

**PROGRAMA DE ESTUDIO DE ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN**

**PLAN DE GESTIÓN DE RIESGOS Y CONTINGENCIA, APLICANDO LA METODOLOGÍA MAGERIT EN EL ISTRFA**

**INTEGRANTES**

Collantes Portilla Candy

Montalván Pintado Edilsa

Nanfuñay Carrión Javier

Neyra Quesquen Renzo

**Chiclayo, Mayo del 2023**

INDICE

[INTRODUCCIÓN 1](#_Toc135752454)

[I. NOMBRE DEL PROYECTO: 2](#_Toc135752455)

[II. DEFINICIÓN DEL PROBLEMA O NECESIDAD DEL NEGOCIO 2](#_Toc135752456)

[III. OBJETIVOS 3](#_Toc135752457)

[3.1. OBJETIVOS DEL NEGOCIO 3](#_Toc135752458)

[3.1.1. OBJETIVO GENERAL: 3](#_Toc135752459)

[3.1.2. OBJETIVOS ESPECÍFICOS: 3](#_Toc135752460)

[3.2. OBJETIVOS DEL PROYECTO 3](#_Toc135752461)

[3.2.1. OBJETIVO GENERAL 3](#_Toc135752462)

[3.2.2. OBJETIVOS ESPECÍFICOS 4](#_Toc135752463)

[IV. ALINEAMIENTO CON PLAN ESTRATÉGICO DEL NEGOCIO 4](#_Toc135752464)

[V. ETAPAS Y ACTIVIDADES CONTEMPLADAS EN EL PROYECTO 6](#_Toc135752465)

[VI. ALCANCE DEL PROYECTO 7](#_Toc135752466)

[VII. NORMAS Y REFERENCIAS 8](#_Toc135752467)

[7.1. Disposiciones legales y normas aplicadas. 8](#_Toc135752468)

[7.2. Métodos, herramientas y prototipos 9](#_Toc135752469)

[7.2.1. Métodos y herramientas: 9](#_Toc135752470)

[7.2.2. Modelos y recursos. 10](#_Toc135752471)

# INTRODUCCIÓN

El Instituto Superior Tecnológico República Federal de Alemania (ISTRFA) se encuentra en constante búsqueda de mejoras en la gestión de la seguridad de la información y la protección de su infraestructura y sus activos. Con el fin de fortalecer su enfoque en la gestión de riesgos, se ha propuesto la implementación de un Plan de Gestión de Riesgos basado en la reconocida metodología MAGERIT.

Este proyecto tiene como objetivo principal desarrollar e implementar un plan integral que permita identificar, evaluar y gestionar los riesgos asociados a los procesos, sistemas y activos tecnológicos del ISTRFA. La metodología MAGERIT proporcionará un marco estructurado para llevar a cabo este proceso, garantizando una comprensión clara de los riesgos y su impacto potencial en el instituto.

A través de la aplicación de este plan, se espera lograr una gestión más efectiva de los riesgos, mejorando la capacidad de respuesta frente a posibles amenazas y minimizando los impactos negativos en las operaciones del ISTRFA. Además, se promoverá una cultura de seguridad sólida, involucrando a todo el personal y fomentando buenas prácticas en la gestión de riesgos.

El presente informe detallará los pasos a seguir, las etapas de implementación y los recursos necesarios para llevar a cabo este plan de gestión de riesgos en el ISTRFA. Se espera que los resultados obtenidos fortalezcan la seguridad y la confiabilidad de las operaciones, contribuyendo al logro de los objetivos estratégicos del instituto.

# NOMBRE DEL PROYECTO:

PLAN DE GESTIÓN DE RIESGOS Y CONTINGENCIA, APLICANDO LA METODOLOGÍA MAGERIT EN EL ISTRFA.

# DEFINICIÓN DEL PROBLEMA O NECESIDAD DEL NEGOCIO

El problema o necesidad del negocio que motiva la implementación de este plan de gestión de riesgos puede estar relacionado con la falta de un enfoque sistemático y estructurado para identificar, evaluar y gestionar los riesgos en el ámbito tecnológico y de seguridad de la información del instituto.

Algunos elementos específicos que podrían considerarse en la definición del problema o necesidad del negocio son:

1. Riesgos no identificados o subestimados: Puede haber una falta de conciencia o conocimiento sobre los riesgos potenciales asociados con los activos tecnológicos y los procesos del instituto. Esto podría llevar a una subestimación de los riesgos y, por lo tanto, a una falta de medidas preventivas y de respuesta adecuadas.

Por lo tanto, el proyecto permitirá identificar y evaluar los riesgos asociados a los activos de la institución, como sistemas de información, infraestructura de red, bases de datos y equipos. Al gestionar adecuadamente estos riesgos, se protegerá la integridad, disponibilidad y confidencialidad de los activos, evitando posibles pérdidas financieras, daños reputacionales y violaciones de la privacidad.

1. Brechas en la seguridad: Podría haber vulnerabilidades o deficiencias en los sistemas de seguridad existentes, lo que puede facilitar la explotación de amenazas y la ocurrencia de incidentes de seguridad. Esto podría poner en riesgo la integridad, disponibilidad y confidencialidad de los datos y activos del instituto.

La implementación de un plan de gestión de riesgos fomenta una cultura de seguridad dentro del instituto. Al involucrar a todo el personal en el proceso de identificación y mitigación de riesgos, promoviendo la conciencia y responsabilidad compartida en la protección de los activos y la información. Esto contribuye a la creación de un entorno seguro y confiable para estudiantes, personal y colaboradores del instituto.

1. Cumplimiento normativo insuficiente: El instituto puede estar enfrentando desafíos para cumplir con las regulaciones y normativas relevantes en materia de seguridad y protección de datos.

Realizar el presente proyecto ayudaría a alinear al Instituto con las regulaciones y normativas en materia de seguridad y protección de datos. Esto garantiza que el instituto cumpla con las obligaciones legales y normativas, evitando sanciones y posibles consecuencias legales.

# OBJETIVOS

## OBJETIVOS DEL NEGOCIO

### OBJETIVO GENERAL:

Fomentar la excelencia en la enseñanza, investigación y práctica académica para brindar una educación de calidad y formar profesionales altamente competentes en sus respectivas disciplinas

### OBJETIVOS ESPECÍFICOS:

* Establecer y fortalecer alianzas estratégicas con empresas, organizaciones y la comunidad local, para fomentar la transferencia de conocimientos, la colaboración en proyectos conjuntos y el apoyo mutuo en la formación de estudiantes y el desarrollo de proyectos de impacto social
* Promover la innovación, la investigación aplicada y el desarrollo tecnológico en áreas relevantes, fomentando la adopción de tecnologías emergentes y preparando a los estudiantes para enfrentar los desafíos del mundo laboral en constante evolución.
* Implementar procesos de aseguramiento de la calidad en todos los aspectos del funcionamiento del instituto, incluyendo la mejora continua de los programas académicos, la infraestructura, los servicios y la satisfacción de los estudiantes y demás partes interesadas.
* Promover la inclusión, la equidad y la diversidad en el acceso a la educación, garantizando que todos los estudiantes tengan igualdad de oportunidades para desarrollar su potencial académico y personal, sin importar su origen, género o cualquier otra característica personal.
* Fomentar la internacionalización de la institución a través de colaboraciones académicas, intercambios estudiantiles y programas de movilidad, para brindar a los estudiantes una perspectiva global y fortalecer la reputación del instituto a nivel internacional.

## OBJETIVOS DEL PROYECTO

### OBJETIVO GENERAL

Implementar un plan de gestión de riesgos utilizando la metodología MAGERIT en el ISTRFA, con el fin de proteger los activos tecnológicos, garantizar la continuidad de las actividades educativas y fortalecer la formación de profesionales altamente competentes en sus respectivas disciplinas.

### OBJETIVOS ESPECÍFICOS

* Identificar y analizar los activos tecnológicos críticos del instituto, incluyendo sistemas de información, infraestructura de red, bases de datos y otros recursos relevantes
* Realizar una evaluación exhaustiva de los riesgos asociados con cada uno de los activos identificados, considerando posibles amenazas, vulnerabilidades y el impacto que podrían tener en la integridad, disponibilidad y confidencialidad de la información
* Diseñar e implementar medidas preventivas para mitigarlos riesgos identificados, priorizando aquellos con mayor impacto y probabilidad de ocurrencia.
* Establecer un plan de respuesta ante incidentes que permita detectar, responder y recuperarse de manera efectiva ante posibles eventos de seguridad o interrupciones en los servicios tecnológicos.
* Capacitar al personal del instituto en temas de seguridad de la información y concientizar sobre las mejores prácticas para evitar incidentes de seguridad y proteger los activos tecnológicos.
* Establecer un proceso de revisión y mejora continua del plan de gestión de riesgos, asegurando que se adapte a los cambios tecnológicos, normativos y a las nuevas amenazas emergentes.
* Evaluar regularmente los resultados y beneficios del plan de gestión de riesgos, midiendo la efectividad de las acciones implementadas y su impacto en la reducción de riesgos y la protección de los activos del instituto.

# ALINEAMIENTO CON PLAN ESTRATÉGICO DEL NEGOCIO

Fomentar la excelencia en la enseñanza, investigación y práctica académica: Al proteger los activos tecnológicos y garantizar la continuidad de las actividades educativas, el proyecto contribuye a brindar una educación de calidad y formar profesionales altamente competentes en sus respectivas disciplinas.

Establecer y fortalecer alianzas estratégicas: Al identificar y gestionar los riesgos en el ámbito tecnológico y de seguridad de la información, el proyecto promueve la transferencia de conocimientos y la colaboración en proyectos conjuntos con empresas, organizaciones y la comunidad local. Esto fortalece las alianzas estratégicas y apoya la formación de estudiantes y el desarrollo de proyectos de impacto social.

Promover la innovación y el desarrollo tecnológico: Al mitigar los riesgos asociados a los activos tecnológicos, el proyecto fomenta la adopción de tecnologías emergentes y prepara a los estudiantes para enfrentar los desafíos del mundo laboral en constante evolución. Esto contribuye a la promoción de la innovación, la investigación aplicada y el desarrollo tecnológico en áreas relevantes.

Implementar procesos de aseguramiento de la calidad: Al identificar y gestionar los riesgos de manera efectiva, el proyecto busca implementar procesos de aseguramiento de la calidad en todos los aspectos del funcionamiento del instituto. Esto incluye la mejora continua de los programas académicos, la infraestructura, los servicios y la satisfacción de los estudiantes y demás partes interesadas.

Promover la inclusión, la equidad y la diversidad: Al proteger los activos tecnológicos y garantizar la seguridad de la información, el proyecto contribuye a crear un entorno seguro y confiable para todos los estudiantes, independientemente de su origen, género u otras características personales. Esto promueve la inclusión, la equidad y la diversidad en el acceso a la educación y brinda igualdad de oportunidades para desarrollar el potencial académico y personal de los estudiantes.

Fomentar la internacionalización: Al implementar un plan de gestión de riesgos y contingencia, el proyecto contribuye a fortalecer la reputación del instituto a nivel internacional. Esto se logra mediante colaboraciones académicas, intercambios estudiantiles y programas de movilidad, que brindan a los estudiantes una perspectiva global y promueven la internacionalización de la institución.

# ETAPAS Y ACTIVIDADES CONTEMPLADAS EN EL PROYECTO

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Grupo** | | | **Organización de Recursos TI** | | | | | | | | | | | **2023** | |
| **N°** | **Actividades** | **Mayo** | | | | | **Junio** | | | | **Julio** | | | | |
| **Meses - Semanas** | **1** | | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | | **4** |
| **1** | **Determinar los activos** |  | |  | **x** | **x** | **x** | **x** | **x** |  |  |  |  | |  |
| **2** | **Determinar las amenazas** |  | |  |  |  | **x** | **x** | **x** | **x** |  |  |  | |  |
| **3** | **Determinar riesgos** |  | |  |  |  | **x** | **x** | **x** | **x** |  |  |  | |  |
| **4** | **Determinar salvaguardias** |  | |  |  |  |  |  |  | **x** | **x** | **x** | **x** | |  |
| **5** | **Determinar riesgo residual** |  | |  |  |  |  |  |  |  |  | **x** | **x** | | **x** |

# ALCANCE DEL PROYECTO

El proyecto tiene como objetivo principal implementar un Plan de Gestión de Riesgos basado en la metodología MAGERIT en el Instituto Superior Tecnológico República Federal de Alemania. El enfoque estará en identificar y mitigar los riesgos asociados a los activos tecnológicos críticos, con el fin de fortalecer la formación de profesionales competentes y garantizar la calidad educativa en el instituto.

**Entregables:**

a) Documento del Plan de Gestión de Riesgos: Un documento detallado que describa las estrategias, acciones y procedimientos para gestionar los riesgos tecnológicos en el instituto.

b) Evaluación de riesgos: Un informe que identifique y evalúe los riesgos asociados a los activos tecnológicos críticos.

c) Plan de respuesta ante incidentes: Un plan que defina las medidas y procedimientos para detectar, responder y recuperarse de posibles incidentes de seguridad.

d) Programa de capacitación en seguridad: Un programa de capacitación diseñado para promover una cultura de seguridad y conciencia de riesgos entre el personal y los estudiantes.

**Características de los entregables:**

Los entregables serán documentos escritos que estarán basados en la metodología MAGERIT. Serán claros, concisos y estarán estructurados de manera lógica, proporcionando detalles y orientación para la gestión de riesgos tecnológicos.

**Criterios de aceptación:**

a) Los entregables deben estar completos y cumplir con los requisitos establecidos en el alcance del proyecto.

b) Los entregables deben ser revisados y aprobados por el comité responsable de la gestión de riesgos del instituto.

c) Los entregables deben ser comprensibles y aplicables para el personal y los responsables de la gestión de riesgos del instituto.

**Restricciones:**

a) El proyecto estará limitado por el presupuesto asignado y los recursos disponibles para la implementación del plan.

b) El proyecto deberá completarse dentro de un marco de tiempo específico, considerando los plazos establecidos por la dirección del instituto.

**Supuestos:**

a) Se asume que se contarán con los recursos necesarios, incluyendo personal capacitado y acceso a información relevante para llevar a cabo la gestión de riesgos.

b) Se asume que el personal y los responsables involucrados en el proyecto estarán comprometidos y participarán activamente en la implementación del plan.

**Exclusiones:**

a) El proyecto no abarcará la gestión de riesgos no relacionados con los activos tecnológicos del instituto.

b) El proyecto no se encargará de la implementación directa de medidas de seguridad, sino que se centrará en el diseño y desarrollo del plan de gestión de riesgos.

# NORMAS Y REFERENCIAS

## Disposiciones legales y normas aplicadas.

**Normas y estándares:**

Norma Técnica Peruana ISO/IEC 27001: Norma que establece los requisitos para la gestión de seguridad de la información.

Norma Técnica Peruana ISO/IEC 31000: Norma que brinda directrices para la gestión de riesgos.

Norma Técnica Peruana ISO/IEC 27005: Norma que proporciona directrices para la gestión de riesgos de seguridad de la información.

MAGERIT: Metodología de análisis y gestión de riesgos de seguridad de la información desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, adaptada y aplicada en el contexto peruano.

**Legislación y regulaciones:**

Ley de Protección de Datos Personales: Legislación que establece los principios y requisitos para la protección de datos personales.

Ley Nº 29783, Ley de Seguridad y Salud en el Trabajo: Legislación que establece los lineamientos para la gestión de riesgos laborales.

Normativas sectoriales: Cualquier normativa específica relacionada con la gestión de riesgos y seguridad de la información en el sector educativo o tecnológico en Perú.

**Documentos internos del instituto:**

Políticas y procedimientos internos: Documentos establecidos por el Instituto Superior Tecnológico República Federal de Alemania que abordan la gestión de riesgos, seguridad de la información y protección de activos tecnológicos en el contexto peruano.

**Mejores prácticas y guías de referencia:**

Guías de la Autoridad de Protección de Datos Personales: Recursos proporcionados por la autoridad competente en materia de protección de datos personales.

Guías específicas de adaptación de MAGERIT para Perú: Recursos adicionales proporcionados por organizaciones o expertos peruanos que adapten la metodología MAGERIT al contexto peruano.

## Métodos, herramientas y prototipos

### Métodos y herramientas:

**Métodos:**

Determinación de activos: En esta etapa se establece el contexto del proyecto, se definen los objetivos y se identifican los activos de información relevantes.

Determinar amenazas: En esta etapa se identifican las amenazas y vulnerabilidades que podrían afectar los activos de información, se evalúa el impacto potencial y se determina la probabilidad de ocurrencia de los riesgos.

Determinación de riesgos: Se priorizan los riesgos identificados en función de su impacto y probabilidad, lo que permite establecer las acciones de mitigación más adecuadas.

Determinar salvaguardas: En esta etapa se desarrollan las estrategias y medidas de mitigación para reducir los riesgos identificados. Esto implica la implementación de controles de seguridad, la asignación de responsabilidades y la definición de planes de acción.

Determinar el riesgo residual: Se establecen mecanismos de monitoreo y revisión continua para garantizar que los controles implementados sean efectivos y se adapten a los cambios en el entorno tecnológico.

**Herramientas:**

Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas): Este modelo te ayudará a identificar y evaluar los factores internos y externos que pueden afectar el instituto. Analizar las fortalezas y debilidades internas te permitirá identificar los riesgos potenciales, mientras que identificar las oportunidades y amenazas externas te ayudará a anticipar posibles situaciones de riesgo.

Matriz de riesgos: Una matriz de riesgos es una herramienta visual que te permite identificar y clasificar los diferentes riesgos asociados con el funcionamiento del instituto. Puedes evaluar la probabilidad de ocurrencia de cada riesgo y su impacto potencial en el instituto. Esto te permitirá priorizar los riesgos y asignar recursos de manera adecuada para su mitigación.

Análisis de causas y efectos: Utilizando técnicas como el diagrama de Ishikawa (también conocido como "espina de pescado" o "diagrama de causa y efecto"), podrás identificar las posibles causas de los riesgos y comprender mejor sus efectos potenciales en el instituto. Esto te ayudará a diseñar estrategias de mitigación más efectivas.

Herramientas de gestión de riesgos: Para la gestión efectiva de los riesgos identificados, se emplearán herramientas que permitan documentar, monitorear y controlar las acciones tomadas. Estas herramientas facilitarán el seguimiento de las medidas de mitigación implementadas, así como la actualización continua de la información relacionada con los riesgos.

### Modelos y recursos.

**Análisis FODA:**

Entrevistas o encuestas a personal docente, administrativo y estudiantes para identificar fortalezas, debilidades, oportunidades y amenazas.

Revisión de informes internos y externos sobre el rendimiento académico, la satisfacción de los estudiantes, la competencia en el mercado, etc.

Análisis de datos demográficos y tendencias educativas para identificar oportunidades y amenazas a largo plazo.

**Matriz de riesgos:**

Plantillas de matriz de riesgos que te permitan clasificar los riesgos según su probabilidad e impacto.

Sesiones de trabajo con equipos multidisciplinarios para identificar y evaluar los riesgos.

Información histórica sobre incidentes previos y problemas recurrentes en el instituto.

**Análisis de causas y efectos:**

Técnicas de lluvia de ideas (brainstorming) para identificar posibles causas de los riesgos.

Diagramas de Ishikawa o diagramas de causa y efecto para visualizar las causas potenciales de los riesgos.

Entrevistas o grupos de enfoque con personas clave para obtener información sobre las posibles causas y efectos.

**Planificación de contingencias:**

Plantillas de planes de contingencia que te guíen en la identificación de acciones y recursos necesarios.

Recursos financieros asignados para hacer frente a situaciones de emergencia.

Lista de contactos de proveedores, personal de emergencia y otros recursos externos relevantes.