comunicación deficiente entre el equipo de desarrollo y el cliente puede resultar en malentendidos y expectativas no cumplidas.
- **Expectativas no claras:** Si las expectativas del cliente no están claramente definidas desde el inicio, el producto final puede no satisfacer sus necesidades.

### 3. Riesgos del Proceso

Estos riesgos se centran en cómo se gestiona y organiza el proyecto. Incluyen el uso de metodologías de desarrollo inadecuadas, mala gestión de recursos como tiempo y personal, y problemas en la planificación y ejecución del proyecto.

- **Metodologías inadecuadas:** El uso de metodologías de desarrollo inapropiadas puede llevar a una planificación deficiente y problemas de ejecución.
- **Mala gestión de recursos:** La falta de una adecuada gestión de los recursos (personales, financieros, materiales) puede afectar gravemente el progreso del proyecto.

## 4. Riesgos del Producto

Estos riesgos están asociados con la calidad y funcionalidad del producto final. Pueden incluir defectos en el código que afectan la funcionalidad del software, o falta de calidad en el producto que no cumple con los estándares requeridos.

- **Defectos en el código:** La presencia de errores en el código puede afectar la funcionalidad y estabilidad del software.
- **Falta de calidad:** Un enfoque insuficiente en el aseguramiento de la calidad puede llevar a un producto final que no cumpla con los estándares y expectativas.

## 5. Riesgos de Desarrollo

Estos riesgos están relacionados con el equipo de desarrollo y el proceso de creación del software. Incluyen la falta de competencias adecuadas en el equipo, problemas de integración entre diferentes componentes del software y sobrecarga de trabajo que puede llevar al agotamiento del equipo y una disminución en la calidad del trabajo.

- **Falta de competencias en el equipo:** La carencia de habilidades y conocimientos adecuados en el equipo de desarrollo puede resultar en soluciones técnicas deficientes.
- **Problemas de integración:** Las dificultades en la integración de diferentes componentes del software pueden causar retrasos y problemas técnicos.
- **Sobrecarga de trabajo:** La sobrecarga de tareas puede llevar al agotamiento del equipo y disminuir la productividad y calidad del trabajo.

## Identificación y evaluación de riesgos:

| Riesgo  | Categoría  | Probabilidad | Impacto | Estrategia de Abordaje |
|---|------------|--------------|---------|------------------------|
| Ataques de hackers y posibles vulnerabilidades en el sistema y los datos. | Cliente    | Ocasional    | Crítico | Evitar                 |
| Diseño poco intuitivo, interactivo y funcional.                           | Cliente    | Probable     | Medio   | Evitar                 |
| Errores en la planificación y diseño de la arquitectura de software.      | Desarrollo | Ocasional    | Crítico | Evitar                 |
| Crecimiento inesperado de usuarios y datos.                               | Desarrollo | Improbable   | Crítico | Evitar                 |

|   |            |            |         |         |
|---|------------|------------|---------|---------|
| Falta de protección en redes, software sin actualizarse, uso de contraseñas inseguras.  | Tecnología | Probable   | Crítico | Evitar  |
| El sitio web puede sufrir problemas de rendimiento bajo carga elevada, afectando la experiencia del usuario.                      | Producto   | Probable   | Crítico | Evitar  |
| Diseño web no responsivo y falta de pruebas en diferentes dispositivos  | Producto   | Improbable | Medio   | Reducir |
| Falta de una planificación detallada podría llevar a la no consecución de hitos importantes del proyecto.                         | Proceso    | Probable   | Medio   | Evitar  |
| Falta de colaboración efectiva entre los miembros del equipo puede llevar a malentendidos y errores.                              | Proceso    | Ocasional  | Crítico | Evitar  |
| Error en el software, caídas con la conexión a internet, fallos en los servidores donde se almacenan los datos de la facturación. | Tecnología | Ocasional  | Crítico | Evitar  |

## Plan de acción y mitigación de riesgos:

| Riesgo  | Acciones de Mitigación   | Responsable     | Plazo     | Seguimiento (Frecuencia) |
|---|--|-----------------|-----------|--------------------------|
| Ataques de hackers y posibles vulnerabilidades en el sistema y los datos. | Implementar protocolos de seguridad como encriptación y auditorías de seguridad. | Risk Analyst    | 1 semana  | Revisión continua        |
| Diseño poco intuitivo, interactivo y funcional.                           | Mejorar la interfaz y realizar pruebas de usabilidad.                            | Quality Manager | 3 semanas | Revisión mensual         |
| Errores en la planificación y diseño de la arquitectura de software.      | Diseñar una arquitectura modular y probar  | Quality Manager | 1 mes     | Revisión mensual         |

|  |   |                 |           |                     |
|--|---|-----------------|-----------|---------------------|
|  | continuamente la integración.   |                 |           |                     |
| Crecimiento inesperado de usuarios y datos.  | Planificar la integración de tecnologías adecuadas desde el inicio y utilizar infraestructuras en la nube.  | Risk Analyst    | 3 semanas | Revisión trimestral |
| Falta de protección en redes, software sin actualizarse, uso de contraseñas inseguras.                       | Implementar medidas de seguridad robustas (firewalls, cifrado de datos), capacitación de empleados en ciberseguridad, uso de contraseñas fuertes y autenticación de 2 factores. | Risk Analyst    | 1 mes     | Revisión continua   |
| El sitio web puede sufrir problemas de rendimiento bajo carga elevada, afectando la experiencia del usuario. | Realizar auditorías de rendimiento regulares y ajustarse a las mejores prácticas de optimización web.   | Quality Manager | 2 meses   | Revisión semanal    |
| Diseño web no responsivo y falta de pruebas en diferentes dispositivos                                       | Utilizar frameworks de diseño responsivo y realizar pruebas con usuarios reales en diferentes dispositivos.   | Quality Manager | 6 semanas | Revisión trimestral |
| Falta de una planificación detallada podría  | Utilizar metodologías ágiles y  | Project Manager | 1 mes     | Revisión mensual    |

|   |   |                 |           |                    |
|---|---|-----------------|-----------|--------------------|
| llevar a la no consecución de hitos importantes del proyecto.   | herramientas de gestión de proyectos  |                 |           |                    |
| Falta de colaboración efectiva entre los miembros del equipo puede llevar a malentendidos y errores.                              | Fomentar una comunicación abierta y utilizar herramientas colaborativas   | Project Manager | 2 semanas | Revisión continua  |
| Error en el software, caídas con la conexión a internet, fallos en los servidores donde se almacenan los datos de la facturación. | Implementar un sistema de respaldo manual (registro físico o digital alternativo), mantener el software actualizado, realizar copias de seguridad constantes. | Risk Analyst    | 2 meses   | Revisión constante |

## Metodología Ágil: Scrum

Scrum es la mejor metodología ágil para gestionar riesgos en una guardería canina debido a su enfoque en la priorización y adaptabilidad. Permite abordar riesgos en ciclos cortos (sprints), priorizando los más críticos, como los fallos en el sistema de facturación. Su estructura de entrega continua facilita la implementación incremental de controles tecnológicos y la obtención de retroalimentación constante de los usuarios, lo que mejora las soluciones de manera continua.

Además, Scrum ofrece flexibilidad para adaptarse a cambios rápidos en el entorno, crucial en el ámbito de la ciberseguridad, donde las amenazas evolucionan constantemente. Fomenta la colaboración entre equipos multidisciplinarios, asegurando una comprensión integral de los riesgos desde diversas perspectivas. En resumen, Scrum proporciona un marco que garantiza que las soluciones sean relevantes y efectivas ante los desafíos tecnológicos en la guardería.