UNIVERSIDAD ESTATAL PENÍNSULA
DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TÍTULO DEL TRABAJO DE TITULACIÓN

PROPUESTA DE UN MODELO DE MEJORA CONTINUA PARA LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN A UNA INSTITUCIÓN EDUCATIVA PRIVADA MEDIANTE EL CICLO CAP-DO

AUTOR

RODRÍGUEZ MONTAÑO JAIME JOEL

MODALIDAD DE TITULACIÓN

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en

INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

ING. WALTER OROZCO IGUASNIA

Santa Elena, Ecuador

Año 2023

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez A., Mgtr.
DIRECTOR DE LA CARRERA

Ing. Walter Orozco I., Mgt.
TUTOR

Ing. Lídice Haz López, Mgt.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel S., Mgti.
DOCENTE GUÍA UIC

UPSE

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por RODRÍGUEZ MONTAÑO JAIME JOEL, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 17 días del mes de febrero del año 2023.

TUTOR

ING. WALTER OROZCO IGUASNIA

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Jaime Joel Rodríguez Montaño**

DECLARO QUE:

El trabajo de Titulación, "**Propuesta de un modelo de mejora continua para la gestión de riesgos de la seguridad de la información a una institución educativa privada mediante el ciclo CAP-Do**", previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 17 días del mes de febrero del año 2023.

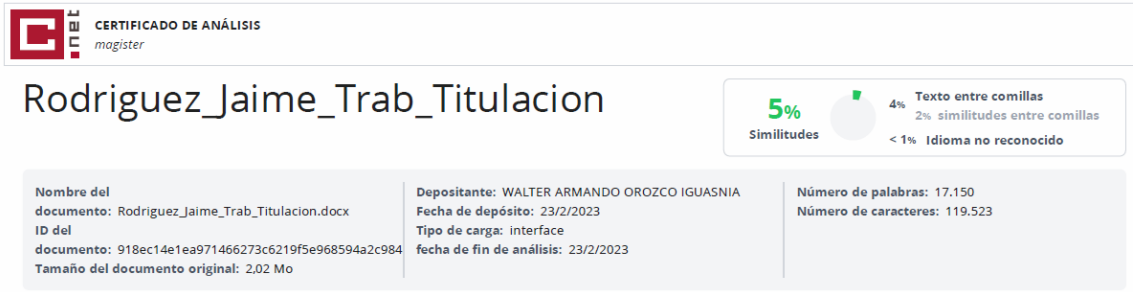
EL AUTOR

Jaime Joel rodríguez Montaño

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado "Propuesta de un modelo de mejora continua para la gestión de riesgos de la seguridad de la información a una institución educativa privada mediante el ciclo CAP-Do", presentado por el estudiante Jaime Joel Rodríguez Montaño fue enviado al Sistema Antiplagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.



CERTIFICADO DE ANÁLISIS
magister

Rodriguez_Jaime_Trab_Titulacion

5% Similitudes

4% Texto entre comillas
2% similitudes entre comillas
< 1% Idioma no reconocido

Nombre del documento: Rodriguez_Jaime_Trab_Titulacion.docx
ID del documento: 918ec14e1ea971466273c6219f5e968594a2c984
Tamaño del documento original: 2,02 Mo

Depositante: WALTER ARMANDO OROZCO IGUASNIA
Fecha de depósito: 23/2/2023
Tipo de carga: interface
fecha de fin de análisis: 23/2/2023

Número de palabras: 17.150
Número de caracteres: 119.523

TUTOR

Ing. Walter Orozco Iguasnia

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **Jaime Joel Rodríguez Montaño**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales de artículo profesional de alto nivel con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

Santa Elena, a los 17 días del mes de febrero del año 2023.

EL AUTOR

Jaime Joel Rodríguez Montaño

AGRADECIMIENTO

Agradezco primero a Dios que me ha guiado en la vida y me ha dado fortalezas para poder culminar con esta investigación. A mis queridos padres y hermanas por siempre darme fuerzas, motivación y palabras de aliento, sobre todo a mí amada madre por enseñarme que todo se consigue bajo esfuerzo y sacrificio. A mis compañeros y amigos que hice en el proceso académico con los que pude compartir conocimientos, risas, alegrías y tristezas y a todas las personas que me dieron su apoyo y buenas vibras, apoyándome a que mi sueño se haga realidad. Gracias a todos.

Jaime Joel Rodríguez Montaño

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍTEM DESCRIPCIÓN PÁGINA

ÍNDICE DE TABLAS

ÍTEM DESCRIPCIÓN PÁGINA

LISTA DE ANEXOS

RESUMEN

La seguridad de la información es un componente importante del plan de seguridad de cualquier institución. Las instituciones almacenan una gran cantidad de datos confidenciales, como información de los estudiantes y registros escolares. No obstante, esta creciente dependencia de la tecnología en el entorno educativo genera que las instituciones sean vulnerables a riesgos de seguridad de la información, tales como: acceso no autorizado a datos confidenciales de estudiantes o profesores, la introducción de software malicioso, violaciones de datos, ataques de phishing, entre otros. Las consecuencias de esta brecha de seguridad pueden incluir datos perdidos o robados, pérdidas financieras, interrupción de servicios y daños a la reputación. Para solucionar el problema mencionado se propuso diseñar una guía de gestión de riesgos en la institución objeto de estudio empleando la metodología CAP-Do. La primera etapa se centró en realizar un estudio comparativo de metodologías de gestión de riesgos. En la segunda etapa se realizó la identificación de los activos de la información. Para esto, se hizo un levantamiento de la información mediante de técnicas de recolección de información como encuestas y entrevistas a la Alta gerencia de la organización. En la tercera etapa se diseñó una guía aplicable en la institución. La cuarta etapa correspondió a la generación de reportes, empleando un dashboard analítico sobre las métricas de riesgos detectadas en el análisis previo. En este proyecto, la herramienta empleada fue Power BI, caracterizada por los procesos relacionados con el análisis de bases de datos y su posterior modelado. En este punto es donde se evaluaron los indicadores clave de riesgos encontrados durante el proceso de análisis de riesgos en la institución objeto de estudio. Entre los resultados esperados se encuentran: un análisis de las métricas de riesgo, controles de seguridad y un dashboard analítico relacionado a la gestión de riesgos.

Palabras claves: análisis de riesgos, CAP-Do, seguridad de la información.

ABSTRACT

Information security is an important component of any institution's security plan. Institutions store a large amount of sensitive data, such as student information and school records. However, this growing dependence on technology in the educational environment makes institutions vulnerable to information security risks, such as: unauthorized access to confidential student or teacher data, the introduction of malicious software, data breaches, phishing attacks, among others. The consequences of this security breach can include lost or stolen data, financial loss, service interruption, and reputational damage. To solve the aforementioned problem, it was proposed to design a risk management guide in the institution under study using the CAP-Do methodology. The first stage focused on carrying out a comparative study of risk management methodologies. In the second stage, the identification of information assets was carried out. For this, a survey of the information was carried out through information gathering techniques such as surveys and interviews with the organization's Senior Management. In the third stage, a guide applicable in the institution was designed. The fourth stage corresponded to the generation of reports, using an analytical dashboard on the risk metrics detected in the previous analysis. In this project, the tool used was Power BI, characterized by the processes related to the analysis of databases and their subsequent modeling. It is at this point that the key risk indicators found during the risk analysis process in the institution under study were evaluated. Among the expected results are an analysis of risk metrics, security controls and an analytical dashboard related to risk management.

Keywords: risk analysis, CAP-Do, information security.

INTRODUCCIÓN

La seguridad de la información es de suma importancia en las instituciones, ya que almacenan y administran una gran cantidad de datos confidenciales, como información personal de estudiantes y personal, información financiera y registros académicos. A medida que las escuelas confían cada vez más en los sistemas digitales, aumenta el riesgo de una brecha de seguridad, con el potencial de causar interrupciones y daños significativos. Sin las medidas de seguridad adecuadas, se puede acceder fácilmente a estos datos y utilizarlos de forma indebida, lo que lleva al robo de identidad, fraude financiero u otras actividades maliciosas.

En la institución objeto de estudio existen diversos riesgos, tales como: la inexistencia de procedimientos de seguridad adecuados, riesgos de que la información sensible de la institución puede ser vulnerada o compartida con personas no autorizadas, entre otros. Los ataques cibernéticos también son una preocupación, ya que los actores maliciosos pueden intentar obtener acceso a las redes o sistemas escolares para interrumpir las operaciones, robar datos o incluso obtener acceso a los registros de los estudiantes. Por esta razón, se propone diseñar una guía de análisis de riesgos mediante un estudio comparativo para gestionar la toma de decisiones de políticas de seguridad de la información en una institución educativa privada.

Entre los trabajos previos relacionados a esta propuesta resalta “Desarrollo de un Modelo de Gestión de Riesgos Según la Norma UNE ISO 31000 para el Tratamiento de Reclamaciones en Edificación”, donde se analiza la implantación conjunta de normas para la gestión de riesgo. Otro trabajo es " Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala ", que consistió en diseñar un plan de seguridad para llevar los riesgos a niveles aceptables.

El trabajo de titulación se estructura en dos capítulos detallados a continuación:

En el primer capítulo se describen de forma detalladas cuáles son los antecedentes que permiten aplicar la propuesta en la institución, abarcando así, los principales problemas

que se deben resolver. Además, se detallan los objetivos, así como la justificación y metodología a emplear, siendo esta CAP-Do.

En el segundo y último capítulo ya se establece el proceso a emplear, que va desde la comparación de metodologías de gestión de riesgos e identificación de los activos de información de la institución, hasta el análisis de métricas de riesgos, mediante un dashboard analítico realizado en Power BI, detectadas durante el análisis de riesgos en la institución de esta manera, CAP-Do se divide en cuatro etapas. En la primera se procede a realizar un estudio comparativo entre las siguientes metodologías de gestión de riesgos. La segunda involucra analizar los riesgos de la información, es decir, identificar amenazas y vulnerabilidades mediante un inventario y valoración de activos en la institución. La tercera se centra en la selección de controles adecuados para la institución y la última etapa abarca la presentación de las soluciones encontradas durante la elaboración de la propuesta.

CAPÍTULO I

1. Fundamentación

1.1. Antecedentes

Los datos son importantes porque ayudan a las organizaciones a tomar decisiones informadas, sin embargo, la información también conlleva riesgos. Las organizaciones deben ser conscientes de estos riesgos y tomar medidas para proteger sus datos. Los riesgos asociados con la importancia de la información pueden incluir la pérdida de valor si la información no se protege adecuadamente, o si se accede a ella y se usa sin permiso. Además, si la información se divulga al público sin el contexto adecuado, podría malinterpretarse o usarse de una manera que sea dañina para el individuo o la organización, más aún, cuando garantizar un nivel de protección total es imposible [1].

Los servicios de TI están sujetos a una variedad de riesgos, esto incluye los riesgos de información. Según el artículo "Metodología y gobierno de la gestión de riesgos de tecnologías de la información" publicado en la revista UNIANDES, "es frecuente que empresas de diversos sectores económicos reporten pérdidas debido a fallas y/o ataques sobre sus servicios de TI, los cuales afectan seriamente su reputación y su solidez financiera y operacional" [2]. Por esta razón, se espera que aumenten los ataques a los servicios y sistemas de TI, particularmente aquellos que explotan vulnerabilidades y aquellos que se originan dentro de la organización.

Bajo este contexto resalta la institución objeto de estudio. Esta institución educativa privada fue creada en el año 1988. Está conformada por un centro especializado para Educación Inicial y un Bachillerato de Inclusión, además, cuenta con un departamento técnico, siendo este, el responsable del mantenimiento del sitio web de la institución. Este departamento también gestiona el desarrollo y mantenimiento de las aplicaciones de software utilizadas en el sitio web.

Mediante una observación en la institución (Ver Anexo 1) se pudo determinar que, en el departamento técnico, hay una variedad de herramientas y equipos que se utilizan para diferentes tareas. Algunas de las herramientas y equipos más comunes incluyen:

computadoras, software, impresoras y escáneres. No obstante, existe el riesgo de que estos puedan estar en riesgo de quedar obsoletos si no pueden equipararse a las tendencias actuales. También, en el caso de recortes presupuestarios, se puede dificultar la compra de nuevos equipos o mantenerse al día con las últimas tecnologías.

Además de lo mencionado, si no existen los procedimientos de seguridad adecuados, la información sensible de la institución puede ser vulnerada o compartida con personas no autorizadas. Esto también podría conllevar a la institución a problemas como multas u otras sanciones. Por ende, si se brinda un servicio deficiente relacionado a las páginas y servicios de la institución o se brinda información incorrecta, se podría dañar la reputación de esta.

Para seguir abordando esta situación, se realizó una entrevista al encargado del departamento técnico (Ver Anexo 2) donde se determinó cómo es el funcionamiento de los servicios de TI que se brindan en la institución. Aparte de la página central que posee la institución, se brindan otros servicios como un entorno virtual de aprendizaje (EVA) y un espacio de trabajo para las tareas estudiantiles. Descrito esto anteriormente, la capacitación constante de los encargados del funcionamiento de estas plataformas debe ser adecuada y constante, caso contrario, se puede generar una violación de datos sensibles, confidenciales o personales sin autorización.

Al realizar una revisión de trabajos alineados a esta propuesta, resaltan soluciones que emplean determinados estándares para el análisis de riesgos de la información como ISO 31000 y Octave, para abordar soluciones orientadas a la mejora de la seguridad de los sistemas, aumento de la confianza de las partes interesadas, e incluso, reducir los costes de seguridad.

Un trabajo que resalta a nivel mundial es “Desarrollo de un Modelo de Gestión de Riesgos Según la Norma UNE ISO 31000 para el Tratamiento de Reclamaciones en Edificación”, desarrollado en la Universidad de Sevilla, España. En esta propuesta se “analiza se propone la implantación de un modelo de gestión de riesgos basado en normas internacionales adaptado al sector de la edificación” [3]. La limitante recae en que no se realiza un análisis detallado mediante la clasificación de amenazas y vulnerabilidades.

Con respecto al ámbito regional sobresale “Implementación de un Sistema de Gestión de Riesgos basados en el estándar ISO 31000 en el proceso de Atención de Requerimientos de la empresa Software Enterprise Services en la ciudad de Lima – 2018”, desarrollado en la Universidad Tecnológica de Perú. Este trabajo “consistió en implementar controles para la empresa, adaptándolos a su necesidad, para cumplir objetivos como la reducción del impacto de los riesgos que se presentan en determinados procesos” [4]. Aunque se realizó una implementación de controles de un estándar definido, no se garantiza la confidencialidad, integridad y disponibilidad del proceso debido a que no se ejecutan todos los controles del estándar.

En el ámbito local resalta “Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala” de la Universidad Politécnica Salesiana, con sede en Cuenca. En este trabajo “se diseña un plan de seguridad, aplicando la metodología Magerit, para llevar a los riesgos a niveles aceptables” [5]. Las limitantes de esta propuesta se centran en que no se abordan problemáticas como el control de cambios tecnológicos ni soluciones relacionadas a la reducción de costos de seguridad de la información.

En conclusión, en los trabajos expuestos anteriormente, si bien no abordan todos los controles en las instituciones donde se ejecutan los estándares definidos, existen restricciones generadas al no haber una comunicación directa con la parte administrativa, o Alta Gerencia, es decir, no existe una reportería eficaz que aborde los riesgos de la seguridad de la información. En el actual trabajo propuesto, además, de emplear una herramienta analítica para lograr una comunicación adecuada sobre los riesgos y vulnerabilidades de información que existen, se pretende diseñar una guía mediante un estudio comparativo de estas, abordando así, diferentes controles que logren describir de forma detallada los riesgos de información de la institución objeto de estudio.

1.2. Descripción del proyecto

Existen varios riesgos de seguridad de la información a los que se enfrentan las empresas y organizaciones en la actualidad [6]. Uno de los riesgos más comunes son las filtraciones de datos, que pueden ocurrir cuando se divulga información confidencial a personas no autorizadas. Las violaciones de datos pueden ocurrir a través de piratería, malware, phishing o ingeniería social. Otro riesgo común es la pérdida de datos, que puede ocurrir cuando los datos se eliminan accidental o intencionalmente [7]. Ante tal situación, se propone diseñar una guía en una institución educativa mediante un estudio comparativo de metodologías de gestión de riesgos para la seguridad de la información.

Este proyecto se divide en cuatro etapas según la metodología CAP-Do:

1. Recopilación de la información de metodologías de gestión de riesgos.
2. Identificación de activos de información.
3. Selección de controles.
4. Creación de reportes.

Recopilación de la información de metodologías de gestión de riesgos: Se realiza una revisión bibliográfica exhaustiva sobre metodologías relacionadas a la gestión de riesgos, verificando de esta manera, cómo se realizan funciones como: el mapeo de riesgos, la evaluación de riesgos y la mitigación de riesgos.

Las metodologías para comparar son las siguientes:

- ISO 31000:2018
- CRAMM (Método de Análisis y Gestión de Riesgos CCTA)
- Octave (Evaluación Operativa Crítica de Amenazas, de Activos y de Vulnerabilidad)
- Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Este estudio comparativo proporciona un enfoque estructurado para identificar, evaluar y prevenir los riesgos de la institución objeto de estudio, ayudando así, a que se puedan tomar decisiones informadas sobre cómo asignar recursos para gestionar los riesgos de manera eficaz. De esta manera, las metodologías de gestión de riesgos pueden ayudar a la institución a comparar su desempeño y sus prácticas de gestión de riesgos con las de otras instituciones.

Identificación de los activos de información: Se realiza el levantamiento de información en la institución, mediante entrevistas a los miembros de la Alta Gerencia en la institución, en base a aspectos de seguridad de la información. Así, se logrará la identificación eficaz de los activos de información que se posee la institución educativa.

Además, se emplean herramientas como matriz de probabilidad de impacto para identificar vulnerabilidades mediante un inventario y valoración de activos, y también, verificar la seguridad de la institución en torno a los criterios de confidencialidad, integridad y disponibilidad de la institución.

También, se emplean análisis como PESTEL y FODA, desde una perspectiva educacional, para describir el entorno de la institución, tanto interno como externo, identificando así, cuál es la situación actual con respecto a la seguridad de la información.

Selección de controles: Se establece una guía de gestión de riesgos aplicable en la institución en base a los controles seleccionados tras la comparativa de metodologías en la primera fase.

En esta fase se incluyen la identificación y priorización de riesgos, el análisis de riesgos para determinar su posible impacto y probabilidad, y el diseño de estrategias para prevenir esos riesgos. Así, se garantiza que solo se consideren los riesgos más significativos para un análisis posterior y la toma de decisiones en la institución.

Creación de reportes: Para posibilitar una mejor comprensión de la información obtenida, se realiza un dashboard analítico en Power BI enfocándose en algunas métricas de riesgo de la institución, comunicando así, los resultados de la investigación.

Esta propuesta no abarca una certificación de una determinada metodología como tal, no obstante, se centra en el planteamiento de una solución en seguridad de la información en base a los lineamientos obtenidos tras realizar una comparativa de metodologías para la gestión de riesgos.

Una de las tecnologías analíticas empleada es la siguiente:

- **Power BI:** Herramienta analítica empleada para la generación de reportes [8].

Este proyecto contribuye a la línea de investigación "Tecnología y Sistemas de la Información (TSI)" en las organizaciones y en la sociedad [9].

1.3. Objetivos

1.3.1. Objetivo general

Realizar un análisis de riesgos mediante un estudio comparativo para gestionar la toma de decisiones de políticas de seguridad de la información en una institución educativa privada.

1.3.2. Objetivos específicos

- Realizar un levantamiento de información sobre las metodologías de gestión de riesgos para identificar las mejores prácticas en la seguridad de la información.
- Establecer los activos relevantes de la institución mediante un diagnóstico del estado actual de la seguridad de la información.
- Identificar las principales métricas de riesgos para gestionar la seguridad de la información en la institución.

1.4. Justificación

La importancia de aplicar los estándares de seguridad de la información es que proporcionan un lenguaje y un marco comunes para que las empresas, organizaciones o instituciones los utilicen al desarrollar sus propias políticas de seguridad. Al tener un conjunto de estándares a seguir, las empresas pueden crear políticas que sean integrales y efectivas, para que, quienes se beneficien de estas, puedan entender fácilmente. Además, al aplicar estos estándares, las empresas pueden demostrar a los reguladores que se toman en serio la protección de datos confidenciales [10].

Desde una perspectiva social, esto ayuda a garantizar la confidencialidad de la información, de modo que solo las personas autorizadas puedan acceder a ella. Adicionalmente, la seguridad de la información puede ayudar a proteger la integridad de la información, para que no sea modificada o destruida sin autorización. Mediante el uso de estándares de seguridad de la información, las organizaciones pueden mejorar su postura de seguridad, proteger mejor sus activos y facilitar la respuesta y la recuperación de incidentes de seguridad. Además, los estándares de seguridad de la información pueden ayudar a las organizaciones a administrar el riesgo, garantizar el cumplimiento y mejorar su postura de seguridad general [11].

La institución educativa privada, al aplicar una guía acorde a sus lineamientos y funcionamiento administrativo, obtiene beneficios como mejorar la postura de seguridad proporcionando una línea de base para los controles de seguridad. La parte más importante de la seguridad de la infraestructura es tener una comprensión clara de las amenazas y vulnerabilidades que existen, y tener un plan para evitar o eliminar esas amenazas.

Otro beneficio recae en facilitar la gestión de riesgos y los esfuerzos de cumplimiento. Una forma de lograr esto es desarrollar e implementar políticas y procedimientos que ayuden a identificar y gestionar los riesgos. Otra manera consiste es brindar capacitación a los empleados sobre cómo identificar y prevenir los riesgos. Además, la institución puede desarrollar controles internos para ayudar a garantizar el cumplimiento de las leyes y reglamentos.

Por otro lado, al emplear herramientas analíticas se permite mejorar la comunicación y la colaboración entre las partes interesadas en la seguridad. Al existir una relación entre el análisis y la gestión de riesgos de TI, esto contribuye a identificar y diagnosticar problemas con los sistemas y redes de la institución. Por ende, un análisis pertinente puede ayudar a la institución a evaluar y monitorear su infraestructura de TI y su rendimiento para realizar mejoras. Además, el análisis puede proporcionar a los encargados del departamento técnico los datos y la información necesarios para identificar problemas y optimizar los sistemas.

El tema propuesto está alineado a los objetivos del Plan de Creación de Oportunidades 2021-2025, específicamente al siguiente eje:

Eje 2.- Eje social.

Objetivo 5.- Proteger a las familias, garantizar sus derechos y servicios, erradicar la pobreza y promover la inclusión social [12].

Política 5.5.- Mejorar la conectividad digital y el acceso a nuevas tecnologías de la población [12].

1.5. Metodología

1.5.1. Metodología de la investigación

Con la finalidad de identificar los métodos y técnicas de investigación más apropiados a utilizar para recopilar los datos necesarios durante la gestión de seguridad de la información, se procede a utilizar una investigación de carácter exploratorio. Este tipo de investigación se centra en "examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes" [13]. Para esto, se realiza una investigación exhaustiva sobre los principales estándares sobre seguridad de la información, abarcando una comparación de estos, y así, diseñar una guía acorde a la institución.

Se aplica, también, una metodología de investigación diagnóstica [13], cuyo propósito es ahondar sobre un problema o situación con el fin de obtener una mejor comprensión del problema a estudiar. Esta metodología se emplea mediante una entrevista dirigida al encargado del departamento técnico de la institución para detallar cómo es el funcionamiento de este y cuáles son los servicios con los que cuenta.

1.5.2. Grupo poblacional involucrado

La población que comprende esta propuesta se conforma por beneficiarios directos e indirectos. En cuanto a los beneficiarios directos, estos corresponden a quienes se encuentran dentro del Departamento Técnico de la institución, mientras que, en los indirectos resaltan tanto los demás departamentos como los estudiantes.

Según la información recopilada en la entrevista (Ver Anexo 2), se establecen los siguientes beneficiarios:

Beneficiarios	**Cantidad**
Directos	
Departamento Técnico	2
Indirectos	
Dpto. Planificación Estratégica	1
Dpto. Asesoría Jurídica	1
Dpto. Talento Humano	1
Dpto. Secretaría General	1
Docentes	32
Estudiantes	650
Total	688

Tabla 1. Grupo poblacional involucrado.

Así, el beneficiario directo de este proyecto es el Departamento técnico de la institución, el mismo que cuenta con una cantidad de dos personas encargadas. Por otro lado, los beneficiarios indirectos, tales como docentes y estudiantes, cubren una cifra de 686 personas.

1.5.3. Metodología de recolección de información

Para el desarrollo de esta propuesta se emplean tres técnicas de recolección de información:

- **Observación:** En esta técnica los investigadores "utilizan un conjunto predeterminado de criterios para registrar datos" [14].
- **Entrevista (aplicada a los directivos de la institución):** Esta técnica consiste en "realizar una entrevista a una persona o grupo con el fin de obtener información" [15].
- **Encuesta (aplicada a docentes de la institución):** Esta técnica generalmente se refiere a "un estudio en el que se le pregunta a un grupo de personas su opinión sobre un tema en particular" [16]. En este caso, la población total de directivos y docentes es de 30.

1.5.4. Análisis de las técnicas de recolección de información empleadas

La técnica de observación (Ver Anexo 1) permitió analizar directamente el comportamiento y las operaciones relacionados con la gestión de riesgos de la institución con énfasis en los objetos y sistemas utilizados, lo que contribuyó a identificar posibles riesgos potenciales. En este caso, se constató la existencia de un departamento técnico, el cual, es el encargado de abordar lo referente a los riesgos.

Este departamento es responsable de analizar los riesgos potenciales asociados a nuevos productos y tecnologías empleadas en la institución. Además, se encarga de analizar y evaluar los riesgos asociados a las operaciones de la institución. El departamento técnico evalúa estos riesgos y brinda recomendaciones a la gerencia sobre cómo evitar estos riesgos. También, monitorea los cambios en el entorno de riesgo y mantiene a los administradores de la institución al tanto de los riesgos nuevos o emergentes.

En cuanto a la entrevista (Ver Anexo 2) se pudo determinar cómo es el manejo de la seguridad de la información en la institución objeto de estudio, así como, las medidas tomadas al afrontar determinadas amenazas informáticas. Entre los hallazgos obtenidos a raíz de esta técnica están:

- No se emplea una metodología específica para el manejo de los riesgos, así, al no estar al tanto de los posibles problemas que podrían surgir, esto causaría consecuencias negativas más adelante. Además, no analizar los riesgos puede conducir a una mala toma de decisiones y a una falta de comprensión sobre cómo tratar ciertos problemas en caso de que surjan.
- No existe una priorización de los riesgos, por ende, al no tener una identificación de estos, las operaciones y/o actividades realizadas dentro de la institución podría retrasarse, o peor aún, suspenderse, generando incluso, pérdidas económicas.
- No se cuenta con un plan de contingencia para lidiar con eventos inesperados y minimizar el impacto de los riesgos.
- Los riesgos no son monitoreados de una forma adecuada. Si los riesgos no se controlan, es difícil saber si están aumentando o disminuyendo. Además, se vuelve más difícil tomar acciones correctivas si es necesario. Finalmente, el impacto global de los riesgos puede ser mayor que si fueran monitoreados.

Con respecto a la encuesta (Ver Anexo 3) se evidenció lo siguiente:

- No existen conocimientos por parte del personal de la institución sobre la existencia de políticas y los procedimientos relacionados a la gestión de riesgos, lo cuales, son importantes para salvaguardar los activos de información dentro de la institución.
- No existe una comprensión adecuada sobre metodologías de riesgos que permita a la institución tomar decisiones informadas sobre cómo protegerse mejor de los riesgos potenciales.
- No se ha establecido una clasificación de datos adecuada, lo que podría generar consecuencias que van desde filtraciones de datos hasta daños a la reputación de la institución y responsabilidades legales.

1.5.5. Variable del proyecto

Para esta propuesta es el marco de tiempo para las actividades de gestión de riesgos la variable empleada donde se realiza una estimación de esta luego de aplicar la guía propuesta en la institución objeto de estudio.

Variable	Definición conceptual	Indicador	Método de medición
Marco de tiempo para las actividades de gestión de riesgos	Es el plazo establecido para llevar a cabo las actividades relacionadas a la gestión de riesgos.	Marco de tiempo para las actividades de gestión de riesgos	Días.

Tabla 2. Variable del proyecto.

En el cuadro anterior destaca que para medir este indicador y, determinar los cambios luego de realizar el estudio de esta propuesta tecnológica, es el número de días.

1.5.6. Metodología de desarrollo del proyecto

Esta propuesta se centra en realizar un estudio comparativo entre metodologías de seguridad de gestión de riesgos de la información. Dado esto, la metodología a aplicar será CAP-Do [17], una variante el enfoque PDCA [18], el cual consiste en las siguientes etapas:

- Primera etapa: Chequear.
- Segunda etapa: Analizar.
- Tercera etapa: Planear.
- Cuarta etapa: Hacer.

Primera etapa. – La finalidad de esta etapa es identificar un problema conciso sobre la seguridad de la información en la institución. Para esto, se procede a realizar un estudio comparativo entre las siguientes metodologías de gestión de riesgos:

- ISO 31000: 2018
- CRAMM (Método de Análisis y Gestión de Riesgos CCTA)
- Octave (Evaluación Operativa Crítica de Amenazas, de Activos y de Vulnerabilidad)
- Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Segunda etapa. – El objetivo de esta etapa es analizar los riesgos de la información, es decir, identificar vulnerabilidades mediante un inventario y valoración de activos en la institución, por esta razón, algunas de las herramientas a emplear son las siguientes:

- Diagramas causa-efecto
- Matriz de riesgos
- Análisis FODA [19]
- Análisis PESTEL [20]

Tercera etapa. – En esta etapa se establecen los controles pertinentes alineados con la institución, los cuales, permitirán implantar determinadas soluciones y las respectivas actividades complementarias que solventen un adecuado manejo de la seguridad de la información dentro de la institución.

Cuarta etapa. – La finalidad de esta etapa abarca la presentación de las soluciones encontradas durante la elaboración de la propuesta. Para esto, se emplea un dashboard analítico que permitirá comunicar de forma eficaz los resultados de la investigación mediante un resumen de información importante para la alta gerencia de la institución.

Mediante esta metodología se podrá identificar, evaluar y controlar los riesgos asociados con las actividades dentro de la institución. CAP-Do también ofrece una serie de

características para ayudar a las partes interesadas a tomar decisiones más informadas y mejorar la eficacia de la gestión de riesgos.

CAPÍTULO II

2. Propuesta

2.1. Marco contextual

2.1.1. Objeto de estudio

La institución objeto de estudio fue creada en el año 1988. Está conformada por un centro especializado para Educación Inicial y un Bachillerato de Inclusión, además, cuenta con un departamento técnico, siendo este, el responsable del mantenimiento del sitio web de la institución. Este departamento también gestiona el desarrollo y mantenimiento de las aplicaciones de software utilizadas en el sitio web.

2.1.2. Tratamiento de la información en las instituciones educativas

El tratamiento de datos personales en el sector educativo es legítimo cuando se realiza de conformidad con las leyes y reglamentos aplicables. Esto incluye las leyes relacionadas con la protección de datos, la seguridad de los datos y la privacidad de los estudiantes. A lo largo de la LOEI y la Ley Orgánica de Educación Superior (LOES) se puede observar que los centros de educación se encuentran legitimados para recopilar y tratar los datos personales de sus estudiantes, para a su vez ser enviados al Ministerio de Educación en el ejercicio de la función educativa [21].

2.1.3. Ley Orgánica de Protección de Datos Personales

De acuerdo con marco legal ecuatoriano, existe la Ley Orgánica de Protección de Datos Personales cuyo objetivo es “garantizar el ejercicio del derecho a la protección de datos

personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección. Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones […]" [22].

Con respecto a la seguridad de datos personales, los responsables de tratar los datos deberán tomar en cuenta [22]:

- Las categorías y volumen de datos personales.
- El estado de la técnica.
- Mejores prácticas de seguridad integral.
- Los costos de aplicación de acuerdo con la naturaleza, alcance, contexto.
- Los fines del tratamiento, así como identificar la probabilidad de riesgos.

2.2. Marco conceptual

2.2.1. Gestión de riesgos

La gestión de riesgos es el proceso de identificación, análisis y respuesta a los factores de riesgo que pueden causar daños a la organización. Incluye la evaluación de la probabilidad y gravedad de los riesgos, y el desarrollo de planes para abordarlos. La gestión de riesgos es un componente crítico de cualquier organización y es esencial para el éxito de cualquier negocio. Se debe desarrollar e implementar un plan de gestión de riesgos para identificar, evaluar y responder a los riesgos. El plan debe revisarse y actualizarse regularmente para garantizar que esté actualizado y sea efectivo [23].

Existen diferentes tipos de riesgos a los que se enfrenta una empresa u organización y estos se pueden clasificar en diferentes categorías. Los riesgos financieros son aquellos que surgen debido a las actividades financieras de la empresa u organización. Estos incluyen riesgos relacionados con la estabilidad financiera de la empresa, riesgo de crédito, riesgo de mercado, riesgo de liquidez y riesgo de tipo de cambio. Los riesgos operativos son aquellos que surgen debido a las operaciones del día a día de la empresa u

organización. Estos incluyen riesgos relacionados con el proceso de producción, el proceso de distribución, el servicio al cliente, los recursos humanos y la tecnología de la información [24].

Por otro lado, los riesgos de proyecto son aquellos que surgen debido a la implementación de nuevos proyectos o la modificación de proyectos existentes. Estos incluyen riesgos relacionados con el cronograma, el costo, la calidad y el alcance del proyecto. Los riesgos legales son aquellos que surgen debido a las responsabilidades legales de la empresa u organización. Estos incluyen riesgos relacionados con el cumplimiento de las leyes y reglamentos, propiedad intelectual, reglamentos ambientales y reglamentos de salud y seguridad [24].

2.2.2. ISO 31000:2018

ISO 31000 es una norma internacional para la gestión de riesgos. Este estándar proporciona a las organizaciones principios, un marco y un proceso para gestionar el riesgo. Describe los procesos para identificar, evaluar y controlar los riesgos, así como para monitorear y revisar las actividades de gestión de riesgos. La ISO 31000 está destinada a ayudar a las organizaciones a aumentar la probabilidad de alcanzar los objetivos, mejorar la identificación de oportunidades y amenazas, y asignar y utilizar eficazmente los recursos para el tratamiento de riesgos. Con este estándar, las organizaciones pueden identificar, analizar, evaluar, tratar, monitorear y comunicar el riesgo de manera efectiva y eficiente [25].

2.2.3. CRAMM (Método de Análisis y Gestión de Riesgos CCTA)

El método de análisis y gestión de riesgos CCTA es un marco desarrollado por el Consejo Canadiense de Técnicos y Tecnólogos (CCTT) para ayudar a las organizaciones a identificar, evaluar y gestionar los riesgos asociados con el uso de la tecnología. El Método de Análisis y Gestión de Riesgos CCTA se basa en la norma de gestión de riesgos

ISO 31000 y está diseñado para ser utilizado por organizaciones de todos los tamaños y en todos los sectores. El Método de Análisis y Gestión de Riesgos CCTA puede utilizarse para identificar, evaluar y gestionar los riesgos asociados al uso de la tecnología en cualquier tipo de organización [26].

2.2.4. Octave (Evaluación Operativa Crítica de Amenazas, de Activos y de Vulnerabilidad)

La metodología OCTAVE [27] es un enfoque sistemático e integral para identificar las vulnerabilidades y los activos críticos operativos de una organización. Fue desarrollado por el Instituto de Ingeniería de Software (SEI) de la Universidad Carnegie Mellon [27].

OCTAVE se basa en la premisa de que la capacidad de una organización para gestionar sus riesgos operativos y vulnerabilidades depende de su capacidad para identificarlos, evaluarlos y comprenderlos. La metodología se estructura en torno a ocho pasos clave [27]:

- Definir el alcance y los objetivos de la evaluación.
- Identificar los activos operativos de la organización.
- Identificar las amenazas operativas de la organización.
- Identificar las vulnerabilidades operativas de la organización.
- Analizar el impacto de las amenazas y vulnerabilidades operativas.
- Identificar y priorizar estrategias de mitigación.
- Implementar estrategias de mitigación.
- Evaluar la efectividad de las estrategias de mitigación.

2.2.5. Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información)

Magerit es un acrónimo en español que significa "Gestión de Riesgos: Lineamientos y Herramientas". Es una metodología abierta para el análisis y la gestión de riesgos que se puede utilizar en una variedad de industrias y organizaciones. Magerit proporciona un

marco para identificar, evaluar y gestionar los riesgos. Se basa en los principios de ISO 31000, un estándar internacional para la gestión de riesgos [28].

2.2.6. Tipos de activos

Dentro de una organización los activos pueden ser tanto tangibles como intangibles. Los activos tangibles van desde archivos de datos hasta activos físicos, como periféricos de computadora, mientras que los activos intangibles incluyen la imagen y la reputación de la organización, las utilidades generales y las habilidades de la fuerza laboral [29].

Entre los principales tipos de activos resaltan los activos de hardware y software [29].

Los activos de información de software son piezas de datos, como programas informáticos, que una empresa o individuo posee y utiliza para generar valor u obtener una ventaja competitiva. Los ejemplos de activos de información de software incluyen software propietario, código fuente, interfaces de programación de aplicaciones, inteligencia comercial y bases de datos [30].

Los activos de información de hardware son componentes físicos de un sistema informático, como componentes de hardware, cables y otros periféricos. Los ejemplos de activos de información de hardware incluyen servidores, computadoras, enrutadores, conmutadores, impresoras y dispositivos de almacenamiento [30].

2.2.7. Vulnerabilidad

Las vulnerabilidades son debilidades en un sistema o en su diseño que un atacante podría explotar para obtener acceso no autorizado a información confidencial, causar interrupciones u otras actividades maliciosas. Pueden existir en software, hardware o firmware, y pueden ser causados por una variedad de factores que incluyen una configuración incorrecta, fallas de diseño o errores de software [29].

2.2.8. Amenaza

Las amenazas son eventos que pueden tener un impacto negativo en una organización, sistema o individuos. Estas se originan en los seres humanos, la tecnología y las condiciones ambientales. Algunos ejemplos son errores humanos al ingresar información, sistemas mal configurados, software malicioso y desastres naturales como inundaciones y terremotos. Cuando existen estas amenazas y no se controlan las vulnerabilidades asociadas, la información podría perderse, dejar de estar disponible o corromperse, lo que comprometería la seguridad de la información [29].

2.2.9. Riesgo

Los riesgos de la información son los riesgos potenciales para los datos y los activos de información de una organización. Estos riesgos pueden incluir acceso no autorizado a datos confidenciales, pérdida de datos, manipulación de datos, malware, ataques cibernéticos, información privilegiada maliciosa y otras actividades maliciosas [31].

El riesgo de seguridad de la información entra en juego cuando existe un evento o circunstancia potencial que podría provocar una interrupción de la organización, un daño a la reputación de la organización o una pérdida financiera debido a la falla de un sistema de información [31].

2.2.10. Análisis de riesgos de la seguridad de la información

El análisis de riesgos de la seguridad de la información es el proceso de identificar y evaluar los riesgos potenciales asociados con el uso, el almacenamiento y la transmisión de la información sensible o confidencial de una organización. Implica identificar y analizar los riesgos potenciales que plantean diversas amenazas a la información, como piratas informáticos, virus, software malicioso y daños físicos. El análisis de riesgos incluye la evaluación de la probabilidad de que una amenaza aproveche una vulnerabilidad, el impacto potencial de dicho ataque y las medidas necesarias para mitigar el riesgo [32].

La realización de una evaluación de la seguridad de la información permite a una organización "conocerse a sí misma" con respecto a su exposición al riesgo. Este conocimiento garantiza que los controles y, en última instancia, los gastos necesarios para implementar y respaldar estos controles sean proporcionales al riesgo al que están expuestos los activos de la organización. Por lo tanto, si la evaluación muestra que existe un mayor riesgo para un activo, entonces se debe aplicar una mayor protección y recursos a ese activo frente a un activo que se muestra como de menor riesgo [32].

2.2.11. Seguridad de la información

La seguridad de la información se encarga de proteger la información digital y los sistemas informáticos de ataques maliciosos. Consiste en medidas técnicas como el cifrado, la autenticación y el control de acceso, así como medidas organizativas como la gestión de riesgos, la formación de los empleados y la respuesta a incidentes [33].

El objetivo principal de la seguridad de la información es proteger la información confidencial del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados. Es importante tener en cuenta que la seguridad de la información no se trata solo de firewalls y software antivirus. Es un enfoque integral para proteger la información digital que tiene en cuenta la tecnología, las personas y los procesos [33].

La seguridad de la información es una parte importante de la estrategia de seguridad general de cualquier organización. Las organizaciones deben contar con políticas y procedimientos que aborden la seguridad de la información y garanticen que los datos confidenciales se mantengan seguros. Entre las cuatro funciones importantes que realiza están [33]:

- Proteger la capacidad de funcionamiento de la organización.
- Permitir el funcionamiento seguro de las aplicaciones que se ejecutan en los sistemas de TI de la organización.
- Protección de los datos que la organización recopila y utiliza.
- Salvaguardar los activos tecnológicos de la organización.

2.2.12. Tratamiento de los riesgos

El tratamiento de riesgos es el proceso de abordar los riesgos que se han identificado para reducir o eliminar su impacto en una organización. Este proceso implica evaluar el riesgo, identificar e implementar medidas apropiadas para reducir el riesgo y monitorear la efectividad de las medidas de reducción de riesgo. El tratamiento de riesgos es una parte importante de cualquier programa de gestión de riesgos y debe ser un proceso continuo para garantizar que los riesgos se gestionen y mitiguen adecuadamente [32].

Los procesos de tratamiento de riesgos implican la identificación de los riesgos que deben abordarse, la asignación de responsabilidades para la gestión del riesgo y la determinación de los mejores medios para abordarlos. Este proceso puede incluir el establecimiento de políticas, procedimientos y controles, el desarrollo y seguimiento de planes de gestión de riesgos y la implementación de herramientas de gestión de riesgos [32].

2.2.13. Análisis cualitativo de los riesgos

El análisis cualitativo de riesgos es un método de evaluación de riesgos que utiliza técnicas cualitativas para evaluar, priorizar y abordar los riesgos. Esta técnica ayuda a identificar, definir y evaluar los riesgos potenciales en función de criterios predefinidos y evaluaciones subjetivas [34].

El análisis cualitativo de riesgos se puede utilizar en cualquier organización. Es particularmente útil para organizaciones que están emprendiendo una nueva iniciativa o proyecto, o para aquellas que están experimentando cambios organizacionales. Además, puede usarse en industrias que están expuestas a altos niveles de riesgo, como finanzas, salud y manufactura [34].

Las herramientas de análisis cualitativo de riesgos incluyen [34]:

- Escalas de calificación de riesgos.

- Diagramas de causa y efecto.
- Análisis de Fortalezas, Debilidades, Oportunidades y Amenazas (FODA).
- Matriz de probabilidad e impacto.
- Brainstorming (lluvia de ideas).

2.2.14. Análisis cuantitativo de los riesgos

El análisis de riesgo cuantitativo es el proceso de utilizar datos numéricos y modelos matemáticos para evaluar la probabilidad y el impacto potencial de los riesgos previsibles. Por lo general, se utiliza para evaluar las posibles consecuencias financieras de los eventos de riesgo, así como para identificar posibles áreas de riesgo [34].

El análisis de riesgo cuantitativo es un proceso utilizado para medir y analizar los riesgos potenciales asociados con un proyecto, tarea, decisión comercial u otra actividad determinada. Las herramientas de análisis cuantitativo de riesgos incluyen [34]:

- Análisis de sensibilidad.
- Análisis del valor esperado monetario (EMV).
- Modelado y simulación.
- Análisis de árboles de decisión.

2.2.15. Métricas de evaluación de los riesgos

Las métricas de evaluación de riesgos son una herramienta esencial para medir el riesgo de cualquier proyecto o actividad. Proporcionan una visión integral de los riesgos potenciales y sus impactos asociados, lo que permite a las organizaciones tomar decisiones informadas y asignar recursos para mitigar los riesgos identificados. Las métricas de evaluación de riesgos pueden ayudar a las organizaciones a identificar el impacto potencial de un riesgo, medir la probabilidad de que ocurra un riesgo y evaluar la efectividad de varias estrategias de gestión de riesgos [35].

Estas métricas también se pueden utilizar para realizar un seguimiento del progreso de los planes de gestión de riesgos y garantizar que los riesgos se aborden de manera oportuna. Mediante el uso de métricas de evaluación de riesgos, las organizaciones pueden asegurarse de que están tomando las mejores decisiones para proteger sus activos y minimizar las pérdidas potenciales [35].

Las métricas comunes de evaluación de riesgos incluyen el valor en riesgo (VaR), la pérdida esperada (EL) y el apetito por el riesgo. También se pueden utilizar otras métricas para evaluar riesgos como la probabilidad de incumplimiento (PD), la pérdida en caso de incumplimiento (LGD) y la exposición en caso de incumplimiento (EAD) [35].

2.3. Marco teórico

2.3.1. Importancia de la gestión de riesgos en la actualidad

Hay muchas razones por las que la gestión de riesgos es importante en el mundo actual. Una de las razones es que el mundo está cada vez más interconectado y los eventos en una parte del mundo pueden tener un efecto dominó en otras partes. Esta interconexión significa que los riesgos que antes se consideraban localizados ahora tienen el potencial de afectar a personas y organizaciones de todo el mundo [36].

Otra razón por la que la gestión de riesgos es importante es que el mundo se está volviendo cada vez más complejo. Esta complejidad puede dificultar la identificación y evaluación de riesgos y el desarrollo de planes eficaces para gestionarlos [36].

La gestión de riesgos también es importante porque a menudo hay mucho en juego. Cuando una organización o individuo no logra gestionar los riesgos de manera efectiva, las consecuencias pueden ser graves. Esto es particularmente cierto en el caso de riesgos que tienen el potencial de causar daños catastróficos, como los relacionados con desastres naturales o accidentes industriales [37].

Finalmente, la gestión de riesgos es importante porque puede ayudar a las organizaciones e individuos a tomar mejores decisiones. Al identificar y evaluar los riesgos y desarrollar planes para gestionarlos, las organizaciones y las personas pueden evitar tomar decisiones que podrían tener consecuencias desastrosas [37].

2.3.2. La mejora continua y la gestión de riesgos

La mejora continua y la gestión de riesgos son dos conceptos clave en el ámbito de la gestión empresarial. La mejora continua se refiere al proceso sistemático de mejora de los productos, procesos y servicios de una organización. La gestión de riesgos, por otro lado, se refiere a la identificación, evaluación y gestión de los riesgos asociados con la operación de un negocio [38].

La mejora continua busca mejorar la calidad y los niveles de servicio para asegurar que los productos y servicios sean satisfactorios para los clientes. Esto puede lograrse mediante la identificación de áreas de oportunidad, la implementación de mejoras, la evaluación de resultados y la adopción de mejores prácticas. La mejora continua también implica el uso de herramientas como el análisis de causa raíz y el análisis de los procesos para identificar oportunidades de mejora [38].

La gestión de riesgos es una parte importante de la mejora continua. La identificación, evaluación y gestión de los riesgos asociados con la operación de un negocio es una parte esencial de la mejora continua. Esto implica el uso de herramientas y técnicas para identificar, evaluar y gestionar los riesgos asociados con la operación y la toma de decisiones. Esto ayuda a asegurar que la organización pueda detectar y mitigar los riesgos de forma adecuada [38].

La mejora continua y la gestión de riesgos deben trabajar juntas para mejorar los resultados de la organización. La mejora continua proporciona un enfoque sistemático para mejorar los productos, procesos y servicios de la organización. Al mismo tiempo, la gestión de riesgos ofrece una forma de identificar y mitigar los riesgos asociados con la operación. Estas dos estrategias deben trabajar juntas para asegurar que la organización pueda mejorar sus resultados de manera efectiva y segura. [38].

2.3.3. Integración de la gestión de riesgos en los procesos de la organización

La gestión de riesgos debe estar integrada en todos los procesos de una organización. Esto incluye procesos como la planificación, la presupuestación, la toma de decisiones, la gestión del desempeño, la comunicación y el control. La gestión de riesgos debe verse como una parte integral del sistema de gestión general de la organización, no como una actividad aislada [39].

La gestión de riesgos debe estar integrada en la cultura de la organización, con la alta dirección proporcionando liderazgo y apoyo. Esto requiere una comunicación clara de la filosofía de riesgo y el apetito por el riesgo de la organización. También requiere el desarrollo de una sólida infraestructura de gestión de riesgos y el establecimiento de políticas y procedimientos de gestión de riesgos [39].

Es importante asegurarse de que la gestión de riesgos esté integrada en los procesos de la organización, no solo al comienzo, sino durante todo el ciclo de vida de cada proceso. Esto es particularmente importante para los procesos que involucran decisiones que tienen consecuencias financieras u operativas significativas [39].

La gestión de riesgos también debe integrarse en el sistema de gestión del desempeño, con métricas y objetivos de desempeño vinculados a los objetivos y actividades de gestión de riesgos. Esto ayudará a garantizar que la gestión de riesgos se gestione de manera eficaz y que la organización esté tomando las medidas adecuadas para gestionar su perfil de riesgo [40].

2.4. Componentes de la propuesta

2.4.1. Estudio comparativo de metodologías de gestión de riesgos

Luego de analizar los aspectos anteriores, se obtiene que la gestión de riesgos es el proceso de identificación de riesgos, evaluación de riesgos e implementación de medidas para reducir los riesgos a un nivel aceptable. Un marco de gestión de riesgos describe los procesos, métodos, herramientas y roles y responsabilidades del equipo para un proyecto en particular. Por ende, permite la identificación de riesgos, su evaluación e implementación de medidas para reducir los riesgos a un nivel aceptable.

Las metodologías de gestión de riesgos están diseñadas para ayudar a las organizaciones a comprender, gestionar y reducir mejor su exposición al riesgo al proporcionar un enfoque estructurado para identificar, evaluar y responder a los riesgos. También pueden ayudar a las organizaciones a tomar mejores decisiones, mejorar su desempeño y aumentar su eficiencia.

A continuación, se muestra una tabla informativa relacionada con cada una de las metodologías seleccionadas para la presente investigación, evaluando: propósito, áreas de aplicación, enfoque, pasos o etapas, técnicas empleadas y tipos de riesgos.

Característica	**Descripción**
Propósito	Se centra en ayudar a las organizaciones a desarrollar una base sólida para la toma de decisiones y la gestión de los riesgos.
Áreas de aplicación	Organizaciones públicas y privadas.
Enfoque	El enfoque de esta metodología es proporcionar directrices para la administración de riesgos. Esta directriz ayuda a las organizaciones a identificar, evaluar, gestionar y controlar los riesgos eficazmente.
Pasos o etapas	Se compone de siete fases donde resaltan 10 secciones y 14 controles.
Técnicas empleadas	Entre las técnicas que emplea se encuentran: árbol de decisión, matrices de riesgos, análisis FMEA, análisis de amenazas y

	vulnerabilidades, planificación de respuestas al riesgo, monitorización y evaluación, comunicación y consulta, etc.; garantizando que los riesgos sean tratados adecuadamente.
Tipos de riesgos	Esta metodología aborda: la gestión de proyectos, la seguridad y la salud, el medio ambiente, el desempeño financiero, los procesos de negocios, la proporcionalidad, los procedimientos, la calidad, etc.

Tabla 3. Características de la metodología ISO 31000:2018.

En el cuadro anterior se puede apreciar que la metodología ISO 31000:2018 exige que los procesos de gestión de riesgos sean sistemáticos, estructurados y orientados hacia los objetivos. También es importante que estos procesos sean integrados en la estructura organizacional y se establezcan mecanismos para la mejora continua.

Característica	**Descripción**
Propósito	Se centra en ayudar a las organizaciones a identificar, evaluar, gestionar y monitorear los riesgos en sus sistemas y servicios de TI.
Áreas de aplicación	Organizaciones públicas y privadas.
Enfoque	Proporciona un enfoque integral y sistemático para la gestión de riesgos que se puede utilizar para evaluar los riesgos asociados con cualquier actividad o proyecto.
Pasos o etapas	Se conforma de tres etapas.
Técnicas empleadas	Las técnicas utilizadas incluyen la identificación de riesgos, el análisis de riesgos, la evaluación de riesgos, el control de riesgos y la aceptación de riesgos. Las herramientas utilizadas incluyen matrices de riesgo, registros de riesgo, listas de verificación y entrevistas.

Tipos de riesgos	Aborda: riesgos estratégicos, riesgos de los procesos de negocio, riesgos financieros, riesgos de seguridad de la información, riesgos de disponibilidad del sistema, riesgos de cumplimiento normativo, riesgos ambientales, riesgos operacionales, riesgos de recursos humanos, riesgos legales, etc.

Tabla 4. Características de la metodología CRAMM.

La metodología CRAMM sigue un enfoque de arriba hacia abajo dividiéndose en tres fases: identificación de riesgos, análisis de riesgos y evaluación de riesgos. Esta metodología está destinada a ser utilizada por organizaciones de todos los tamaños, y es particularmente útil para organizaciones que necesitan administrar riesgos complejos.

Característica	**Descripción**
Propósito	Se puede utilizar para evaluar la eficacia de los controles de seguridad existentes y proporcionar orientación sobre cómo mejorarlos.
Áreas de aplicación	Pequeñas y medianas empresas.
Enfoque	Posee un enfoque que posibilita la comprensión del impacto de los riesgos y vulnerabilidades en las operaciones comerciales.
Pasos o etapas	Compuesto por cuatro fases.
Técnicas empleadas	Esta metodología utiliza una variedad de técnicas y herramientas que incluyen: análisis de vulnerabilidades, modelado de árboles de ataque, revisión de la arquitectura de seguridad, pruebas de control de seguridad, revisión de operaciones de seguridad, pruebas de penetración, etc.
Tipos de riesgos	Se centra en los riesgos técnicos y no técnicos y cubre una amplia gama de temas, incluida la

	seguridad del sistema, la privacidad, la disponibilidad, la confiabilidad y la integridad. Además, la metodología Octave tiene en cuenta el impacto de los factores organizacionales, ambientales y de otro tipo que podrían afectar la seguridad de los sistemas de información de una organización.

Tabla 5. Características de la metodología OCTAVE.

La metodología Octave presenta la construcción de perfiles de amenazas. Estos perfiles son modelos basados en datos que se utilizan para identificar y evaluar posibles amenazas para las organizaciones. Están diseñados para ayudar a las organizaciones a desarrollar estrategias para protegerse de amenazas como ataques cibernéticos, violaciones de datos y otras actividades maliciosas

Característica	**Descripción**
Propósito	Ayuda a las organizaciones a alcanzar sus objetivos a través de la gestión eficaz de riesgos y la implementación de procesos de gestión de riesgos.
Áreas de aplicación	Gobierno, pequeñas y medianas empresas.
Enfoque	Busca proporcionar a las organizaciones un enfoque sistemático y estructurado para gestionar los riesgos y mejorar la resiliencia organizacional.
Pasos o etapas	Se agrupa en cuatro etapas.
Técnicas empleadas	Utiliza una combinación de técnicas y herramientas para facilitar el proceso de gestión de riesgos de seguridad. Estos incluyen entrevistas, encuestas, talleres, herramientas de evaluación de riesgos, evaluación comparativa, sistemas de informes de riesgos y herramientas de monitoreo de riesgos. Estas herramientas se

	pueden utilizar para crear mapas de riesgo, generar informes y realizar un seguimiento del progreso.
Tipos de riesgos	Aborda una amplia gama de riesgos, incluidos los riesgos de seguridad cibernética, seguridad física, legales, financieros, operativos, de continuidad, estratégicos y reputacionales. Este enfoque integral permite que las organizaciones identifiquen, analicen y gestionen los riesgos de una manera que les permita evitar mejor su exposición a posibles pérdidas.

Tabla 6. Características de la metodología Magerit.

La metodología Magerit se encuentra relacionada de forma directa con la generalización del uso de tecnologías de la información.

Estas cuatro metodologías varían en su enfoque de la gestión de riesgos, ISO 31000:2018 se centra en un proceso estructurado de identificación, evaluación y mejora continua, CRAMM enfatiza la evaluación y mitigación continuas de riesgos, OCTAVE enfatiza la identificación y gestión proactiva de riesgos y Magerit se enfoca en desarrollar e implementar estrategias de gestión de riesgos.

De esta manera, se obtiene el siguiente cuadro comparativo de las metodologías seleccionadas:

CUADRO COMPARATIVO				
	ISO 31000:2018	**CRAMM**	**OCTAVE**	**Magerit**
Descripción	ISO 31000 es una guía de gestión de riesgos diseñada para ayudar a las organizaciones a administrar y minimizar los riesgos involucrados en	Se centra en la identificación, el análisis y la gestión de riesgos relacionados con la seguridad de la información. Es un proceso estructurado	Utiliza un enfoque basado en equipos para evaluar la seguridad de los activos de TI de una organización e identificar amenazas, vulnerabilidades y riesgos.	Está diseñado para ayudar a las organizaciones a identificar, analizar y administrar sus riesgos asociados con los sistemas de TI. Magerit se

	sus operaciones. Establece una serie de principios, marcos y procesos para la identificación, evaluación, tratamiento, monitoreo y comunicación de riesgos.	que incluye tanto la evaluación cuantitativa como cualitativa del riesgo y utiliza una variedad de técnicas, como entrevistas, cuestionarios y encuestas, para identificar y evaluar el riesgo.	OCTAVE se centra en los aspectos operativos de la gestión de riesgos y proporciona un enfoque integral que incluye análisis de amenazas, gestión de activos y evaluación de vulnerabilidades.	centra en la identificación y evaluación sistemáticas de los riesgos potenciales y proporciona un enfoque estructurado para la gestión de riesgos.
Tipo de análisis	• Cuantitativo satisfactorio. • Cualitativo completo. • Mixto satisfactorio.	• Cuantitativo completo. • Cualitativo completo.	• Cuantitativo satisfactorio. • Cualitativo satisfactorio. • Mixto satisfactorio.	• Cuantitativo completo. • Cualitativo completo.
Tipos de riesgos	• Efectivo completo. • Residual pobre.	• Intrínseco completo. • Residual completo	• Efectivo completo. • Residual pobre.	• Intrínseco completo. • Residual completo.

Tabla 7. Comparación de metodologías.

De acuerdo con la información proporcionada en la tabla anterior, se procede se procede a seleccionar los siguientes aspectos correspondientes a cada metodología de gestión de riesgos estudiada:

- *De ISO 31000:2018.* - Se selecciona el desarrollo de controles de seguridad de la información, así como el empleo de la matriz de riesgos, ayudando a las organizaciones a desarrollar una cultura de gestión de riesgos y seguridad en toda la organización fomentada por medio de la mejora continua.
- *De CRAMM.* - Se selecciona su enfoque de análisis, tanto cualitativo como cuantitativo, donde se emplean herramientas como entrevistas para identificar y evaluar los riesgos, e incluso, evaluando el impacto de la organización bajo un enfoque empresarial.

- *De OCTAVE*. - Se selecciona la creación de los perfiles de amenazas, los cuales pueden usar para identificar vulnerabilidades en sistemas, redes, aplicaciones y datos, así como para monitorear las actividades de los usuarios y detectar comportamientos sospechosos. También se pueden utilizar para proporcionar una alerta temprana de posibles ataques y permitir que las organizaciones respondan de forma rápida y eficaz.
- *De Magerit*. - Se selecciona la división de los activos de la información de forma rigurosa, siendo una de sus ventajas centrarse específicamente en los riesgos asociados a los sistemas de información.

A continuación, se destacan otros puntos importantes de esta propuesta tecnológica:

- El empleo de métricas de riesgos, tales como el estado de riesgo de fallas en los equipos de la institución.
- Un enfoque cualitativo donde se emplean herramientas como la matriz de riesgos y el análisis FODA orientado a la gestión de riesgos.
- Con respecto a la metodología Magerit, esta plantea el uso de herramientas para análisis de riesgos como PILAR, no obstante, al no ser una herramienta pública, para esta propuesta se empleará Power BI, una plataforma de inteligencia empresarial.

2.4.2. Identificación de activos de información

Los activos de información son los recursos valiosos que una empresa u organización utiliza para llevar a cabo su negocio [41]. Estos activos pueden incluir datos de clientes, información financiera, secretos de la empresa y otros tipos de datos confidenciales. Siendo la información el activo más importante de cualquier empresa, se tiene la siguiente clasificación:

- **Información pública:** Este tipo de información está disponible para el público en general y cualquier persona puede acceder a ella.

- **Información privada:** Este tipo de información es confidencial y solo es accesible a personas autorizadas.
- **Información de propiedad exclusiva:** este tipo de información es propiedad de una organización específica y no está disponible para el público en general.

A partir de lo anterior, la entrevista realizada al encargado del departamento técnico de la institución permitió identificar y agrupar los activos de información de la siguiente manera:

- Servicios
- Software
- Hardware
- Comunicaciones
- Equipamiento auxiliar
- Instalaciones
- Soportes de información
- Personal

Para realizar la respectiva evaluación de estos activos, se dispondrá de los siguientes criterios de seguridad:

- Confidencialidad
- Integridad
- Disponibilidad

Estos criterios son las dimensiones que establece Magerit para la evaluación de los activos. La confidencialidad garantiza que los datos solo sean accedidos y vistos por personas autorizadas, manteniendo la información sensible segura. La integridad garantiza la precisión y consistencia de los datos, previniendo de modificaciones no autorizadas. Por otro lado, la disponibilidad asegura que los datos sean accesibles a las personas autorizadas bajo demanda, manteniendo los niveles de servicio y minimizando el tiempo de inactividad. A continuación, se muestra la ponderación de estos criterios:

Descripción	Valoración
Despreciable	0
Bajo	1
Medio	2
Alto	3

Tabla 8. Ponderación de los criterios de seguridad de la información.

La ponderación consta de cuatro niveles que van desde “Despreciable”, valorado en 0, hasta “Alto”, cuyo valor es de 3.

Diagramas causa-efecto

Los diagramas de causa y efecto se utilizan en la gestión de riesgos para identificar las posibles causas del riesgo y las consecuencias que podrían derivarse de ellas [42]. Para esta propuesta, los diagramas de causa-efecto se agrupan según:

1. Riesgos de desastres naturales.
2. Riesgos de seguridad cibernética.
3. Riesgos financieros.
4. Riesgos de proyecto.
5. Riesgos operacionales.
6. Recursos humanos.
7. Riesgos de cumplimiento.

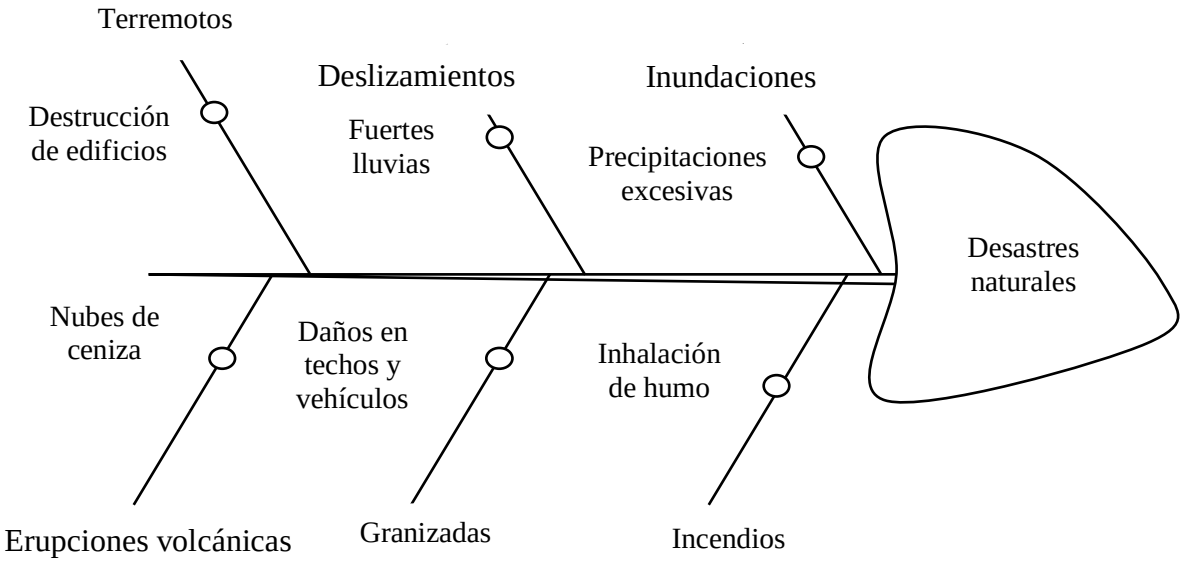


Figura 1. Diagrama de causa y efecto de los riesgos de desastres naturales.

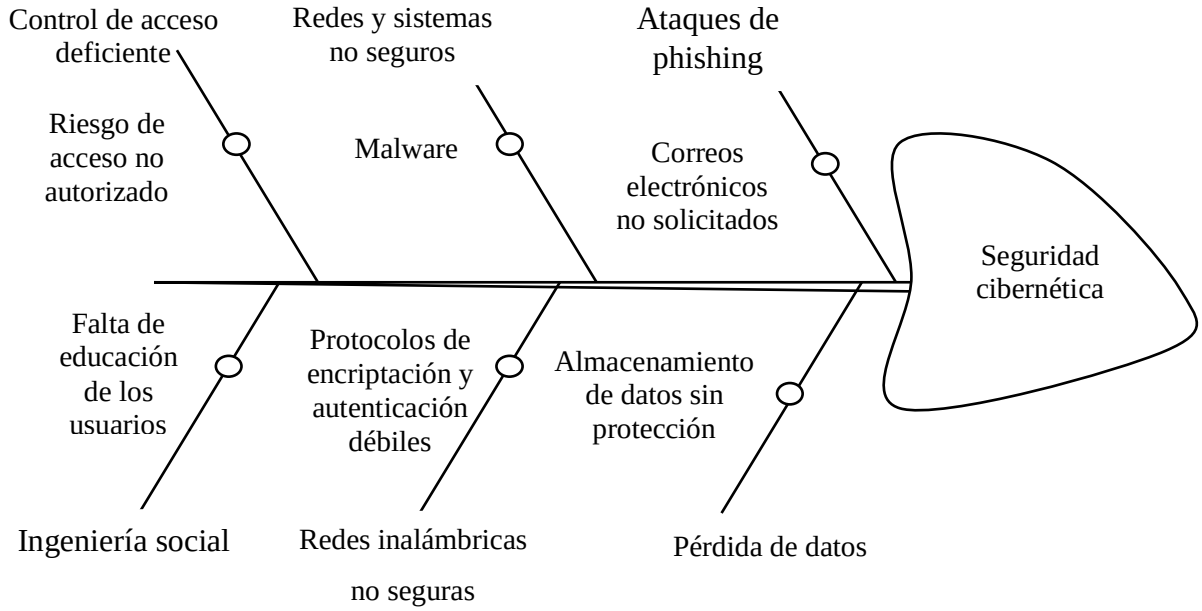


Figura 2. Diagrama de causa y efecto de los riesgos de seguridad cibernética.

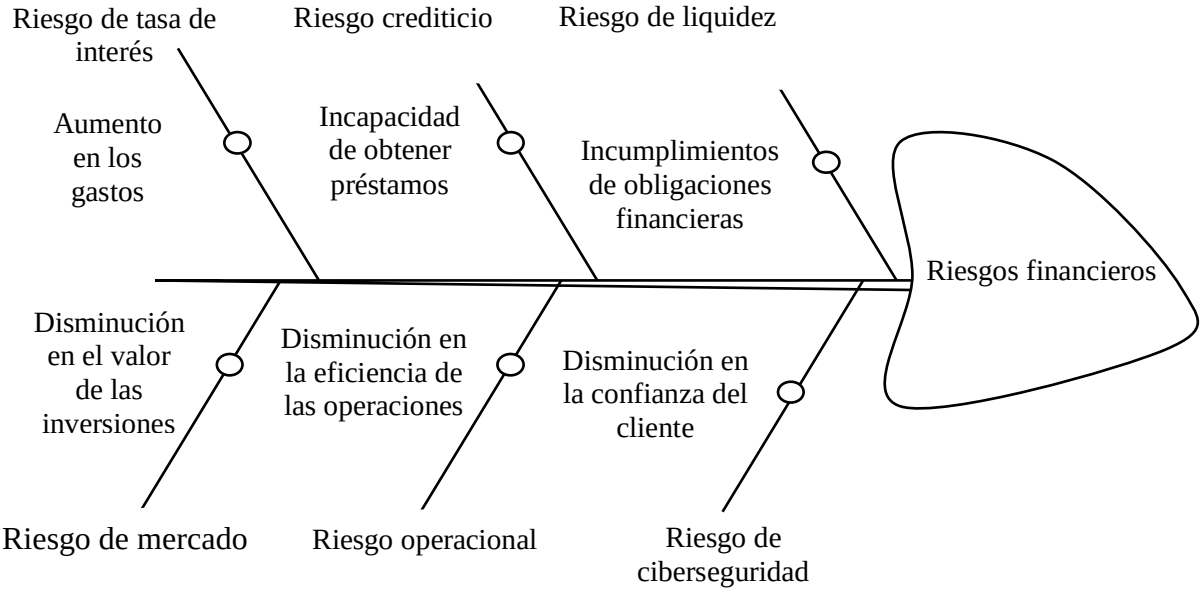


Figura 3. Diagrama de causa y efecto de los riesgos financieros.

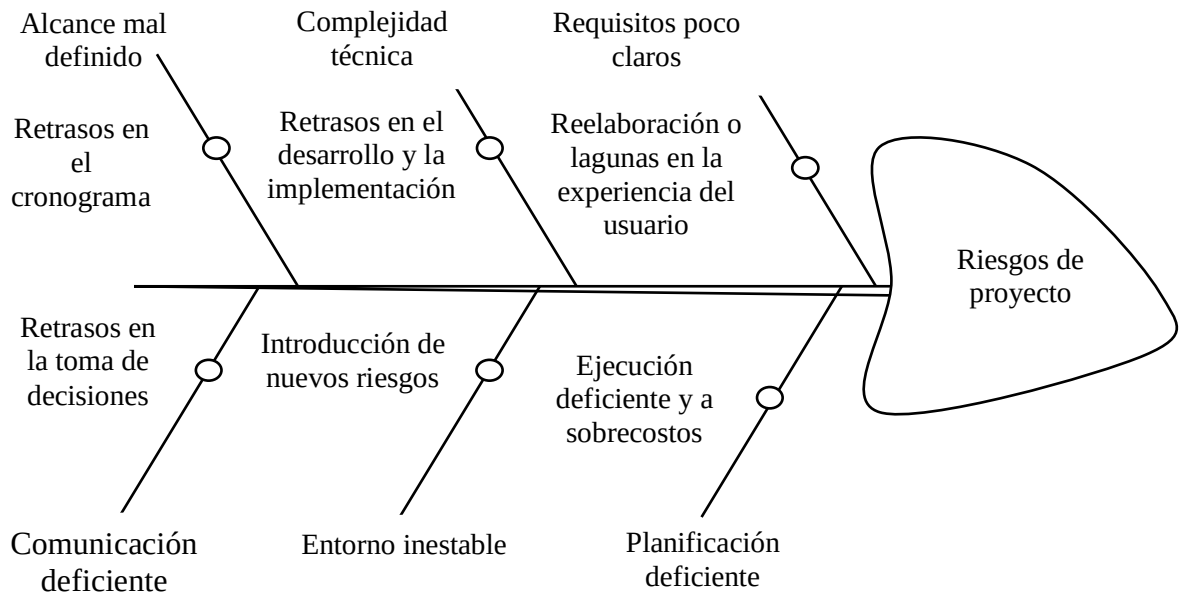


Figura 4. Diagrama de causa y efecto de los riesgos de proyecto.

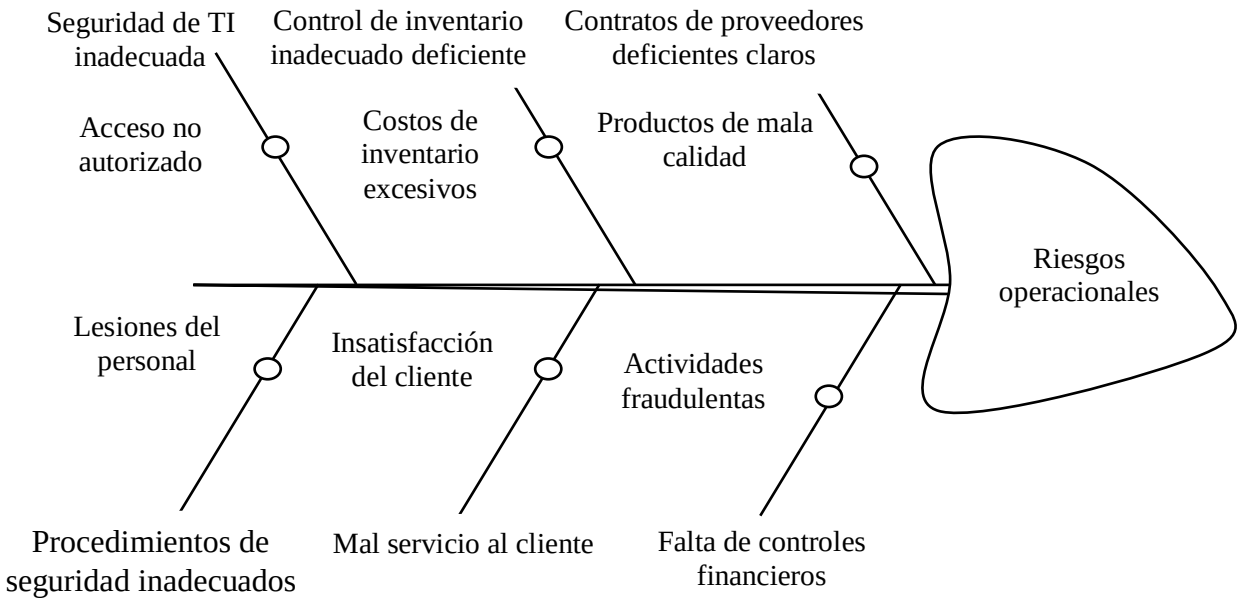


Figura 5. Diagrama de causa y efecto de los riesgos operacionales.

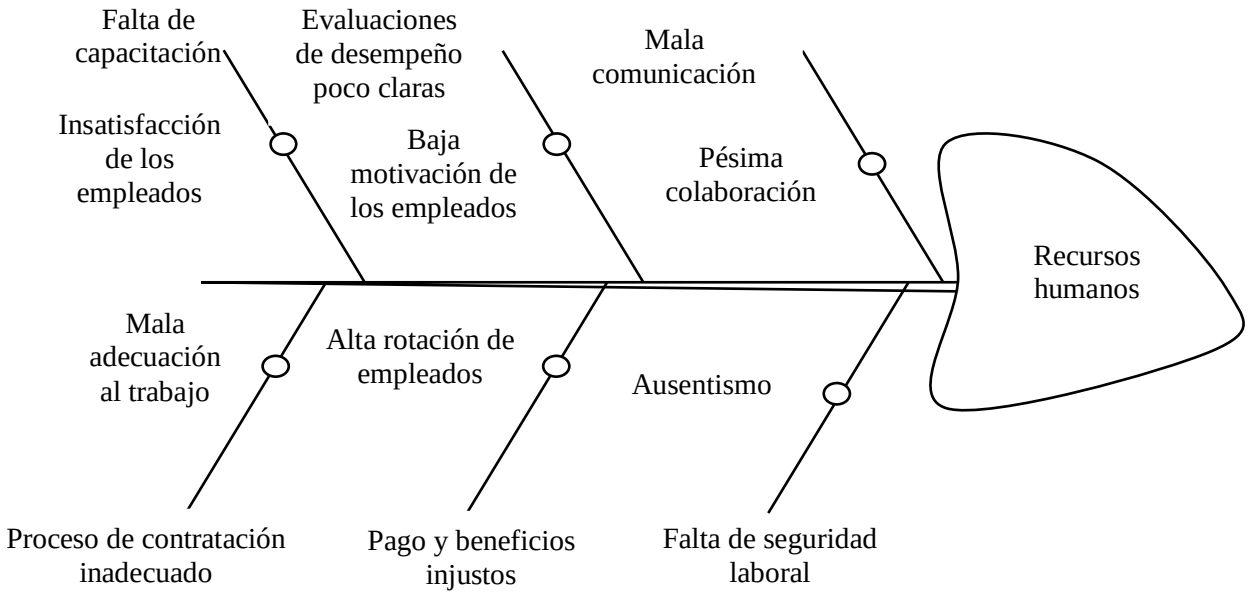


Figura 6. Diagrama de causa y efecto de los riesgos de recursos humanos.

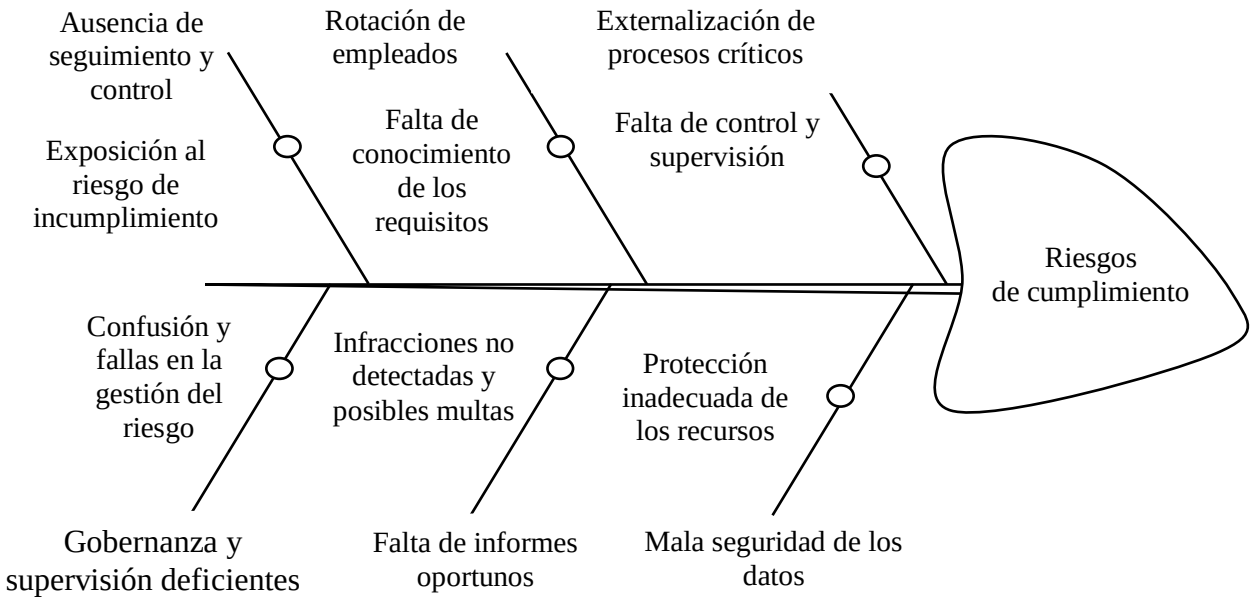


Figura 7. Diagrama de causa y efecto de los riesgos de cumplimiento.

Matriz de riesgos

La matriz de riesgos a emplear en este proyecto será la siguiente:

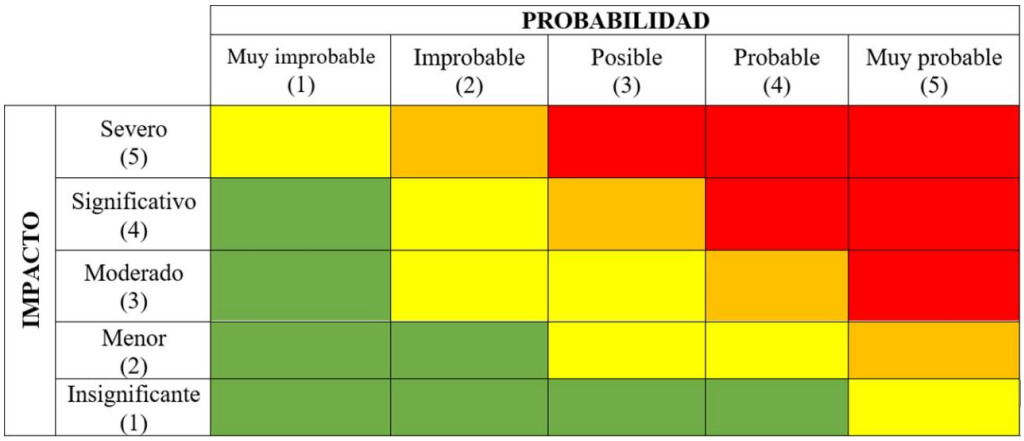


Figura 8. Matriz de riesgos. Fuente: ISO 31000:2018.

La matriz mostrada anteriormente permite visualizar la probabilidad y el impacto de los riesgos potenciales, lo que facilita determinar qué riesgos deben abordarse primero y cuál es la mejor manera de abordarlos. La matriz de riesgos también proporciona una forma efectiva de rastrear y monitorear el progreso de los esfuerzos para gestionar los riesgos.

Análisis FODA

El análisis FODA (Fortalezas, Oportunidades, Debilidades, Amenazas) permite identificar los riesgos potenciales relacionados con una empresa, negocio, o en este caso, una institución, para su posterior evaluación.

Para esta propuesta, se ha realizado el siguiente análisis FODA:

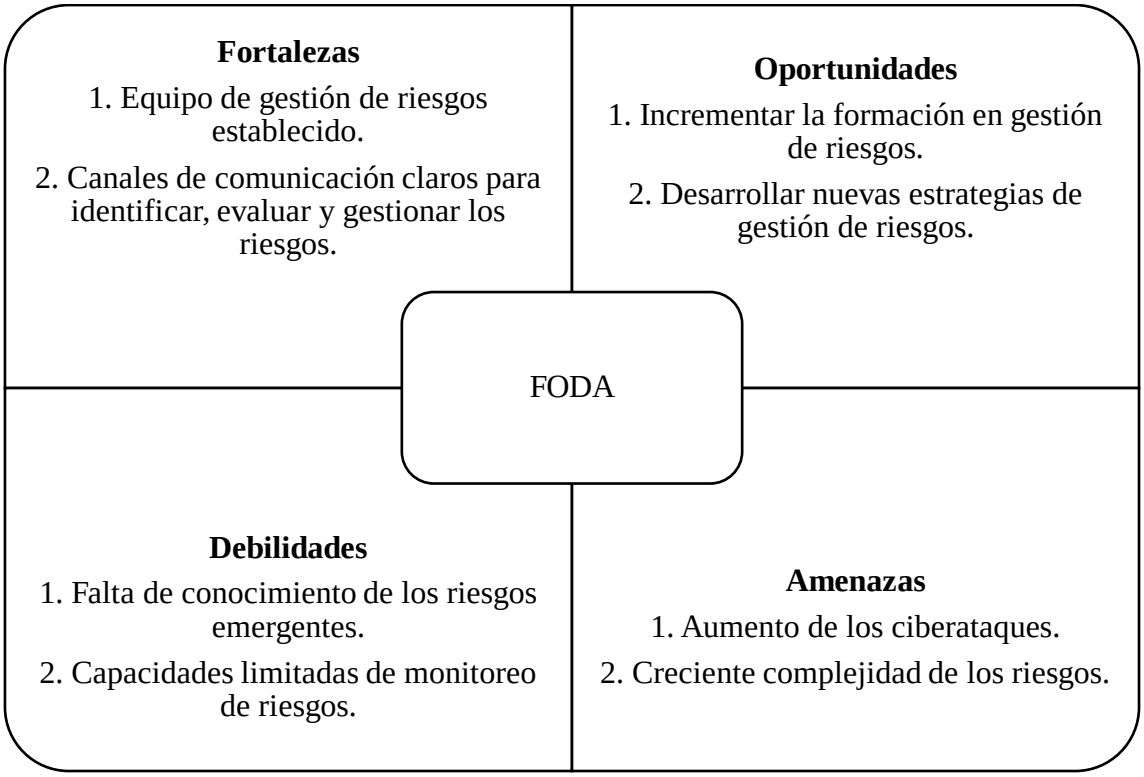


Figura 9. Análisis FODA de riesgos.

Análisis PESTEL

El análisis PESTEL hace referencia a los aspectos: político, económico, social, tecnológico, ambiental y legal. Esta es una herramienta útil para la gestión de riesgos, que permite a las empresas identificar los factores de riesgo potenciales que pueden afectar sus operaciones. En cuanto a esta propuesta, se ha podido identificar lo siguiente:

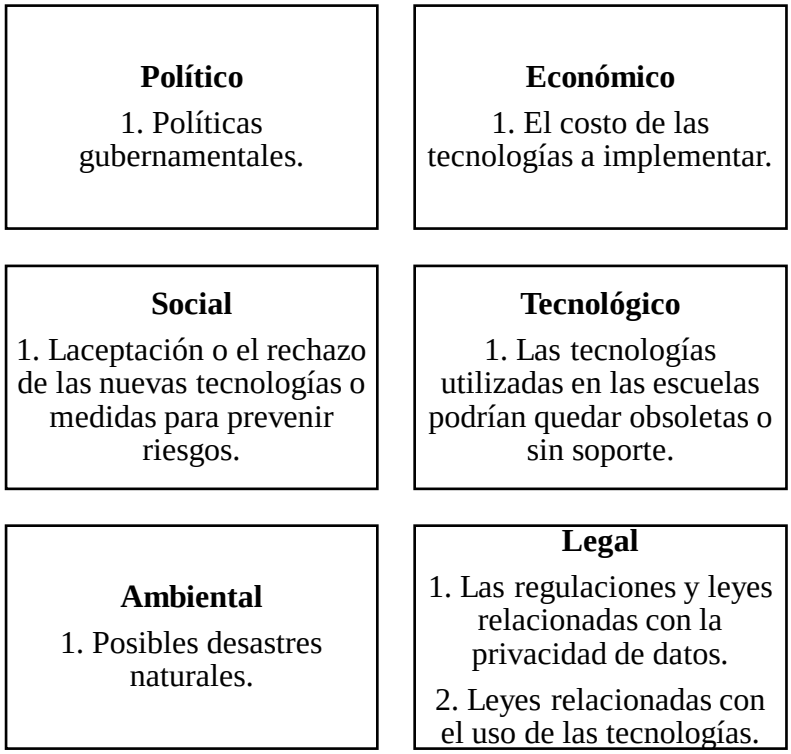


Figura 10. Análisis PESTEL de riesgos.

2.4.3. Selección de controles

Después de realizar la comparación de metodologías y analizando los recursos con los que cuenta la institución objeto de estudio, algunas consideraciones comunes que se pueden tener en cuenta incluyen el tipo de riesgos que se enfrentan, el impacto potencial de esos riesgos y los recursos disponibles para la organización. Por esta razón, la selección de controles involucra los siguientes pasos:

1. **Creación de controles de gestión de riesgos:** Este primer paso implica establecer controles claros para identificar, evaluar y gestionar el riesgo.
2. **Identificación de los riesgos potenciales:** Este paso implica analizar las amenazas y vulnerabilidades detectadas por medio de técnicas cualitativas como las entrevistas.
3. **Evaluar la probabilidad de cada riesgo:** Una vez que se han identificado todos los riesgos potenciales, el siguiente paso es evaluar la probabilidad e impacto de

que ocurran cada uno. Esto se puede hacer usando una escala simple como bajo, medio y alto.

4. **Monitoreo y revisión de riesgos:** El paso final en el proceso de análisis de riesgos es monitorear y revisar los riesgos de forma continua. Esto incluye hacer un seguimiento de cualquier cambio que ocurra y que pueda afectar los riesgos, así como reevaluar periódicamente la probabilidad y el impacto de cada riesgo.

2.4.4. Creación de reportes

La creación de reportes involucra el análisis de las métricas de riesgo detectadas en la institución, tanto antes como después de implementar los controles enlistados anteriormente. Algunos de las métricas más comunes son:

- Estado de falla de los equipos
- Tiempo medio entre fallas
- Tiempo de inactividad medio
- Valor en riesgo (VaR)

A continuación, se muestra un reporte sobre el indicador de estado de falla de los equipos realizado mediante la herramienta Power BI.

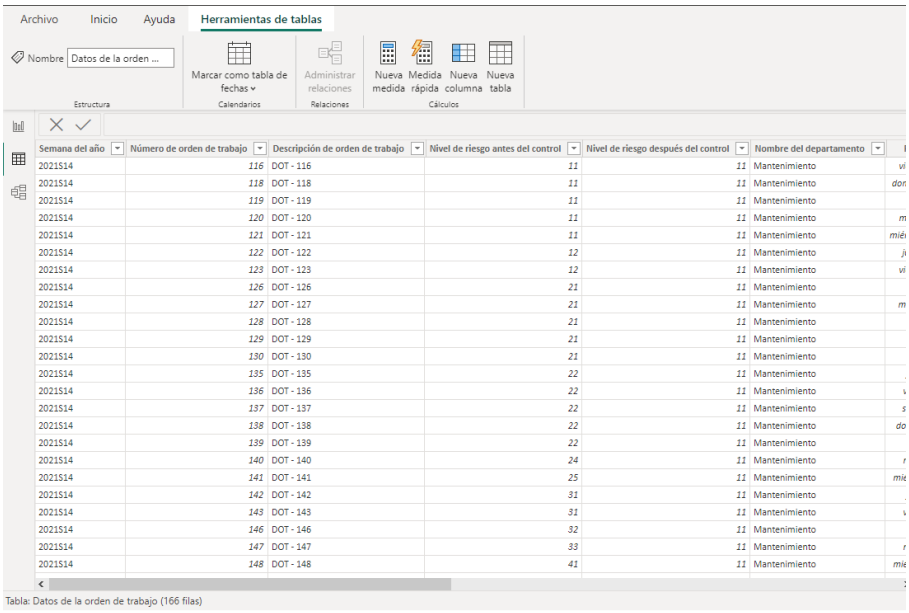


Figura 11. Datos empleados para el reporte.

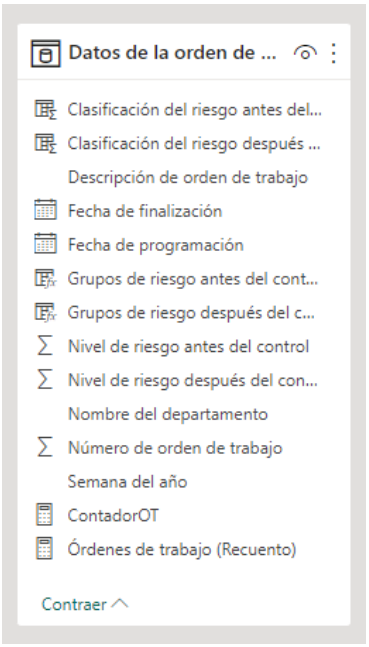
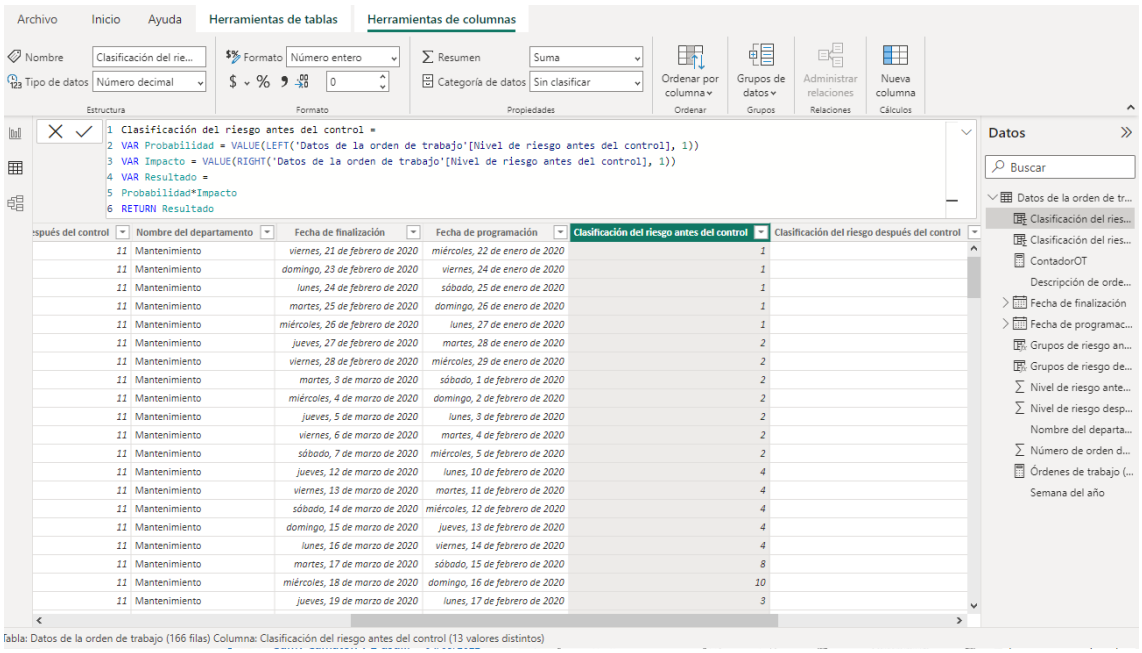


Figura 12. Modelo de datos.



spués del control	Nombre del departamento	Fecha de finalización	Fecha de programación	Clasificación del riesgo antes del control	Clasificación del riesgo después del control
11	Mantenimiento	viernes, 21 de febrero de 2020	miércoles, 22 de enero de 2020	1	
11	Mantenimiento	domingo, 23 de febrero de 2020	viernes, 24 de enero de 2020	1	
11	Mantenimiento	lunes, 24 de febrero de 2020	sábado, 25 de enero de 2020	1	
11	Mantenimiento	martes, 25 de febrero de 2020	domingo, 26 de enero de 2020	1	
11	Mantenimiento	miércoles, 26 de febrero de 2020	lunes, 27 de enero de 2020	1	
11	Mantenimiento	jueves, 27 de febrero de 2020	martes, 28 de enero de 2020	2	
11	Mantenimiento	viernes, 28 de febrero de 2020	miércoles, 29 de enero de 2020	2	
11	Mantenimiento	martes, 3 de marzo de 2020	sábado, 1 de febrero de 2020	2	
11	Mantenimiento	miércoles, 4 de marzo de 2020	domingo, 2 de febrero de 2020	2	
11	Mantenimiento	jueves, 5 de marzo de 2020	lunes, 3 de febrero de 2020	2	
11	Mantenimiento	viernes, 6 de marzo de 2020	martes, 4 de febrero de 2020	2	
11	Mantenimiento	sábado, 7 de marzo de 2020	miércoles, 5 de febrero de 2020	2	
11	Mantenimiento	jueves, 12 de marzo de 2020	lunes, 10 de febrero de 2020	4	
11	Mantenimiento	viernes, 13 de marzo de 2020	martes, 11 de febrero de 2020	4	
11	Mantenimiento	sábado, 14 de marzo de 2020	miércoles, 12 de febrero de 2020	4	
11	Mantenimiento	domingo, 15 de marzo de 2020	jueves, 13 de febrero de 2020	4	
11	Mantenimiento	lunes, 16 de marzo de 2020	viernes, 14 de febrero de 2020	4	
11	Mantenimiento	martes, 17 de marzo de 2020	sábado, 15 de febrero de 2020	8	
11	Mantenimiento	miércoles, 18 de marzo de 2020	domingo, 16 de febrero de 2020	10	
11	Mantenimiento	jueves, 19 de marzo de 2020	lunes, 17 de febrero de 2020	3	

Figura 13. Creación de los grupos de riesgo antes del control.

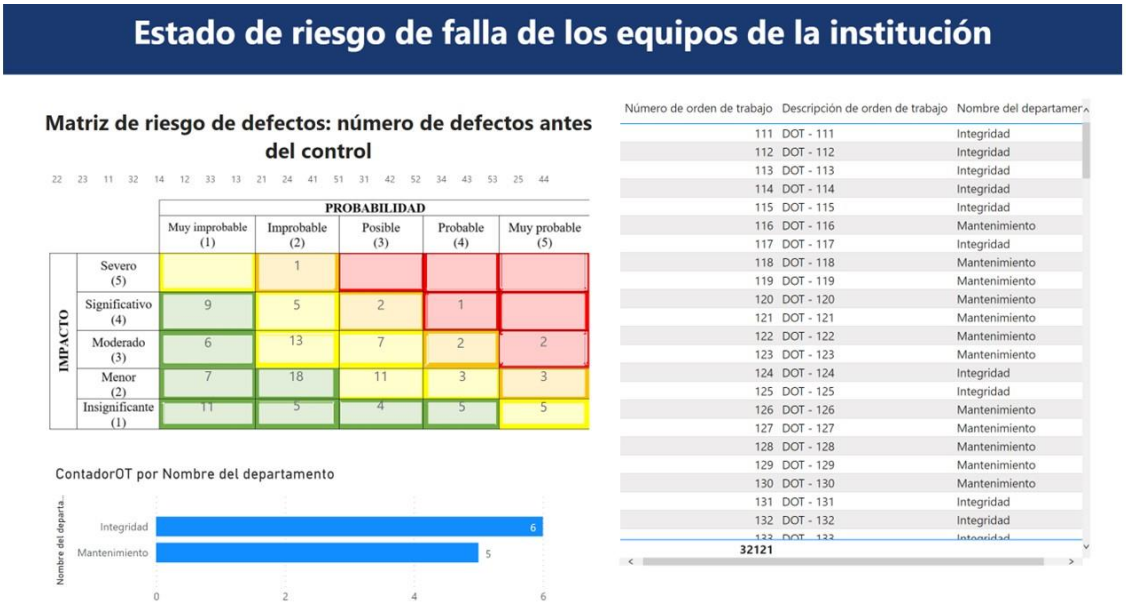


Figura 14. Informe sobre el estado de riesgo de falla de los equipos.

2.4.5. Requerimientos

Los requerimientos para la gestión de riesgos varían según el tipo de institución y la industria específica. Sin embargo, existen algunas mejores prácticas generales que todas las organizaciones deberían seguir:

1. Establecer un plan de respuesta a incidentes para manejar los incidentes de seguridad.
2. Implementar fuertes medidas de control de acceso para limitar el acceso a datos confidenciales.
3. Implementar un sistema de clasificación de datos para identificar y proteger la información confidencial.
4. Evaluar periódicamente los riesgos de seguridad asociados con las nuevas tecnologías.
5. Desarrollar e implementar políticas y procedimientos de seguridad para proteger los datos.

6. Implementar un proceso de ciclo de vida de desarrollo de software seguro.
7. Realizar periódicamente análisis de seguridad y evaluaciones de vulnerabilidad.
8. Supervisar y registrar las actividades de los usuarios en el Sistema de Educación Virtual.
9. Almacenar y proteger de forma segura las copias de seguridad de datos.
10. Educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
11. Identificar los responsables de la gestión de riesgos dentro de la institución.
12. Implementar medidas de control de riesgos.
13. Dar seguimiento y revisión de los procesos y procedimientos de gestión de riesgos.
14. Actualizar el plan de gestión de riesgos según sea necesario.
15. Comunicar la información de gestión de riesgos a todas las partes relevantes.
16. Documentar todas las actividades de gestión de riesgos.

2.5. Diseño de la propuesta

2.5.1. Arquitectura de la solución

La arquitectura de la solución es la siguiente:

Figura 15. Arquitectura de la solución.

2.6. Estudio de Factibilidad

2.6.1. Técnica

Componente	Costo ($)	Cantidad	Subtotal	Total ($)
Hardware				650.00
Procesador Core i5	650.00	1	650.00	
4Gb de RAM				
CPU a 2 GHz				
Software				0.00
Power BI Desktop	0.00	1	0.00	
Draw.io	0.00	1	0.00	
Personal				1824.00
Analista de riesgos	457.00	1	914.00	
Operador en tecnologías	455.00	1	910.00	
Otros gastos				368.00
Energía eléctrica	10.00	1	20.00	
Internet	24.00	1	48.00	
Capacitaciones básicas	150.00	1	300.00	

Tabla 9. Presupuesto del proyecto.

La tabla anterior muestra los valores correspondientes al presupuesto de la solución en cuanto a hardware, software, personal y los gatos varios. En cuanto a software, el costo total será de $0.00 debido a que las herramientas a emplear son gratuitas. Los valores contemplados de personal se obtuvieron mediante la tabla de salarios mínimos sectoriales 2023 del Ministerio de Trabajo [43]. La propuesta tendrá una duración de 2 meses, además, se recalca que, aunque el presupuesto total aproximado para el desarrollo del proyecto es de $2842, todos los valores son cubiertos por el tesista.

2.6.2. Operativa

Dentro de la propuesta, se considera la importancia de tener conocimientos relacionados a la gestión de riesgos, así como métricas orientadas a la inteligencia de negocios, por ende, para cumplir con la factibilidad operativa de la misma, es recomendable realizar capacitaciones constantes en la institución encaminadas a la orientación de los encargados del Departamento Técnico, los cuales, estarán encargados de revisar los lineamientos de

la guía elaborada en esta propuesta. Entre los objetivos de estas capacitaciones se encuentran:

- Comprender el propósito y el alcance de la gestión de riesgos.
- Explicar las leyes, reglamentos, políticas y procedimientos pertinentes relacionados con la gestión de riesgos.
- Enseñar técnicas para identificar los riesgos potenciales, evaluarlos y gestionarlos.
- Enseñar métodos para comunicar las políticas y procedimientos de gestión de riesgos a las partes interesadas.
- Métodos didácticos para el seguimiento y reporte de las actividades de gestión de riesgos.
- Explicar las funciones y responsabilidades de las personas en la gestión de riesgos.
- Explicar la importancia de la toma de decisiones éticas y el cumplimiento en la gestión de riesgos.

2.7. Resultados

2.7.1. Identificación y valoración de activos

Tipo de activo	Descripción	Confidencialidad	Integridad	Disponibilidad	Promedio	Valor
Servicios	Portal web	3	3	3	3	Alto
Software	Ofimática	2	2	2	2	Medio
	Antivirus	1	1	1	1	Bajo
	Sistema de educación virtual	3	3	3	3	Alto
Hardware	Ordenadores portátiles	3	2	2	2	Medio
	Ordenadores de escritorio	3	2	2	2	Medio
	Miniordenadores	3	1	2	2	Medio
	Tabletas	3	1	2	2	Medio
	Cámaras web	1	1	1	1	Bajo
	Proyectores	1	1	1	1	Bajo
	Enrutadores	2	2	2	2	Medio
	Switches	2	2	2	2	Medio
	Puntos de acceso	1	1	1	1	Bajo
	Servidor dedicado	3	3	3	3	Alto
Comunicaciones	Red Local (LAN)	2	2	2	2	Medio
	Red Local Virtual (VLAN)	2	2	2	2	Medio

	Red Privada Virtual (VPN)	2	2	2	2	Medio
Equipamiento auxiliar	Fuentes de alimentación	0	0	0	0	Despreciable
	Generadores eléctricos	0	0	0	0	Despreciable
	Cableado de datos	0	0	0	0	Despreciable
Instalaciones	Centro de gestión informática	3	3	3	3	Alto
Soportes de información	Tarjetas de memoria	2	1	3	2	Medio
	Discos duros	2	3	1	2	Medio
	Memorias USB	2	1	3	2	Medio
Personal	Departamento técnico	1	1	1	1	Bajo
	Departamento de Planificación Estratégica	1	1	1	1	Bajo
	Departamento de Asesoría Jurídica	1	1	1	1	Bajo
	Departamento de Talento Humano	1	1	1	1	Bajo
	Mantenimiento	1	1	1	1	Bajo
	Guardianía	1	1	1	1	Bajo

Tabla 10. Identificación y valoración de activos de la institución.

La tabla anterior detalla la valoración de los 30 activos identificados en la institución, con su respectiva división, empleando las dimensiones de confidencialidad, integridad y disponibilidad, para su respectiva ponderación en escala del 0 al 3.

2.7.2. Identificación de amenazas y vulnerabilidades

Para proseguir con la identificación de amenazas y vulnerabilidades, primero se clasifican las amenazas.

Identificador	Amenaza	Descripción
D	Desastres naturales	Pueden causar daños significativos a la propiedad, la infraestructura y la vida humana, así como pérdidas económicas.
S	Seguridad cibernética	Son cualquier tipo de amenaza, ataque malicioso u otro evento que podría comprometer la seguridad de un sistema informático, una red o datos.
B	Continuidad del negocio	Son cualquier interrupción potencial de las operaciones, productos o servicios de una empresa que podría causar un daño financiero u operativo significativo.
F	Financieras	Son aquellas que pueden afectar la salud financiera de una empresa, como el aumento de los costos, los gastos inesperados y la disminución de las ventas.
P	Proyecto	Son riesgos potenciales que podrían afectar negativamente la finalización exitosa de un proyecto.
O	Operacionales	Son riesgos que surgen de procesos, personas y sistemas internos inadecuados o fallidos, o de eventos externos.
R	Recursos humanos	Pueden incluir posibles violaciones de datos, rotación de empleados y acoso en línea.
C	Cumplimiento	Se refieren a los riesgos que plantea la falta de cumplimiento de las reglas, normas y reglamentos.

Tabla 11. Clasificación de amenazas.

La tabla anterior muestra la clasificación de amenazas detectadas durante la aplicación de la guía (Ver Anexo 4) en la institución, las cuales se realizaron mediante el empleo de los diagramas causa y efecto. A continuación, se procede con la clasificación de amenazas y vulnerabilidades según la tabla de identificación de activos detallada anteriormente:

Tipo de activo	Descripción	Tipo	Amenazas	Vulnerabilidades	Dimensiones de seguridad afectadas
Servicios	Portal web	S	Autenticación defectuosa y robo de sesiones	Mecanismos de autenticación inseguros, mal manejo de credenciales de sesión	Confidencialidad
		S	Ataques de denegación de servicio	Monitoreo inadecuado y ausencia de reglas de prevención de intrusiones	Disponibilidad
		S	Ejecución de archivos maliciosos	Ausencia de restricciones en la carga de archivos	Confidencialidad, Integridad, Disponibilidad
Software	Ofimática	O	Información errónea de los usuarios	Falta de capacitación y revisiones	Integridad
		O	Errores en la actualización de los programas	Conflicto de versiones	Disponibilidad
		S	Ejecución de programas maliciosos	Uso de programas con licencias falsas o activadores	Confidencialidad, Integridad, Disponibilidad
	Antivirus	O	Errores en la actualización de antivirus	Conflicto de versiones	Disponibilidad
		O	Licencias caducadas	Ausencia de renovación de licencias automáticas	Disponibilidad
	Sistema de educación virtual	O	Errores de los usuarios	Falta de capacitación	Integridad
		S	Mala seguridad del sistema	Contraseñas compartidas o sin cifrar	Confidencialidad
		S	Ataques de denegación de servicio	Monitoreo inadecuado y ausencia de reglas de prevención de intrusiones	Disponibilidad

		S	Autenticación defectuosa y robo de sesiones	Mecanismos de autenticación inseguros, mal manejo de credenciales de sesión	Confidencialidad
		S	Ejecución de archivos maliciosos	Ausencia de restricciones en la carga de archivos	Confidencialidad, Integridad, Disponibilidad
		S	Exposición de información sensible	Código fuente expuesto a inyección de código.	Confidencialidad, Integridad
Hardware	Ordenadores portátiles	S	Dispersión de programas maliciosos en la red	Ordenador previamente infectado, conectándose a la red empresarial. Ausencia de cortafuegos	Confidencialidad, Integridad, Disponibilidad
		O	Pérdida de datos	Inexistente respaldo periódico de datos	Integridad, Disponibilidad
		O	Daños en el equipo	Mal manejo del dispositivo y falta de mantenimiento periódico	Disponibilidad
		S	Ejecución de programas maliciosos	Ausencia de antivirus y uso de dispositivos USB de dudosa procedencia	Confidencialidad, Integridad, Disponibilidad
	Ordenadores de escritorio	O	Pérdida de datos	Inexistente respaldo periódico de datos	Integridad, Disponibilidad
		O	Daños en el equipo	Mal manejo del dispositivo y falta de mantenimiento periódico	Disponibilidad
		S	Ejecución de programas maliciosos	Ausencia de antivirus y uso de dispositivos USB de dudosa procedencia	Confidencialidad, Integridad, Disponibilidad
	Miniordenadores	O	Pérdida de datos	Inexistente respaldo periódico de datos	Integridad, Disponibilidad

		O	Daños en el equipo	Mal manejo del dispositivo y falta de mantenimiento periódico	Disponibilidad
		S	Ejecución de programas maliciosos	Ausencia de antivirus y uso de dispositivos USB de dudosa procedencia	Confidencialidad, Integridad, Disponibilidad
	Tabletas	O	Pérdida de datos	Inexistente respaldo periódico de datos	Integridad, Disponibilidad
		O	Daños en el equipo	Mal manejo del dispositivo y falta de mantenimiento periódico	Disponibilidad
		S	Ejecución de aplicaciones maliciosas	Ausencia de antivirus e instalación de aplicaciones de dudosa procedencia	Confidencialidad, Integridad, Disponibilidad
		O	Robo del dispositivo	Ausencia de protocolos de control, descuido de los usuarios	Confidencialidad, Disponibilidad
		O	Robo de datos del dispositivo	Dispositivo sin contraseñas, descuido de los usuarios	Confidencialidad, Disponibilidad
	Cámaras web	O	Robo del dispositivo	Ausencia de protocolos de control, descuido de los usuarios	Confidencialidad, Disponibilidad
		O	Daños en el equipo	Falta de mantenimiento, mal uso del equipo	Integridad, Disponibilidad
	Proyectores	O	Robo del dispositivo	Ausencia de protocolos de control, descuido de los usuarios	Confidencialidad, Disponibilidad
		O	Daños en el equipo	Falta de mantenimiento, mal uso del equipo	Integridad, Disponibilidad

	Enrutadores	S	Intrusión de usuarios en la red	Uso de contraseñas por defecto o sin contraseñas. Ausencia de cortafuegos	Confidencialidad, Integridad
		S	Desconexión de red maliciosa	Ausencia de reglas y privilegios en la red	Integridad, Disponibilidad
		O	Daños en el equipo	Falta de mantenimiento, mal uso del equipo	Integridad, Disponibilidad
	Switches	S	Desconexión de red maliciosa	Ausencia de reglas y privilegios en la red	Integridad, Disponibilidad
		O	Daños en el equipo	Falta de mantenimiento, mal uso del equipo	Integridad, Disponibilidad
		O	Desconfiguración accidental	Ausencia de mecanismos de recuperación en caso de interrupciones	Disponibilidad
	Puntos de acceso	S	Intrusión de usuarios en la red	Uso de contraseñas por defecto o sin contraseñas. Ausencia de cortafuegos	Confidencialidad, Integridad
		O	Daños en el equipo	Falta de mantenimiento, mal uso del equipo	Integridad, Disponibilidad
		S	Dispersión de programas maliciosos en la red	Ausencia o desconexión de cortafuegos	Confidencialidad, Integridad, Disponibilidad
	Servidor dedicado	O	Daños en el equipo	Falta de mantenimiento, mal uso del equipo	Integridad, Disponibilidad
		S	Intrusión de usuarios en la red	Uso de contraseñas por defecto o sin contraseñas. Ausencia de cortafuegos	Confidencialidad, Integridad
		S	Ejecución de programas maliciosos en el equipo	Ausencia de mecanismos de seguridad, antivirus, cortafuegos.	Confidencialidad, Integridad, Disponibilidad

		S	Robo de datos	Ausencia de mecanismos de gestión de privilegios	Confidencialidad
Comunicaciones	Red Local (LAN)	S	Ejecución de programas maliciosos	Flujo o descarga de archivos de dudosa procedencia en la red	Confidencialidad, Integridad, Disponibilidad
		S	Ataque de intercepción (Man-in-the-middle)	Configuración de red insegura y ausencia de mecanismos de protección	Confidencialidad, Integridad, Disponibilidad
		S	Ataque interno	Ausencia de restricciones de red, usuarios con privilegios extendidos	Confidencialidad, Disponibilidad
	Red Local Virtual (VLAN)	S	VLAN desconfigurada con brechas de seguridad	Red sin restricciones de acceso o incorrectamente configuradas	Confidencialidad
		S	Suplantación de red	Etiquetas de red sin restricciones, falta de reglas de identificación de VLANs	Confidencialidad, Integridad
		S	Intrusión por saltos entre VLANs	Configuración de VLAN con vulnerabilidades explotables, protocolo ARP desactualizado	Confidencialidad
	Red Privada Virtual (VPN)	S	Ataque de intercepción (Man-in-the-middle)	Configuración de red insegura y ausencia de mecanismos de protección	Confidencialidad, Integridad, Disponibilidad
		S	Ejecución de programas maliciosos	Flujo o descarga de archivos de dudosa procedencia en la red	Confidencialidad, Integridad, Disponibilidad
		S	Redes inseguras	Ausencia de algoritmos de cifrado o uso de protocolos puramente HTTP	Confidencialidad

Equipamiento auxiliar	Fuentes de alimentación	D	Cortes de energía por desastres naturales	Ausencia de mecanismos de recuperación de energía, o fuentes de energías de respaldo	Disponibilidad
		O	Saltos de energía	Ausencia de reguladores de voltaje en los equipos de la empresa	Disponibilidad
		O	Cortes de energía por fallas externas	Ausencia de fuentes de energía de respaldo UPS	Disponibilidad
	Generadores eléctricos	O	Fallos mecánicos del equipo	Falta de mantenimiento periódico	Disponibilidad
		C	Fallo por combustible contaminado	Incumplimiento en la revisión del combustible antes de su uso	Disponibilidad
	Cableado de datos	O	Daño físico	Cortes accidentales, daño por doblaje o daño accidental durante mantenimientos y construcción	Disponibilidad
		O	Interrupción electromagnética	El cableado se encuentra muy cerca de generadores de energía u otros equipos eléctricos que producen campos electromagnéticos	Disponibilidad
Instalaciones	Centro de gestión informática	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		O	Pérdida de información sensible	Errores humanos, o borrado accidental de datos	Integridad, Disponibilidad
		D	Destrucción de la información por desastres naturales	Falta de respaldo de datos basados en la nube, o en	Disponibilidad

				lugares secundarios a la empresa	
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad
Soportes de información	Tarjetas de memoria	O	Daño físico	Caídas accidentales, almacenamiento y manipulación inadecuado	Disponibilidad
		O	Pérdida de información sensible	Errores humanos, o borrado accidental de datos	Integridad, Disponibilidad
		S	Dispersión de programas maliciosos	Almacenamiento de archivos o programas infectados	Confidencialidad, Integridad, Disponibilidad
		O	Robo del dispositivo	Ausencia de protocolos de control, descuido de los usuarios	Confidencialidad, Disponibilidad
	Discos duros	O	Daño físico	Caídas accidentales, almacenamiento y manipulación inadecuado	Disponibilidad
		O	Pérdida de información sensible	Errores humanos, o borrado accidental de datos	Integridad, Disponibilidad
		S	Dispersión de programas maliciosos	Almacenamiento de archivos o programas infectados	Confidencialidad, Integridad, Disponibilidad
		O	Robo del dispositivo	Ausencia de protocolos de control, descuido de los usuarios	Confidencialidad, Disponibilidad

	Memorias USB	O	Daño físico	Caídas accidentales, almacenamiento y manipulación inadecuado	Disponibilidad
		O	Pérdida de información sensible	Errores humanos, o borrado accidental de datos	Integridad, Disponibilidad
		S	Dispersión de programas maliciosos	Almacenamiento de archivos o programas infectados	Confidencialidad, Integridad, Disponibilidad
		O	Robo del dispositivo	Ausencia de protocolos de control, descuido de los usuarios	Confidencialidad, Disponibilidad
		O	Daño físico	Caídas accidentales, almacenamiento y manipulación inadecuado	Disponibilidad
		O	Pérdida de información sensible	Errores humanos, o borrado accidental de datos	Integridad, Disponibilidad
		S	Dispersión de programas maliciosos	Almacenamiento de archivos o programas infectados	Confidencialidad, Integridad, Disponibilidad
Personal	Departamento técnico	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		O	Pérdida de información sensible	Errores humanos, o borrado accidental de datos	Integridad, Disponibilidad
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad

	Departamento de Planificación Estratégica	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad
		P	Atrasos en los proyectos	Mal manejo de los recursos y errores de planificación	Disponibilidad
		F	Falta de presupuesto	Gastos imprevistos o estimación de costos errónea	Disponibilidad
	Departamento de Asesoría Jurídica	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad
		F	Problemas de precisión financiera	Errores humanos o uso de procesos desactualizados	Integridad
	Departamento de Talento Humano	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad
		R	Rotación de personal	Malas condiciones laborales o mala compensación al	Disponibilidad

				empleado. Falta de regulación	
		O	Imprecisión de datos	Errores humanos, procesos desactualizados, falta de sistemas administrativos	Integridad
	Mantenimiento	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad
		O	Fallas en los equipos de mantenimiento	Mantenimiento inadecuado, o pobre control de calidad	Disponibilidad
	Guardianía	O	Accesos no autorizados	Falta de control de acceso a personas sin credenciales y permisos adecuados	Confidencialidad, Integridad
		D	Destrucción por incendios	Falta de mecanismos de prevención de incendios como extintores, rociadores, etc.	Disponibilidad
		O	Brechas de seguridad física	Medidas de seguridad inadecuada o falta de control de acceso	Confidencialidad, Integridad
		O	Negligencia en los empleados	Falta de capacitación y entrenamiento, falta de motivación o inadecuada supervisión	Confidencialidad, Integridad

Tabla 12. Identificación de amenazas y vulnerabilidades de los activos de la institución.

Las amenazas y vulnerabilidades pueden variar desde intrusos físicos hasta atacantes cibernéticos, y es importante identificar las posibles fuentes de riesgo para estar preparado y poder responder de manera rápida y efectiva en caso de un ataque. En este caso, la mayor cantidad de amenazas recaen en la clasificación de amenazas operacionales y de seguridad cibernética.

2.7.3. Identificación de métricas de riesgo

Luego de realizar la respectiva identificación de activos y, posterior, clasificación de amenazas y vulnerabilidades dentro de la institución, se han identificado algunas métricas de riesgo, entre estas, destaca el estado de riesgo de falla de los equipos de la institución relacionada a los activos de hardware.

Tipo de activos	Amenazas	Vulnerabilidades	Métrica para evaluar
Hardware	Daños en el equipo	Mal manejo del dispositivo y falta de mantenimiento periódico	Estado de falla de los equipos

Tabla 13. Identificación de métricas de riesgo.

La tabla anterior denota una vulnerabilidad existente, en su mayoría, en los activos de hardware, la cual se encuentra relacionada al mantenimiento de los equipos de la institución objeto de estudio.

El estado de riesgo de falla de los equipos es una métrica de gestión de riesgos que ayuda a identificar, evaluar y gestionar el riesgo de falla de los equipos. Esta métrica utiliza factores como el estado de mantenimiento, las condiciones ambientales y la antigüedad de los equipos para determinar el nivel de riesgo de falla. Esto permite a los equipos de operaciones y gestión de riesgos tomar medidas preventivas para reducir el riesgo de falla y minimizar el impacto de una posible falla.

Para esta propuesta, los datos proporcionados permitirán evaluar esta métrica mediante las órdenes de trabajo en la institución, estableciendo la siguiente división dentro del Departamento Técnico:

- Mantenimiento
- Integridad

Esta división permitirá corroborar, mediante una matriz de riesgos, cuál es el nivel de riesgo para esta métrica luego de aplicar los controles propuestos (Ver Anexo 5).

2.7.4. Perfiles de amenazas basados en los activos

Para realizar la creación de los perfiles de amenazas basados en los activos, se seleccionaron los activos cuya valoración de seguridad fue "Alta". En esto caso, los activos seleccionados son los siguientes:

- Portal web
- Sistema de educación virtual
- Servidor dedicado
- Centro de gestión informática

A continuación, se muestran los perfiles de amenazas:

Perfil de activos de información		
Activo	Portal web	
Descripción: Un portal web es un sitio web que sirve como punto único de acceso a información y servicios de múltiples fuentes, a menudo de diferentes organizaciones o instituciones.		
Fecha de creación:	2/02/2023	
Titular del activo	Personal del Departamento Técnico	
Contenedores		
Hardware:	Servidor dedicado	
Requerimientos de seguridad		
Confidencialidad: Los datos sólo se recopilarán para un propósito determinado (Cookies), respetándose la identidad de los usuarios.		
Integridad: La información que se muestre mediante el portal web deberá siempre estar actualizada y sin errores.		
Disponibilidad: El portal web deberá estar disponible las 24 horas del día de forma indefinida.		
Valoración		
Confidencialidad:	Integridad:	Disponibilidad: X
Observación: El portal web debe estar disponible de forma continua ya que su audiencia serán usuarios internos y ajenos a la institución. Su indisponibilidad causará incomodidad y desconfianza en la institución.		

Tabla 14. Perfil de amenazas del activo Portal Web.

El perfil de amenazas de activos anterior, correspondiente al portal web describe los posibles riesgos de seguridad asociados con el portal web de la institución, donde, su valoración más significativa se realiza en cuanto a la dimensión de disponibilidad.

Perfil de activos de información		
Activo	Sistema de educación virtual	
Descripción: El sistema de educación virtual es una plataforma web sobre la que se ejecuta Moodle y sirve para administrar el ambiente de educación en línea, permitiendo gestionar, cursos, tareas, calificaciones, etc.		
Fecha de creación:	2/02/2023	
Titular del activo	Personal de Departamento técnico	
Contenedores		
Hardware:	Servidor dedicado	
Requerimientos de seguridad		
Confidencialidad: Solo los usuarios con las credenciales correspondientes podrán acceder al sistema con un usuario y contraseñas únicos. El acceso que se otorgue dependerá del rol de cada usuario.		
Integridad: La información mostrada deberá ser verídica y confiable para el correcto desenvolvimiento académico.		
Disponibilidad: La plataforma deberá estar disponible las 24 horas del día de manera indefinida.		
Valoración		
Confidencialidad:	Integridad:	Disponibilidad: X
Observación: La indisponibilidad de la plataforma de educación virtual generará molestias y retrasará las actividades planificadas tanto por docentes como estudiantes.		

Tabla 15. Perfil de amenazas del activo Sistema de educación virtual.

El perfil de amenaza de un activo del sistema de educación virtual dependerá del sistema específico y de los datos que almacena y procesa. En este caso la valoración también se centra en la dimensión de disponibilidad, ya que, al generarse molestias, causará retrasos en las actividades planificadas tanto por docentes como estudiantes.

Perfil de activos de información			
Activo	Servidor dedicado		
Descripción: El servidor dedicado es un dispositivo donde se alojan los servicios virtuales de la institución, por ejemplo: plataformas, aplicaciones, páginas web, etc.			
Fecha de creación:	2/02/2023		
Titular del activo	Personal de Departamento técnico		
Contenedores			
Hardware:	Centro de gestión informática		
Requerimientos de seguridad			
Confidencialidad: Solo los usuarios con las credenciales correspondientes podrán acceder al servidor dedicado siguiendo el respectivo control de acceso, tanto físico como con un usuario y contraseñas únicos. El acceso que se otorgue dependerá del rol de cada usuario.			
Integridad: La información y aplicaciones almacenadas en el servidor deben ser íntegras y confiables.			
Disponibilidad: La plataforma deberá estar disponible las 24 horas del día de manera indefinida.			
Valoración			
Confidencialidad: X	Integridad: X	Disponibilidad: X	
Observación: La indisponibilidad del servidor dedicado generará muchas molestias y detendrá el flujo normal de trabajo en la organización.			

Tabla 16. Perfil de amenazas del activo Servidor dedicado.

En cuanto al perfil de amenazas del servidor dedicado, este posee una valoración en los tres criterios de seguridad (confidencialidad, integridad y disponibilidad) pues, es aquí donde se alojan servicios virtuales de la institución, por ejemplo: plataformas, aplicaciones, páginas web, etc.

Perfil de activos de información			
Activo	Centro de gestión informática		
Descripción: El departamento de gestión informática es la división responsable de mantener la infraestructura tecnológica de la institución.			
Fecha de creación:	2/02/2023		
Titular del activo	Personal de Departamento técnico		
Contenedores			
Hardware:	Centro de gestión informática		
Requerimientos de seguridad			
Confidencialidad: Solo los empleados con las credenciales correspondientes podrán acceder al departamento siguiendo el respectivo control de acceso. El rol del empleado permitirá acceder a cierta información o infraestructura dependiendo de sus necesidades.			
Integridad: La información y equipos almacenados en el departamento deben ser íntegras y confiables.			
Disponibilidad: El departamento de gestión informática deberá estar disponible las 8 horas del día durante días laborales. Y en cualquier momento en casos extraordinarios.			
Valoración			
Confidencialidad:	Integridad:	Disponibilidad: X	
Observación: La indisponibilidad del centro de gestión informática podrá causar retrasos al momento de tratar la atención al usuario o proveer soluciones adecuadas a fallas específicas.			

Tabla 17. Perfil de amenazas del activo Centro de Gestión Informática.

De acuerdo con el perfil de amenazas anterior, la valoración más importante, en cuanto al Centro de Gestión Informática, recae en la dimensión de disponibilidad pues, al ser este activo el responsable de la infraestructura tecnológica de la institución, en el caso de que haya retrasos, no se podrán proveer soluciones adecuadas a fallas específicas.

2.7.5. Áreas de preocupación

Las áreas comunes de preocupación halladas al aplicar la guía son las siguientes:

Activos	Áreas de preocupación
Portal web	Ataques de denegación de servicio
Sistema de Educación Virtual	Autenticación defectuosa y robo de sesiones
Servidor dedicado	Exposición de información sensible
Centro de Gestión Informática	Destrucción de la información por desastres naturales

Tabla 18. Áreas de preocupación según activos críticos.

En la tabla anterior se identifica al menos un área de preocupación por cada activo crítico detectado en el proceso de identificación y valoración de activos. En este caso, debido a que se han seleccionado cuatro activos, el número de áreas de preocupaciones también es cuatro.

Área de preocupación según activo				
Activo:	Portal web			
Área de preocupación:	Ataques de denegación de servicio			
Actor:	Atacantes externos			
Medio:	Monitoreo inadecuado Vulneración de contraseñas débiles Explotación de vulnerabilidades en la plataforma Explotación de los protocolos de seguridad			
Motivos:	Falta de capacitación del personal Ausencia de protocolos de seguridad Ausencia de reglas de prevención de intrusiones			
Resultados:	Divulgación:	Modificación:	Destrucción:	Interrupción: X
Requisito de seguridad:	Utilizar servicios de mitigación de DDoS, implementar segmentación de red y monitorear la actividad de la red de forma constante.			

Tabla 19. Área de preocupación de activo Portal web.

En cuanto a los ataques de denegación de servicio se identifican cuatro medios que propician esta área de preocupación, entre los que destacan monitoreos inadecuados y la explotación de los protocolos de seguridad.

Área de preocupación según activo				
Activo:	Sistema de Educación Virtual			
Área de preocupación:	Autenticación defectuosa y robo de sesiones			
Actor:	Atacantes externos			
Medio:	Explotación de contraseñas Clonación de Cookies de sesión Explotación de brechas en la autenticación			
Motivos:	Uso de computadores infectadas con malware. Fallas en el sistema de autenticación. Mal manejo y almacenamiento de cookies en el navegador. Envío de contraseñas sin encriptar en cookies.			
Resultados:	Divulgación: X	Modificación:	Destrucción:	Interrupción:
Requisito de seguridad:	Usar servicios de autenticación certificados. Asegurar el manejo de las cookies de sesión y encriptar contraseñas en cada petición que las requiera.			

La mala autenticación y el robo de sesiones pueden deberse a contraseñas débiles, uso de contraseñas compartidas o genéricas, falta de autenticación de dos factores y administración de sesiones insegura.

Área de preocupación según activo				
Activo:	Servidor dedicado			
Área de preocupación:	Exposición de información sensible			
Actor:	Atacantes internos o externos			
Medio:	Salto de privilegios en el servidor Explotación de contraseñas vulnerables Uso de credenciales por defecto Explotación de vulnerabilidades en el servidor			
Motivos:	Ausencia de mecanismos de gestión de privilegios Exposición de contraseñas			
Resultados:	Divulgación: X	Modificación: X	Destrucción: X	Interrupción:

Requisito de seguridad:	Mantener actualizados los controles de acceso, realizar auditorías de seguridad recurrente, garantizar un sistema de respaldo de información de forma periódica y limitar el acceso físico o por credenciales a información sensible.

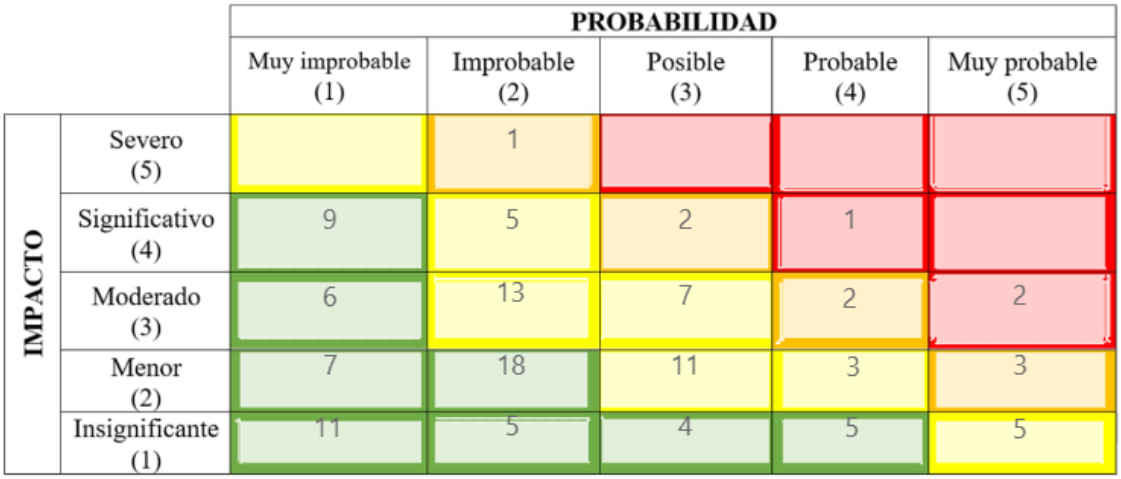
Una forma de proteger la información confidencial en las instituciones es contar con políticas claras con respecto a la seguridad y el acceso a los datos. Estas políticas deben especificar quién está autorizado a acceder a ciertos tipos de datos y cómo se pueden utilizar. Según esta área de preocupación, entre los resultados negativos que pueden ocurrir se encuentran: divulgación, modificación y destrucción de la información.

Área de preocupación según activo				
Activo:	Centro de Gestión Informática			
Área de preocupación:	Destrucción de la información por desastres naturales			
Actor:	Eventos externos			
Medio:	Destrucción física de los dispositivos de almacenamiento. Pérdida o desaparición de los dispositivos de almacenamiento.			
Motivos:	Falta de respaldo de datos recurrente. Falta de respaldo de datos en la nube. Almacenamiento de toda la información de forma centralizada.			
Resultados:	Divulgación:	Modificación:	Destrucción: X	Interrupción:
Requisito de seguridad:	Implementar sistemas de respaldos de datos basados en la nube y realizarlos de forma periódica o poseer dispositivos de almacenamiento secundarios donde se respaldará esta información en un lugar seguro y recuperable.			

Los desastres naturales pueden causar daños significativos en las instituciones, lo que lleva a la destrucción de la información. Esto puede incluir documentos físicos como registros de estudiantes, datos financieros y registros de empleados, así como materiales digitales como computadoras y sistemas de software.

2.7.6. Evaluación de métricas de riesgo

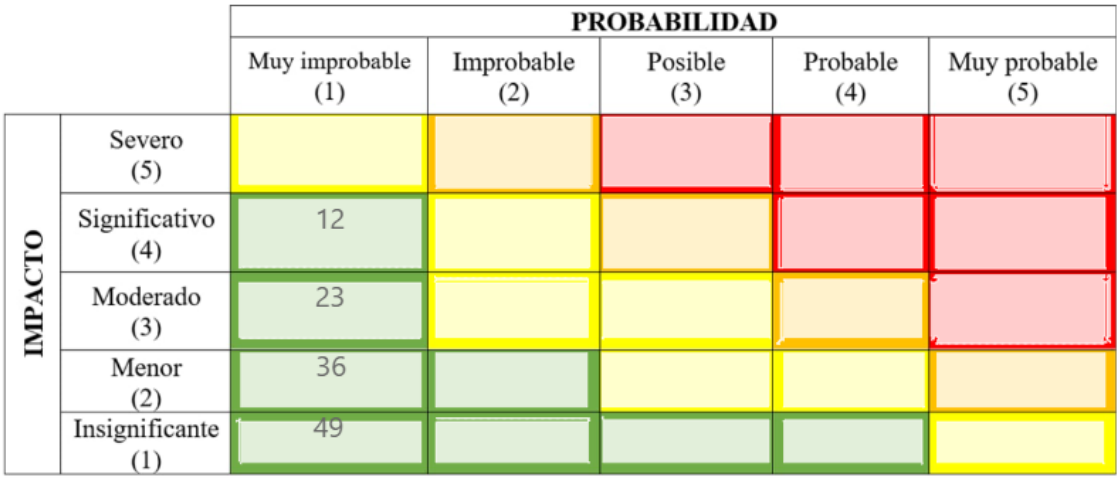
La métrica identificada durante la aplicación de la guía de gestión de riesgos fue el estado de falla de los equipos donde los resultados, analizados mediante la matriz de riesgos, se muestran a continuación:



		PROBABILIDAD				
		Muy improbable (1)	Improbable (2)	Posible (3)	Probable (4)	Muy probable (5)
IMPACTO	Severo (5)		1			
	Significativo (4)	9	5	2	1	
	Moderado (3)	6	13	7	2	2
	Menor (2)	7	18	11	3	3
	Insignificante (1)	11	5	4	5	5

Figura 16. Matriz de riesgos antes del control.

En la figura anterior se evidencia que antes de aplicar los controles, con respecto a la métrica de estado de riesgo de falla de los equipos de la institución, se habían detectado riesgos cuya ponderación de impacto era de cuatro (significativo) y su probabilidad también era de cuatro (probable), e incluso, hubo riesgos cuya probabilidad fue de cinco (muy probable).



		PROBABILIDAD				
		Muy improbable (1)	Improbable (2)	Posible (3)	Probable (4)	Muy probable (5)
IMPACTO	Severo (5)					
	Significativo (4)	12				
	Moderado (3)	23				
	Menor (2)	36				
	Insignificante (1)	49				

Figura 17. Matriz de riesgos después del control.

Una vez aplicados los controles pertinentes de la guía, los riesgos identificados poseían una probabilidad de uno (Muy improbable), cuya ponderación del impacto fue de uno (insignificante) hasta cuatro (significativo).

2.7.7. Resultados de la variable del proyecto

Marco de tiempo para las actividades de gestión de riesgos	
Antes	**Después**
De 14 a 21 días	De 5 a 7 días

Tabla 20. Resultados de la variable del proyecto.

Los resultados de la variable del proyecto reflejan cuánto disminuye el marco de tiempo para las actividades de gestión de riesgos, donde, antes de que se aplicara la guía en la institución, la duración era de 14 a 21 días, respuesta fundamentada en la entrevista realizada (Ver Anexo 2). Ahora, este marco de tiempo se logró disminuir a una duración de 5 a 7 días.

CONCLUSIONES

- Se logró diseñar una guía de análisis de riesgos mediante un estudio comparativo para gestionar la toma de decisiones de políticas de seguridad de la información en una institución educativa privada. Esta guía está compuesta por tres etapas, partiendo desde la identificación y valoración de activos hasta el análisis de las métricas de riesgos. Esto permitió identificar cuáles eran las amenazas y vulnerabilidades presentes, así como los riesgos a los que se encuentran expuestos los activos de la información garantizando medidas que solventen la seguridad de la información en la institución de forma eficaz.

- Se realizó el levantamiento de información sobre las metodologías de gestión de riesgos para identificar las mejores prácticas en la seguridad de la información, siendo estas: ISO 31000:2018, CRAMM, Magerit y OCTAVE. Esto permitió comparar la estructura de cada metodología seleccionando elementos determinados, de cada una, para el diseño de la guía aplicada para esta propuesta. En cuanto a ISO 31000:2018, se escogió el empleo de controles de seguridad, así como la aplicación de una matriz de riesgos; de CRAMM, se seleccionó su método, cuyo enfoque cualitativo, permite analizar los riesgos a través de técnicas como entrevistas; con respecto a Magerit, su elemento más significado se halla en la clasificación de los activos de la información; finalmente, de OCTAVE, se escogió la creación de perfiles de amenazas de activos.

- Se establecieron cuáles eran los activos relevantes de la institución mediante un diagnóstico del estado actual de la seguridad de la información. Así, se logró clasificar los activos en nueve categorías, las cuales fueron: servicios, software, hardware, comunicaciones, equipamiento auxiliar, instalaciones, soportes de información y personal. Esto permitió realizar una valoración mediante criterios de seguridad en donde los activos críticos fueron: el portal web, el Sistema de Educación Virtual, el servidor dedicado y el Centro de Gestión Informática. También, esto contribuye a garantizar que las decisiones tomadas se basen en conocimientos precisos y actualizados.

- Se logró realizar una identificación de las métricas de riesgos que existen en la institución, en donde, la métrica más determinante fue el estado de riesgo de falla en los equipos de la institución. Esta métrica se relaciona con los activos pertenecientes al hardware de la institución. Esto permitió proporcionar información sobre cómo las decisiones están afectando a la organización. Con esta información, las organizaciones pueden tomar decisiones más informadas y estar mejor preparadas para abordar los riesgos potenciales al realizar una identificación de amenazas y vulnerabilidades latentes en los activos de la información.

- Se logró la identificación de áreas de preocupación, mediante la valoración de los activos, que necesitan más atención o recursos, las cuales, se relacionan directamente con los activos críticos detectados en la institución. De esta manera, se realizó una posterior identificación de las áreas de preocupación en cuanto a las amenazas que caracterizan a los activos de la información más críticos. Esto permite a la institución priorizar los recursos y centrarse en las áreas que necesitan más atención que otras, así como, ayudar a optimizar las operaciones y mejorar la eficiencia general.

RECOMENDACIONES

- Emplear otras herramientas relacionadas a la gestión de riesgos para evaluar el correcto desempeño de otros indicadores de gestión de riesgo. Con el uso de otras herramientas, la institución puede comunicar mejor la información sobre riesgos a las partes interesadas, lo que le permitirá tomar decisiones más informadas. Estas herramientas también permitirán desarrollar planes de riesgo, e incluso, pueden realizar un mejor seguimiento y cumplir con las reglamentaciones locales de la institución.

- Emplear otras métricas de riesgos para su respectiva evaluación antes y después de aplicar los controles pertinentes. Hay varias otras métricas de riesgo que se pueden usar para evaluar los riesgos de seguridad antes y después de la aplicación de los controles pertinentes. Entre estas resalta el valor de riesgo, utilizada para identificar y gestionar las pérdidas potenciales causadas por una variedad de riesgos, como los riesgos financieros y operativos.

- Establecer un enfoque cuantitativo en cuanto a la gestión de riesgos, implicando analizar y cuantificar los riesgos asociados con una actividad o decisión en particular. Esto puede incluir el uso de herramientas cuantitativas, como simulaciones de Monte Carlo, para estimar los posibles resultados de una determinada decisión o actividad, o el uso de modelos estadísticos para evaluar la probabilidad de ciertos eventos.

BIBLIOGRAFÍA

[1] C. Merino Bada y R. Cañizares Sales, Auditoría de Sistemas de Gestión de Seguridad de la Información, Madrid: FC Editorial, 2014.

[2] R. Gómez, D. H. Pérez y A. Herrera, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información,» *UNIANDES*, vol. I, nº 31, pp. 109-118, 2010.

[3] U. Espino Pérez, «Desarrollo de un Modelo de Gestión de Riesgos Según la Norma UNE ISO 31000 para el Tratamiento de Reclamaciones en Edificación,» 2014. [En línea]. Available: https://idus.us.es/bitstream/handle/11441/26883/Q_Tesis_MUEP.pdf?sequence=1&isAllowed=y. [Último acceso: 2022].

[4] G. M. d. l. M. Alama Visitación, «Implementación de un Sistema de Gestión de Riesgos basados en el estándar ISO 31000 en el proceso de Atención de Requerimientos de la empresa Software Enterprise Services en la ciudad de Lima – 2018,» 2019. [En línea]. Available: https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/1840/Gloria%20Alama_Trabajo%20de%20Suficiencia%20Profesional_Titulo%20Profesional_2019.pdf?sequence=1&isAllowed=y. [Último acceso: 2022].

[5] K. d. R. Gaona Vásquez, «Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito S.A. en la ciudad de Machala,» 2013. [En línea]. Available: https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf. [Último acceso: 2022].

[6] E. J. Santiago Chinchilla y J. Sánchez Allende, «Riesgos de ciberseguridad en las Empresas,» *Revista Tecnología y Desarrollo*, vol. XV, nº 5, pp. 1-33, 2018.

[7] «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.,» *Revista Tecnológica ESPOL*, vol. XXVIII, nº 5, pp. 492-507, 2015.

[8] A. Aspin, Pro Power BI Desktop, Primera ed., Staffordshire: Apress, 2016, pp. 1-3.

[9] Universidad Estatal Península de Santa Elena, «RCS-SE-06-03-2022,» 6 Marzo 2022. [En línea]. Available: https://www.upse.edu.ec/secretariageneral/images/archivospdfsecretaria/RESOLUCIONES/RESOLUCIONES_2022/RESOLUCIONES_SESIONES_EXTRAORDINARIA_2022/RESOLUCIONES_SESION_EXTRAORDINARIA_No._06-2022/RCS-SE-06-03-2022_REAJUSTE_DE_PROYECTOS_DE_INVESTIGACION_1-signe. [Último acceso: 24 Noviembre 2022].

[10] M. Orozco Alzate y F. J. Valencia Duque, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» *RISTI*, nº 22, pp. 73-88, 2017.

[11] Y. Ramos, O. Urrutia, A. Bravo y D. Ordóñez, «Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca.,» *Memorias De Congresos UTP*, pp. 88-95, 2017.

[12] Secretaría Nacional de Planificación, «Plan de Creación de Oportunidades 2021-2025 de Ecuador,» 2021. [En línea]. Available: https://observatorioplanificacion.cepal.org/es/planes/plan-de-creacion-de-oportunidades-2021-2025-de-ecuador. [Último acceso: 2022].

[13] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, Metodología de la Investigación, Sexta ed., México D.F.: McGraw Hill, 2014, p. 91.

[14] M. I. Baas Chable, M. G. Barceló Méndez y G. R. d. F. Herrera Garnica, Metodología de la Investigación, Naucalpan de Juárez: Pearson, 2012.

[15] N. Quezada Lucio, Metodología de la investigación: estadística aplicada en la Investigación, Lima: Macro, 2010.

[16] C. Blanco, Encuesta y estadística: Métodos de investigación cuantitativa en las ciencias sociales y comunicación, Córdoba: Brujas, 2011.

[17] A. Premkumar, «Sistematización de la Capacitación para las actividades de Rigging & Slinging con el Nivel Mínimo de KSA's a través del Ciclo CAP-DO,» *Indian Journal Of Training and Development,* vol. L, nº 4, pp. 67-70, 2020.

[18] W. Rivera Yanasupo, «Modelo de gestión de mantenimiento bajo el enfoque PDCA y su influencia en la eficiencia general de máquinas en los buques de la armada peruana,» 2019. [En línea]. Available: http://repositorio.unac.edu.pe/bitstream/handle/20.500.12952/4406/rivera%20yanasupo%20fime%20maestria%202019.pdf?sequence=1&isAllowed=y. [Último acceso: 2022].

[19] «La matriz FODA: alternativa de diagnóstico y determinación de estrategias de intervención en diversas organizaciones,» *Enseñanza e Investigación en Psicología,* vol. XII, nº 1, pp. 113-130, 2007.

[20] O. Alvarado Cervantes, «Administración estratégica: Análisis PESTEL,» 2015. [En línea]. Available: https://articulateusercontent.com/rise/courses/V7SMhP4TwoZ4eYrnn01rrgF2aklylKAi/PvwDvDPW2sopgW2t-administraci-c-3-b-3-n-20-estrat-c-3-a-9-gica.pdf.

[21] B. Viteri, «Legitimidad del tratamiento de datos personales en el sector de la educación,» 2 Septiembre 2021. [En línea]. Available: https://www.avl.com.ec/legitimidad-del-tratamiento-de-datos-personales-en-el-sector-de-la-educacion/#:~:text=A%20lo%20largo%20de%20la,ejercicio%20de%20la%20funci%C3%B3n%20educativa.. [Último acceso: 29 Enero 2023].

[22] Asamble Nacional, «Ley Orgánica de Protección de Datos Personales,» 21 Mayo 2021. [En línea]. Available: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf. [Último acceso: 29 Enero 2023].

[23] R. Gómez, D. Hernán Pérez, Y. Donoso y A. Herrera, «Metodología y gobierno de la gestión de riesgos de tecnologías de la información,» *Uniandes,* vol. I, nº 31, pp. 109-118, 2010.

[24] Deloitte, «Los riesgos de la tecnología de la información en los servicios financieros: Lo que los miembros de junta necesitan saber y hacer,» 2016. [En línea]. Available: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf.

[25] ISO, «Norma Internacional ISO 31000:2018,» 2018. [En línea]. Available: https://gateway.ipfs.io/ipfs/bafykbzaceair45aunn2b7wufrrap6s5jifpt2g2yyyaa2nputpl4qia2ip4fi?filename=ISO%20-%20Norma%20Internacional%20ISO%2031000_2018-ISO%20%282018%29.pdf.

[26] I. El Fray, «Un estudio comparativo de los métodos de evaluación de riesgos, MEHARI y CRAMM con un nuevo modelo formal de evaluación de riesgos (FoMRA) en sistemas de información,» *Springer,* vol. X, nº 15, pp. 428-442, 2012.

[27] C. Alberts, A. Dorofee, J. Stevens y C. Woody, Introducción al enfoque OCTAVE, Pensilvania: Carnegie Mellon University, 2003.

[28] G. Cordero Torres, «Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información,» 2015. [En línea]. Available: https://dspace.uazuay.edu.ec/bitstream/datos/5051/1/11490.pdf.

[29] S. Hernández y C. Schou, Information assurance handbook: effective computer security and risk management strategies, New York: McGraw-Hill Education, 2015.

[30] R. Reid, Facility manager's guide to security: protecting your assets, Atlanta: Fairmont Press, 2005.

[31] D. Death, Information Security Handbook, Birmingham: Packt Publishing, 2017.

[32] M. Talabis y J. Martin, Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data Analysis, Waltham: Syngress, 2012.

[33] M. Whitman y H. Mattord, Principles of Information Security, Boston: Course Technology , 2011.

[34] K. Heldman, Project Manager's Spotlight on Risk Management, San Francisco: Harbor Light Press, 2005.

[35] L. Hayden, IT Security Metrics: A Practical Framework for Measuring Security Protecting Data, New York: McGraw Hill, 2010.

[36] A. Al Murad Chowdhury y S. Arefeen, «Gestión de riesgos de software: importancia y prácticas,» *IST Involvement Fair,* vol. II, nº 1, pp. 49-54, 2011.

[37] M. M. Arteaga Martínez, «Gestión de riesgos de TI,» Octubre 2017. [En línea]. Available: http://repository.ucc.edu.co/bitstream/20.500.12494/17596/1/2017_NC_Gesti%C3%B3n%20de%20riesgos%20de%20ti_Arteaga.pdf.

[38] A. Novales, Valor en Riesgo, Madrid: Universidad Complutense, 2016.

[39] Y. Gutiérrez y A. Sánchez Ortiz, «Diseño de un Modelo de Gestión de Riesgos basado en ISO 31.000:2012 para los Procesos de Docencia de Pregrado en una Universidad Chilena,» *SciELO,* vol. XI, nº 4, pp. 15-32, 2018.

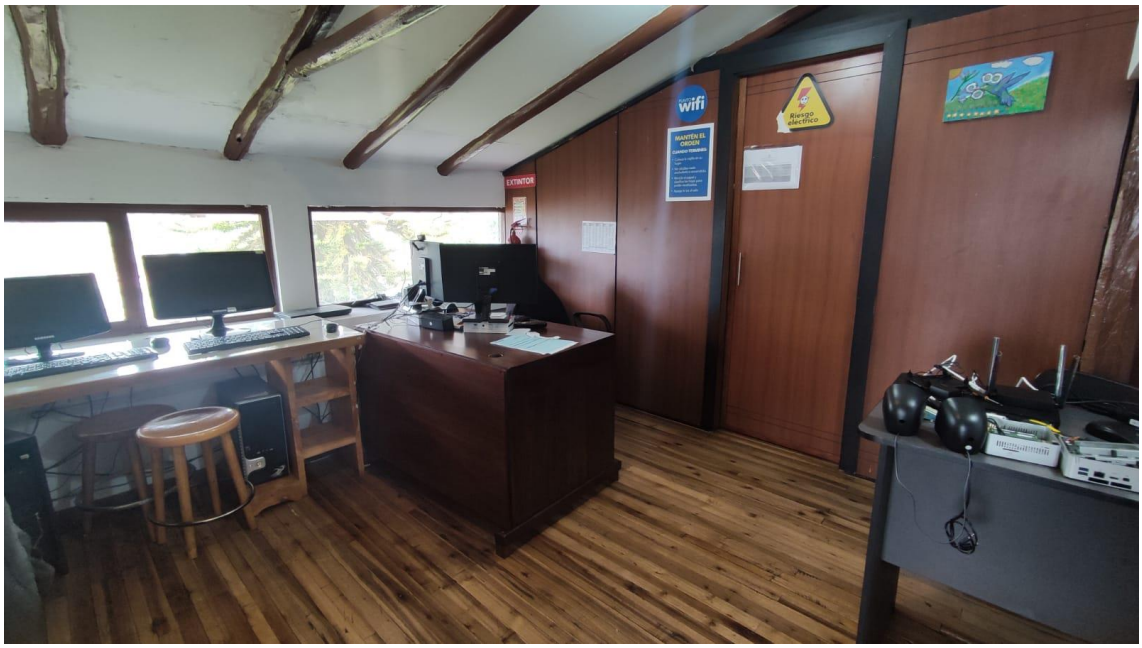
[40] Y. Bolaño Rodríguez, D. Alfonso Robaina, A. Pérez Barnés y M. Arias Pérez, «Modelo de Dirección Estratégica basado en la Administración de Riesgos,» *SciELO,* vol. XXXV, nº 3, pp. 344-357, 2014.

[41] E. Crespo Martínez, «Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs,» *Enfoque UTE,* vol. VIII, nº 1, pp. 107-121, 2017.

[42] D. Valverde Barrantes, «Propuesta de un Programa para el Control de Riesgos Operacionales y Mecánicos durante el Manejo de las Grúas Torre en la empresa Yoses S.A.,» 2014. [En línea]. Available: https://repositoriotec.tec.ac.cr/bitstream/handle/2238/3926/propuesta-programa-control-riesgos.pdf?sequence=1&isAllowed=y. [Último acceso: 22 Diciembre 2022].

[43] Ministerio del trabajo, «Salarios Mínimos Sectoriales y Tarifa,» 6 Enero 2023. [En línea]. Available: https://www.ecuadorlegalonline.com/laboral/tabla-de-salarios-minimos-sectoriales/#:~:text=Para%20la%20elaboraci%C3%B3n%20de%20la,con%20respecto%20al%20a%C3%B1o%202022.. [Último acceso: 31 Enero 2023].

ANEXOS



Anexo 1. Técnica de observación.

Guía de entrevista sobre seguridad de la información en la institución educativa

Fecha: Viernes, 10 de junio de 2022. **Hora:** 11:00 am

Modalidad: Virtual

Entrevistador: Jaime Joel Rodríguez Montaño

Entrevistado: Encargado del Departamento Técnico de la institución

Introducción:

La presente entrevista tiene la finalidad de indagar acerca del manejo de la seguridad de la información en la institución objeto de estudio, así como, las medidas tomadas al afrontar determinadas amenazas informáticas.

Características:

Entrevista confidencial de 25 minutos.

Preguntas:

1. ¿Qué tipos de amenazas a la seguridad de la información se han suscitado en la institución?
2. ¿Cuáles son algunos pasos tomados en la institución para mitigar estas amenazas?
3. ¿Existen políticas o procedimientos para tratar con tales amenazas?
4. ¿Emplean alguna metodología de gestión de riesgos?
5. ¿Cuáles son los activos con mayor probabilidad a ser vulnerados dentro de la institución?
6. ¿Cuál cree que es el error más común que comete la institución cuando se trata de seguridad de la información?
7. ¿Existen programas de capacitación y concientización para garantizar que el personal comprenda y cumpla con los procedimientos de la organización para administrar los riesgos de la información?
8. ¿Se asegura la institución de que sus empleados conozcan cuáles son las mejores prácticas de seguridad de la información?
9. ¿Cuáles son las consecuencias de los incidentes de seguridad de la información?
10. ¿Cuáles son algunas de las consecuencias de no abordar adecuadamente los riesgos de seguridad de la información?
11. ¿Cómo la institución se preparar y responde a los incidentes de seguridad de la información?
12. ¿Cuáles son los procedimientos de la organización para comunicar los riesgos de la información?
13. ¿Cree que se otorga un presupuesto adecuado para solventar las necesidades de seguridad de la información?

Anexo 2. Formato de entrevista.

Encuesta sobre seguridad de la información

Objetivo: El objetivo de esta encuesta es indagar acerca del manejo de la seguridad de la información en la institución objeto de estudio.

Preguntas:

1. ¿Cree usted que se aborda de una manera significativa importancia la seguridad de la información en la institución?

   Sí _____ No _____ A veces _____

2. ¿Cómo calificaría la postura actual de seguridad de la información de su organización?

   Excelente _____ Buena _____ Mala _____

3. ¿Se han promovido campañas o programa de seguridad de la información dentro de la institución?

   Sí _____ No _____

4. ¿Cuenta con personal de seguridad de la información designado en el caso de algún problema general o específico?

   Sí _____ No _____

5. ¿Tiene usted conocimientos sobre metodologías de gestión de riesgos?

   Sí _____ No _____

6. ¿Tiene usted conocimientos sobre políticas y procedimientos para salvaguardar sus activos de información dentro de la institución?

   Sí _____ No _____

7. ¿Cuentan con un plan de respuesta a incidentes en caso de una brecha de seguridad?

   Sí _____ No _____

8. ¿Cómo considera su conocimiento sobre amenazas y delitos informáticos?

   Sí _____ No _____

9. ¿Cuentan con programas antivirus en sus ordenadores?

   Sí _____ No _____

10. ¿Sus equipos son monitoreados regularmente?

    Sí _____ No _____

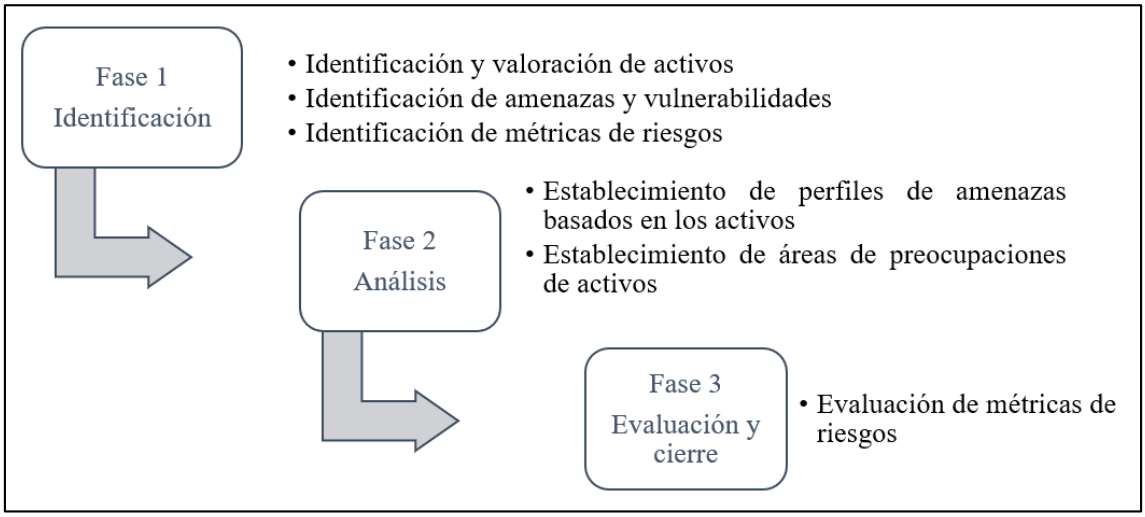
11. ¿Cuenta su organización con un esquema de clasificación de datos?

    Sí _____ No _____

12. ¿Existen procedimientos de manejo y almacenamiento de datos para proteger los datos confidenciales?

    Sí _____ No _____

Anexo 3. Guía de encuesta.



Anexo 4. Fases de la guía de gestión de riesgos propuesta.

CONTROLES DE SEGURIDAD

1. Seguridad ante desastres naturales.
- 1.1. Áreas seguras.
  - 1.1.1. Protección contra las amenazas externas y ambientales.
  - 1.1.2. Trabajo en áreas seguras.
  - 1.1.3. Áreas de acceso público.

2. Seguridad cibernética.
- 2.1. Control de accesos.
  - 2.1.1. Control de acceso a redes y servicios asociados.
- 2.2. Gestión de acceso de usuarios.
  - 2.2.1. Gestión de información confidencial de autenticación.
  - 2.2.2. Gestión de los derechos de acceso con privilegios especiales.
  - 2.2.3. Retirada o adaptación de los derechos se acceso.
- 2.3. Control de acceso a sistemas y aplicaciones.
  - 2.3.1. Restricción del acceso a la información.
  - 2.3.2. Procedimientos seguros de inicio de sesión.
  - 2.3.3. Gestión de contraseñas de usuario.
  - 2.3.4. Uso de herramientas de administración de sistemas.
  - 2.3.5. Control de acceso al código fuente.
- 2.4. Cifrado.
  - 2.4.1. Política de uso de controles criptográficos.

3. Seguridad financiera.
- 3.1. Responsabilidad sobre los activos.
  - 3.1.1. Inventario de activos.
  - 3.1.2. Propiedad de los activos.
- 3.2. Control de accesos.
  - 3.2.1. Política de control de accesos.
- 3.3. Áreas seguras.
  - 3.3.1. Controles físicos de entrada.
- 3.4. Contratación.
  - 3.4.1. Responsabilidades de gestión.
  - 3.4.2. Concienciación, educación y capacitación en seguridad de la información.
  - 3.4.3. Proceso disciplinario.

4. Seguridad del proyecto.
- 4.1. Contratación.
  - 4.1.1. Responsabilidades de gestión.
  - 4.1.2. Concienciación, educación y capacitación en seguridad de la información.
  - 4.1.3. Proceso disciplinario.
- 4.2. Gestión de la prestación de servicios por suministradores.
  - 4.2.1. Supervisión y revisión de los servicios prestados por terceros.
  - 4.2.2. Gestión de cambios en los servicios prestados por terceros.

5. Seguridad operacional.
- 5.1. Responsabilidades y procedimientos de operación.
  - 5.1.1. Documentación de procedimientos de operación.
  - 5.1.2. Gestión de cambios.
  - 5.1.3. Gestión de capacidades.
- 5.2. Copias de seguridad.
  - 5.2.1. Copias de seguridad de la información.
- 5.3. Protección contra código maliciosos.
  - 5.3.1. Controles contra el código malicioso.
- 5.4. Consideraciones de las auditorias de los sistemas de información.
  - 5.4.1. Controles de auditoría de los sistemas de información.

6. Seguridad de recursos humanos.
- 6.1. Antes de la contratación.
  - 6.1.1. Investigación de antecedentes.
  - 6.1.2. Términos y condiciones de contratación.
- 6.2. Durante la contratación.
  - 6.2.1. Responsabilidades de gestión.
  - 6.2.2. Concienciación, educación y capacitación en seguridad de la información.
  - 6.2.3. Proceso disciplinario.
- 6.3. Cese o cambio de puesto de trabajo
  - 6.3.1. Cese o cambio de puesto de trabajo.

7. Seguridad de cumplimiento
- 7.1. Cumplimiento de los requisitos legales y contractuales.
  - 7.1.1. Identificación de la legislación aplicable.
  - 7.1.2. Derechos de propiedad intelectual.
  - 7.1.3. Protección de los registros de la organización.
  - 7.1.4. Protección de datos y privacidad de la información.
  - 7.1.5. Regulación de los controles criptográficos.
- 7.2. Revisiones de la seguridad de la información.
  - 7.2.1. Revisión independiente de la seguridad de la información.
  - 7.2.2. Cumplimiento de las políticas y normas de seguridad.
  - 7.2.3. Comprobación de cumplimiento.

Anexo 5. Controles de seguridad de la guía propuesta.