**Plan de Gestión**

**de Riesgos**

***FenrirCyberWolf $5.773.806***

***Fecha: [03/09/2002]***

**Tabla de contenido**

Información del Proyecto 3

Metodología 3

Roles y Responsabilidades 3

Presupuesto 4

Calendario 4

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

Formatos de los Informes 7

Seguimiento 7

Aprobaciones 8

**Información del Proyecto**

| Empresa / Organización | Info Shield Analytics |
| --- | --- |
| Proyecto | FenrirCyberWolf |
| Fecha de preparación | 03-09-2024 |
| Cliente | **Grupo GTD** |
| Patrocinador principal | Jorge Vita Haeussler |
| Gerente de Proyecto | Juan Manuel Casanueva |

**Metodología**

| La gestión de riesgos es fundamental para asegurar el éxito del proyecto de integración de la ciencia de datos en la ciberseguridad (FenrirCyberWolf). A continuación se presenta la estructura que seguiremos para desarrollar el plan de gestión de riesgo efectivo:  1.- Identificación de Riesgos:   * Técnicas: Utilizar sesiones de lluvia de ideas, entrevistas con expertos y análisis de documentación previa para identificar posibles riesgos. * Categorías: Clasificar los riesgos en diferentes categorías, como técnicos, operativos, financieros y de cumplimiento.   2.- Análisis de Riesgos   * Evaluación de Impacto: Para cada riesgo identificado, evaluar su impacto potencial en el proyecto (alto, medio, bajo) * Probabilidad de Ocurrencia: Estimar la probabilidad de que cada riesgo ocurra (alta, media, baja) * Matriz de Riesgos: Crear una matriz para visualizar la relación entre la probabilidad y el impacto, lo que ayudará a priorizar los riesgos.   3.- Planificación de Respuesta a los Riesgos:   * Estrategias de respuesta: Definir acciones específicas para cada riesgo, que pueden incluir:   + Evitar: Cambiar el plan para eliminar el riesgo.   + Mitigar: Implementar acciones para reducir la probabilidad o el impacto del riesgo.   + Transferir: Pasar el riesgo a un tercero (por ejemplo, mediante seguros o subcontrataciones)   + Aceptar: Reconocer el riesgo y planificar su monitoreo. * Desarrollo de un Plan de Acción: Para cada riesgo, detallar las acciones específicas, responsable y plazos.   4.- Monitoreo y Control de Riesgos:   * Revisiones Periódicas: Establecer reuniones regulares para revisar el estado de los riesgos y la efectividad de las respuestas implementadas. * Actualización de la Matriz de Riesgos: Revisar y actualizar la matriz de riesgos conforme avanza el proyecto y se identifican nuevos riesgos. * Documentación: Mantener un registro detallado de todos los riesgos, sus evaluaciones y las acciones tomadas.   5.- Comunicación de Riesgos:   * Informes a Stakeholders: Establecer un plan de comunicación para informar a los interesados sobre el estado de los riesgos y las acciones de mitigación. * Cultura de Riesgos: Fomentar una cultura de identificación y gestión de riesgos dentro del proyecto, alentando a todos a reportar problemas y preocupaciones. |
| --- |

**Roles y Responsabilidades**

| 1. Project Manager (PM)  Responsabilidades:   * Planificar, ejecutar y cerrar el proyecto. * Coordinar todas las actividades del equipo y asegurar que se cumplan los plazos. * Gestionar la comunicación con los stakeholders y reportar el progreso del proyecto. * Supervisar la gestión de riesgos y asegurar la implementación de acciones correctivas.   2. Scrum Master   * Responsabilidades: * Facilitar las reuniones diarias, revisiones y retrospectivas del equipo. * Ayudar al equipo a seguir los principios ágiles y eliminar obstáculos que impidan el progreso. * Fomentar la colaboración y la mejora continua dentro del equipo.   3. Product Owner  Responsabilidades:   * Definir y priorizar el backlog del proyecto. * Actuar como el enlace entre el equipo y los stakeholders, asegurando que se alineen los objetivos del proyecto. * Tomar decisiones sobre el alcance y las características del producto.   4. Data Scientist  Responsabilidades:   * Recopilar, limpiar y preparar los datos para el análisis. * Desarrollar y validar modelos de aprendizaje automático para la detección de amenazas. * Interpretar los resultados y traducirlos en recomendaciones prácticas.   5. Analista de Datos  Responsabilidades:   * Realizar análisis exploratorio de datos para identificar patrones y tendencias. * Colaborar con el Data Scientist en la visualización de datos y la interpretación de resultados. * Documentar hallazgos y crear informes para el equipo y los stakeholders.   6. Ingeniero de Datos  Responsabilidades:   * Diseñar y mantener la infraestructura necesaria para la recopilación y almacenamiento de datos. * Implementar procesos de ETL (extracción, transformación y carga) para asegurar la calidad de los datos. * Colaborar con el Data Scientist y el Analista de Datos en la integración y acceso a los datos.   7. Especialista en Ciberseguridad  Responsabilidades:   * Evaluar riesgos de ciberseguridad asociados al proyecto. * Proporcionar orientación sobre prácticas y normativas de seguridad. * Desarrollar estrategias para mitigar riesgos identificados.   8. Gestor de Riesgos  Responsabilidades:   * Identificar, analizar y documentar riesgos potenciales del proyecto. * Desarrollar y supervisar la implementación de planes de mitigación. |
| --- |

**Presupuesto**

| El presupuesto total del proyecto es de $23.095.227 el cual utilizaremos $5.773.806 que fue el dinero destinado a la caja chica para sustentar estos tipos de inconvenientes |
| --- |

**Calendario**

| **Semana 1-2: Inicio y Preparación del Proyecto (12 - 25 de agosto)**   * **Actividades:**   + Definir el alcance del plan de gestión de riesgos.   + Identificar los roles y responsabilidades del equipo.   + Configurar herramientas de seguimiento y control de riesgos. * **Entregables:**   + Acta de constitución del proyecto.   + Asignación de responsabilidades.   **Semana 3-4: Identificación de Riesgos (26 de agosto - 8 de septiembre)**   * **Actividades:**   + Reuniones de identificación de riesgos con los equipos clave (ciencia de datos, ciberseguridad, desarrollo).   + Crear una lista inicial de riesgos.   + Documentar los riesgos identificados, sus causas y efectos. * **Entregables:**   + Registro inicial de riesgos.   **Semana 5-6: Análisis y Priorización de Riesgos (9 - 22 de septiembre)**   * **Actividades:**   + Evaluar la probabilidad y el impacto de cada riesgo.   + Clasificar los riesgos según su nivel de criticidad.   + Priorizar los riesgos más importantes que requieren atención inmediata. * **Entregables:**   + Matriz de probabilidad e impacto de riesgos.   + Lista priorizada de riesgos críticos.   **Semana 7-8: Planificación de Respuesta a los Riesgos (23 de septiembre - 6 de octubre)**   * **Actividades:**   + Desarrollar estrategias para mitigar, evitar, transferir o aceptar cada riesgo.   + Establecer planes de contingencia para los riesgos críticos.   + Asignar responsables para implementar las respuestas a los riesgos. * **Entregables:**   + Plan de respuesta a los riesgos.   **Semana 9-10: Implementación de las Estrategias de Mitigación (7 - 20 de octubre)**   * **Actividades:**   + Ejecutar las estrategias de mitigación según el plan.   + Implementar controles de seguridad y procesos de monitoreo.   + Asegurar que los equipos asignados lleven a cabo las acciones necesarias. * **Entregables:**   + Estrategias de mitigación implementadas.   **Semana 11-12: Monitoreo y Control de Riesgos (21 de octubre - 3 de noviembre)**   * **Actividades:**   + Monitorear continuamente los riesgos y la efectividad de las medidas implementadas.   + Actualizar el registro de riesgos y ajustar las estrategias según sea necesario.   + Realizar reuniones periódicas para evaluar el estado de los riesgos. * **Entregables:**   + Informes de monitoreo de riesgos.   + Ajustes al plan de mitigación según resultados.   **Semana 13-14: Auditorías y Revisiones (4 - 17 de noviembre)**   * **Actividades:**   + Realizar auditorías internas para evaluar el cumplimiento de las estrategias de mitigación.   + Revisar los controles de seguridad implementados.   + Ajustar las medidas de control según las auditorías. * **Entregables:**   + Informes de auditoría de seguridad.   **Semana 15-16: Evaluación Final de Riesgos (18 de noviembre - 1 de diciembre)**   * **Actividades:**   + Evaluar los riesgos que aún persisten o han cambiado a lo largo del proyecto.   + Realizar ajustes finales en las estrategias de respuesta.   + Asegurar que los riesgos críticos se hayan mitigado eficazmente. * **Entregables:**   + Evaluación final del estado de los riesgos.   **Semana 17: Preparación del Informe Final (2 - 8 de diciembre)**   * **Actividades:**   + Compilar todos los resultados y lecciones aprendidas en un informe final.   + Preparar un resumen ejecutivo para los interesados clave.   + Proporcionar recomendaciones para la gestión de riesgos futuros. * **Entregables:**   + Informe final de gestión de riesgos.   **Semana 18: Cierre del Proyecto (9 - 15 de diciembre)**   * **Actividades:**   + Cierre formal del plan de gestión de riesgos.   + Reunión final con los interesados para presentar los resultados.   + Asegurar la transferencia de responsabilidades para la gestión continua de riesgos. * **Entregables:**   + Cierre del proyecto y transferencia de responsabilidades. |
| --- |

**Categorías de Riesgo**

| Categorías:   * Riesgos Técnicos. * Riesgos de Tiempo y Costos. * Riesgos de seguridad. * Riesgos Externos. * Riesgos de Calidad. * Riesgos de gestión. |
| --- |

**Estructura de Desglose de Riesgos (RBS)**

| 1. Amenazas de Seguridad de la Información   1.1 Alto índice de falsos positivos y negativos  1.1.1 Generación de alertas incorrectas sobre actividades normales   * Riesgo asociado: Las alertas incorrectas pueden llevar a la falta de respuesta adecuada ante eventos verdaderamente importantes.   1.1.2 Desensibilización hacia alertas legítimas   * Riesgo asociado: Puede causar que el personal ignore o minimice alertas válidas, aumentando la posibilidad de incidentes graves.   1.2 Fuga de datos  1.2.1 Pérdida de confidencialidad   * Riesgo asociado: Información sensible puede ser expuesta a personas no autorizadas, afectando la privacidad y la seguridad.   1.2.2 Uso malintencionado de datos   * Riesgo asociado: Los datos comprometidos pueden ser utilizados para actividades fraudulentas o perjudiciales. |
| --- |

**Definiciones de Probabilidad e Impacto de Riesgos**

**Definiciones de Probabilidad**

| Muy Alta | Indica que un evento tiene una probabilidad extremadamente alta de ocurrir, generalmente superior al 80-90%. Es casi seguro que sucederá |
| --- | --- |
| Alta | Refleja una probabilidad equilibrada de que un evento ocurra, generalmente entre el 60% y el 80%.Aunque no es seguro, es muy probable. |
| Media | Representa una probabilidad equilibrada de que un evento ocurra, generalmente entre el 40% y el 60%. Hay una posibilidad igual de que ocurra o no. |
| Baja | Señala que la probabilidad de que un evento ocurra es baja, típicamente entre el 20% y el 40%. Es poco probable que suceda, pero no imposible. |
| Muy Baja | Indica que un evento tiene una probabilidad extremadamente baja de ocurrir, generalmente por debajo del 20%. Es muy poco probable que suceda. |

**Definiciones de Impacto**

| Objetivo de Proyecto | Muy bajo (0,05) | Bajo  (0,10) | Medio (0,20) | Alto  (0,40) | Muy Alto (0,80) |
| --- | --- | --- | --- | --- | --- |
| Alcance |  |  |  |  |  |
| Cronograma |  |  |  |  |  |
| Costo |  |  |  |  |  |
| Calidad |  |  |  |  |  |

**Matriz de Probabilidad e Impacto**

**Amenazas (Riesgos)**

| Impacto  Probabilidad | | Muy Bajo | Bajo | Medio | Alto | Muy Alto |
| --- | --- | --- | --- | --- | --- | --- |
| 0,05 | 0,10 | 0,20 | 0,40 | 0,80 |
| Muy Alta | 0,90 | 0,045 | 0,09 | 0,18 | 0,36 | 0,72 |
| Alta | 0,70 | 0,035 | 0,07 | 0,14 | 0,28 | 0,56 |
| Media | 0,50 | 0,025 | 0,05 | 0,10 | 0,20 | 0,40 |
| Baja | 0,30 | 0,015 | 0,03 | 0,06 | 0,12 | 0,24 |
| Muy Baja | 0,10 | 0,005 | 0,01 | 0,02 | 0,04 | 0,08 |

**Generación de alertas incorrectas sobre actividades normales**

* **Probabilidad**: Alta (0.70) **Impacto**: Bajo (0.10) **Riesgo**: 0.70×0.10=0.070.

**Desensibilización hacia alertas legítimas**

* **Probabilidad**: Media (0.50) **Impacto**: Alto (0.40) **Riesgo**:0.50×0.40=0.20

**Pérdida de confidencialidad**

* **Probabilidad**: Baja (0.30) **Impacto**: Muy Alto (0.80) **Riesgo**:0.30×0.80=0.24

**Uso malintencionado de datos**

* **Probabilidad**: Muy Baja (0.10) **Impacto**: Muy Alto (0.80) **Riesgo**: 0.10×0.80=0.08

**Oportunidades**

| Impacto  Probabilidad | | Muy Alto | Alto | Medio | Bajo | Muy Bajo |
| --- | --- | --- | --- | --- | --- | --- |
| 0,05 | 0,10 | 0,20 | 0,40 | 0,80 |
| Muy Alta | 0,90 | 0,72 | 0,36 | 0,18 | 0,09 | 0,045 |
| Alta | 0,70 | 0,56 | 0,28 | 0,14 | 0,07 | 0,035 |
| Media | 0,50 | 0,40 | 0,20 | 0,10 | 0,05 | 0,025 |
| Baja | 0,30 | 0,24 | 0,12 | 0,06 | 0,03 | 0,015 |
| Muy Baja | 0,10 | 0,08 | 0,04 | 0,02 | 0,01 | 0,005 |

**Revisión de la tolerancia de los interesados (Stakeholders)**

|  |
| --- |

**Formatos de los Informes**

| * 1. Introducción   + Breve descripción del proyecto.   + Objetivos del informe. * 2. Identificación de KRI   + Definición de KRI.   + Importancia de los KRI en la gestión de riesgos. * 3. KRI Seleccionados   + Lista de KRI específicos utilizados en el proyecto.   + Justificación de la selección de cada KRI. * 4. Metodología de Monitoreo   + Herramientas y técnicas utilizadas para monitorear los KRI.   + Frecuencia de monitoreo. * 5. Resultados de los KRI   + Presentación de los datos recopilados.   + Análisis de los resultados.   + Comparación con los umbrales establecidos. * 6. Interpretación de Resultados   + Impacto de los resultados en el proyecto.   + Identificación de tendencias y patrones. * 7. Acciones Correctivas   + Medidas tomadas en respuesta a los resultados de los KRI.   + Planes de acción futuros. * 8. Conclusiones y Recomendaciones   + Resumen de los hallazgos clave.   + Recomendaciones para mejorar la gestión de riesgos en futuros proyectos. * 9. Anexos   + Gráficos y tablas de datos.   + Documentación adicional relevante. |
| --- |
|  |

**Seguimiento**

| El seguimiento de los riesgos se realizará mediante la monitorización continua de los Key Risk Indicators (KRI) definidos. Se utilizarán herramientas de software para recopilar y analizar datos periódicamente. Los resultados se compararán con los umbrales establecidos para identificar desviaciones. Se realizarán reuniones regulares del equipo para revisar los riesgos y actualizar el plan de mitigación según sea necesario. Los informes de seguimiento se generarán mensualmente y se compartirán con todas las partes interesadas. Además, se implementarán auditorías internas para asegurar la efectividad de las medidas de mitigación. |
| --- |

**Aprobaciones**

| **Aprobador** | **Fecha** | **Firma** |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |