# Universidad Tecnológica de Morelia - Universidad Tecnológica de Morelia

***Caso de Estudio:***

***Implementación de una Base de Datos Institucional***

MATERIA: ADMINISTRACION DE PROYECTOS

ALUMNO: CARLOS EDUARDO GUIJOSA RAMIREZ

UTM221103TI

9A MATUTINO

PROFESOR: GUSTAVO VENEGAS CONTRERAS

# Tabla de identificacion de riesgos potenciales

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Riesgo Potencial | Tipo | Descripción |
| **R1** | **Diseño incorrecto del modelo Entidad-Relación (ER)** | Técnico | El modelo no representa adecuadamente las reglas del negocio, generando inconsistencias y redundancia de datos. |
| **R2** | **Falta de experiencia del Administrador de Bases de Datos (DBA)** | Humano | El DBA carece de las habilidades necesarias para optimizar el rendimiento, la seguridad y la disponibilidad de la base de datos. |
| **R3** | **Resistencia al cambio por parte del personal administrativo** | Organizacional | Los usuarios finales se oponen a adoptar el nuevo sistema, prefiriendo sus métodos anteriores (hojas de cálculo). |
| **R4** | **Fuga o acceso no autorizado a la información de los estudiantes** | Técnico / Seguridad | Vulnerabilidades en el sistema permiten el robo de datos sensibles como expedientes académicos, información personal o datos de pago. |
| **R5** | **Retrasos en la entrega de hardware o licencias de software** | Externo | Los proveedores no entregan a tiempo los servidores, el software de la base de datos (DBMS) o las licencias necesarias. |
| **R6** | **Disponibilidad limitada del personal clave del proyecto** | Humano | El líder del proyecto, el DBA o los desarrolladores son reasignados a otras tareas o abandonan la universidad, dejando un vacío de conocimiento. |

**¿Qué podría fallar si no se hace bien el modelo ER?**

Un modelo Entidad-Relación (ER) mal diseñado es la base de un sistema deficiente. Las fallas principales serían:

* **Inconsistencia y redundancia de datos:** La misma información podría estar duplicada en diferentes lugares y no coincidir, generando reportes incorrectos.
* **Bajo rendimiento:** Consultas simples podrían volverse lentas y complejas, afectando la experiencia del usuario al inscribirse o consultar calificaciones.
* **Dificultad para el mantenimiento y la escalabilidad:** Agregar nuevas funcionalidades sería muy complicado y costoso, ya que requeriría reestructurar la base del sistema.
* **Pérdida de integridad de los datos:** No se podrían aplicar reglas de negocio esenciales, como impedir que un estudiante se inscriba a una materia sin haber aprobado los prerrequisitos.

**¿Qué pasa si el DBA no tiene suficiente experiencia?**

El rol del DBA es crítico. Si no tiene la experiencia suficiente, las consecuencias directas serían:

* **Configuración deficiente:** La base de datos podría estar mal configurada, llevando a un uso ineficiente de los recursos del servidor y a una lentitud generalizada.
* **Vulnerabilidades de seguridad:** Podría dejar brechas de seguridad abiertas, facilitando accesos no autorizados.
* **Planes de respaldo y recuperación ineficaces:** En caso de un fallo del sistema, la universidad podría perder toda la información por no tener un plan de recuperación probado y funcional.
* **Falta de optimización:** Tareas críticas como la generación de reportes masivos o los procesos de inscripción podrían fallar.

**¿Qué consecuencias tendría una fuga de información?**

Una fuga de información tendría consecuencias graves para la universidad:

* **Legales y financieras:** La institución podría enfrentar demandas millonarias por parte de los afectados y multas por incumplir leyes de protección de datos.
* **Daño reputacional:** La confianza de los estudiantes y futuros aspirantes se vería severamente afectada.
* **Pérdida de confianza interna:** El personal académico y administrativo perdería la confianza en los sistemas de la institución.
* **Consecuencias para los afectados:** Los estudiantes y el personal podrían ser víctimas de robo de identidad, fraude y otros delitos.

**¿Qué dependencias externas podrían afectar el avance?**

Las principales dependencias externas son:

* **Proveedores de hardware y software:** Cualquier retraso en la entrega de servidores o licencias del DBMS paralizaría el proyecto.
* **Servicios de conectividad:** Si el especialista en redes depende de un proveedor de internet o red, cualquier fallo de este tercero afectará el cronograma.
* **Regulaciones gubernamentales:** Un cambio inesperado en la legislación sobre protección de datos podría forzar un rediseño del sistema.
* **Integración con sistemas de terceros:** Si la base de datos debe conectarse a plataformas externas (ej. sistemas de pago), el proyecto dependerá de la disponibilidad de esos proveedores

# Matriz de riegos cualitativa

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| ID | Riesgo Identificado | Tipo | Probabilidad | Impacto | Nivel de Riesgo | Justificación |
| R1 | Diseño incorrecto del modelo ER | Técnico | Media | Alto | Crítico | El equipo es pequeño y la presión del tiempo (4 meses) puede llevar a omitir validaciones. El impacto es alto porque afecta a todo el sistema. |
| R2 | Falta de experiencia del DBA | Humano | Media | Alto | Crítico | Solo hay un DBA. Si su experiencia no es sólida, la seguridad y el rendimiento de toda la base de datos están en juego. |
| R3 | Resistencia al cambio del personal | Organizacional | Alta | Medio | Alto | Es común que los usuarios se resistan a nuevos sistemas. Si no se gestiona, puede llevar al fracaso de la adopción del proyecto. |
| R4 | Fuga de información sensible | Técnico | Baja | Alto | Alto | Siempre existe una probabilidad. El impacto de una fuga de datos estudiantiles es extremadamente alto por las consecuencias legales y de reputación. |
| R5 | Retrasos en entrega de hardware/software | Externo | Media | Medio | Moderado | La dependencia de proveedores es un riesgo común. Puede generar retrasos, pero es gestionable con una buena planificación. |
| R6 | Disponibilidad limitada de personal clave | Humano | Baja | Alto | Alto | Con un equipo tan pequeño, la pérdida de una sola persona (líder o DBA) tendría un impacto muy alto, paralizando el proyecto. |

**1. ¿Cuáles son los 2 riesgos más críticos?**

Con base en la matriz, los dos riesgos más críticos son:

1. **R1: Diseño incorrecto del modelo Entidad-Relación (ER)** (Nivel Crítico)
2. **R2: Falta de experiencia del Administrador de Bases de Datos (DBA)** (Nivel Crítico)

**2. ¿Qué estrategias aplicarías para cada uno?**

* **Para R1 (Diseño incorrecto del modelo ER):** La estrategia es **Mitigar**. No se puede evitar la tarea, pero se puede reducir la probabilidad y el impacto de hacerlo mal.
* **Para R2 (Falta de experiencia del DBA):** La estrategia es **Mitigar**. Se buscará reducir el impacto potencial de la falta de experiencia.

**3. ¿Qué acciones preventivas y correctivas propondrías?**

|  |  |  |
| --- | --- | --- |
| Riesgo Crítico | Acciones Preventivas (Antes de que ocurra) | Acciones Correctivas (Si ocurre) |
| **R1: Diseño incorrecto del modelo ER** | • **Validación por pares:** Involucrar a desarrolladores y al analista en la revisión del modelo ER. • **Creación de prototipos:** Desarrollar y probar un prototipo funcional para validar que el modelo soporta las operaciones clave. • **Documentación exhaustiva:** Documentar cada entidad, atributo y relación. | • **Reingeniería controlada:** Si se detecta un fallo, detener esa parte del desarrollo y asignar al equipo la tarea prioritaria de rediseñar el componente afectado. • **Plan de migración de datos:** Ejecutar un plan para migrar los datos al modelo corregido sin pérdida de información. |
| **R2: Falta de experiencia del DBA** | • **Capacitación y certificación:** Invertir en la capacitación del DBA en el DBMS seleccionado. • **Contratación de consultoría externa:** Contratar a un DBA senior por horas para que audite el diseño y la seguridad. • **Uso de mejores prácticas:** Asegurarse de que el DBA siga las guías de seguridad y rendimiento recomendadas. | • **Asignación de un mentor:** Si se detectan deficiencias, contratar a un consultor externo para que actúe como mentor del DBA. • **Auditoría de emergencia:** Realizar una auditoría completa de la base de datos para identificar y corregir todas las fallas. |

**4. ¿Cómo monitorearías estos riesgos durante el resto del proyecto?**

* **Reuniones de seguimiento semanales:** Dedicar tiempo en cada reunión de equipo para revisar el estado de los riesgos críticos.
* **Hitos de revisión (Gate Reviews):** Establecer puntos de control formales al final de fases clave para presentar evidencia de que el riesgo está controlado.
* **Métricas de rendimiento (para R2):** En el entorno de pruebas, monitorear métricas como el tiempo de respuesta de las consultas y el uso de CPU para detectar problemas de rendimiento.
* **Registro de riesgos (Risk Log):** Mantener un documento vivo donde se registre cada riesgo, su estado actual, las acciones tomadas y el responsable de su seguimiento

# Conclusiones

La gestión de riesgos es fundamental para el éxito de un proyecto de TI. La identificación temprana de amenazas como un diseño de base de datos deficiente o la falta de experiencia en roles clave permite al equipo pasar de una postura reactiva a una **proactiva**. Mediante el uso de herramientas como la matriz de riesgos, es posible **priorizar las amenazas** más graves y enfocar los recursos en mitigarlas eficazmente. Para este caso, asegurar la calidad del modelo de datos y garantizar la competencia del DBA son las dos acciones más importantes que determinarán si el proyecto cumple sus objetivos de crear un sistema robusto, seguro y escalable.