PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

ESCUELA DE SISTEMAS

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TEMA:

GESTIÓN DE RIESGOS CONFORME ISO 31000 EN LA UNIDAD EDUCATIVA PARTICULAR ATENAS SCHOOL

AUTOR:

KAMILA IDABEL NINABANDA OCAMPO

DIRECTOR:

MST. SUYANA ARCOS

TRABAJO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

QUITO DM, 2022

DEDICATORIA

Quisiera dedicar este trabajo a mis padres, su apoyo y motivación han guiado mis pasos para alcanzar todas las metas que me he propuesto, a mi hermano quien siempre me ha impresionado con su ingenio y su forma de ver el mundo, finalmente a mi hermana, la dedicación y pasión que ha demostrado en todas sus acciones es la mayor inspiración que he presenciado.

AGRADECIMIENTO

Quiero agradecer a mi padre por convertirse en un gran modelo a seguir, a mi madre porque sus palabras me han alentado a superarme constantemente, a mi hermano por ser un gran apoyo durante todo este tiempo, a mi hermana por ser quien me ha guiado y acompañado en todo momento.

RESUMEN

El presente trabajo, revisa los temas de la gestión de riesgos y cómo estos pueden mejorar la situación de cualquier organización, esto acorde con sus objetivos y las actividades que realice, además se contempla desde un análisis de la situación actual de una institución educativa hasta la realización de un plan de tratamiento para los riesgos identificados, sin embargo, no se contempla una ejecución de este plan.

Para realizar el análisis de riesgos, se empleó la norma ISO 31000: 2018, en conjunto con la herramienta MAGERIT, para completar aquellos pasos que indica ISO 31000 o que se dejaban a decisión del autor, esto ofreció una mejor identificación de las amenazas que se podrían encontrar, y se establecieron escalas apropiadas para la valoración del riesgo.

ABSTRACT

The present work reviews the issues of risk management and how these can improve the situation of any organization, in accordance with its objectives and the activities it carries out. In addition, it is contemplated from an analysis of the current situation of an educational institution to the realization of a treatment plan for the identified risks. However, execution of this plan is not contemplated.

To carry out the risk analysis, the ISO 31000: 2018 standard was used, in conjunction with the MAGERIT tool, to complete those steps indicated by ISO 31000 or that were left to the author's decision. This offered a better identification of the threats that could be encountered, and appropriate scales were established for risk assessment.

ÍNDICE

Tabla de Contenidos

ÍNDICE DE FIGURAS, GRÁFICOS Y TABLAS

ÍNDICE DE TABLAS

CAPITULO I: INTRODUCCIÓN

1. MARCO DE REFERENCIA

1.1. JUSTIFICACIÓN

En la actualidad el uso de las tecnologías de la información (TI) ha incrementado en las instituciones del Ecuador, sin embargo, este aumento en la utilización de la tecnología ha generado un riesgo informático en las organizaciones ocasionando pérdidas o alteración de la información, muchas veces las organizaciones no suelen llevar a cabo un control de riesgos apropiado, el cual impida que los procesos se realicen con éxito.

La gestión de riesgos representa un componente importante dentro de las empresas ya que esta hace referencia al estudio y evaluación de los distintos tipos de riesgo existentes en todas las áreas de una empresa, los riesgos se encuentran en todo tipo de actividad sin importar la sencillez de esta, como consecuencia se deben establecer mecanismos de control para su correcta administración, motivo por el que la gestión de riesgos se manifiesta como una buena práctica o aplicación de estrategias y políticas a seguir para reducir las consecuencias que los riesgos pueden infligir, lo cual permite agregar valor a los bienes, productos o servicios (Guerrero Aguiar, Medina León, & Nogueira Rivera, 2020).

La norma ISO 31000:2018 permitirá establecer una guía sobre cómo llevar a cabo una gestión de riesgos adecuada, en conjunto con la metodología de análisis y gestión de riesgos MAGERIT la cual ofrece una perspectiva clara sobre las fases a seguir para evaluar el impacto que un quebrantamiento de la seguridad tiene en la entidad, esto representará en un beneficio para la institución debido a que con una buena gestión de riesgos se fomenta la búsqueda de soluciones y mitigación de los riesgos presentes. El desarrollo de esta investigación se presenta debido a que en los centros educativos no se suele llevar a cabo un plan de gestión de riesgos de TI detallado, por lo que se espera que existan ciertas deficiencias en este, motivo por el cual el resultado de esta investigación repercutirá en establecer un plan de mejora continua en cuanto a los riesgos que pueda presentar la institución.

1.2. PLANTEAMIENTO DEL PROBLEMA

La Unidad Educativa Particular Atenas School, es un centro de enseñanza que cuenta con educación inicial, básica y bachillerato general unificado, en donde se pudo apreciar que no se lleva a cabo un sistema de gestión de incidentes detallado en el que manejen buenos estándares de gestión de riesgos.

La utilización de la tecnología en los planteles educativos ha incrementado de forma progresiva, y en la actualidad se ha convertido en un factor importante tanto en la enseñanza, como en la realización de actividades administrativas, este empleo de la tecnología en cualquier organización aporta una mayor importancia para el éxito de un negocio, asimismo es posible observar que en las instituciones educativas no existe una suficiente formación tecnológica, lo que manifiesta deficiencias cuando se debe llevar a cabo su dirección; a pesar de que el proceso de gestión de riesgos no es reciente aún es posible destacar ejecuciones poco prácticas o simplemente no son llevadas a cabo (Granda Ayabaca, Jaramillo Alba, & Espinoza Guamán , 2019) (CABRERA, 2019).

En base a lo comentado anteriormente se puede destacar que la gestión de riesgos debe verse como un proceso cíclico el cual incluye el análisis y la priorización de riesgos, estas actividades brindan a las organizaciones una comprensión detallada y precisa del riesgo y una excelente herramienta para determinar qué riesgo se puede administrar en un entorno con recursos limitados.

Es importante reconocer que los procesos de gestión de riesgos orientado a centros educativos son de gran trascendencia, debido a que es necesario informar y analizar las amenazas a las que están expuestos, el nivel de vulnerabilidad que poseen y el riesgo que representa.

1.3. OBJETIVO GENERAL

Elaborar un plan de gestión de riesgos conforme ISO 31000:2018 en conjunto con la metodología MAGERIT en la Unidad Educativa Particular Atenas School

1.4. OBJETIVO ESPECÍFICO

Analizar la estructura de la norma ISO 31000:2018 y del método MAGERIT.

Identificar el estado actual referente al manejo y control de riesgos en la Unidad Educativa Particular Atenas School

Elaborar un plan en el que se describa como se realizaría la implantación de ISO 31000:2018 en un plantel educativo.

1.5. ANTECEDENTES

En Ecuador se presentan varias iniciativas para resolver la gestión en TI y en la mayoría se han detectado una gran cantidad de factores por mejorar para conseguir una gestión eficiente, como ejemplo se encuentra Villacís y William que han ofrecido guías de evaluación de la gestión TI con aplicación de COBIT y COSO, sin embargo, estas propuestas no se masifican y terminan desatendidas en el tiempo, motivo que genera un problema de la gestión integral de TI.

De acuerdo con Cuzme M. y Pinargote R. (2015) en la investigación titulada “Plan de gestión de incidentes que afectan a los equipos informáticos de la ESPAM MFL (Escuela Politécnica Agropecuaria de Manabí), se tuvo como objetivo la elaboración de un plan de gestión de incidentes para reducir el impacto de posibles fallas y mejorar la productividad de los usuario, los autores llegaron a la conclusión que el inventario de equipos permitió establecer su disponibilidad y los riesgos a las que están expuestos los activos, recalcando la importancia de llevar acciones preventivas y tener en cuenta las consideraciones regulatorias, este trabajo es importante para esta investigación porque demuestra el desarrollo de un plan de gestión de incidentes orientado en una institución educativa superior.

1.6. ALCANCE

El presente trabajo tiene como alcance la realización de un plan de gestión conforme ISO 31000:2018 en conjunto con la metodología MAGERIT en una institución educativa, la selección de un centro educativo (secundaria) se debe a que la mayor parte de trabajos revisados como referencia para efectuar esta investigación están orientados a otra clase de sectores (empresas y universidades), pero se observó una menor tendencia a este tipo de planteles educativos. Para ejecutar este trabajo se realizará una investigación acerca de la estructura organizativa, procesos, sistemas de información y las relaciones con las partes interesadas, lo cual corresponde a uno de los aspectos de un plan de gestión de riesgos.

Por último, el resultado esperado de este trabajo corresponderá a la elaboración de una planificación de tratamiento en el cual se detallen los pasos a llevar a cabo para ejecutar las cláusulas del estándar ISO 31000:2018, empleando diversas técnicas que sugiere MAGERIT para realizar esta clase de análisis de riesgos, dentro de este centro educativo, mas no se realizará ninguna acción o implementación dentro del centro educativo.

CAPITULO II: FUNDAMENTACIÓN TEÓRICA

2. MARCO TEÓRICO

2.1. SEGURIDAD INFORMÁTICA

2.1.1. DEFINICIÓN

Antes de establecer una definición para la seguridad informática es preciso comprender por qué y cuándo surge; su historia comienza a partir del año 1980, y se limitaba a los computadores personales y sobre como conservar los datos que en ellas se almacenaban. Alrededor del año 1990 se da la producción de virus y gusanos, dando paso a la identificación de ataques a sistemas informáticos y donde la palabra *hacker* comienza a moldearse. Desde el año 2000 los cambios acelerados, el exceso de información han generado una cantidad masiva de amenazas, donde muchas veces los usuarios no se percatan de la dimensión de este problema, motivo por el cual es importante analizar esta problemática (Palacios, 2020).

La seguridad informática de acuerdo con ISO 27001 es presentada como una rama de la ingeniería de sistemas la cual está al pendiente de coordinar acciones con el fin de proteger la integridad y la privacidad de la información que está siendo almacenada en algún sistema informático, esta debe analizar prácticas para la implementación de sistemas los cuales reduzcan los riesgos a los que se encuentran expuestos estos sistemas.

Por otro lado, la organización **CN-Cert** define la seguridad informática de la siguiente manera según el método MAGERIT: La capacidad de las redes o sistemas de información para resistir con cierto grado de confianza, accidentes o acciones ilegales o maliciosas que comprometan la disponibilidad, autenticidad o integridad y seguridad de los datos almacenados o transmitidos y los servicios que tales redes y sistemas proporcionan o brindan.

En ambas definiciones podemos comprender que la seguridad informática se describe como las prácticas necesarias que se deben llevar a cabo en cualquier organización con el fin de conservar nuestra información salvaguardada, de amenazas internas o externas, sin

embargo, para llevar a cabo estas acciones es necesario efectuar un análisis o plan en el que se prioricen los elementos a ser protegidos y como se lo realizará.

2.1.2. TIPOS

Clasificamos los tipos de seguridad en cuatro ramas principales;

Activa

Esta es la que se encarga de evitar daños a los sistemas informáticos, como, por ejemplo, los computadores emplean claves para acceder a ciertas funciones, pero para prevenir algún tipo de amenaza es posible emplear acciones de encriptación de datos, utilizar software de seguridad como antivirus o contraseñas seguras.

Pasiva

Se refiere a la reducción de desastres que se producen durante un accidente, como es el caso en el que se sufra de un ataque de malware hacia el sistema y una acción que se llevaría a cabo es la realización de copias de seguridad.

Física

Como su nombre la describe es la encargada de proteger aquellos elementos de hardware, en el cual se incluye las instalaciones o entornos, y los dispositivos físicos con los que cuente una organización.

Lógica

Por otro lado, la seguridad lógica se ocupa de la protección de los aspectos de software, aplicaciones o elementos del sistema, además, es donde se toman acciones de protección y mantenimiento de las aplicaciones y de la integridad de los datos.

2.2. RIESGO

En 1921 el autor Frank Knight presenta su obra denominada “Risk, uncertainty and profit”, trabajo en el cual se define el término de riesgo en sus inicios, en este texto se describe al riesgo como un aspecto medible el cual se puede cuantificar a través del establecimiento de un nivel aceptable de confianza. Las distintas concepciones sobre la definición de riesgo son esenciales para verificar que tan duradero y complejo es el tema.

Los riesgos en cualquier área se refieren a la probabilidad de que un hecho se produzca y atente contra la integridad o el desarrollo de un determinado objeto, de igual forma se lo puede definir como una desviación ya sea positiva o negativa con respecto a lo previsto, igualmente hace referencia a eventos potenciales y sus posibles consecuencias (Pazmiño Zabala, Serrano Castro, & González Rivera, 2020).

En el caso de la informática la Organización Internacional para la Estandarización (ISO) manifiesta que un riesgo es la probabilidad de que una amenaza determinada se materialice, explotando las vulnerabilidades de un activo o grupo de activos, generando daño o pérdidas a la organización.

Elementos del riesgo

- **Activos de información:** se refiere a los elementos que lleven consigo información, estos deben ser clasificados de acuerdo con la sensibilidad de la información.

- **Amenazas:** cualquier incidente que dé como consecuencia daños a los activos; estas se pueden clasificar en base a: su origen natural, entorno, por defecto, generado por personas accidentalmente o a propósito.

- **Vulnerabilidades:** estas tienden a ser expresadas en escalas numéricas para así poder cuantificar su impacto, es importante identificarlas y calificarlas.

- **Impacto:** es la medida que se emplea para analizar el daño causado por una amenaza.

2.2.1. CATEGORÍAS DE RIESGO

Como se ha revisado anteriormente los riesgos afectan a procesos, recursos, personas, entre otros, por lo que al evaluar que objetos son propensos a sufrir amenazas se identificó que los activos propensos incluyen a todo aquel que utilice información, y da paso a tres categorías esenciales de riesgos (Peña & Lugani, 2019):

Riesgos externos

Los riesgos externos incluyen:

- ***Intrusión:*** nos referimos a riesgos de intrusión a todo aquel que implique un acceso no autorizado ya se de individuos o sistemas al activo informático, ya sea un acceso físico o remoto.

- ***Ambiental:*** un riesgo ambiental abarca factores climáticos o de origen ambiental que atenten contra el activo.

- ***Regulaciones:*** está relacionado con normas y regulaciones vigentes las cuales rigen el funcionamiento óptimo de los activos y de la información utilizada por este.

- ***Proveedores y subcontratados:*** se refiere a las relaciones con terceros y el cumplimiento de sus responsabilidades.

Riesgos organizacionales

En los riesgos organizacionales podemos describir los siguientes:

- ***Proyectos tecnológicos:*** los riesgos de esta clase representan a aquellos que se manifiestan en los proyectos que involucren tecnología, en la especificación de responsabilidades en los contratos y el cumplimiento de estos.

- ***Personal:*** en referencia a las acciones del personal dentro de la organización.

- ***Procesos de negocio:*** se refiere a amenazas en el flujo de procesos de negocio, donde se encuentre involucrado algún activo informático.

Riesgos tecnológicos

Dentro de los riesgos tecnológicos se puede apreciar:

- ***Requerimientos:*** engloba aquellos riesgos que se relacionen con requerimientos de sistema o de recursos tecnológicos.
- ***Diseño:*** como su nombre lo especifica se refiere a los riesgos que corresponden \ al diseño de un sistema o recurso tecnológico.
- ***Programación:*** relacionados con el código fuente de los sistemas.
- ***Performance:*** incluye a los riesgos que afectan al activo en cuanto a sus aspectos relacionado con su rendimiento o el de otros activos relacionados.

Es posible definir otro tipo de riesgos relacionados con los tecnológicos como los mencionados a continuación:

- Riesgo de integridad
- Riesgo de relación
- Riesgo de acceso
- Riesgo de utilidad
- Riesgo en la infraestructura
- Riesgo de seguridad en general

2.2.2. GESTIÓN DE RIESGOS

La gestión de riesgos es trascendental para cualquier tipo de negocio, esto porque los riesgos pueden alterar los resultados de los procesos internos y es fundamental garantizar el logro de los objetivos estratégicos, es por eso por lo que la gestión de riesgos corresponde a una actividad que se plantea “el aumentar la probabilidad de éxito de cualquier actividad, gestión de proyectos y desarrollo de productos”.

De igual forma se puede describir a la gestión de riesgos en base a lo mencionado por (Altamirano, 2019) “La gestión de riesgos es una disciplina que existe para hacer frente a los riesgos no especulativos, que son aquellos riesgos de los cuales solo puede incurrir en una pérdida para la organización”. Para ejecutar este proceso, debe tener en cuenta lo siguiente:

- Los activos que sean relevantes para la organización, su valor e interacción.
- Establecer a qué amenazas se encuentran expuestos estos activos.
- Estimar el impacto, que se refiere al daño sobre el activo.
- Estimar el riesgo, el cual describe el impacto ponderado con la tasa de ocurrencia.

Es importante aclarar que realizar una gestión de este tipo no busca erradicar por completo todos los riesgos de una entidad, su objetivo principal radica en la minimización de estos, empleando un enfoque de identificación, medición y control. De esta manera la gestión de riesgos debe ser comprendida con un enfoque práctico incluido en el plan estratégico considerando los aspectos del entorno organizativo interno y externo y mostrarse alerta en el seguimiento de esta gestión (Silva Rampinia, Takia, & Tobal Berssanetia, 2019) (Suárez Pérez & Nieto Acosta, 2020).

2.2.3. IMPORTANCIA DEL ANÁLISIS DE REDUCCIÓN DE RIESGOS

Previo a describir la importancia de un análisis de reducción de riesgos, es preciso referir en qué consiste, el análisis de riesgos consiste en un proceso sistemático en el cual se busca determinar la magnitud que puede llegar a tener posibles riesgos dentro de una organización, realizando esto es posible determina la naturaleza, protección del sistema y el costo que puede representar el ser víctimas de algún ataque.

El objetivo de un análisis de reducción de riesgos es el de satisfacer los objetivos/metas que la organización se ha propuesto y no superar la cantidad de riesgos establecidos por la empresa, además busca mitigar la incertidumbre de que este tipo de eventos afecten los proyectos de la entidad y disminuyan su productividad.

Es importante reconocer que las amenazas, vulnerabilidades o riesgos no pueden erradicarse por completo, mas es posible emplear planes, estrategias o buenas prácticas que minoricen las consecuencias que estos eventos pueden llegar a causar en una organización, por lo que al realizar esta clase de análisis se busca comprender el riesgo, identificar los recursos y esfuerzos que deberán llevarse a cabo para reducirlos y prever futuras incertidumbres.

Toda organización es propensa a sufrir algún riesgo de cualquier índole, además con el constante desarrollo tecnológico estos han aumentado considerablemente, por lo que llevar a cabo planes que reduzcan la cantidad de riesgo es una acción esencial para proteger los activos de una organización, es por eso que se deben organizar los riesgos de acuerdo a sus efectos en caso de que estos se den, las pérdidas que puede representar para la empresa, entre otros, motivo por el cual actualmente se da mayor importancia a la gestión de los riesgos.

2.3. AMENAZAS

2.3.1. DEFINICIÓN

En base a los manuales de MAGERIT una amenaza se describe como “alguna cosa que ocurre”, y de todo lo que puede llegar a ocurrir, se considere relevante aquello que pueda ocurrir a los activos ocasionando algún tipo de daño, por lo general correspondiente a:

- **Origen natural:** accidentes naturales tales como: terremotos, inundaciones, entre otros.
- **Defecto de la aplicación:** inconvenientes directos en el equipamiento, ya sea por defectos en la implementación o en su diseño.
- **Por personas de forma accidental:** errores por omisión, causados de forma intencionada.
- **Por personas de manera deliberada:** ataques por parte del personal con acceso al sistema, con el fin de beneficiarse indebidamente o por generar estragos y perjuicios a los propietarios.

2.3.2. REPERCUSIONES DE LAS AMENAZAS ANTE LOS ACTIVOS

Cuando se determina que una amenaza puede afectar a cualquier activo, es necesario valorar la influencia en la valía del activo:

- **Degradación:** se refriere a que tan perjudicada resultaría el valor del activo, la degradación se encarga de medir el daño causado por algún incidente en el caso de que ocurriese.

- **Probabilidad:** se refiera a que tan probable o improbable es que se materialice la amenaza, también puede describirse como la probabilidad de ocurrencia, algunas veces se describe de forma cualitativamente mediante una escala nominal, por otra parte, se puede modelar numéricamente como una frecuencia de ocurrencia.

2.4. ISO 31000:2018

2.4.1. DESCRIPCIÓN

ISO 31000 presenta la primera versión de esta directriz en 2009, representando un marco que estandariza la gestión de riesgos empleando su propio marco, conceptos y terminología, en su primer lanzamiento mostro una aceptación remarcable en las empresas, debido a que esta norma incluye a todo tipo de organización, y también debido a que no está dirigida a un sector específico. A pesar de que el estándar no es certificable sigue mostrando una gran aceptación.

En febrero de 2018 se da la publicación de la nueva versión de ISO 31000, en esta versión se muestra una visión integral y estratégica de la gestión, detalla los principios y metodologías que se pueden emplear en la gestión de riesgo, a breves rasgos la metodología pretende establecer estrategias, lograr objetivos y tomar decisiones informadas. Esta norma muestra 3 pilares fundamentales: principios, estructuras y procesos.

ISO 31000 presenta 5 componentes para un marco de gestión de riesgos: integración, diseño, implementación, evaluación y mejora, estos componentes deben alinearse con la cultura organizacional de la entidad, además, esta estructura permite evaluar las prácticas actuales. El último pilar menciona los procesos, el cual implica la aplicación sistemática de procesos, procedimientos y prácticas a las actividades de comunicación, establecimiento de contexto, evaluación, tratamiento, seguimiento, análisis crítico, registro y reporte de

riesgos, esto se lleva como un proceso iterativo y es aplicable a nivel estratégico, operativo, de programa o de proyecto.

2.4.2. PRINCIPIOS REFRENTES A LA NORMA ISO 31000:2018

Los principios descritos en las directrices ISO son: hacia una gestión eficaz que comunique su valor y explique su intención y propósito, los principios se detallan a continuación:

Ilustración 1Principios de la norma ISO 31000:2018

Nota, la imagen que se presenta se obtuvo de (Cardona, J, 2020)

- Es una parte integral de cualquier entidad
- Un enfoque de gestión estructurado y global que contribuye a resultados consistentes y comparables.
- Los marcos y procesos de gestión de riesgos se adaptan al contexto interno o externo de la empresa en relación con sus objetivos.
- Plena participación de las partes interesadas, para obtener sus conocimientos, opiniones y conciencia.

- Los riesgos cambian dependiendo del contexto interno o externo, la gerencia debe anticipar, detectar, reconocer y reaccionar rápidamente a los cambios y eventos.

- La información proporcionada debe ser clara y accesible para las partes interesadas.

- Mejora de la gestión de riesgos basada en las lecciones aprendidas y la experiencia adquirida.

2.4.3. MARCO DE REFERENCIA (ISO 31000)

El marco de referencia incluye: integración, diseño, implementación, evaluación, mejora de la gestión de riesgos, se seguirá una descripción de cada uno de ellos:

Ilustración 2 Marco de referencia

Nota, la imagen que se presenta se obtuvo en base al modelo de ISO (ISO 31000:2018 Risk management Guidelines)

Liderazgo y compromiso

Los altos mandos (órganos de supervisión, administrativos), deben mostrar compromiso para que se efectúe una gestión de riesgos alineada con las actividades de la organización:

- Personalizar e implementar los componentes del marco
- Emitir una declaración que establezca un enfoque, plan de acción de gestión de riesgos
- Velar por que los recursos necesarios sean asignados a la gestión del riesgo
- Alinear la gestión de riesgos con objetivos, estrategias y cultura
- Comunicar el valor de la gestión de riesgos a la organización y a los interesados
- Asegurarse de que el marco de gestión de riesgos sea el adecuado para el contexto de la entidad

Los altos mandos están a cargo de la gestión de riesgos, mientras que los órganos de supervisión están encargados de vigilar la gestión de riesgo, siendo sus actividades las siguientes:

- Comprender los riesgos que presenta la organización en la búsqueda de sus objetivos.
- Garantizar que la información sobre los riesgos y su gestión lleven una comunicación adecuada.
- Garantizar que los sistemas para gestionar los riesgos se implementen y funcionen de forma eficaz
- Asegurarse de que se consideren adecuadamente los riesgos al establecer los objetivos de la organización

Integración

La integración es la comprensión de la organización tanto su estructura como su contexto, las estructuras difieran de acuerdo con los objetivos y complejidad de la empresa, y los riesgos son gestionados en cada parte de la estructura.

La gobernanza guía el curso de la empresa, relaciones internas y externas, reglas, procesos, y prácticas necesarias para alcanzar su propósito, una estructura se refiere a la dirección de la gobernanza en la estrategia y los objetivos asociados necesarios para alcanzar los niveles óptimos de rendimiento sostenible y viabilidad a largo plazo.

Diseño

- ***Entender la organización y su contexto:*** se debe comprender el contexto interno y externo:
    - En el caso del contexto externo se incluye: factores sociales, culturales, legales, políticos, financieros, tecnológicos, económicos y ambientales. Además de comprender las tendencias clave que afecten los objetivos de la organización.
    - En el caso de los contextos internos: visión, misión, valores, estrategia, gobernanza, estructura organizativa, cultura de la organización, funciones y responsabilidades.
- ***Articulación del compromiso de gestión de riesgos:*** la alta dirección debe manifestar su compromiso con la gestión de riesgos empleando políticas o declaraciones, este compromiso incluye:
    - Los objetivos de gestión de riesgos de la entidad.
    - Liderar la integración de la gestión de riesgos en el negocio principal y la toma de decisiones.
    - Medir y reportar en el marco de los indicadores de desempeño de la organización.
- ***Asignación de roles organizacionales, autoridades, responsabilidades y responsabilidades:*** los altos mandos deben confirmar que las autoridades y responsabilidades de los roles concernientes a la gestión de riesgos sean asignados y comunicados a toda la organización y deben:

    - Enfatizar que la gestión de los riesgos es una responsabilidad central.
    - Identificar a las personas que tienen la responsabilidad y autoridad para gestionar los riesgos.

- ***Asignación de recursos:*** se incluye:
    - Personas, experiencia, competencia y habilidades
    - Procesos, herramientas y métodos que la entidad emplea para la gestión de riesgos.
    - Sistema de gestión de información
    - Procedimientos documentados.

- ***Establecer comunicación y consulta:*** el marco debe ser respaldado y se debe facilitar la aplicación eficaz de la gestión de los riesgos, las consultas implican retroalimentaciones por parte de los participantes.

Implementación

Se debe dar empleando:

- Desarrollo de un plan apropiada que incluya tiempo y recursos.
- Identificar donde, cuando y como se toman diferentes tipos de decisiones en la organización y sus responsables
- Modificar procesos de toma de decisiones aplicables cuando se requiera
- Asegurarse de que las disposiciones de la organización para gestionar el riesgo se entiendan y practiquen claramente.

Evaluación

El proceso de evaluación implica:

- Medir periódicamente el desempeño del marco de gestión de riesgos frente a sus propósitos, planes de implementación, indicadores y comportamientos esperados.

- Determinar si aún es adecuado para apoyar el logro de los objetivos de la organización.

Mejora

La mejora incluye;

- **Adaptación:** monitoreos y adaptación continua del marco de gestión de riesgos para abordar cambios internos y externos.

- **Mejora continua:** se debe mejorar la idoneidad, adecuación y eficacia, y la manera en la que se integra el proceso de gestión de riesgos.

2.4.4. PROCESO DE GESTIÓN DE RIESGOS

El proceso de gestión de riesgos se describe en la siguiente ilustración:

Ilustración 3 Proceso de gestión de riesgos

Nota, la imagen que se presenta se obtuvo en base al modelo de ISO (ISO 31000:2018 Risk management Guidelines)

Comunicación y consulta

Se realiza con el fin de que los interesados comprendan el riesgo, la base sobre la que se realizan las decisiones y los motivos por lo que se requieren acciones especiales. La consulta por su parte busca la obtención de retroalimentación e información para apoyar la toma de decisiones, la coordinación de estos factores promueve el intercambio de información fática, oportuna, pertinente, precisa y comprensible, considerando la confidencialidad e integridad de la información, sus objetivos son los siguientes:

- Reunir distintas áreas de especialización para cada parte del proceso de gestión de riesgos
- Crear un sentido de inclusión y de propiedad entre los involucrados por el riesgo.
- Asegurarse de que se consideren correctamente los puntos de vista al determinar los criterios de riesgo y la evaluación del riesgo.

Ámbito, contextos y criterios

- **Definición del alcance:** se debe tomar en cuenta los objetivos relevantes, alineación con los objetivos de la organización

- **Contexto interno y externo:** el propósito y el alcance del proceso de gestión de riesgos deben estar interrelacionados con los objetivos de la organización en su conjunto.

- **Definición de criterios de riesgo:** se debe especificar la cantidad y el tipo de riesgo que es posible asumir con relación a los objetivos, a parte se deben establecer criterios para analizar la importancia del riesgo y para apoyar los procesos de toma de decisiones.

Evaluación de riesgos

Es un proceso en el que se identifican, analizan y evalúan riesgos, esta evaluación se realiza sistemáticamente, de forma iterativa y colaborativa.

- ***Identificación de riesgos:*** se refiere a la identificación de un riesgo, su reconocimiento, y descripción con el fin de identificar si será de ayuda o representará un impedimento para que la entidad alcance sus objetivos.

- ***Análisis de riesgos:*** se debe comprender la naturaleza del riesgo, características y nivel, este incluye una evaluación detallada de las incertidumbres, fuentes, consecuencias, probabilidad, eventos, escenarios, controles y eficacia.

- ***Evaluación de riesgos:*** se efectúa con el fin de apoyar decisiones, se deben comparar resultados del análisis de riesgos con los criterios de riesgo establecidos para determinar las acciones futuras.

Tratamiento de riesgos

En esta sección se lleva a cabo un proceso iterativo que comprende las siguientes acciones:

- Plantear y escoger opciones para el tratamiento de los riesgos

- Evaluar la eficacia del tratamiento
- Decidir su el riesgo residual es aceptable
- En caso de no ser aceptable, se debe realizar un tratamiento adicional

Se debe llevar a cabo:

- ***Selección de opciones de tratamiento de riesgos:*** se debe analizar los beneficios potenciales en relación con el cumplimiento de los objetivos frente a los costos, y pueden incluir: eliminar el origen del riesgo, cambiar la probabilidad, evitar el riesgo.
- ***Elaboración e implementación de planes de tratamiento de riesgos:*** se describe como se realizará la implementación las opciones de tratamiento seleccionadas con el fin de monitorear su progreso, debe incluir: acciones propuestas, responsables, medidas de rendimiento y el seguimiento requerido.

Seguimiento y revisión

Se debe asegurar y mejorar la calidad, eficacia del diseño, implementación y los resultados del proceso. Este seguimiento se debe dar en todas las etapas del proceso, este seguimiento incluye la planificación, recopilación y análisis de información a más del registro de resultados y comentarios.

Registro y notificación

Los resultados deben documentarse y comunicarse a través de los mecanismos apropiados, estos informes presentan los siguientes objetivos:

- Comunicación de las actividades y resultados de la gestión de riesgos en la organización
- Ofrece información para la toma de decisiones
- Mejora las actividades de gestión de riesgos

2.5. MAGERIT

MAGERIT creada por el Consejo Superior de administración electrónica de origen español, puede concebirse como una metodología que es posible utilizarla libremente y sin solicitar autorización para emplearla, actualmente se encuentra en su tercera versión y comprende de una metodología de análisis y gestión de riesgos, actualmente se encuentra a cargo de la Secretaría General de Administración Digital en colaboración con el Centro Criptológico Nacional.

2.5.1. Objetivos

MAGERIT muestra los siguientes objetivos directos:

- Concienciar a cualquier responsable de las entidades de información de la presencia de riesgos además de la necesidad de gestionarlos.
- Ofrecer un soporte para descubrir y planear un tratamiento oportuno para mantener los riesgos bajo intervenciones indirectas.
- Brindar un método sistemático para considerar los riesgos derivados del uso de las tecnologías de la información y comunicación.

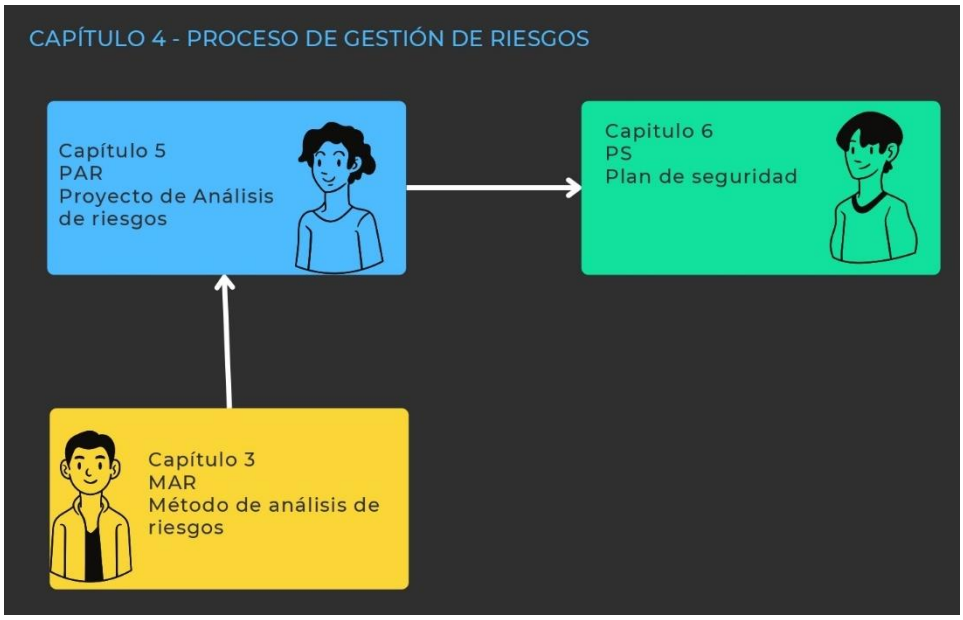
2.5.2. Método

Se puede distinguir la siguiente estructura en MAGERIT:

- **Capítulo 2:** se describen conceptos, se distingue la actividad de análisis y tratamiento de riesgos.
- **Capítulo 3:** muestra pasos y define actividades por realizar dentro de la fase de análisis.
- **Capítulo 4:** contempla opciones y criterios para la realización del tratamiento de los riesgos y establece actividades para la realización de gestión de riesgos.
- **Capítulo 5:** enfocado en los proyectos de análisis de riesgos.

- **Capítulo 6:** destaca los planes de seguridad o planes estratégicos.
- **Capítulo 7:** se observa como el análisis de riesgos ayuda a gestionar la seguridad
- **Capítulo 8:** establece algunos problemas que surgen cuando se realiza un análisis de riesgos

Ilustración 4 MAGERIT



Nota, la imagen que se presenta se obtuvo en base al modelo MAGERIT de la Secretaría General de Administración Digital.

CAPITULO III: METODOLOGÍA

3. METODOLOGÍA DE DESARROLLO DEL PLAN DE TESIS

3.1. INVESTIGACIÓN APLICATIVA

Investigación Aplicada

La investigación aplicada tiene como objetivo resolver problemas que ocurren en el proceso de producción, distribución y consumo de productos y servicios de las actividades humanas. Se llama investigación aplicada porque se basa en investigación básica, investigación pura o investigación básica en física o ciencia formal. Se formulan problemas o hipótesis de trabajo para resolver los problemas de la vida productiva en sociedad. (Nieto, 2019).

Esta investigación está orientada a mejorar, perfeccionar u optimizar el funcionamiento de los sistemas, procedimientos, las normas, reglas tecnológicas actuales a la luz de los avances de la ciencia y tecnología; por tanto, esta investigación no se presta a la calificación de lo verdadero, falso o probable, sino a lo eficiente, deficiente, ineficiente, eficaz o ineficaz (Nieto, 2019).

En otras palabras, la investigación aplicada se entiende como el uso práctico del conocimiento, con la finalidad de aplicar ese conocimiento en beneficio de los grupos involucrados en estos procesos y para la sociedad, en términos de esta, en la ciencia pura y la investigación experimental, estudiar cómo funcionan las cosas para su uso posterior, mientras que en la ciencia práctica la investigación aplicada tiene como objetivo hacer un uso inmediato de este conocimiento existente (Vargas Cordero, 2009).

La ejecución de este trabajo da comienzo con la exploración de la situación actual de la institución educativa y el establecimiento del contexto el cual incluye los criterios para la gestión de riesgos, esto con el fin de establecer un correcto enfoque en la definición de estos riesgos dentro de la institución (Vargas Cordero, 2009).

La estructura que propone Padrón (2006), para quien la investigación aplicada tiene como fruto la búsqueda y consolidación del saber, la aplicación de conocimientos para el enriquecimiento del acervo cultural y científico, así como la producción, comprende de los siguientes pasos:

- Partir de una situación problemática, la cual se debe intervenir o mejorar, se debe describir sistemáticamente esa situación, de manera que se justifique con criterios relevantes su orden práctico.

- Seleccionar una teoría, para exponerla en sus conceptos centrales y rasgos contextuales

- Examinar la situación *problema*, para derivar un prototipo de acción, con el cual se desea resolver favorablemente este problema, esto contempla la descripción sistemática con sus secuencias e instrumentaciones pues resultará ser el método o modelo por emplear y comprobar en este proceso aplicado.

- Repetir y probar el prototipo descrito en el paso anterior para determinar la probabilidad de que el modelo de aplicación como forma de resolución al contexto del problema.

Al momento de realizar esta delimitación de contextos se dará paso a la definición de metas, objetivos y actividades que se llevarán a cabo.

Como se ha mencionado anteriormente se utilizará ISO 31000 para realizar un plan de gestión de riesgos lo cual incluye:

1. Definición de Objetivos

2. Identificación de riesgos

3. Análisis de riesgos

4. Definir respuestas a cada riesgo

5. Planificación del tratamiento del riesgo

Una vez que se efectúen los enfoques necesarios se podrá obtener la información necesaria para realizar un análisis crítico que permitirá elaborar el plan, es necesario mencionar que el proyecto concluye con la elaboración de esta planificación.

3.2. Plan de recolección de información

Para la recolección de la información se emplearon dos técnicas, la primera consiste en la simple observación de la situación de la institución y como se efectuaban los procesos que se realizaban dentro de ésta, mientras que la segunda involucraba la aplicación de entrevistas no estructuradas, en su mayoría se desarrollaban mientras se efectuaba el proceso de inventarios.

Al emplear entrevistas no estructuradas se observaron diversas ventajas como la fácil obtención de información concreta con respecto a lo que se deseaba, con el fin de interpretar la situación del plantel educativo.

A continuación, se muestra las preguntas básicas para la entrevista:

Preguntas
¿Podría comentarme sobre la situación en la que se encuentra la institución?
¿Qué personal se encuentra involucrado?
¿Existe algún tipo de conocimiento sobre el tema de gestión de riesgos a nivel de TI?
¿Los bienes tecnológicos se encuentran en un listado general del inventario?

Nota, las preguntas que se encuentran en la parte superior son en base a investigación propia

3.3. Plan para la realización del procesamiento de información

Con la finalidad de procesar la información que se ha recolectado se establecen los siguientes pasos a seguir:

- Revisión de la información que se obtuvo.
- Manejo de la información (reajuste con los datos que sean reducidos cuantitativamente que no alteran de forma significativa en los análisis).

- Análisis e interpretación de la información, destacando aquella que se muestre relevante

- Efectuación de conclusiones y recomendaciones

CAPITULO IV: DESARROLLO DE LA INVESTIGACIÓN

4. Establecimiento de contextos

4.1. Educación Media Superior

4.1.1. Descripción del bachillerato general unificado

El Diplomado de Bachillerato General Unificado corresponde al tercer nivel de educación, en el cual se perfeccionan las competencias de los tres niveles básicos de educación general, permitiendo a los estudiantes vincularse con el sistema de educación superior y contribuyendo así a su proyecto de vida.

Abarca temas relacionados con los orígenes de los movimientos sociales, las revoluciones liberales, el desarrollo, las reivindicaciones de derechos, así como cuestiones relacionadas con la lengua y las variedades lingüísticas, se considera la evolución de los cambios de la cultura de la escritura en la era digital y sus impactos.

Por otro lado, se utilizan diversos recursos analógicos y digitales (TIC) para desarrollar el trabajo de campo, la experimentación, la base técnica y la argumentación lógica y crítica.

4.1.2. Currículo priorizado con énfasis en competencias comunicaciones, matemáticas, digitales y socioemocionales

Ley Orgánica de Educación Intercultural LOEI (2021)

Tabla 1 LOEI

Artículo 2.3 literal h	Garantiza el derecho de todos a una educación de calidad, cálida, pertinente, completa, contextual, actualizada y clara en todo el proceso educativo, dentro del sistema, en todos los niveles y subniveles o sus modalidades; y eso incluye revisiones continuas. Asimismo, asegura que el educando sea el centro del proceso

Artículo 19	educativo, con la flexibilidad y adaptabilidad de los contenidos, procesos y metodologías a las necesidades básicas y realidades de los alumnos. Promover las condiciones adecuadas de respeto, tolerancia y afecto, creando un ambiente escolar propicio para el proceso de aprendizaje.
	La Agencia Nacional de Educación tiene como objetivo diseñar y garantizar la adopción obligatoria de un currículo nacional, tanto en las instituciones públicas, municipales, privadas y financieras, en todos los niveles diferentes: primaria, básica y secundaria, y por modalidades: directa, semipresencial -presencial ya distancia. […] El plan de estudios podrá complementarse de acuerdo con las peculiaridades específicas y culturales de la región, provincia, estado o comunidad de las diversas Instituciones Educativas que forman parte de la Educación Nacional.

Nota, la imagen se obtuvo del currículo con énfasis en CC-CM-CD-CS publicado en el sitio web del ministerio de educación.

Reglamento general a la LOEI

Tabla 2 LOEI

Artículo 11	El Currículo Nacional incluye los conocimientos básicos requeridos para los estudiantes del Sistema Educativo Nacional y lineamientos técnicos y pedagógicos para su aplicación en el aula, así como ejes de transición, metas y objetivos de cada asignatura y diagrama de salida de cada nivel y modalidad.

Nota, la imagen se obtuvo del currículo con énfasis en CC-CM-CD-CS publicado en el sitio web del ministerio de educación.

Este currículo es parte del currículo priorizado del año 2020, el cual incluye destrezas con criterios de desempeño e indicadores de evaluación, en el cual se indica que es indispensable el desarrollo de las competencias de la comunicación, las matemáticas, socioemocionales y digitales en el cual se incluye el pensamiento computacional y la ciudadanía digital

- **Competencias comunicacionales:** se refiere a todas las habilidades, relacionados con los actos de habla con pertinencia y fluidez, implica la lectura y el crecimientos intelectual y humano.

- **Competencias matemáticas:** hace referencia a las formas de expresión y de razonamiento matemático, siendo sus principales competencias el pensamiento crítico, toma de decisiones y resolución de problemas.

- **Competencias digitales:** se describe como las habilidades y conocimiento los cuales ayudan a la obtención de información mediante el uso de dispositivos digitales, las competencias principales son: cálculo y la utilización elemental de dispositivos digitales.

- **Competencias socioemocionales:** con respecto a esta competencia se abarca los aspectos cognitivos y no cognitivos, como, por ejemplo, la ética, desarrollo humano integral y prevención de cualquier clase de violencia y riesgos psicosociales.

4.2. Unidad Educativa Particular Atenas School

Misión

La Misión del plantel se describe de la siguiente manera: Somos una institución educativa privada, que opera en base a los cuatro pilares establecidos por la UNESCO: (A PRENDER A CONOCER, A SER, A HACER, Y CONVIVIR), mostrándose pioneros en el desarrollo de una forma de aprendizaje mediante la experiencia cultural, ecológica y también mediante la experiencia cultural, ecológica y experiencias solidarias, tanto a nivel nacional como internacional.

Visión

La unidad de educación privada Atenas School, muestra un rol de liderazgo social y académico, brindando una educación de calidad, cálida, inclusiva y centrada en el ser humano, critica y participativa, democrática, e interactiva, incluyendo la equidad de género con base ancestral, a la plurinacional y pluricultural, con identidad de pertenencia que satisfaga la necesidad de aprendizaje, pasantías individuales y colectivas, brindando al país un bachillerato de excelencia rivalizando con el milenio.

Valores

Paz

Una situación o estado donde no se muestran guerras u hostilidades entre dos o más partes opuestas. Pertenecer a la RED UNESCO de escuelas afiliadas y emplear el BUEN VIVIR, ayudándolos a establecer acuerdos comunitarios para evitar conflictos y vivir armonía para generar confianza en las relaciones con los demás.

Responsabilidad

Un compromiso u obligación de naturaleza moral que aparece de la probable equivocación de un individuo en algún asunto en particular, la responsabilidad implica también una obligación para corregir un error y reparar el daño causado cuando las circunstancias sean resolubles, estar al tanto de las faltas o errores cometidos es fundamental para los miembros de una comunidad (estudiantes, administrativos, docentes, y padres de familia), pues solo de esa forma podrán ser corregidos.

Liderazgo

El liderazgo es una función que desempeña alguien que se destaca por encima de los demás y tiene la capacidad de tomar las decisiones correctas para un grupo, equipo u organización que le inspira a los demás a unirse al equipo para lograr un objetivo común, motivo por el cual, el lema característico es: Yo puedo, soy capaz, y yo soy importante.

Emprendimiento

El emprendimiento se puede describir como un proyecto que se efectúa ante diversos retos y esfuerzos encaminados a alcanzar un determinado punto y alcanzar las metas propuestas. En Salinas de Guaranda, los estudiantes de bachillerato, en específico los alumnos de 2ndo año, comprenden esta habilidad y pueden implementarla más adelante a su manera.

Ecología

Se conoce como las acciones relacionadas con la protección del medio ambiente, al momento de realizar cualquier salida, los alumnos deben comprender el amor y defensa de la naturaleza, ofreciendo cuidado a la madre tierra.

Solidaridad

Comprende el cumplimiento incondicional o apoyo a otras causas o intereses, en especial en situaciones difíciles o comprometidas, los miembros de una comunidad educativa cooperan entre si ante los problemas o necesidades de su entorno y se solidarizan en situaciones complicadas.

Respeto

Es la atención, consideración y diferencia que se presenta en el otro, aceptar o tolerar las opiniones o su comportamiento, es reconocer los derechos de los demás, Respetándose a uno mismo, a los demás, y a la naturaleza, sin tener que olvidar las leyes y las normas sociales.

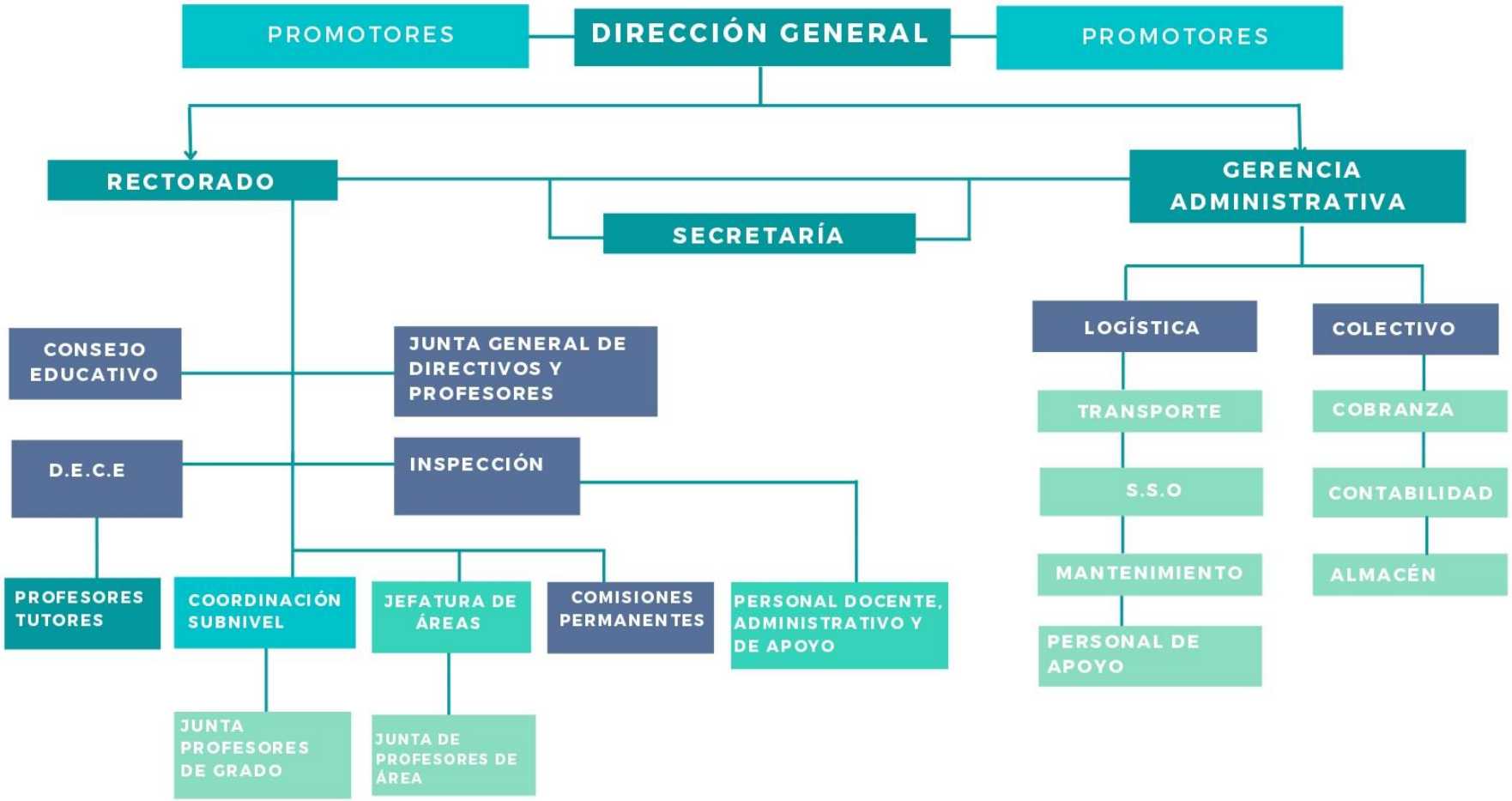
Coherencia

Está descrita como una relación lógica entre la manera en la que piensa una persona y la forma de actuar de esta, la conexión ente el ser y el hacer, en todos los actos que se realizan.

Honradez

Son las cualidades morales, de las personas, actuar según normas éticas, decir la verdad, ser justos, se debe evitar la discriminación, aceptando a los demás como son.

Organigrama

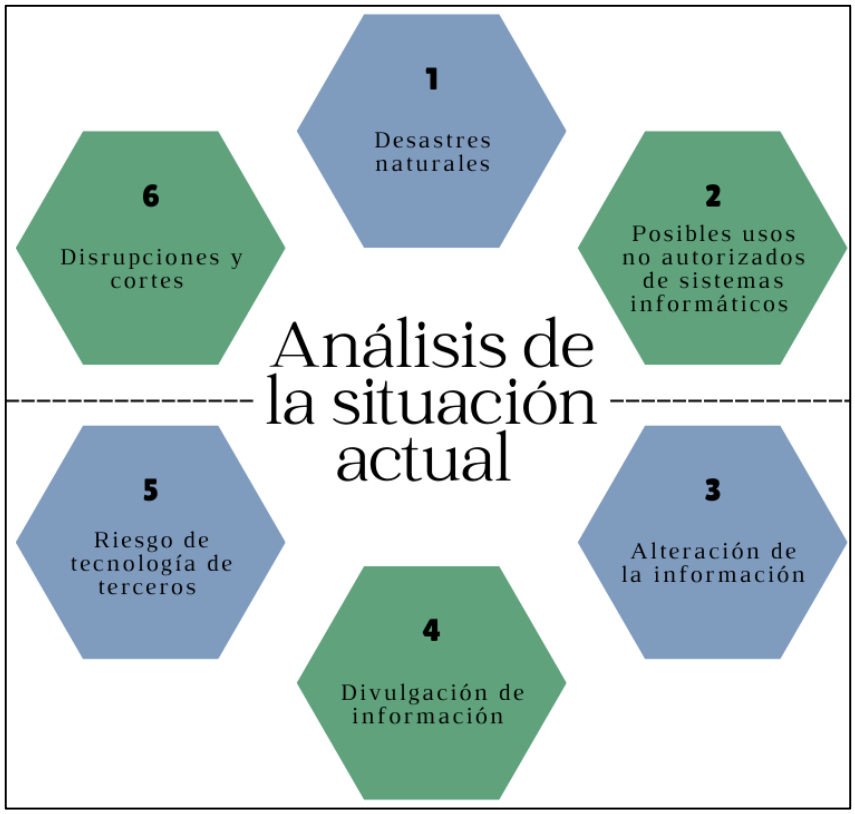

PROMOTORES
DIRECCIÓN GENERAL
PROMOTORES
RECTORADO
SECRETARÍA
GERENCIA ADMINISTRATIVA
CONSEJO EDUCATIVO
JUNTA GENERAL DE DIRECTIVOS Y PROFESORES
D.E.C.E
INSPECCIÓN
PROFESORES TUTORES
COORDINACIÓN SUBNIVEL
JEFATURA DE ÁREAS
COMISIONES PERMANENTES
PERSONAL DOCENTE, ADMINISTRATIVO Y DE APOYO
JUNTA PROFESORES DE GRADO
JUNTA DE PROFESORES DE ÁREA
LOGÍSTICA
COLECTIVO
TRANSPORTE
S.S.O
MANTENIMIENTO
PERSONAL DE APOYO
COBRANZA
CONTABILIDAD
ALMACÉN

Situación actual del plantel educativo

La institución educativa muestra un estado moderado en cuanto a la organización de sus equipos y presenta algunas estrategias en caso de daño de alguno de sus equipos, sin embargo, esto consta únicamente de la respuesta de terceros, como el caso del seguro en caso de un fallo grave a los equipos o contar con la docente encargada del laboratorio de computación, aunque se muestran ciertas prácticas con respecto a los bienes tecnológicos es posible mejorarlos con el fin de obtener la menor cantidad de interrupciones que involucren el área de tecnología.

A continuación, se muestran los principales riesgos que pueden considerarse dentro de esta institución:

Ilustración 5 Identificación de posibles riesgos



Nota, la imagen se realizó en base a la información obtenida (Deloitte, 2016)

Es posible que en el plantel educativo se observen diversas amenazas su impacto dependerá de si existan o no planes de tratamiento de riesgo, sin embargo, como se mencionó anteriormente el centro de enseñanza no presenta un plan estructurado en su totalidad ya que recurre a servicios de terceros para poder mitigar los fallos que se presenten

Los activos se encuentran en sitios accesibles por la mayor parte del personal, aunque no se presenta una posibilidad de que el personal interfiera con esta de forma consciente es posible que al estar en contacto directo con docentes y estudiantes se produzcan accidentes la mayoría siendo la causa inintencionada, más esto aun representa un riesgo contra este tipo de bienes.

CAPITULO V: APLICACIÓN DE LA HERRAMIENTA ISO 31000 EN LA INSTITUCIÓN EDUCATIVA

5. Plan de gestión de riesgos

Definición del contexto

De acuerdo con la norma ISO 31000:2018 antes de evaluar cualquier tipo de amenaza es necesario definir el alcance de las actividades de la futura gestión de riesgos.

Con la finalidad de determinar el contexto organizacional interno se debe analizar y comprender la gobernanza, estructura de la organización, funciones y responsabilidades, a parte se deben considerar los siguientes criterios:

- Políticas, objetivos y estrategias
- Capacidades, las cuales comprenden en termino de recursos y conocimientos, por ejemplo, personas, recursos, tecnología, etc.
- Cultura de la organización
- Procedimientos y flujos de información, para efectuar una toma de decisiones
- Normas, lineamientos y modelos adoptados por la entidad

Por otra parte, para definir el contexto estratégico (externo), se debe tener en cuenta el ambiente social, político, legal, cultural, tecnológico, económico, natural y competitivo, a continuación, se define una serie de características a tomar en cuenta:

- Impulsores estratégicos o las tendencias que presentan impacto en los objetivos de la empresa
- Relaciones con las partes involucradas externas, las percepciones y valores de estas.

Para definir el contexto interno y externo se realizará un análisis de la misión de la institución, visión, productos, clientes, entre otros, a parte se debe establecer un proceso de gestión de riesgo, en base al alcance establecido al comienzo de este documento y al análisis de objetivos de la institución se establece que el proceso de gestión de riesgos debe aplicarse a nivel de capacidades, comprendidas en términos de recursos y conocimientos, además de considerar la cultura de la organización y como se orienta a la aplicación de la tecnología y finalmente con los sistemas de información y flujos de información.

5.1. Identificación de activos

Activos

Los activos se describen como algún componente o funcionalidad de un sistema informático el cual es susceptible de ser atacado de forma deliberada o accidentalmente dando como resultado ciertas consecuencias para la organización.

De forma general se pueden categorizar a los activos relevantes en el siguiente listado:

- Los servicios auxiliares que son requeridos para organizar los sistemas
- Aplicaciones informáticas
- Equipos informáticos
- Soportes de información (almacenamiento)
- Redes de comunicaciones
- Personas que utilizan los elementos mencionados con anterioridad

La clasificación de los activos es de vital importancia ya que la naturaleza de cada uno determinará las salvaguardas necesarias para estos.

Valoración cuantitativa y cualitativa de los activos

Tabla 3 Valoraciones

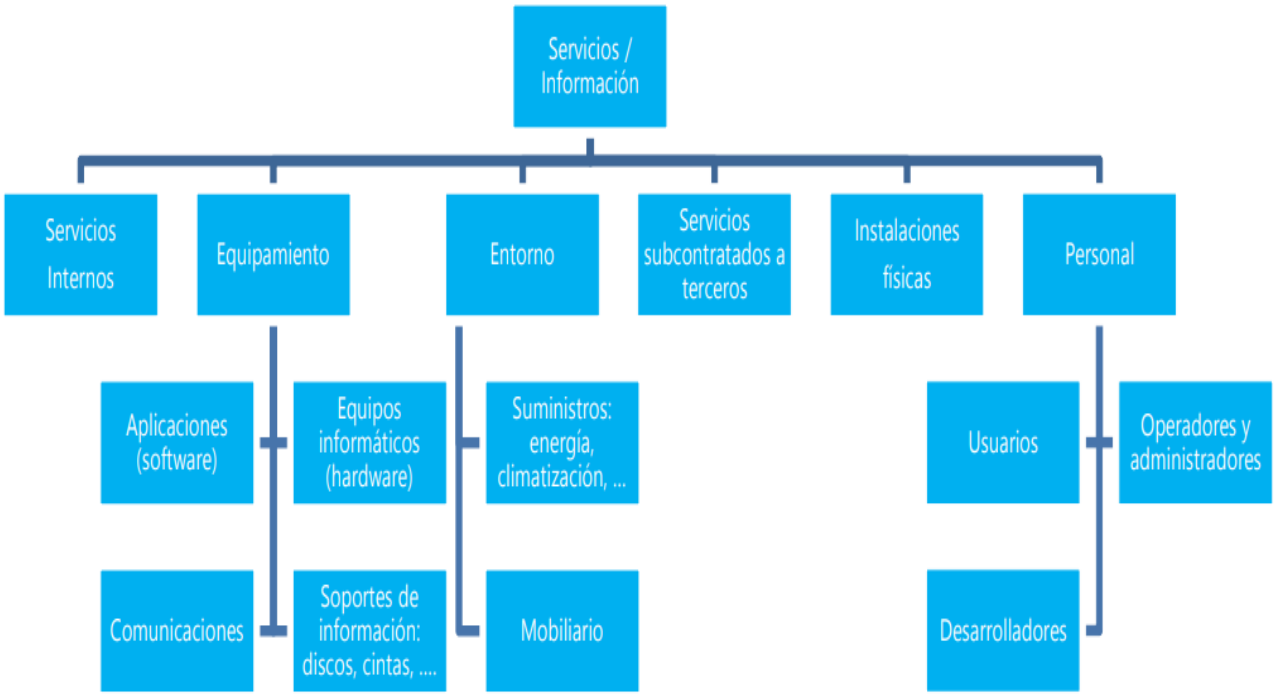
Valoración cuantitativa de los activos	Valoración cualitativa de los activos
Las valoraciones numéricas absolutas presentan un mayor esfuerzo	Las escalas cualitativas, permiten avanzar con rapidez
Presentan de ventaja una suma de valores numéricos de forma completamente natural	Es posible posicionar el valor de cada activo en un orden relativo respecto del resto
Al efectuar una interpretación de las sumas no se manifiesta una causa de controversia	Es común emplear escalas como órdenes de magnitud, siendo como efecto una derivación de estimaciones del orden de magnitud del riesgo
Su valoración es dineraria, a parte se pueden efectuar estudios económicos en comparación con lo que se arriesga	Se muestra la limitante de esta clase de valoración en cuanto a su dificultad al momento de efectuar comparaciones más allá de su orden relativo, no es posible sumar valores

Nota, la tabla representa una adaptación de (Rodríguez & Peralta, 2013)

Dependencia entre los activos

Los activos generan relaciones que forman árboles de dependencias en los cuales la seguridad de los activos que se encuentran en las posiciones superiores (arriba) dependen de los activos que se hallan en las partes inferiores.

Ilustración 6 Dependencias



Nota, la tabla representa una adaptación de (Rodríguez & Peralta, 2013)

En estas relaciones se puede determinar de arriba hacia abajo, mientras que los activos inferiores muestran las dependencias, los activos superiores describen la propagación del daño en caso de que se materializarán las amenazas

Clasificación de activos

Se manifiestan dos aspectos esenciales con respecto a la clasificación de los activos:

- La información que manejan
- Los servicios que ofrecen

Estos activos denominados esenciales definen los aspectos de seguridad para el resto de las componentes del sistema.

De acuerdo con MAGERIT los activos presentan la siguiente clasificación:

Tabla 4 Clasificación de activos

Nombre del Activo	Descripción del activo	Ejemplos del activo
Instalaciones (L)	Se refiere al sitio donde se alojan los sistemas de información.	• [site] recinto • [building] edificio • [local] cuarto • [mobile] plataformas móviles • [car] vehículo terrestre
Hardware (HW)	Todo medio material, físico los cuales se dedican a ofrecer soporte de manera directa o indirecta a los servicios que presta la organización.	• [vhost] equipo virtual • [peripheral] periféricos • [scan] escáneres • [crypto] dispositivos criptográficos • [network] soporte de la red • [modem] módems • [switch] conmutadores • [router] encaminadores • [firewall] cortafuegos

		• [wap] punto de acceso inalámbrico
Software (SW)	Actividades automatizadas, estas aplicaciones analiza, gestionan y transforman los datos admitiendo la utilización de la información para la prestación de servicios.	• [prp] desarrollo propio • [browser] navegador web • [app] servidor de aplicaciones • [email_client] cliente de correo electrónico • [file] servidor de ficheros • [dbms] sistema de gestión
Datos (D)	Información la cual ayuda a la entidad a ofertar sus servicios.	• [files] ficheros • [backup] copias de respaldo • [password] credenciales • [auth] datos de validación de credenciales • [log] registro de actividad
Claves criptográficas (K)	Son utilizadas para proteger el secreto o autenticar a las partes	• [info] protección de la información • [sign] claves de firma

		• [com] protección de las comunicaciones
Redes de comunicaciones (COM)	Se describen como los medios de transporte que se encargan de llevar los datos de un lugar a otro.	• [LAN] red local • [MAN] red metropolitana • [Internet] Internet • [PSTN] red telefónica
Equipamiento Auxiliar (AUX)	Implica al equipamiento que sirve de soporte para los sistemas de información, sin mantener una relación directa con estos.	• [power] fuentes de alimentación • [gen] generadores eléctricos • [ac] equipos de climatización • [cabling] cableado • [supply] suministros esenciales
Personal (P)	El recurso humano que se relaciona con los sistemas de información	• [ue] usuarios externos • [ui] usuarios internos • [op] operadores • [prov] proveedores
Soportes de información (Media)	Implica a los dispositivos físicos que admitan almacenar información permanentemente, o por un periodo prologando de tiempo.	• [electronic] electrónicos • [disk] discos • [vdisk] discos virtuales

	• [san] almacenamiento en red • [non_electronic] no electrónicos • [printed] material impreso

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3 (Públicas, 2012)

Como se ha especificado con anterioridad un activo representa un valor para cualquier organización en este caso la institución educativa, motivo por el que se efectúa un listado de los activos de este plantel, incluyendo únicamente aquellos bienes que se encuentran operativos, siendo los activos de la institución los mencionados a continuación:

Tabla 5 Activos identificados en el centro educativo

Activos de la unidad educativa				
Tipo de activo	**Nombre del activo**	**Código del activo**	**Cantidad del activo**	**Ubicación**
Hardware [HW]	Proyector NEC	AEA001	25	Aulas
Hardware [HW]	Monitor	AEA002	26	Laboratorio de computación Administración
Hardware [HW]	PC	AEA003	26	Laboratorio de computación Administración
Redes de comunicaciones [COM]	Router	AEA004	14	Laboratorio de computación Aulas

Redes de comunicaciones [COM]	Access Point	AEA005	1	Laboratorio de computación
Hardware [HW]	Impresora	AEA006	8	Administración Biblioteca
Hardware [HW]	Parlantes	AEA007	5	Administración Biblioteca
Software [SW]	Programa de contabilidad SAGI	AEA008	1	Colecturía
Software [SW]	Deep Freeze	AEA009	1	Laboratorio de computación
Software [SW]	Sistema operativo Windows 10	AEA010	1	Laboratorio de computación Administración
Software [SW]	Office 2016	AEA011	1	Laboratorio de computación Administración
Software [SW]	Navegador web Chrome	AEA012	1	Laboratorio de computación Administración
Hardware [HW]	Teclado	AEA013	26	Laboratorio de computación Administración
Hardware [HW]	Mouse	AEA014	26	Laboratorio de computación Administración
Personal (P)	Personal administrativo, secretaria	AEA015	n/c	Administración

Personal (P)	Docentes y estudiantes	AEA016		n/c	Institución educativa

Nota, la tabla es de propia autoría en colaboración con la información otorgada por la institución educativa

Como se observa en *la Tabla 5 Activos identificados en el centro educativo*, los activos fueron clasificados por tipo, cantidad y ubicación, se utiliza este tipo de clasificación debido a su simpleza para visualizar los datos, sin embargo, MAGERIT proporciona un archivo para describir cada activo de una organización, que se puede ver en el *Apéndice 1*.

Escenarios de Amenazas

Al emplear MAGERIT se puede observar los siguientes casos de amenazas, clasificado ya sea por factores físico, lógicos, internos y externos de la siguiente manera:

Tabla 6 amenazas

Amenazas descritas de acuerdo con Magerit	**Amenazas**		**Descripción**
Desastres naturales [N]	N1	Fuego	Se manifiesta la probabilidad de que el fuego acabe con los recursos.
	N2	Daños por agua	Probabilidad de que el agua acabe con los recursos.
	N*	Desastres naturales	Aquellos que se produzcan sin la intervención del ser humano excluyendo N1 y N2

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3 (Públicas, 2012)

Tabla 7 Amenazas

Amenazas descritas de	**Amenazas**	**Descripción**

acuerdo con Magerit			
De origen industrial [I]	I1	Fuego	Se manifiesta la probabilidad de que el fuego acabe con los recursos.
	I2	Daños causados por el agua	Escapes, fugas, inundaciones
	I3	Contaminación mecánica	Polvo, vibraciones, impurezas
	I5	Deterioro de origen físico o lógico	Implica fallos en los equipos o programas, ya sea durante el funcionamiento de este o de origen
	I6	Corte de suministro eléctrico	Se detenga la alimentación de potencia
	I7	Condiciones inadecuadas de temperatura o humedad	Deficiencia en la aclimatación de los locales: calor o frio excesivo
	I8	Fallo de servicios de comunicaciones	Se detiene la capacidad de emitir daros de un lugar a otro (por destrucción o incapacidad)
	I9	Complicación de otros servicios esenciales	Servicios y recursos dependen de la operación de otros equipos
	I10	Deterioro de los soportes de almacenamiento de la información	Resultado que se manifiesta por el efecto del paso del tiempo

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3, incluyendo solo aquellas relacionadas con las posibles amenazas de la institución (Públicas, 2012)

Tabla 8 Amenazas

Amenazas descritas de acuerdo con Magerit	Amenazas		Descripción
Errores y fallos no intencionados [E]	E1	Faltas de los usuarios	Despistes de las personas

	E2	Errores del administrador	Falencias de las personas que efectúan tareas de instalación u operación
	E3	Errores de monitorización	Falta de registros, registros incompletos, registros incorrectamente fechados, etc.
	E4	Errores de configuración	Se introduce datos de configuración erróneos
	E7	Deficiencias en la organización	Cuando no se comprende que funciones debe desempeñar el personal
	E8	Difusión de software dañino	Propagación de virus, spyware, troyanos, etc.
	E9	Fallas relacionadas con el re - encaminamiento	Envío de información mediante un sistema o red, de forma accidental; una ruta incorrecta que lleve información donde no corresponde
	E10	Errores de secuencia	Modificación accidental del orden de los mensajes enviados
	E14	Escapes de información	La información es conocida por personal no autorizado
	E15	Alteración accidental de la información	Alteración accidental de la información
	E18	Catástrofe ocurrida a la información	Pérdida esporádica de información
	E19	Fugas de información	Revelación por indiscreción
	E20	Vulnerabilidades de los programas	Desperfectos en el código que dan como resultado una operación defectuosa
	E21	Errores de mantenimiento / actualización de programas	Defectos en los procedimientos o controles de actualización del código
	E23	Faltas alusivas al sostenimiento o actualización de equipos	Desperfectos en las operaciones o controles de actualización de los aparatos

	E24	Caída del sistema por agotamiento de recursos	Falta de recursos suficientes lo que provoca la caída del sistema
	E25	Pérdida de equipos	Perdida de equipos generando una carencia de un medio
	E28	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3 (Públicas, 2012)

Tabla 9 Amenazas

Amenazas descritas de acuerdo con Magerit	Amenazas		Descripción
Ataques intencionados [A]	A3	Manipulación de los registros de actividad	-
	A4	Manipulación de la configuración	La mayor parte de activos dependen de su configuración y esta de la diligencia del administrador
	A5	Suplantación de la identidad del usuario	Un usuario no autorizado accede a ciertos privilegios para sus propios fines
	A6	Abuso de privilegios de acceso	Un usuario abuso de su nivel de privilegios
	A7	Uso no previsto	Empleo de los recursos del sistema por interés personal
	A8	Difusión de software dañino	Propagación intencional de virus, gusanos troyanos, etc.
	A9	Re – encaminamiento de mensajes	Envío de información mediante un sistema o red el cual lleva información donde no corresponde
	A10	Modificación de la secuencia	Variación del orden de los mensajes emitidos.

	A11	Acceso no autorizado	Un atacante consigue acceder a los recursos del sistema sin autorización para esto
	A12	Exploración de tráfico	Un atracador emplea un análisis del contenido de las comunicaciones extrayendo conclusiones
	A13	Rechazo	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado
	A14	Interceptación de información	Un atacante obtiene acceso a información que no le corresponde
	A15	Modificación deliberada de la información	Alteración intencional de la información
	A18	Destrucción de información	Eliminación intencional de la información
	A19	Propagación de información	Develamiento de información
	A22	Manipulación de programas	Alteración intencional del funcionamiento de algún programa
	A23	Manipulación de los equipos	Alteración intencional del funcionamiento de algún equipo
	A24	Denegación de servicio	Carencia de algún recurso lo cual provoca la caída del sistema
	A25	Hurto	El robo de dispositivos conduce directamente a la falta de medios para prestar el servicio (indisponibilidad)
	A26	Ataque destructivo	Amenaza efectuada por el personal interno o ajenas a la entidad, ejemplo: vandalismo
	A27	Ocupación enemiga	Cuando los establecimientos son invadidos y carece de control sobre el propio medio de trabajo

	A28	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo
	A29	Extorsión	A través de amenazas, un atacante ejerce presión para obligar a obrar en determinada forma a otra persona
	A30	Ingeniería Social (engaño al usuario)	Abusar de la confianza de la gente

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3 (Públicas, 2012)

Correspondencia de errores y ataques

Los errores y amenazas son situaciones que ocurren ya sea de forma accidental o debido a una acción deliberada, con esto a consideración se obtienen tres combinaciones posibles:

- Aquellas amenazas que pueden denominarse errores, mas no se clasifican como ataques deliberados
- Las amenazas que no representan errores, esto significa que son ataques deliberados
- Representan amenazas que pueden generarse ya sea por un error o de forma deliberada

Tabla 10 Errores y amenazas

N.	Error	Ataque
1	**Errores cometidos por los usuarios**	
2	**Falencias realizadas por un administrador**	
3	**Fallas de monitorización (log)**	Manejo de los registros de actividad
4	**Equivocaciones de configuración**	Manejo de la configuración
5		Reemplazo de la identidad algún usuario
6		Extralimitación de los privilegios de acceso

7	**Irregularidades en la organización**	Uso no advertido
8	**Propagación de software perjudicial**	Propagación de software perjudicial
9	**Fallas de [re-]encaminamiento**	El Re - encaminamiento de los mensajes
10	**Errores de secuencia**	Variación de secuencia
11		Acceso injustificable
12		Estudio de tráfico
13		Rechazo
14	**Fugas de información**	Apropiación de información
15	**Modificación accidental de la información**	Modificación premeditada de la información
18	**Quebrantamiento de la información**	Quebrantamiento de información
19	**Escapes de información**	Develamiento de información
20	**Decaimientos de los programas**	
21	**Omisiones en el mantenimiento / actualización de programas**	
22		Manejo de programas
23	**Equivocaciones de mantenimiento o de actualización de equipos**	Manipulación de los equipos
24	**Desplome del sistema por extenuación de los recursos**	Rechazo del servicio
25	**Carencia de equipos**	Desfalco
26		Agresión destructiva
27		Ocupación enemiga
28	**Falta de disponibilidad del personal**	Carencia del personal
29		Usurpación

Esta tabla se elaboró en base a las guías de calificación de activos de MAGERIT versión 3 (Públicas, 2012)

Criterios de valoración

Los activos al ser clasificados de acuerdo con su naturaleza deben ser valorados, para establecer una escala apta, se deben considerar diversos aspectos, el valor que obtenga cada bien representa su grado de importancia, teniendo en cuenta la disponibilidad, integridad y confiabilidad de cada uno.

Como fue comentado anteriormente la apreciación de los bienes puede ser cuantitativa o cualitativa, en este caso se empleará una valoración cuantitativa, en específico un rango numérico de 1 a 5, se debe mostrar objetividad para obtener un resultado preciso en cuanto a la realidad de los activos del plantel educativo.

Es fundamental que la valoración de los activos debe ser sencillos de comprender para todos los interesados/participantes, con el fin de que se puedan comparar los valores y una vez establecido los resultados se puedan determinar los activos que muestran una mayor prioridad, y de esta manera su atención será oportuna.

IMPACTO

El impacto representa el daño que puede ser causado por algún incidente.

Tabla 11 Impacto

Valor		Criterio
1	Despreciable	Irrelevante a efectos prácticos
2	bajo	Daño menor
3	Medio	Daño importante
4	Alto	Daño grave
5	Muy alto	Daño muy grave

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3 (Públicas, 2012)

FRECUENCIA

Esta se refiere a la tasa de ocurrencia, de cada cuanto se materializa alguna amenaza.

Tabla 12 Frecuencia

Escala	Criterio
1	**Raro**
2	**Bajo**
3	**Posible**
4	**Alto**
5	**Muy alto**

Esta tabla se realizó en base a la calificación de activos de MAGERIT v.3 (Públicas, 2012)

5.2. Análisis de riesgos

Una vez se estableció una escala para determinar tanto el impacto como la frecuencia, se procede a efectuar la calificación del riesgo, en esta fase se efectúa una estimación y se obtienen los criterios de probabilidad de ocurrencia del riesgo y el impacto que traería, en el caso de que se materialice.

Tabla 13 Análisis del riesgo

Tipo de activo	Nombre de activo	Valoración de frecuencia (1-5)	Valoración del impacto (1-5)	Riesgo = frecuencia x impacto
Hardware [HW]	Proyector	2	4	8
	Monitor	3	3	9
	PC	4	4	16
	Impresora	3	2	6
	Parlantes	2	1	2

	Teclado	3	3	9
	Mouse	3	3	9
Redes de comunicaciones [COM]	Router	2	4	8
	Access Point	2	4	8
Software [SW]	Programa de contabilidad SAGI	2	2	4
	Programa de congelación de las configuraciones	1	2	2
	Sistema operativo Windows 10	2	3	6
	Office 2016	1	2	2
	Navegador web Chrome	1	2	2
Personal (P)	Personal administrativo, secretaría	2	3	6
	Docentes y estudiantes	3	4	12

Esta tabla se realizó en base a la valoración de riesgos MAGERIT y a la interpretación de la autora

5.3. Valoración de riesgos

La valoración de los riesgos se presenta de una forma cualitativa, lo cual ofrece una comparación en la que se presenta el análisis de la probabilidad (frecuencia) versus el impacto que este tendría, dando como resultado la denominada Matriz de calificación, ofreciendo zonas

de riesgo, mostrando posibles formas de tratamiento que se puede tener para un determinado riesgo

Tabla 14 Matriz de calificación

Probabilidad		Matriz de riesgos				
		Consecuencia				
		Despreciable	Bajo	Medio	Alto	Muy alto
		Uno	Dos	Tres	Cuatro	Cinco
Muy alto	Cinco	5	10	15	20	25
Alto	Cuatro	4	8	12	16	20
Posible	Tres	3	6	9	12	15
Bajo	Dos	2	4	6	8	10
Raro	Uno	1	2	3	4	5

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Las zonas que se describen en la siguiente tabla son parte de la valoración de riesgos de MAGERIT

Tabla 15 Zonas de riesgo

Áreas	***Nivel de riesgo***	***Color / Identificador***
Zona N1	Muy probable y alto riesgo de impacto	
Zona N2	Desde situaciones inalcanzables y de mediano impacto, hasta situaciones altamente probables, pero de poco o ningún impacto	
Zona N3	Bajo riesgo y bajo impacto	

Zona N4	Bajo riesgo, pero muy alto impacto	

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

De forma simplificada se puede observar la siguiente tabla en la que se representa por zona, color y valoración las distintas variaciones que puede tener un riesgo.

Tabla 16 Tabla de riesgos

Riesgo clasificado según las bandas de colores					
Zona N.1	16-17	18-19	20-21	22-23	24-25
Zona N.2	5-6	7-8	9		
Zona N.3	1	2	3	4	
Zona N.4	10-11	12-13	14-15		

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Cuando los riesgos tienen un valor cuantitativo y cualitativo, se da paso a la siguiente fase, en la que se debe tener en cuenta los valores mostrados anteriormente, en otras palabras, cada activo presenta un nivel de gravedad, el cual permite priorizar e indicar como deberá tratarse en el futuro aparte de que se identifica la naturaleza de cada bien, los clasifica de una forma sencilla de comprender para todos los interesados.

Tabla 17 Valoración del riesgo de los activos

Tipo de activo	Código del activo	Nombre de activo	Valoración frecuencia	Valoración impacto	Zona de riesgo	Código riesgo
Hardware [HW]	AEA001	Proyector	Bajo	Alto	Zona 2	RA001
	AEA002	Monitor	Bajo	Medio	Zona2	RA002
	AEA003	PC	Alto	Alto	Zona 1	RA003
	AEA004	Impresora	Posible	Bajo	Zona 2	RA004
	AEA005	Parlantes	Bajo	Despreciable	Zona 3	RA005
	AEA006	Teclado	Posible	Medio	Zona 2	RA006
	AEA007	Mouse	Posible	Medio	Zona 2	RA007
Redes de comunicaciones [COM]	AEA008	Router	Bajo	Alto	Zona 2	RA008
	AEA009	Access Point	Bajo	Alto	Zona 2	RA009
Software [SW]	AEA010	Programa de contabilidad SAGI	Bajo	Bajo	Zona 3	RA010
	AEA011	Programa de congelación de las configuraciones	Raro	Bajo	Zona 3	RA011
	AEA012	Sistema operativo Windows 10	Bajo	Medio	Zona 2	RA012
	AEA013	Ofimática	Raro	Bajo	Zona 3	RA013
	AEA014	Navegador web Chrome	Raro	Bajo	Zona 3	RA014

Personal (P)	AEA015	Personal administrativo, secretaria	Raro	Medio	Zona 2	RA015
	AEA016	Docentes y estudiantes	Raro	Alto	Zona 4	RA016

Esta tabla se realizó en base a la valoración de riesgos MAGERIT y a los resultados obtenidos en fases anteriores

Cada riesgo muestra un identificador, el cual se ha ubicado en la matriz de calificaciones esto permite conocer de forma intuitiva la gravedad de cada amenaza y la prioridad que se debería ofrecer a cada uno de estos.

Tabla 18 Perfil de riesgos

PERFIL DE RIESGOS							
IMPACTO	**Muy alto**	**5**					
	Alto	**4**		RA001, RA008, RA009	RA016	RA003	
	Posible	**3**		RA012, RA015	RA002-RA006-RA007		
	Bajo	**2**	RA011, RA013	RA010. RA014	RA004		
	Raro	**1**		RA005			
	Frecuencia		**Despreciable**	**Bajo**	**Medio**	**Alto**	**Muy alto**
			1	**2**	**3**	**4**	**5**

Esta tabla se realizó en base a la valoración de riesgos MAGERIT y a los resultados obtenidos en fases anteriores

5.4. Plan de tratamiento

Durante el análisis del tratamiento de riesgo propuesto según ISO 31000:2018, el proceso de tratamiento se vuelve iterativo, incluyendo las siguientes etapas:

- Formación y selección de opciones para hacer frente a los riesgos
- Planificar y efectuar la administración de riesgos
- Comprobar la eficacia de este tratamiento
- Discutir si el riesgo residual es aceptable

- Si el riesgo residual se considera inaceptable, se deben realizar procedimientos de tratamiento adicionales

Escoger la opción adecuada para el tratamiento del riesgo conlleva a realizar un balance entre los beneficios potenciales resultado del logro de los objetivos contra los costes, esfuerzos o desventajadas de la implementación, las opciones de tratamiento del riesgo no son mutuamente excluyentes o adecuadas en todas las situaciones, sin embargo, se establece ciertas opciones. Seleccionar la opción de tratamiento de riesgos adecuada implica sopesar los beneficios potenciales de lograr los objetivos frente al costo, el esfuerzo o los inconvenientes de la implementación. La gestión de riesgos no es mutuamente excluyente ni apropiada en todas las situaciones, sin embargo, se establecen ciertas opciones de tratamiento de riesgos que pueden implicar algunos de las siguientes listas:

- El riesgo debe evitarse decidiendo no iniciar o continuar la actividad que genera el riesgo.
- Aceptar o aumentar el riesgo para encontrar oportunidades
- Eliminar la fuente de riesgo
- Modificación de probabilidad
- Editar consecuencias
- Distribución de riesgos, tales como: a través de contratos, suscripción de seguros.
- Retener el riesgo basado en decisiones informadas

En base a lo mencionado anteriormente se establece la siguiente escala:

Tabla 19 Niveles de riesgo

Niveles de riesgo	Zona	Respuesta al riesgo	Descripción
Muy probable y alto riesgo de impacto	**Zona 1**	Eliminar la fuente del riesgo	Es necesario una acción inmediata, planes de

			tratamiento requeridos, implementados y reportados a los directivos
Desde situaciones inalcanzables y de mediano impacto, hasta situaciones altamente probables, pero de poco o ningún impacto	**Zona 2**	Modificar la probabilidad y las consecuencias	Es posible admitir ciertos errores y realizar acciones correctivas después una vez identificado su origen e impacto
Bajo riesgo y bajo impacto	**Zona 3**	Retener el riesgo con base en una decisión informada	Se debe administrar con procedimientos de controles rutinarios
Bajo riesgo, pero muy alto impacto	**Zona 4**	Aceptar o incrementar el riesgo en busca de alguna oportunidad	Se necesita atención de los lideres de los procesos, elaboración de planes de tratamiento implementados y reportados a los altos directivos

Esta tabla se realizó en base a la valoración de riesgos MAGERIT y a los resultados obtenidos en fases anteriores

Tabla 20 Niveles de riesgo

Tipo de activo	Código del activo	Nombre de activo	Valoración frecuencia	Valoración impacto	Zona de riesgo	Respuesta al riesgo	Código riesgo
Hardware [HW]	AEA001	Proyector	Alto	Medio	Zona 4	Aceptar o incrementar el riesgo en busca de alguna oportunidad	RA001
	AEA002	Monitor	Posible	Medio	Zona 2	Modificar la probabilidad y las consecuencias	RA002
	AEA003	PC	Alto	Alto	Zona 1	Eliminar la fuente del riesgo	RA003
	AEA004	Impresora	Posible	Medio	Zona 2	Modificar la probabilidad y las consecuencias	RA004
	AEA005	Parlantes	Bajo	Bajo	Zona 2	Modificar la probabilidad y las consecuencias	RA005
	AEA006	Teclado	Posible	Medio	Zona 2	Modificar la probabilidad y las consecuencias	RA006
	AEA007	Mouse	Posible	Medio	Zona 2	Modificar la probabilidad y las consecuencias	RA007
Redes de comunicaciones [COM]	AEA008	Router	Posible	Alto	Zona 4	Aceptar o incrementar el riesgo en busca de alguna oportunidad	RA008

	AEA009	Access Point	Posible	Alto	Zona 4	Aceptar o incrementar el riesgo en busca de alguna oportunidad	RA009
Software [SW]	AEA010	Programa de contabilidad SAGI	Bajo	Medio	Zona 2	Modificar la probabilidad y las consecuencias	RA010
	AEA011	Programa de congelación de las configuraciones	Posible	Medio	Zona 4	Aceptar o incrementar el riesgo en busca de alguna oportunidad	RA011
	AEA012	Sistema operativo Windows 10	Posible	Medio	Zona 4	Aceptar o incrementar el riesgo en busca de alguna oportunidad	RA012
	AEA013	Ofimática	Bajo	Medio	Zona 2	Modificar la probabilidad y las consecuencias	RA013
	AEA014	Navegador web Chrome	Raro	Bajo	Zona 3	Retener el riesgo con base en una decisión informada	RA014
Personal (P)	AEA015	Personal administrativo, secretaria	Raro	Alto	Zona 2	Modificar la probabilidad y las consecuencias	RA015
	AEA016	Docentes y estudiantes	Bajo	Alto	Zona 4	Aceptar o incrementar el riesgo en busca de alguna oportunidad	RA016

Esta tabla se realizó en base a la valoración de riesgos MAGERIT y a los resultados obtenidos en fases anteriores

En MAGERIT, los planes de tratamiento califican como salvaguardas que permiten tomar acciones o instrucciones en respuesta a las amenazas, en especial estos "salvaguardas", se modifican de acuerdo con el progreso tecnológico porque:

- La aparición de nuevas tecnologías
- Desaparición de algunas tecnologías
- Los activos incluidos han sido modificados
- La capacidad de un atacante para realizar una acción que dañe a una entidad ha evolucionado
- Por último, el número de copias de seguridad o salvaguardas ha aumentado o disminuido

Cabe señalar que los salvaguardas cumplen el rol de paraguas taxonómico con el fin de organizar y clasificar diversas correcciones, ya sean físicas, tecnológicas, procedimentales u organizativas.

Portafolio de acciones MAGERIT

Si bien los controles totales de MAGERIT se encuentran en el *Anexo 2*, en las líneas subsiguientes se presentan los controles que se han considerado para el caso de estudio en cuestión.

Protecciones generales u horizontales

Tabla 21 Portafolio de acciones

Código	Descripción
Row	Protección General
R.IDA	Identificación y autenticación
R.CAL	Control de acceso lógico

R.DT	Disyunción de tareas
R.GI	Gestión de las incidencias
R. instrumentos (instr)	Herramientas de seguridad
R. instr.CD	Herramienta contra código dañino
R. instr.IDS	IDS: detección de intrusos IPS: prevención de intrusión
R. instr.CC	Chequeo de configuración
R. instr.AV	Instrumentos de análisis de vulnerabilidades
R. instr.MT	Herramienta de monitorización de tráfico
R. instr.DLP	DLP: Monitorización de contenido
R. instr.AL	Análisis de logs
R. instr.HP	Honey pot
R. instr.VFS	Verificación de las funciones de seguridad
R.GV	Gestión de vulnerabilidades
R.RA	Registro y auditoría

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Protecciones de los datos / información

Tabla 22 portafolio de acciones

Código	Descripción
Info	Defensa de la Información
Info.A	Copias de seguridad (backup)
Info.I	Fortalecimiento de la integridad
Info.C	Cifrado de la información
Info.DS	Manejo de firmas electrónicas
Info.TS	Utilización de servicios de fechado electrónico

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Protecciones de las aplicaciones

Tabla 23 Portafolio de acciones

Código	Descripción
AI	Resguardo de las Aplicaciones Informáticas
AI.A	Copias de seguridad
AI.comienzo	Puesta en marcha
AI.SC	Emplean perfiles de seguridad
AI.op	Explotación / Producción
AI.CM	Variaciones (actualización y mantenimiento)
AI.fin	Desenlace

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Protecciones de los equipos (hardware)

Tabla 24 Portafolio de seguridad

Código	Descripción
EI	Guarda de los Equipos Informáticos
EI.comienzo	Puesta en producción
EI.SC	Se aplican perfiles de seguridad
EI.RD	Refuerzo de la disponibilidad
EI.op	Operación
EI.CM	Variaciones (actualización y mantenimiento)
EI.fin	Terminación
EI.IM	Informática móvil
EI.DOC	Generación de documentos

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Salvaguardas relativas al personal

Tabla 25 Portafolio de seguridad

Código	Descripción
GP	Manejo del Personal
GP.FC	Formación y concienciación

GP.AD	Aseguramiento de la disponibilidad

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Plan de seguridad

En MAGERIT se denomina plan de seguridad a la fase en la que se llevan a cabo planes de seguridad, los cuales reflejan las decisiones que se tomarán para efectuar el tratamiento de los riesgos.

Los planes de seguridad comprenden diferentes contextos y circunstancias como:

- Plan de mejora de la seguridad
- Plan director de seguridad
- Plan estratégico de seguridad
- Plan de adecuación (en este caso es el nombre utilizado es el de ENS)

Las tareas principales se dividen en:

Tabla 26 Portafolio de seguridad

PS – Plan de seguridad
✓ **PS.1: Referencia a la identificación de los proyectos de seguridad**
✓ **PS.2: Plan para efectuar la ejecución**
✓ **PS.3 Ejecución**

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

Tarea: Plan Seguridad N1: Identificación de proyectos de seguridad

Tabla 27 Plan de Seguridad 1

Tarea: Plan Seguridad N1: Identificación de proyectos de seguridad	
Objetivo	Crear un conjunto armonizado de programas de seguridad.
Productos de entrada	▪ Productos y servicios de seguridad ▪ Conocimientos técnicos y productos de seguridad ▪ Producto de las acciones de análisis y tratamiento de los riesgos
Producto de salida	Lista de programas de seguridad
Técnica, prácticas y pautas	Implementar la planificación del proyecto
Colaboradores	Expertos, equipo de proyecto conjunto.

Esta tabla se realizó en base al plan de seguridad de MAGERIT

Tarea Plan de Seguridad N.2: Planificación de los proyectos de seguridad

Tabla 28 Plan de Seguridad 2

PS – Plan de seguridad **PS.2: Planificación de los proyectos de seguridad**

Objetivo	Organizar de forma temporal los programas de seguridad
Productos de entrada	▪ Los resultados de las actividades de análisis y tratamiento de riesgos ▪ Los resultados de la actividad PS.1
Producto de salida	▪ Cronograma de ejecución del plan ▪ Plan de seguridad que se efectuó en la tarea anterior
Técnica, prácticas y pautas	▪ Efectuar un análisis de riesgos ▪ Planificar proyectos
Colaboradores	Departamento de compras y desarrollo

Esta tabla se realizó en base al plan de seguridad de MAGERIT

Tarea Plan de Seguridad N.3: Ejecución del plan

Tabla 29 Plan de Seguridad 3

PS – Plan de seguridad **PS.3: Ejecución del plan**	
Objetivo	
Productos de entrada	▪ Los resultados de las actividades de análisis y tratamiento de riesgos ▪ Los resultados de la actividad PS.1
Producto de salida	▪ Cronograma de ejecución del plan ▪ Plan de seguridad

Técnica, prácticas y pautas	▪ Efectuar un análisis de riesgos ▪ Planificar proyectos
Colaboradores	Departamento de compras y desarrollo

Esta tabla se realizó en base a la valoración de riesgos MAGERIT

CAPÍTULO V: CONCLUSIONES Y RECOMENDACIONES

Producto del estudio realizado se puede concluir y recomendar lo siguiente:

6.1. CONCLUSIONES

- ✓ Establecer una clasificación de los bienes o activos puede ayudar a determinar el impacto que debe tener una amenaza al momento de materializarse, lo cual ofrecerá una ventaja para que se efectúen planes de tratamiento que fueron previamente concebidos al momento de realizar una adecuada gestión de riesgos.

- ✓ Los centros educativos muestran un incremento en la utilización de la tecnología no únicamente en procesos administrativos sino también en la enseñanza, aunque estos aspectos ofrecen una cantidad de beneficios a sus usuarios, ya sea internos y externos, esto significa que se deben llevar a cabo controles más rigurosos, debido a que estos bienes o activos se encuentran en contacto con el personal que no tiene un gran conocimiento en tecnología.

- ✓ MAGERIT se describe como una metodología para el análisis y gestión de riesgos, y ofrece un apoyo para descubrir y efectuar medidas para mantener los riesgos bajo un umbral aceptable, una de sus cualidades es el establecer escalas para identificar el impacto de los riesgos, además representa una herramienta sencilla para incluirla en la gestión de riesgos.

- ✓ La ISO 31000 señala que cualquier organización, sin considerar su tamaño, es susceptible a sufrir riesgos los cuales impidan el cumplimiento de sus objetivos o metas, es por eso por lo que al emplear esta norma se presenta la posibilidad de reducir la incertidumbre y gestionar los riesgos con una orientación sistemática, de esta forma es viable evaluar qué procesos de la gestión de riesgos se llevan a cabo correctamente e identificar las prácticas necesarias para realizar una correcta gestión de riesgos.

- ✓ La gestión de riesgos se describe como el manejo de posibles amenazas/incertidumbres que pueden darse al realizar cualquier actividad dentro de una organización, no solo es útil al momento de reducir la cantidad de riesgos que una empresa pueda tener, también fortalece al cumplimiento de metas y objetivos estratégicos de las organizaciones, además que permite tener planes de acción para reducir el impacto que cualquier amenaza pueda generar si llegase a materializarse.

6.2. RECOMENDACIONES

- Es necesario considerar que otros estándares, normativas o buenas prácticas implementadas en instituciones, incrementan el nivel de confianza de una organización, es importante tener en cuenta que no todos los negocios requieren el mismo nivel de rigurosidad al momento de aplicar estas buenas prácticas, motivo por el cual se recomienda determinar correctamente los objetivos, misión y visión de una entidad son de vital importancia para determinar qué prácticas se deben llevar a cabo.

- Si bien existen normativas e incluso manuales sobre cómo implementar ciertos estándares, también se recomienda incluir un juicio propio, de la persona que efectúa la gestión de riesgos, ya sea al momento de elaborar escalas, clasificación de activos, identificación de amenazas, entre otros; esto debido a que las normas tienden a ser generalizadas y deben ajustarse acorde a la orientación del negocio.

- Las herramientas de gestión de riesgo, aplicadas en las instituciones educativas representan una gran ventaja debido a que se puede llevar a cabo un control de activos, procesos, personal, entre otros, que permita identificar las posibles amenazas que se puedan presentar y efectuar un plan de tratamiento, además, en la actualidad los planteles educativos empiezan a adquirir equipos que requieren un mayor control debido a que manejan información privilegiada y sensible, es por eso que se sugiere, que se analice el impacto que puede representar para la institución si no se lleva a cabo un análisis de riesgos y cómo se elaboraría un plan de tratamiento para centros educativos que emplean equipos tecnológicos.

- La gestión de riesgos es un proceso sistemático, y puede ser empleada con normas como ISO 31000, sin embargo, se puede apreciar que estas normas pueden mostrarse incompletas debido que han sido creadas con el fin de que sean aplicables a cualquier negocio, es por eso por lo que se recomienda emplear en conjunto otras herramientas como el caso de RISK IT y MAGERIT, esto debido a que tienen una visión orientada al sector de TI, en este caso específico se orienta a la gestión de riesgos en base al valor y beneficios que una organización obtiene a través de sus iniciativas y la inclusión de TI.

BIBLIOGRAFÍA

Silva Rampinia, G. H., Takia, H., & Tobal Berssanetia, F. (2019). Critical Success Factors of Risk Management with the Advent of ISO 31000 2018 - Descriptive and Content Analyzes. *Procedia Manufacturing, 39*, 894-903. doi:https://doi.org/10.1016/j.promfg.2020.01.400

CABRERA, W. E. (2019). *MODELO DE GESTIÓN DE RIESGOS DE TI ENFOCADO EN ESTÁNDARES ADAPTADOS PARA CONTRIBUIR EN LA PROTECCIÓN DEL ACTIVO DE TI EN EL SECTOR DE DISTRIBUIDORAS DE LA REGIÓN LAMBAYEQUE.* Chiclayo.

Deloitte. (2016). *Information technology risks in financial services: What board members need to know*. Obtenido de www2.deloitte.com: https://www2.deloitte.com/content/dam/Deloitte/co/Documents/risk/Riesgos%20TI%20%20Servicios%20Financieros%20(ok).pdf

Granda Ayabaca, D. M., Jaramillo Alba, J. A., & Espinoza Guamán , E. E. (2019). IMPLEMENTACIÓN DE LAS TIC EN EL ÁMBITO EDUCATIVO ECUATORIANO. *Revista Sociedad & Tecnología*, 45-53.

Guerrero Aguiar, M., Medina León, A., & Nogueira Rivera, D. (2020). *Procedimiento de gestión de riesgos como apoyo a la toma de decisiones.* La Habana, Cuba: Scielo.

Nieto, N. E. (2019). Tipos de Investigación. *Repositorio institucional - USDG*.

Palacios, A. P. (2020). Seguridad Informatica . En A. P. Palacios, *Seguridad Informatica* (págs. 2-6). Graficas Summa.

Pazmiño Zabala, C. A., Serrano Castro, A. K., & González Rivera, M. M. (2020). Las Tics como herramienta para la gestión de riesgos. *Recimundo*, 173-181. doi:10.26820/recimundo/4.(1).esp.marzo.2020.173-181

Peña, R. L., & Lugani, C. F. (2019). Monitoreo de riesgos de activos de información en la Universidad Nacional de Río Negro. *XIII Simposio de Informática en el Estado (SIE 2019)* (págs. 1-11). Argentina: Sociedad Argentina de Informática e Investigación Operativa. Obtenido de http://sedici.unlp.edu.ar/handle/10915/89716

Públicas, M. d. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de administracionelectronica.gob.es: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

Rodríguez, J. M., & Peralta, I. (2013). *Gestión de Riesgos Magerit*. Obtenido de tithink: https://www.tithink.com/publicacion/MAGERIT.pdf

Suárez Pérez , Y., & Nieto Acosta, O. M. (2020). Metodología para gestionar riesgos en la autoevaluación de las maestrías del Instituto de Farmacia y Alimentos de la Universidad de La Habana. *Revista Cubana de Educación Superior, 39*. doi:http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0257-43142020000300019&lng=es&tlng=es.

Vargas Cordero, Z. R. (2009). LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA. *Revista Educación*, 155-165.

GLOSARIO DE TÉRMINOS

- **LOEI:** En Ecuador corresponde a la Ley Orgánica de Educación Intercultural

- **Errores de re-encaminamiento:** Se refiere al envío de información mediante un sistema o reda, empleando, accidentalmente, una ruta incorrecta que lleva la información por donde no es debido.

- **CN-Cert:** describe la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, anexado al Centro Nacional de Inteligencia. Su misión es contribuir a la mejora de la ciberseguridad de España, que es el centro nacional de respuesta y alerta.

- **COSO:** Committee of Sponsoring Organizations of the Tradeway Commission, representa una organización compuesta por colectividades privados, se dedica a ofrecer un modelo común de orientación a las entidades sobre aspectos como: ética empresarial, gestión del riesgo empresaria, control interno, entre otros.

- **Secretaría General de Administración Digital (España):** Es el organismo encargado de promover la racionalización de las tecnologías de la información y de la comunicación.

- **Risk, uncertainty and profit:** Es un trabajo que se refiere al análisis de Knight sobre la distinción entre riesgo e incertidumbre, y el rol que presenta cada uno de estos en el cálculo de la toma de decisiones del emprendedor o la empresa.

- **COBIT:** Control Objetives for Information and Related Technology, es un marco de trabajo para el gobierna y gestión de las tecnologías de la información empresariales

ANEXOS

Anexo 1

Las fichas constituyen una ayuda para la captura de datos en cualquier proyecto de análisis y gestión de riesgos, las fichas se deben realizar por cada activo, de acuerdo con su tipo

A2.6. [SW] Aplicaciones (software)

[SW] Aplicaciones (software)	
Código:	**Nombre:**
Descripción:	
Responsable:	
Tipo:	

Dependencias que identifican

- Personas relacionadas con la aplicación: operadores, administradores y desarrolladores

Dependencias de activos inferiores (hijos)	
Activo:	**Grado:**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	

Activo:	Grado
¿Por qué?:	

A2.7. [HW] Equipamiento informático (hardware)

[HW] Equipamiento informático (hardware)	
Código:	**Nombre:**
Descripción:	
Responsable:	
Ubicación:	
Número:	
Tipo:	

Dependencias:

- Personas relacionadas con el equipo: operadores, administradores
- Instalaciones

Dependencias de activos inferiores (hijos)	
Activo:	**Grado:**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	

A2.8. [COM] Redes de comunicaciones

[COM] Redes de comunicaciones	
Código:	**Nombre:**
Descripción:	
Responsable:	
Ubicación:	
Número:	
Tipo:	

Dependencias:

- Personas relacionadas con el equipo: operadores, administradores
- Instalaciones

Dependencias de activos inferiores (hijos)	
Activo:	**Grado:**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	

A2.11. [L] Instalaciones

[COM] Redes de comunicaciones	
Código:	**Nombre:**
Descripción:	
Responsable:	
Ubicación:	
Número:	
Tipo:	

Dependencias:

- Personas relacionadas con la instalación: guardias, encargados de mantenimiento

Dependencias de activos inferiores (hijos)	
Activo:	**Grado:**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	
Activo:	**Grado**
¿Por qué?:	

A2.12. [P] Personal

[P] Personal	
Código:	**Nombre:**

Descripción:
Número:
Tipo:

No se muestran dependencias

Anexo 2

6.3. Protección de las claves criptográficas

Código	Descripción
CK	Manejo de las claves criptográficas
CK.CI	Manejo de contraseñas de cifra de información
CK.DS	Control de contraseñas de firma de información
CK.disc	Manejo de contraseñas para los contenedores criptográficos
CK.com	Manejo de claves de comunicaciones
CK.Cert(509)	Gestión de certificados

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.4. Protección de los servicios

Código	Descripción
SP	Protección de los Servicios
SP.DA	Fortalecimiento de la disponibilidad
SP.inicio	Aprobación y puesta en marcha
SP.PS	Perfiles de seguridad
SP.EXP	Explotación
SP.CM	Cambios: incluyendo mejoras y renuevos
SP.fin	Terminación
SP.web	Defensa de servicios, incluyendo aplicaciones web
SP.mail	Resguardo de e-mail
SP.direc	Fortificación del directorio
SP.dns	Seguridad del servidor de nombres de dominio
SP.TT	Teletrabajo
SP.voip	Referente a Voz sobre IP

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.7. Protección de las comunicaciones

Código	Descripción

PCOMM	Resguardo de las Comunicaciones
PCOMM.begin	Entrada en servicio
PCOMM.SP	Perfil de seguridad
PCOMM.GD	Garantía a la disponibilidad
PCOMM.autc	Autentificación de canal
PCOMM.ID	Guarda de la integridad de aquellos datos intercambiados
PCOMM.CC	Resguardo criptográfico de la confidencialidad de aquellos datos intercambiados
PCOMM.op	Operación
PCOMM.CAM	Cambios incluyendo: actualizaciones y mantenimiento
PCOMM.fin	Terminación
PCOMM.internet	Internet
PCOMM.wifi	Seguridad Wireles
PCOMM.mob	Telefonía móvil
PCOMM.DS	Segregación de las redes en dominios

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.8. Protección en las conexiones entre franjas de confidencia

Código	Descripción

INTER	Puntos de interconexión: conexiones entre franjas de confidencia
INTER.SPP	Sistema de protección perimetral
INTER.BS	Resguardo de equipos de frontera

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.9. Protección de los soportes de información

Código	Descripción
PSI	Resguardo de Soportes de Información
PSI.AD	Aseguramiento de disponibilidad
PSI.PC	Seguridad criptográfica de contenido
PSI.limp	Limpieza de los contenidos
PSI.fin	Destrucción de los soportes

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.10. Protección de los elementos auxiliares

Código	Descripción
AUXE	Elementos Auxiliares
AUXE.AD	Aseguramiento de disponibilidad

AUXE.inst	Establecimiento
AUXE.sum	Suministro de electricidad
AUXE.clim	Climatización
AUXE.wired	Protección de cableado

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.11. Seguridad física – Protección de la infraestructura

Código	Descripción
LA	Resguardo de las Instalaciones
LA.dis	Diseño
LA.defpd	Defensa a profundidad
LA.CAF	Control de accesos físicos
LA.AD	Aseguramiento de disponibilidad
LA.fin	Terminación

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.13. Salvaguardas de tipo organizativo

Orientadas al buen gobierno de la seguridad

Código	Descripción
ORG	Organización

ORG.MR	Gestión de los riesgos
ORG.plans	Planificación de seguridad
ORG.insps	Inspecciones de seguridad

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.14. Continuidad de operaciones

Correctivos para situaciones de desastres

Código	Descripción
CN	Continuidad de negocio
CN.BIA	Análisis del impacto
CN.DRP	Plan de Recuperación de Desastres

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.15. Externalización

Es comprensible empelar servicios de seguridad externos, considerando los siguientes aspectos:

Código	Descripción
ER	Relaciones Externas
ER.N1	Arreglos para el intercambio de información y de software
ER.N2	Acceso externo

ER.N3	Servicios proporcionados por otras organizaciones
E.4	Personal que sea subcontratado

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3

6.16. Adquisición y desarrollo

Código	Descripción
AQD	Adquisición o desarrollo
AQD.Serv	Servicios que comprenden: Adquisición o desarrollo
AQD.AP	Aplicaciones que comprenden: Adquisición o desarrollo
AQD.EQ	Equipos que impliquen: Adquisición o desarrollo
AQD.COMM	Comunicaciones que incluyan: Adquisición o contratación
AQD.SPI	Soportes de Información: Adquisiciones
AQD.PCA	Productos que sean certificados o acreditados

Nota, la tabla representa una adaptación a la observada en el manual de metodologías de MAGERIT versión 3