**Plan de Gestión**

**de Riesgos**

**Proyecto web para el registro de actividades clínicas**

***Fecha: [24/10/2023]***

**Tabla de contenido**

Información del Proyecto 3

Categorías de Riesgo 4

Estructura de Desglose de Riesgos (RBS) 5

Definiciones de Probabilidad e Impacto de Riesgos 5

Definiciones de Probabilidad 5

Definiciones de Impacto 6

Matriz de Probabilidad e Impacto 6

Amenazas (Riesgos) 6

Oportunidades 6

Revisión de la tolerancia de los interesados (Stakeholders) 7

Aprobaciones 8

# Información del Proyecto

|  |  |
| --- | --- |
| Empresa / Organización | Universidad Autónoma del Estado de México |
| Proyecto | Proyecto web para el registro de actividades clínicas. |
| Fecha de preparación | 15/8/2023 |
| Cliente | - |
| Patrocinador principal | Universidad Autónoma del Estado de México |
| Gerente de Proyecto | José Mario Martínez Serrato |

# Metodología

|  |
| --- |
| Se empleo la metodología FMEA (Failure Mode and Effective Analysis) donde se toman en cuenta los siguientes puntos:  1. Frecuencia.  2. Gravedad.  3. Detección.  El FMEA es un método cualitativo que establece una lista de fallos, sistemática, con sus consiguientes efectos y puede ser de fácil aplicación para cambios en el diseño o modificaciones de planta. |

# 

# 

# Riesgos del proyecto

|  |
| --- |
| **Riesgos de Seguridad de Datos:**  Brechas de seguridad que exponen información confidencial del paciente.  Acceso no autorizado a datos médicos.  Amenazas de ciberseguridad, como ataques de hackers.  **Riesgos de Privacidad:**  Violaciones de la privacidad del paciente debido a la recopilación y almacenamiento inadecuados de datos personales.  Falta de cumplimiento con regulaciones de privacidad de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea.  **Riesgos Técnicos:**  Problemas de rendimiento, como tiempos de carga lentos o caídas del sistema.  Fallos en la integración de sistemas de salud existentes.  **Riesgos de Usabilidad y Experiencia del Usuario:**  Interfaz de usuario poco intuitiva que dificulta la entrada de datos clínicos.  Falta de formación adecuada del personal para utilizar la plataforma.  **Riesgos de Integridad de Datos:**  Pérdida o corrupción de datos clínicos críticos debido a errores en el sistema o problemas de respaldo.  Falta de procedimientos de recuperación de desastres efectivos.  **Riesgos de Costos y Presupuesto:**  Desviaciones en el presupuesto del proyecto debido a costos imprevistos.  Cambios en los requisitos del proyecto que aumentan los gastos.  **Riesgos de Recursos Humanos:**  Escasez de personal calificado para el desarrollo y mantenimiento del proyecto.  Rotación de personal clave que afecta la continuidad del proyecto.  **Riesgos de Plazos:**  Retrasos en la entrega del proyecto debido a problemas técnicos o cambios en los requisitos. Falta de planificación adecuada que pueda afectar los plazos de implementación.  **Riesgos de Evaluación de Proveedores:**  Problemas con proveedores de servicios, como falta de soporte técnico o incumplimiento de contratos de servicio.  **Riesgos de Reputación:**  Daño a la reputación del hospital, clínica u organización médica si se producen incidentes de seguridad de datos o problemas de calidad del sistema. |

# 

# Definiciones de Frecuencia y Gravedad de Riesgos

## Definiciones de Probabilidad

|  |  |
| --- | --- |
| Muy Alta | Este nivel de riesgo indica una probabilidad extremadamente alta de que ocurra un evento no deseado.  Los impactos pueden ser catastróficos, con consecuencias graves para la seguridad, la salud, el medio ambiente o los activos.  Se requieren medidas inmediatas y drásticas para mitigar o evitar estos riesgos. |
| Alta | En este nivel, el riesgo sigue siendo significativamente elevado, con una probabilidad sustancial de que ocurra un evento no deseado.  Los impactos pueden ser graves y requerir acciones urgentes para reducir el riesgo a niveles más manejables. |
| Media | El nivel de riesgo medio indica una probabilidad moderada de que ocurra un evento no deseado.  Los impactos, aunque no tan graves como en los niveles de riesgo más altos, aún pueden ser significativos.  Se necesitan medidas para gestionar y controlar el riesgo, pero no con la misma urgencia que en niveles más altos. |
| Baja | En este nivel, el riesgo es relativamente bajo, con una probabilidad baja de que ocurra un evento no deseado.  Los impactos son generalmente menores y pueden manejarse de manera efectiva con medidas de control y seguimiento adecuadas. |
| Muy Baja | El riesgo es extremadamente bajo en este nivel, con una probabilidad prácticamente nula de que ocurra un evento no deseado.  Los impactos, si ocurren, son insignificantes o prácticamente inexistentes. |

## 

## Detección de Impacto

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Objetivo de Proyecto | Muy bajo (0,05) | Bajo  (0,10) | Medio (0,20) | Alto  (0,40) | Muy Alto (0,80) |
| Riesgos de Seguridad de Datos |  |  | X |  |  |
| Riesgos de Privacidad |  |  | X |  |  |
| Riesgos de Usabilidad y Experiencia del Usuario |  |  | X |  |  |
| Riesgos de Integridad de Datos |  |  |  | X |  |
| Riesgos de Costos y Presupuesto |  | X |  |  |  |
| Riesgos de Recursos Humanos |  | X |  |  |  |
| Riesgos de Plazos |  | X |  |  |  |
| Riesgos de Evaluación de Proveedores |  |  | X |  |  |
| Riesgos de Reputación | X |  |  |  |  |

# 

|  |  |
| --- | --- |
| Riesgo | Nomenclatura |
| Riesgos de Seguridad de Datos |  |
| Riesgos de Privacidad |  |
| Riesgos de Usabilidad y Experiencia del Usuario |  |
| Riesgos de Integridad de Datos |  |
| Riesgos de Costos y Presupuesto |  |
| Riesgos de Recursos Humanos |  |
| Riesgos de Plazos |  |
| Riesgos de Evaluación de Proveedores |  |
| Riesgos de Reputación |  |

# Matriz de Probabilidad e Impacto

## Amenazas (Riesgos)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Gravedad  Frecuencia | | Muy Bajo | Bajo | Medio | | Alto | | Muy Alto |
| 0,05 | 0,10 | 0,20 | | 0,40 | | 0,80 |
| Muy Alta | 0,90 |  |  |  | |  | |  |
| Alta | 0,70 |  |  |  | |  | |  |
| Media | 0,50 |  |  |  | |  |  |  |
| Baja | 0,30 |  |  |  |  |  | |  |
| Muy Baja | 0,10 |  |  |  | |  | |  |

# 

# Mitigación de daño

|  |  |
| --- | --- |
| Riesgos | Mitigaciones |
| Riesgos de Seguridad de Datos | Acceso restringido y controlado: Implementa un sistema de autenticación sólido para asegurarte de que solo el personal autorizado pueda acceder a la plataforma.  Almacenamiento seguro de datos: Almacena datos clínicos en servidores seguros con copias de seguridad regulares. Implementa medidas de seguridad física en los centros de datos. |
| Riesgos de Privacidad | Política de contraseñas seguras: Exige contraseñas fuertes y de larga duración para todos los usuarios. Fomenta la rotación regular de contraseñas. |
| Riesgos de Usabilidad y Experiencia del Usuario | Investigación de usuario: Realiza investigaciones de usuario para comprender las necesidades y expectativas de los usuarios finales, incluyendo médicos, enfermeros y personal clínico. Obtén retroalimentación regular durante el desarrollo.  Diseño centrado en el usuario: Diseña la interfaz de usuario y la navegación de la plataforma de manera intuitiva y fácil de usar, considerando las habilidades y necesidades de los usuarios clínicos. |
| Riesgos de Integridad de Datos | Auditorías de seguridad regulares: Realiza auditorías de seguridad regulares para identificar vulnerabilidades y debilidades en la infraestructura de seguridad.  Cumplimiento normativo: Asegúrate de cumplir con todas las regulaciones de privacidad de la información médica. |
| Riesgos de Costos y Presupuesto | Revisión continua del presupuesto: Lleva a cabo revisiones regulares del presupuesto a lo largo del proyecto para evaluar y ajustar los costos en función del progreso y posibles cambios en los requerimientos. |
| Riesgos de Recursos Humanos | Contar con personal extra: Siempre contar con un excedente pequeño de personal capacitado para poder manejar el control de citas en caso de que los encargados no se encuentren por algún motivo. |
| Riesgos de Plazos | Monitorear las actividades de manera periódica:  Al hacer el monitoreo de las actividades se puede percatar de que alguna de las actividades no se está cumpliendo en el plazo establecido y corregir antes de que esta actividad ralentice las que la precedan. |
|  | Transferencias |
| Riesgos de Evaluación de Proveedores | Tener proveedores extra: Contar con al menos un proveedor extra para satisfacer las necesidades si el proveedor primario falle. |
|  | Asume |
| Riesgos de Reputación | Se asume el riesgo de reputación. |

# Aprobaciones

|  |  |  |
| --- | --- | --- |
| **Aprobador** | **Fecha** | **Firma** |
| José Mario Martínez Serrato | 12/102023 |  |
| Josué Garatachia Mejía | 12/10/2023 |  |
|  |  |  |
|  |  |  |