ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“ANÁLISIS Y GESTIÓN INTEGRAL DE RIESGOS, ORIENTADO A LA SEGURIDAD DE LA INFORMACIÓN Y CONTROL, PARA LA INFRAESTRUCTURA EN DATA CENTERS DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR PÚBLICA EN ECUADOR”

TESIS DE GRADO

Previa a la obtención del Título de:

MAESTRÍA EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. LUIS MIGUEL ANDRADE DEL PEZO

ING. LUIS DANIEL MONTALEZA ORTIZ

Guayaquil – Ecuador

2024

AGRADECIMIENTO

Mi gratitud, está dirigida hacia Dios y a mi familia por su motivación para lograr avanzar en mi formación profesional, al Mgtr. Lenin Eduardo Freire Cobo, por su tutoría en el desarrollo del presente trabajo y por brindarnos la oportunidad de tomar este reto profesional llevándolo a término, y a todas las personas que han hecho posible este nuevo paso.

Ing. Luis Daniel Montaleza Ortiz

AGRADECIMIENTO

Agradezco profundamente al Mgtr. Lenin Eduardo Freire Cobo], por su invaluable orientación y apoyo durante este proceso; a mis profesores y compañeros por sus aportes y críticas constructivas; y a mi familia y mis amigos por su amor, paciencia y constante motivación, sin los cuales este logro no habría sido posible.

Ing. Luis Miguel Andrade del Pezo

DEDICATORIA

Se dedica el presente trabajo a mi familia por su apoyo, a todos los involucrados en el actual proceso formativo, docentes que han brindado su orientación con profesionalismo ético en la adquisición de nuevos conocimientos, afianzando así mi formación y a los futuros estudiantes de la maestría, que el mismo motive a continuar profundizando investigaciones relacionadas.

Ing. Luis Daniel Montaleza Ortiz

DEDICATORIA

Dedico esta tesis a mi familia, cuyo amor y apoyo incondicional han sido mi mayor fortaleza; a mi madre Consuelo del Pezo y a mi padre Miguel Andrade, por enseñarme el valor del esfuerzo y la perseverancia; a Yaritza Suarez por demostrarme que puedo dar más del que estoy acostumbrado; y a mis amigos y mentores, por su constante inspiración y confianza en mis capacidades.

Ing. Luis Miguel Andrade del Pezo

TRIBUNAL DE GRADUACIÓN

Firmado electrónicamente por:
LENIN EDUARDO FREIRE COBO

Mgs. Lenin Eduardo Freire Cobo

TUTOR

Firmado electrónicamente por:
JUAN CARLOS GARCIA PLUA

Mgs. Juan C. García

REVISOR

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesis de Grado nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral.

ING. LUIS MIGUEL ANDRADE DEL PEZO

ING. LUIS DANIEL MONTALEZA ORTIZ

RESUMEN

El presente trabajo procura abordar la importancia de la seguridad de la información en instituciones educativas, centrándose en la necesidad imperante de proteger los datos confidenciales de estudiantes y personal docente en un entorno cada vez más digitalizado y expuesto a riesgos cibernéticos. Destacándose la relevancia de implementar un enfoque integral de seguridad que garantice la confidencialidad, integridad y disponibilidad de la información almacenada en Data Centers, especialmente en el contexto de una Institución de Educación Superior Pública en Ecuador.

La presencia de múltiples vulnerabilidades y debilidades en los sistemas, aumentan la probabilidad de explotación, especialmente para un entorno en constante transformación digital, lo cual ofrece nuevas oportunidades a los atacantes. Por ello se hace hincapié en la gravedad de las consecuencias de los riesgos, clasificando un impacto crítico cuando las repercusiones pueden afectar sustancialmente la integridad, disponibilidad o confidencialidad de la información, así como la amenaza a activos críticos y las consecuencias financieras o legales.

El análisis de riesgos se posiciona como un componente clave para desarrollar estrategias de mitigación y mejores prácticas que garanticen la seguridad de los datos en los Data Centers. Con esta base, se plantean objetivos específicos como realizar un análisis detallado de los riesgos que afectan la

seguridad de la información en estos entornos, así como desarrollar estrategias de mitigación adaptadas a las necesidades y características de la infraestructura informática.

Se hace referencia a normativas y metodologías como la familia de normas ISO 27000, que se centran en la gestión de la seguridad de la información, y se resalta la necesidad de implementar controles de seguridad adecuados, con la finalidad de mejorar la toma de decisiones, afrontar desafíos de seguridad y garantizar la confidencialidad, integridad y disponibilidad de los datos. Destacándose así la importancia de abordar proactivamente los riesgos de seguridad en un contexto donde la protección de la información se vuelve cada vez más crítica.

ÍNDICE GENERAL

ABREVIATURAS

CNT	Corporación Nacional de Telecomunicaciones
ISO	International Organization for Standardization
SGSI	Sistema de Gestión de Seguridad de la Información
TI	Tecnologías de la Información
UPS	Uninterruptable Power Supply

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el actual panorama tecnológico, la seguridad de la información se erige como un pilar fundamental en la protección de los activos digitales de las organizaciones, siendo de especial relevancia en instituciones educativas donde la confidencialidad, integridad y disponibilidad de los datos desempeñan un papel crucial en el desarrollo académico y administrativo. En este contexto, la presente investigación se adentra en el complejo entramado de desafíos y riesgos que enfrentan los Data Centers de instituciones de educación superior pública en Ecuador, con el objetivo primordial de establecer un marco integral para el análisis y la gestión de riesgos orientado a la seguridad de la información.

La creciente digitalización de los procesos educativos y administrativos ha propiciado un escenario propenso a amenazas cibernéticas cada vez más sofisticadas, que ponen en riesgo la estabilidad operativa y la reputación de las instituciones educativas. En este contexto, la adopción de medidas proactivas y la implementación de controles de seguridad efectivos se tornan imperativos para salvaguardar la integridad de los datos sensibles, prevenir accesos no autorizados y garantizar la continuidad de los servicios educativos.

La normativa ISO 27001 y otras metodologías reconocidas en el ámbito de la seguridad de la información se erigen como pilares fundamentales en la gestión de riesgos cibernéticos, proporcionando un marco de referencia sólido para el diseño e implementación de estrategias de seguridad efectivas. Asimismo, la revisión y mejora continua del sistema de gestión de seguridad de la información se postula como un elemento clave para garantizar la eficacia de los controles implementados y mitigar los riesgos asociados a posibles brechas de seguridad.

En este contexto, el presente trabajo propone abordar los desafíos y riesgos específicos que enfrentan los Data Centers de instituciones de educación superior en Ecuador, con el fin de evaluar, mitigar y gestionar eficazmente los riesgos de seguridad de la información. A través de un enfoque detallado, se busca proporcionar a las instituciones educativas una guía práctica para fortalecer sus sistemas de seguridad, mejorar la toma de decisiones y garantizar la protección de los datos en un entorno digital en constante evolución.

Cabe mencionar que la importancia del análisis de riesgo aporta en asegurar la continuidad del negocio y mejorar la atención de la alta gerencia, centrándose en la gestión de la seguridad de la información, resaltando la necesidad de implementar controles adecuados para mejorar la toma de

decisiones, afrontar desafíos de seguridad y garantizar la confidencialidad, integridad y disponibilidad de los datos.

CAPÍTULO I

GENERALIDADES

1.1. Antecedentes

La relevancia de la seguridad de la información en instituciones educativas es un factor fundamental en la actualidad, numerosos estudios académicos han destacado la importancia de la seguridad de la información en el contexto de universidades y centros de educación superior. La creciente digitalización de datos y la necesidad de proteger información confidencial, como registros académicos y datos personales de estudiantes y personal docente, subrayan la urgencia de un enfoque integral de seguridad.

La existencia de incidentes de seguridad ocurridos en instituciones educativas a nivel global, que por confidencialidad no son expuestos, como los experimentados por la institución objeto del presente estudio

a inicios del 2023 que expone clara de la necesidad de medidas más efectivas en materia de seguridad de la información, subrayando la importancia de abordar los riesgos de manera proactiva.

Existen diversas normativas y estándares de seguridad de la información, como el marco NIST Cybersecurity Framework y la familia de normas ISO 27000, que establecen estándares y mejores prácticas para la gestión de la seguridad de la información; las normas ISO 31000, metodologías como MAGERIT, utilizadas en la administración de riesgos de seguridad de la información, COBIT (Control Objetives for Information and Related Technology) enfocado en la gobernanza de TI, incluyendo la seguridad de la información, e ITIL que se centra en la gestión de servicios de TI.

La pandemia del COVID-19 atravesada en 2020 y el nuevo paradigma de Industria 5.0 [1] dan como resultados los nuevos procesos de transformación digital, donde la evolución tecnológica, como la virtualización y la nube, presenta nuevas oportunidades y riesgos ante crecientes amenazas cibernéticas, por lo cual la importancia de la educación y la concienciación en seguridad en el entorno académico es un componente clave para garantizar un cumplimiento efectivo de las políticas de seguridad.

1.2. Descripción del Problema

La gestión de riesgos y la seguridad de la información de los Data Centers son temas de vital importancia y un aspecto crítico para su operación en el actual panorama tecnológico para diversas organizaciones, desde empresas privadas hasta instituciones gubernamentales. Los ataques cibernéticos y la pérdida de datos representan una amenaza significativa, con el potencial de generar consecuencias devastadoras para las organizaciones, tanto en términos de daños financieros, de reputación, y la posible violación a las leyes sobre protección de datos.

El Data Center de una institución de educación superior pública en Ecuador no es la excepción, ya que cuenta con entornos tecnológicos críticos como lo son la infraestructura de TI, capaz de almacenar y procesar grandes volúmenes de datos; información sensible de aproximadamente 50.000 (cincuenta mil) cuentas activas, entre las asociadas al personal administrativo, docente y estudiantil; así como de diversos proyectos de investigación, de acuerdo con el registro del directorio activo. Por lo tanto, garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en estos es esencial.

Siendo el personal de TI relacionado con la administración y soporte del mismo tal como el Director y Analistas de Infraestructura, los Analistas

y Asistentes de Soporte Informático junto con el Director de Seguridad y Control de Sistemas y su personal a cargo, los principales actores responsables, ante eventos debido a software instalado sin control, o de correos maliciosos al cual acceden los usuarios, e incluso intrusiones externas registradas.

Sumado a lo expuesto, el constante crecimiento institucional por la incorporación de nuevos colaboradores en diversas áreas y nuevos estudiantes en cada término académico, que demandan los servicios tecnológicos de la institución ponen en evidencia la necesidad de un enfoque unificado que aborde de manera efectiva las amenazas y vulnerabilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de los datos almacenados en el Data Center de la institución.

Se puede agregar que el desconocimiento de un marco adecuado que aborde de manera integral el análisis y gestión de riesgos para la seguridad de la información en el Data Center de una institución de educación superior pública en Ecuador deriva en dificultades para evaluar y comprender plenamente los riesgos asociados con la confidencialidad, integridad y disponibilidad de los datos almacenados, y que la falta de un enfoque orientado al control de la infraestructura tecnológica limita la capacidad de las organizaciones para tomar decisiones informadas y mejorar la calidad de los servicios brindados.

Cabe destacar que en Ecuador, varias instituciones han experimentado incidentes de seguridad, según informe de ESET, Ecuador lidera la detección de phishing a nivel global con un 8% [2]. Dos casos destacados de ransomware fue el ataque a CNT en 2019 [3], que resultó en acciones legales contra individuos acusados de acceso no autorizado a sistemas informáticos, y al Banco del Pichincha en 2021 [4], [5]. En general, la falta de medidas efectivas de seguridad informática en las instituciones ecuatorianas puede llevar a graves pérdidas de datos, daños a la reputación y para este caso particular afectar negativamente la retención de estudiantes y acreditaciones.

Se considera viable la ejecución del presente trabajo de titulación, al contar con el acceso a la documentación pertinente, así como al espacio de trabajo. Principalmente, debido al apoyo que brindan los directivos responsables del área que forma parte del estudio y la vinculación laboral existente con la misma de quienes lo desarrollan.

1.3. Solución Propuesta

Bajo el contexto expuesto en el planteamiento del problema, es crucial abordar la necesidad de desarrollar una solución que aborde de manera adecuada el análisis y la gestión integral de riesgos, orientándose a la seguridad de la información y el control, con enfoque hacia la

infraestructura en el Data Center de una institución de educación superior pública en Ecuador, buscando generar las bases metodológicas para desarrollo de sistemas de seguridad de la información eficientes y confiables, permitiendo el acceso a una guía estructurada y práctica para evaluar los riesgos, proporcionando estrategias de mitigación efectivas.

Contribuyéndose de esta manera a mejorar la toma de decisiones, de tal manera que se afronten los desafíos y las necesidades de seguridad asociados con la confidencialidad, integridad y disponibilidad de los datos.

Este proyecto de titulación se centrará en la propuesta de un marco integral para el análisis y la gestión de riesgos orientado a la seguridad de la información en el Data Center de una institución de educación superior pública en Ecuador. Generando para el campo de la seguridad informática, un enfoque práctico y efectivo que pueda ser implementado y replicado en un proceso de mejora continua.

Se han escrito diversos artículos que se pueden tomar como perspectivas para la “Propuesta de marco para el análisis y gestión integral de riesgos, orientado a la seguridad de la información y control para la infraestructura en Data Centers de una institución de educación superior pública del Ecuador”, como por ejemplo lo expuesto por

Barrezueta [6], donde define al análisis de riesgo como parte de una Guía de Gestión de Seguridad de la Información, destacándose que algunos beneficios del análisis de riesgo son: “Ampliar las oportunidades del negocio, maximizar el retorno de las inversiones, asegurar la continuidad del negocio”, pero así también que es un gran reto incrementar los niveles de atención de la alta gerencia.

El aporte que nos brinda Almagro [7], indica que actualmente las amenazas de ciberseguridad continúan creciendo y afectan a todas las organizaciones sin importar su rubro o tamaño. Entre los beneficios de la gestión de riesgos de ciberseguridad se resalta que puede utilizarse para generar un nuevo programa de ciberseguridad, pero el reto es la adaptabilidad, adecuarse a diferentes sectores, industria.

Otro artículo destacable es la posición del modelo Magerit [8], destacando beneficios de la gestión de riesgo en cuanto su ejecución, tales como una reducción en el esfuerzo que ponerse a analizar y decidir para cada caso que se presenta en el momento que se presente, y que se logra un nivel homogéneo con otras organizaciones parecidas. El reto más grande está en calificar correctamente los errores humanos de los ataques deliberados

El enfoque que presenta el estudio de Mosquera [9] prestan una exposición únicamente en marco de la normativa ISO, destacando que

puede llegar a niveles satisfactorios con una solución de este tipo para logos entorno a la seguridad de la información.

En consecuencia, el análisis profundo de riesgos es un componente fundamental de esta propuesta de solución, ya que permitirá identificar y evaluar las amenazas y vulnerabilidades específicas a las que se enfrentan los Data Centers. Esto proporcionará una base sólida para el desarrollo de estrategias de mitigación efectivas y la implementación de controles de seguridad adecuados.

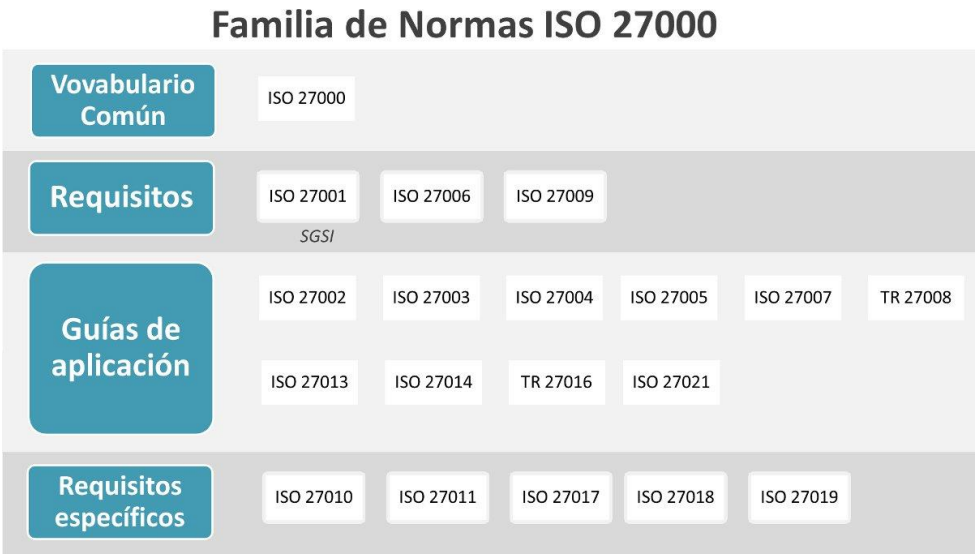

Figura 1.1. ISO 27000 LA FAMILIA DE NORMAS.[10]

Se muestra las distintas normas dentro de esta familia y cómo se interrelacionan para abordar diferentes aspectos de la seguridad de la información.

Fuente: https://normaiso27001.es/wp-content/uploads/2019/01/familia_normas_iso_27000.jpg

Para lograr los objetivos planteados por la propuesta, se utilizará el aporte de diversas normativas y metodologías, enfocándose en el aporte que presenta la familia de normas ISO 27000, que incluye ISO 27001, ISO 27002 y ISO 27005, que se centra en la gestión de la seguridad de la información. ISO 27001 establece requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), mientras que ISO 27002 ofrece buenas prácticas en este ámbito. ISO 27005 aborda la gestión de riesgos de seguridad, por ello, el énfasis del presente trabajo profundizará en la norma ISO 27001.

En términos de convergencias, todas estas normas y marcos comparten un enfoque en la gestión de la seguridad de la información y el reconocimiento de la importancia de la gestión de riesgos en este ámbito. Además, pueden utilizarse de manera complementaria para mejorar la seguridad de la información y la gobernanza de TI.

El aporte hacia la praxis se puede apreciar también como una metodología eficiente y confiable para prevenir y detectar rápidamente cualquier incidencia de seguridad, tomando las medidas que reduzcan su impacto, y llegando a que mediante la automatización de procesos y el monitoreo en tiempo real permita asegurar la continuidad de los servicios brindados, implementándose sistemas de seguridad de la información y control en Data Centers orientados a mejorar la

reputación de la empresa y la confianza de los clientes en la gestión de sus datos.

Al finalizar el análisis podremos incluso escalar a soluciones de automatización y monitoreo en tiempo real que pueden ayudar a detectar y prevenir rápidamente incidentes de seguridad, pero para lo cual es importante contar un marco para su implementación efectiva.

Por lo tanto, se ha justificado que el análisis de riesgos es un componente clave, que permite desarrollar estrategias de mitigación y mejores prácticas para garantizar la confidencialidad, integridad y disponibilidad de los datos almacenados en los Data Centers, por lo cual, cabe destacar que las bases metodológicas que esta investigación provean, contribuirán al desarrollo de sistemas de seguridad de la información y control, en los cuales es esencial garantizar la seguridad de los datos, mejorar la toma de decisiones y la calidad de los servicios brindados.

1.4. Objetivos

1.4.1. Objetivo General

Realizar el análisis y gestión de riesgos orientado a la seguridad de la información en EL Data Center de una Institución de Educación Superior Pública en Ecuador, concentrándose en la

infraestructura de este, con el fin de proporcionar una guía efectiva y práctica para la organización.

1.4.2. Objetivos Específicos

- Realizar un análisis de los riesgos específicos que afectan la seguridad de la información en Data Centers
- Desarrollar estrategias de mitigación de riesgos adaptadas a las necesidades y características de la infraestructura informática del Data Center.
- Establecer un conjunto de mejores prácticas en seguridad de la información específicas según la familia de normas ISO 27000, para entornos tecnológicos críticos como Data Centers.

1.5. Metodología

En cuanto a la metodología, el alcance del estudio es de carácter descriptivo, y se realizará un enfoque no experimental de tipo transversal. Este enfoque implica que se recopilarán datos en un momento específico para analizar la situación actual en la institución de educación superior pública en Ecuador en relación con la seguridad de la información en su Data Center. No se realizará un seguimiento longitudinal a lo largo del tiempo.

Para el perfil de los informantes o sujetos de estudio, se trabajará con informantes en el campo de seguridad de la información y que estén familiarizados con la infraestructura del Data Center de la institución. Además, se recopilará información de documentación técnica y registros relacionados con la seguridad de la información y la gestión de riesgos en el Data Center. Se utilizará una muestra representativa de estos, pero la cantidad exacta dependerá de la disponibilidad y la accesibilidad de la que dispongan, esperando contar con la participación mínima de 8 personas.

El tipo de muestreo que se usará es el de conveniencia, debido al contexto y la naturaleza del proyecto. El muestreo por conveniencia implica seleccionar sujetos o informantes basándose en su disponibilidad y accesibilidad. Esto incluye la colaboración del personal de TI, tal como administración y soporte del Data Center, entre el que el Director y Analistas de Infraestructura, los Analistas y Asistentes de Soporte Informático junto con el Director de Seguridad y Control de Sistemas y su personal a cargo, son identificados como los profesionales familiarizados con la infraestructura y los procesos de seguridad de la información en la institución.

Los instrumentos pertinentes que se utilizarán son cuestionarios estructurados y entrevistas semiestructuradas con 20 a 25 preguntas, como herramienta para recopilación de datos de los informantes. Los

cuestionarios contendrán preguntas relacionadas con la seguridad de la información y la gestión de riesgos en el Data Center, así como su percepción sobre los mismos, aplicadas a personal involucrado de manera general en la operatividad diaria del Data Center; mientras que en las entrevistas que se realizarán a los informantes identificados como los profesionales familiarizados con la infraestructura y los procesos de seguridad de la información, se utilizarán de 10 a 15 preguntas orientadas a obtener información más detallada y contextual sobre procedimientos y metodologías asociadas a la seguridad de la información y gestión de riesgos que se practiquen en el Data Center y que puedan o no estar documentadas.

De manera tentativa, se realizará un análisis cuantitativo de los datos recopilados a través de los cuestionarios, utilizando técnicas para identificar patrones y tendencias en los datos. También se realizará un análisis cualitativo de las entrevistas para obtener información más detallada y contexto sobre las prácticas de seguridad y los riesgos.

Se espera que los resultados proporcionen un panorama completo de la situación actual de la infraestructura del Data Center, ayudando a comprender de manera profunda de los riesgos y desafíos específicos que enfrenta la institución en relación con la seguridad de la información en su Data Center, además de permitir identificar claramente las áreas de mejora y permitan proponer recomendaciones específicas para

abordar los riesgos identificados para la elaboración del marco integral de análisis y gestión de riesgos.

En base a los resultados de la información analizada se procede a identificar y valorar las amenazas, vulnerabilidades para la formulación del marco conceptual ajustado a la visión completa del estado actual del Data Center en términos de seguridad de la información, identificando desafíos y áreas de mejora con el objetivo de establecer un diseño preliminar de marco integral que aborde el análisis y la gestión de riesgos, con enfoque práctico y específico donde con la exploración de las necesidades y características de la infraestructura del Data Center se abordan las normas ISO y su comparativa pertinente para exponer como resultado en el marco metodológico adaptado como “Propuesta de marco para el análisis y gestión integral de riesgos, orientado a la seguridad de la información y control para la infraestructura en Data Centers de una institución de educación superior pública del Ecuador”.

CAPÍTULO II

MARCO TEÓRICO

2.1. Seguridad de la información.

La norma ISO 27001 representa un estándar internacional reconocido que establece directrices para la gestión de la seguridad de la información dentro de las organizaciones. Dicho estándar ofrece un marco de referencia para el establecimiento de Sistemas de Gestión de Seguridad de la Información (SGSI) y aborda las fases de planificación, implementación, supervisión y control de un SGSI. Asimismo, pone un énfasis especial en la evaluación de riesgos y en la formulación de estrategias para mitigarlos

2.1.1. Definición y objetivo de la seguridad de la información.

La seguridad de la información, como se define en la norma ISO 27001 [11], se refiere a la protección de la confidencialidad, integridad y disponibilidad de la información. Su objetivo principal es garantizar que la información crítica de una organización esté segura contra amenazas y riesgos. Esta seguridad no solo se refiere a los datos digitales, sino que abarca todos los aspectos de la información, incluyendo los documentos en papel, la comunicación verbal y la información transmitida electrónicamente. El propósito de la seguridad de la información es preservar la confidencialidad de los datos, asegurar su integridad y garantizar su disponibilidad cuando sea necesario, y así proteger la información de amenazas y vulnerabilidades para garantizar su confidencialidad, integridad y disponibilidad. Esto se logra mediante la implementación de políticas, procedimientos y medidas tecnológicas. La norma ISO 27001, titulada "Sistemas de Gestión de Seguridad de la Información - Requisitos" [11], proporciona un marco sólido para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información (SGSI).

2.1.2. Pilares para la seguridad de la información.

Con el propósito de que la seguridad de la información logre efectivamente el proceso de proteger y asegurar los datos de amenazas y vulnerabilidades, ésta se fundamenta en tres pilares esenciales: [12]

- **Confidencialidad:** Este pilar se enfoca en garantizar que la información solo sea accesible para aquellos que tengan autorización para acceder a ella. Implica la implementación de políticas de acceso, cifrado y control de la información para evitar su divulgación no autorizada, salvaguardando así el derecho de los individuos y organizaciones a controlar quién tiene acceso a su información.
- **Integridad:** La integridad se refiere a la precisión y confiabilidad de la información. Asegurándose de que los datos no sean alterados de manera no autorizada durante su procesamiento o almacenamiento. El uso de firmas digitales y registros de auditoría son ejemplos de medidas para garantizar la integridad de la información. Obteniéndose así la seguridad de que la información es exacta y completa
- **Disponibilidad:** Garantizar la disponibilidad significa que la información esté accesible cuando sea necesario. Esto

implica la implementación de estrategias de copia de seguridad, recuperación ante desastres y redundancia para evitar interrupciones en el acceso a la información.

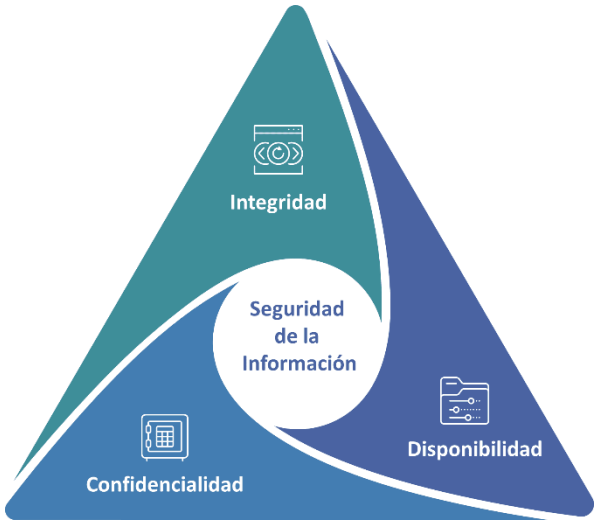

Figura 2.1. PILARES DE LA SEGURIDAD DE LA INFORMACIÓN.

Se expone cada pilar siendo igualmente importante y complementario a los demás para construir una sólida estrategia de seguridad de la información.

Fuente: https://blogger.googleusercontent.com/img/b/R29vZ2xl/AVvXsEg-yJeNaODkmFSTsfHrz9sLaUjynkIDMjchobLHIy54rD7_-SG9q5vA6nQEQrT_BQ5TBNOCMOoVKWrOCg5HqxQ2N7JWztDzxeL0Ib1CzkBhjKwaNS9zhcjbbcoP58375oYjnFAI1nWglFrj/s1731/CID.png

Estos pilares permiten dirigir el despliegue de estrategias entorno a:

- **Seguridad física:** Medidas para proteger la información de daños físicos, como incendios, inundaciones o desastres naturales.
- **Seguridad lógica:** Medidas para proteger la información de accesos no autorizados, como intrusiones informáticas o malware.
- **Gestión de riesgos:** Proceso para identificar, evaluar y mitigar los riesgos de seguridad de la información.

2.1.3. Beneficios y retos de la seguridad de la información.

Algunos de los beneficios de la seguridad de la información incluyen: [13]

- **Protección de la privacidad:** Garantizar que la información personal se mantiene confidencial y segura.
- **Protección de la propiedad intelectual:** Garantizar que la información comercial sensible se mantiene segura.
- **Protección del negocio:** Evitar interrupciones del negocio causadas por ataques informáticos o pérdida de datos.

En consecuencia, la implementación efectiva de la seguridad de la información conlleva varios beneficios, como la protección de la reputación de una organización, la reducción de riesgos y

financieros legales, y el cumplimiento de las regulaciones de privacidad de datos. Además, mejora la confianza de los clientes y socios comerciales.

Sin embargo, también presenta retos, como el costo asociado a la implementación de seguridad, la complejidad de mantenerse al día con las amenazas emergentes y la necesidad de equilibrar la seguridad con la accesibilidad de la información, detallándose: [14]

- **La complejidad de los sistemas informáticos:** Los sistemas informáticos modernos son cada vez más complejos, lo que dificulta su protección.
- **La rápida evolución de las amenazas:** Las amenazas de seguridad de la información evolucionan constantemente, lo que dificulta su detección y prevención.
- **La falta de concienciación:** La falta de concienciación sobre la seguridad de la información puede provocar que los empleados cometan errores que puedan comprometer la seguridad.

2.2. Data centers.

2.2.1. Definición y objetivo de los data centers.

Un Data Center se configura como una instalación que centraliza la infraestructura y operaciones de Tecnologías de la Información (TI) albergando servidores, sistemas de almacenamiento, equipos de red y otros componentes críticos de TI para respaldar las operaciones tecnológicas de una organización. Su objetivo principal es proporcionar un entorno seguro y confiable para el procesamiento, y almacenamiento de datos y aplicaciones. [15]

Los Data Centers son fundamentales para la infraestructura de TI de organizaciones, ya que permiten la disponibilidad constante de servicios en línea, respaldan la gestión de datos y aplicaciones críticas, y facilitan la recuperación ante desastres, por lo cual y desempeñan un papel esencial en la continuidad de las operaciones diarias de una organización.

2.2.2. Componentes y evolución de los data centers.

Los Data Centers comprenden componentes como servidores, estaciones de trabajo, sistemas de almacenamiento como los discos duros y las cintas magnéticas de respaldo físico, redes que proporciona la conectividad entre los sistemas informáticos y el

almacenamiento, sistemas de enfriamiento, sistemas de energía ininterrumpida (UPS), sistemas de seguridad, y sistemas de gestión. [15]

Los data centers han evolucionado a lo largo del tiempo para adaptarse a las necesidades cambiantes de las organizaciones, robusteciendo su infraestructura para almacenar más datos y a utilizar aplicaciones más complejas. Cabe destacar que evolución ha estado marcada por avances tecnológicos, como la virtualización, la computación en la nube y la automatización.

La virtualización, por ejemplo, permite la consolidación de servidores y la optimización del uso de recursos. La computación en la nube ha llevado a la creación de Centros de Datos en la nube, ofreciendo flexibilidad y escalabilidad. La automatización agiliza la administración y la respuesta a la demanda de servicios de TI.

En la actualidad, los data centers se pueden alojar en las instalaciones de las organizaciones o en centros de datos externos que ofrecen una serie de ventajas, como escalabilidad, disponibilidad y seguridad.

2.2.3. Beneficios y limitaciones de los data centers.

Los Data Centers ofrecen beneficios significativos, como eficiencia en el uso de recursos, alta disponibilidad al estar diseñados para

garantizar que la información y los sistemas informáticos estén accesibles cuando se necesitan, escalabilidad para adaptarse a las necesidades cambiantes de las organizaciones y seguridad ya que están protegidos por medios físicos y lógicos que permitan proteger los sistemas informáticos y la información, entre ellos mediante respaldos. [16]

Sin embargo, también tienen limitaciones, como costos de construcción, mantenimiento y operación, la alta demanda de energía y desafíos de impacto ambiental, como la gestión del calor.

CAPÍTULO III

ANÁLISIS DE RIESGO

3.1. Identificación de riesgos.

La identificación de riesgos en el contexto del presente estudio es esencial para comprender las posibles amenazas y vulnerabilidades que podrían comprometer la seguridad de la información. Este proceso se realizará mediante un enfoque estructurado que abarque la identificación de activos de información, vulnerabilidades y amenazas.

3.2. Identificación de activos de información.

En esta fase, se llevará a cabo el análisis para identificar los activos de información críticos presentes en un Data Center. Esto incluirá servidores, redes, y cualquier otro componente relevante para la operación y seguridad de la infraestructura.

Con el objetivo de preservar la confidencialidad pertinente sobre la infraestructura, y por la sensibilidad de la información que esta representa, se expone la composición genérica en materia de activos de información con los que se cuenta, para de esta manera encapsular su anonimidad.

Tabla 1: Descripción de activos.

Activo	Descripción
Desktops	Compuesta por hardware como la CPU, la memoria RAM y el almacenamiento, junto con un sistema operativo, para suplir las necesidades tanto del personal técnico.
Portátiles	Compuesta por hardware como la CPU, la memoria RAM y el almacenamiento, junto con un sistema operativo, para suplir las necesidades tanto del personal técnico. Normalmente usadas para reuniones o trabajo remoto del personal.
Servidores	Están diseñados para ofrecer rendimiento, disponibilidad y capacidad de almacenamiento robustos, cumpliendo un papel fundamental en la infraestructura de redes.
Balanceadores	Son dispositivos diseñados para distribuir equitativamente la carga de tráfico entre varios

	servidores, optimizando así el rendimiento y la disponibilidad de los recursos.
Centrales de aire	Para distribuir el aire acondicionado en todo el edificio, en especial en el área de los servidores.
UPS	Dispositivo eléctrico diseñado para proporcionar energía continua a equipos electrónicos en caso de cortes de energía o fluctuaciones en la corriente eléctrica.
Generador	Los generadores de voltaje son esenciales para la generación de electricidad en diversas aplicaciones en este caso por si hay alguna falla eléctrica pude proveer de energía por un lapso de tiempo para completar alguna tarea o por otro lado dejar todo bien apagado para prevenir futuros daños.
Biométrico	Sirve para poder tener un orden de entrada/salida de la jornada laboral por parte del personal.
Firewall	Su objetivo principal es proteger una red privada o un sistema informático al actuar como una barrera entre este y redes no confiables, como Internet.

Tabla para descripción de activos standard en un Data Center de Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

3.3. Identificación de vulnerabilidades.

Se procederá a listar las posibles vulnerabilidades a las que podría estar expuesta la infraestructura del Data Center. Esto considerando aspectos como la seguridad física de los equipos, parámetros lógicos, la configuración de los sistemas, y la protección contra amenazas cibernéticas.

Tabla 2: Vulnerabilidades físicas.

Categoría	Vulnerabilidad
Acceso no autorizado	Puertas desprotegidas.
	Sistemas de control de acceso débiles.
	Cámaras de vigilancia insuficientes o mal configuradas.
	Falta de seguridad en la recepción de visitantes.
	Falta de sistemas de detección de intrusos físicos
Protección contra desastres	Falta de Sistemas de extinción de incendios.
	Infraestructura eléctrica vulnerable a cortocircuitos.
	Falta de detección temprana de fugas de agua.
	Ausencia de planes de evacuación.
Energía y climatización	Sistemas de energía inestables.
	Fallos en la climatización y Sistemas de refrigeración.
	Sobrecargas eléctricas.
	Falta de generadores de respaldo.

Hardware y equipos	Robo o vandalismo de hardware.
	Fallos en componentes críticos.
	Ausencia de Sistemas de monitorización de hardware.
Equipamiento con fallas o averías	Fallas o averías en los equipos Desktop.
	Fallas o averías en los discos duros
	Fallas o averías en los servidores.

Tabla de vulnerabilidades físicas comunes en un Data Center de Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 3: Vulnerabilidades lógicas.

Categoría	**Vulnerabilidad**
Autenticación y Autorización	Contraseñas débiles o predeterminadas.
	Insuficiente gestión de usuarios.
	Fallos en la implementación de políticas de acceso.
Configuración del Sistema	Configuraciones por defecto no modificadas.
	Configuraciones incorrectas de cortafuegos.
	Falta de actualizaciones y parches de seguridad.
	Malas Configuraciones de permisos.
	Falta de cifrado de datos sensibles

Monitoreo y Auditoría	Falta de Sistemas de monitorización de eventos.
	Registros de auditoría insuficientes o mal gestionados.
	Ausencia de alertas tempranas.
Gestión de Riesgos	Falta de procesos formales de gestión de riesgos.
	Ausencia de evaluaciones de impacto de riesgos.
	Deficiencias en la identificación y clasificación de activos.
	Falta de planes de contingencia y recuperación ante desastres

Tabla de vulnerabilidades físicas comunes en un Data Center de Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 4: Vulnerabilidades cibernéticas.

Categoría	**Vulnerabilidad**
Malware y Virus	Falta de Sistemas de detección y prevención de malware.
	Descuidos en la actualización de bases de datos antivirus.
	Uso de dispositivos USB no verificados.
Ataques de Red	Vulnerabilidades en la configuración de la red.
	Falta de detección de intrusiones.

	Insuficiente segmentación de red.
	Acceso a la red del Data Center sin autorización.
	Falta de monitoreo de actividad de red
Phishing y Ingeniería Social	Falta de concienciación y formación en seguridad.
	Ausencia de filtros efectivos de correo electrónico.
	Políticas débiles de manejo de contraseñas.
Ataques de Denegación de Servicio (DDoS)	Insuficientes medidas de mitigación contra ataques DDoS.
	Falta de redundancia en servicios críticos.
	Ausencia de Sistemas de detección temprana de DDoS.

Tabla de vulnerabilidades cibernéticas comunes en un Data Center de Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

3.4. Identificación de amenazas.

Se analizarán las posibles amenazas que podrían afectar la seguridad de la información en el Data Center. Esto incluirá amenazas externas

como ciberataques, intrusiones, y desastres naturales, así como amenazas internas como errores humanos o mal uso de privilegios.

Tabla 5. Amenazas físicas.

Tipo	Descripción
Desastres naturales	Tormenta eléctrica, terremoto, derrumbes, lluvias torrenciales
Robo de utensilios de acceso	Credenciales o llaves al acceso al departamento.
Fallas mecánicas	Fallos con los equipos de infraestructura como PC, server, UPS, etc.
Maquinas externas infectadas con malware que se conecten	Podrían dar el control remoto a la misma

Tabla de amenazas físicas comunes para el Data Center de una Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 6. Amenazas lógicas.

Tipo	Descripción
Usuarios que distribuyen su de claves de acceso	Claves fáciles de detectar o tener la misma clave para varios sistemas y

	estas son entregadas para acceder a ellos sin control ni responsabilidad
Actividades no controladas sobre los sistemas de vigilancia	Ya sea por motivos técnicos, pueden producir mal funcionamiento o manipulación intencionada.
Falta de apoyo para la comunicación sobre formas de riesgos	No contar con manual o forma de capacitar al personal

Tabla de amenazas lógicas comunes para el Data Center de una Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 7. Amenazas cibernéticas.

Tipo	Descripción
Ataques sobre puertos abiertos	Tener puertos de fácil acceso para el atacante
Ataques sobre firewall mal configurado	Da puerta a que cualquier atacante entre sin tener un arma de defensa
Ataques cibernéticos en constante evolución	Archivos de nuevas formas para generar equipos infectados, phishing o DoS

Pendrives maliciosos	Llenos de malware o en el peor de los casos un keygen de accesos
Aprovechamiento de brechas por mal funcionamiento del balanceador	El tráfico en la red hará percibir la lentitud en los llamados a dicha dirección, que un atacante puede aprovechar para una denegación de servicios

Tabla de amenazas cibernéticas comunes para el Data Center de una Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

3.5. Definición del mapa de calor.

Una vez identificados los activos, vulnerabilidades y amenazas, se procederá a crear un mapa de calor que represente la probabilidad e impacto de cada riesgo identificado. Este mapa permitirá visualizar de manera clara los riesgos críticos que requieren una atención prioritaria. Para ello se dispone de las escalas explicadas a continuación, justificándose que para la categorización del máximo nivel de probabilidad se toman en cuenta la presencia de múltiples vulnerabilidades o debilidades significativas en sistemas relacionados con el riesgo, lo cual aumenta la probabilidad de explotación, así como los actuales cambios en el entorno externo, como avances tecnológicos

o normativos, presentes en los actuales momentos de transformación digital también pueden incrementar la probabilidad al ofrecer nuevas oportunidades para los atacantes:

La gravedad de las consecuencias se basa en diversos criterios. Un impacto crítico, calificado con nivel 5, se asigna cuando las repercusiones de la materialización del riesgo pueden afectar sustancialmente la integridad, disponibilidad o confidencialidad de la información. La amenaza a activos críticos, como sistemas fundamentales o datos altamente sensibles, también justifica un impacto máximo. Las consecuencias financieras, capaces de causar pérdidas significativas o dañar irreparablemente la reputación organizacional, se consideran para la valoración como críticas. Asimismo, el riesgo de incumplimiento legal o normativo, con posibles sanciones, se asocia con un alto impacto. La amplitud del impacto, especialmente cuando afecta a múltiples áreas de la organización y diversos interesados, respalda la asignación de un nivel máximo en la evaluación del impacto del riesgo.

Tabla 8. Tabla de probabilidad.

Probabilidad	Descripción
1 (Bajo)	Ocurrencia altamente improbable, evento raro.

2 (Moderadamente Bajo)	Baja probabilidad, pero no descartable.
3 (Moderado)	Probabilidad significativa, ocurrencia común.
4 (Moderadamente Alto)	Alta probabilidad, probable en condiciones normales.
5 (Alto)	Altamente probable, ocurrencia frecuente.

Tabla de nivel de probabilidad para los riesgos, asociado con escala de color para cada nivel.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 9. Tabla de impacto

Impacto	Descripción
1 (Bajo)	Mínimo impacto, consecuencias insignificantes.
2 (Moderadamente Bajo)	Impacto leve, consecuencias manejables.
3 (Moderado)	Impacto significativo, afecta eficiencia.
4 (Moderadamente Alto)	Impacto sustancial, requiere medidas significativas.
5 (Alto)	Impacto crítico, consecuencias graves.

Tabla de nivel de impacto para los riesgos, asociado con escala de color para cada nivel.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 10. Mapa de Calor.

Tabla mapa de calor, para identificar de manera cuantitativa la probabilidad de ocurrencia e impacto de materialización de un riesgo, asociado con escala de color para cada nivel.

		Impacto				
		Bajo (1)	Moderadamente Bajo (2)	Moderado (3)	Moderadamente Alto (4)	Alto (5)
Probabilidad	Bajo (1)	1	2	3	4	5
	Moderadamente Bajo (2)	2	4	6	8	10
	Moderado (3)	3	6	9	12	15
	Moderadamente Alto (4)	4	8	12	16	20
	Alto (5)	5	10	15	20	25

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Tabla 11. Valoración del riesgo.

NIVEL RIESGO	CALIFICACIÓN
Alto	**15 a 25**
Moderadamente Alto	**9 a 12**
Moderado	**5 a 8**
Moderadamente Bajo	**3 a 4**
Bajo	**1 a 2**

Tabla para valoración del riesgo, asocia de manera cualitativa sesgos cuantitativos identificados en la Tabla 10. Mapa de calor, y asigna franjas de color para cada nivel.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

3.6. Asignación a los riesgos del impacto y la probabilidad.

El riesgo puede entenderse como como el resultado de relacionar la amenaza de un evento, y la vulnerabilidad de los elementos expuestos, para este caso activos de información. La visualización clara de cómo las amenazas y las vulnerabilidades afectan a la seguridad de los activos de una organización, puede ayudar a identificar y priorizar las medidas de protección adecuadas para mitigar el riesgo.

Figura 3.1. Relación entre amenaza, vulnerabilidad, activos y riesgo.

Fuente: https://www.civittas.com/wp-content/uploads/2020/10/Componentes-del-riesgo-en-seguridad-1.jpg

Cada riesgo identificado será evaluado en términos de su impacto potencial y su probabilidad de ocurrencia. Se utilizará una escala predefinida para asignar valores a estos dos factores, permitiendo una cuantificación objetiva de los riesgos. Esta evaluación ayudará a priorizar los riesgos y enfocar los esfuerzos en aquellos que representan mayores amenazas.

Tabla 12. Cuantificación de riesgos

Activo	cat. vulnerabilidad	Vulnerabilidad	Amenaza	Riesgo	Probabilidad (1-5)	Impacto (1-5)	Probabilidad x Impacto
Desktops	Hardware y equipos	Robo o vandalismo de hardware.	Robo de utensilios de acceso	Falta de sistemas de detección de intrusos físicos	4	4	v

		Ausencia de Sistemas de monitorización de hardware	Aprovechamiento de brechas por mal funcionamiento	Falta de implementación de sistemas de inventarios de equipos	4	4	16
		Fallas o averías en los equipos	Fallas mecánicas	Fallas en los equipos físicos de las desktops	3	4	12
		Fallas o averías en los discos duros					
	Configuración del Sistema	Falta de actualizaciones y parches de seguridad.	Ataques sobre puertos abiertos	Dejar una brecha de seguridad que puede ser aprovechada por una atacante	4	4	16
	Malware y Virus	Falta de Sistemas de detección y prevención de malware.	Aprovechamiento de brechas por mal funcionamiento	Podría infectarse dando acceso total a toda la máquina ya si poder acceder a toda la institución	4	5	20
		Descuidos en la actualización de bases de datos antivirus.	Aprovechamiento de brechas por mal funcionamiento	Descuidos en la actualización de bases de datos antivirus	3	4	12
		Uso de dispositivos USB no verificados.	Pendrives maliciosos	Dar camino libre a troyanos y otros malware que podrían estar en las páginas u archivos a trabajar.	4	5	20

		Ausencia de filtros efectivos de correo electrónico	Ataques sobre firewall mal configurado	Poder estar revisando correos spam que podría estar infectado de cualquier tipo.	3	4	12
Portátiles	Hardware y equipos	Robo o vandalismo de hardware.	Robo de utensilios de acceso	Falta de sistemas de detección de intrusos físicos o robo en los exteriores de la institución	4	4	16
		Fallas o averías en los equipos	Fallas mecánicas	Fallos al tratar de guardar y leer información	3	4	12
		Fallas o averías en los discos duros					
		Ausencia de Sistemas de monitorización de hardware	Aprovechamiento de brechas por mal funcionamiento	Deficiencias en la identificación y clasificación de activos	3	3	9
	Configuración del Sistema	Falta de actualizaciones y parches de seguridad.	Aprovechamiento de brechas por mal funcionamiento	Dejar quizás desactualizadas con parches que ayudan a la seguridad del quipo.	4	4	16
	Malware y Virus	Falta de Sistemas de detección y prevención de malware.	Aprovechamiento de brechas por mal funcionamiento	Poder estar revisando correos spam que podría	4	5	20

				estar infectado de cualquier tipo.			
		Descuidos en la actualización de bases de datos antivirus.		Descuidos en la actualización de bases de datos antivirus	3	4	12
		Uso de dispositivos USB no verificados.	Pendrives maliciosos	Falta de Sistemas de detección y prevención de malware	4	5	20
		Ausencia de filtros efectivos de correo electrónico	Ataques sobre firewall mal configurado	Poder estar revisando correos spam que podría estar infectado de cualquier tipo.	3	4	12
Servidores	Acceso no autorizado	Puertas desprotegidas.	Actividades no controladas sobre los sistemas de vigilancia	Falta de seguridad en la recepción de visitantes	3	4	12
	Protección contra desastres	Infraestructura eléctrica vulnerable a cortocircuitos.	Fallas mecánicas	Daño a los equipos o mucho peor perdida por la falta de equipos prendidos o equipos dañados.	3	4	12
	Hardware y equipos	Robo o vandalismo de hardware.	Robo de utensilios de acceso	Falta de detección de intrusiones	3	3	9

		Fallas o averías en los equipos Fallas o averías en los discos duros	Fallas mecánicas	Fallas en los equipos físicos de los servidores	3	4	12
		Ausencia de Sistemas de monitorización de hardware	Aprovechamiento de brechas por mal funcionamiento	Deficiencias en la identificación y clasificación de activos	3	3	9
	Autenticación y Autorización	Contraseñas débiles o predeterminadas.	Usuarios que distribuyen su de claves de acceso	Fácil de vulnerar debido a las claves débiles o predeterminadas	4	4	16
		Insuficiente gestión de usuarios.	Robo de utensilios de acceso	podría caer en un ataque de ingeniería social.	3	3	9
		Fallos en la implementación de políticas de acceso.	Actividades no controladas sobre los sistemas de vigilancia	Entidades físicas como cibernéticas accederían sin permiso por falta de políticas de acceso.	3	4	12
	Configuración del Sistema	Falta de actualizaciones y parches de seguridad.	Ataques sobre puertos abiertos	Brechas de seguridad no parchadas y tener versiones de sistemas muy depreciadas se podría aprovechar	4	4	16

				para atacar las vulnerabilidades de esa versión.			
		Malas Configuraciones de permisos		Malas Configuraciones de permisos	3	3	9
		Falta de cifrado de datos sensibles		Datos como claves o datos sensibles podrían ser utilizados de mala forma.	4	5	20
	Monitoreo y Auditoría	Falta de Sistemas de monitorización de eventos.	Actividades no controladas sobre los sistemas de vigilancia	Falta de procesos formales de gestión de riesgos	4	4	16
		Registros de auditoría insuficientes o mal gestionados.					
	Gestión de Riesgos	Deficiencias en la identificación y clasificación de activos.	Falta de apoyo para la comunicación sobre formas de riesgos	Tener a la vistas datos que son muy sensibles o que en la institución sean muy confidenciales	3	3	9
		Falta de procesos formales de gestión de riesgos.		No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16

		Ausencia de evaluaciones de impacto de riesgos.		No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12
	Malware y Virus	Falta de Sistemas de detección y prevención de malware.	Ataques sobre puertos abiertos	Fácil acceso a intrusos desde algún archivo o página infectada	4	5	20
		Uso de dispositivos USB no verificados.	Pendrives maliciosos	Falta de Sistemas de detección y prevención de malware	4	5	20
		Ausencia de Sistemas de detección temprana de DDoS.	Ataques de Denegación de servicios				
	Ataques de Red	Vulnerabilidades en la configuración de la red.	Ataques sobre puertos abiertos	Insuficiente segmentación de red	3	4	12
		Falta de monitoreo de actividad de red		Propenso a ciberataques de todo tipo a la falta de monitoreos a la red	3	4	12
Balanceadores	Protección contra desastres	Infraestructura eléctrica vulnerable a cortocircuitos.	Fallas mecánicas	Se perderá la fluides del contenido debido a que no hay un buen manejo de la carga	3	4	12
	Autenticación y Autorización	Contraseñas débiles o predeterminadas.	Usuarios que distribuyen su de claves de acceso	Fácil de vulnerar debido a las	4	4	16

				claves débiles o predeterminadas			
		Fallos en la implementación de políticas de acceso.		Entidades físicas como cibernéticas accederían sin permiso por falta de políticas de acceso.	3	4	12
	Configuración del Sistema	Falta de actualizaciones y parches de seguridad.	Aprovechamiento de brechas por mal funcionamiento	Brechas de seguridad no parchadas y tener versiones de sistemas muy depreciadas se podría aprovechar para atacar las vulnerabilidades de esa versión.	4	4	16
		Falta de cifrado de datos sensibles	Usuarios que distribuyen su de claves de acceso	Datos como claves o datos sensibles podrían ser utilizados de mala forma.	4	5	20
		Malas Configuraciones de permisos		Malas Configuraciones de permisos	3	3	9

	Monitoreo y Auditoría	Falta de Sistemas de monitorización de eventos.	Falta de apoyo para la comunicación sobre formas de riesgos	Falta de procesos formales de gestión de riesgos	4	4	16
		Registros de auditoría insuficientes o mal gestionados.					
	Ataques de Red	Insuficiente segmentación de red.	Ataques sobre puertos abiertos	No tener una buena cobertura entre cada segmento de la red	3	4	12
		Falta de monitoreo de actividad de red		Propenso a ciberataques de todo tipo a la falta e monitoreos a la red	3	4	12
Centrales de aire	Acceso no autorizado	Puertas desprotegidas.	Actividades no controladas sobre los sistemas de vigilancia	Falta de seguridad en la recepción de personas no autorizadas para el acceso al área determinado	3	4	12
		Falta de seguridad en la recepción de visitantes.					
	Protección contra desastres	Falta de Sistemas de extinción de incendios.	Desastres naturales	Estar propenso a un incendio sin las debidas precauciones	2	5	10
UPS	Acceso no autorizado	Puertas desprotegidas.	Actividades no controladas sobre los sistemas de vigilancia	Falta de seguridad en la recepción de visitantes	3	4	12

	Protección contra desastres	Falta de Sistemas de extinción de incendios.	Desastres naturales	Estar propenso a un incendio sin las debidas precauciones	2	5	10
		Infraestructura eléctrica vulnerable a cortocircuitos.	Fallas mecánicas	Se perderá la fluides del contenido debido a que no hay un buen manejo de la carga	3	4	12
	Energía y climatización	Sistemas de energía inestables.	Fallas mecánicas	provocar daños en los equipos a largo plazo	3	4	12
		Falta de generadores de respaldo.					
		Sobrecargas eléctricas.	Desastres naturales	Provocar daños a los equipos directamente a sus integrados	3	3	9
	Gestión de Riesgos	Deficiencias en la identificación y clasificación de activos.	Falta de apoyo para la comunicación sobre formas de riesgos	Tener a la vistas datos que son muy sensibles o que en la institución sean muy confidenciales	3	3	9
		Falta de procesos formales de gestión de riesgos.		No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16

		Ausencia de evaluaciones de impacto de riesgos.		No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12
Generador	Acceso no autorizado	Puertas desprotegidas.	Aprovechamiento de brechas por mal funcionamiento	Falta de seguridad en la recepción de visitantes	3	4	12
	Protección contra desastres	Falta de Sistemas de extinción de incendios.	Desastres naturales	Estar propenso a un incendio sin las debidas precauciones	2	5	10
		Falta de Sistemas de extinción de incendios.	Fallas mecánicas	Estar propenso a un incendio sin las debidas precauciones	3	4	12
	Energía y climatización	Sistemas de energía inestables.	Fallas mecánicas	Provocar daños a equipos a largo plazo	3	4	12
		Sobrecargas eléctricas.		Ausencia de evaluaciones de impacto de riesgos	3	4	12
		Falta de generadores de respaldo.		Provocar daños a equipos a largo plazo	3	4	12
	Gestión de Riesgos	Deficiencias en la identificación y clasificación de activos.	Fallas mecánicas	Tener a la vistas datos que son muy sensibles o que en la institución	3	3	9

				sean muy confidenciales			
		Falta de procesos formales de gestión de riesgos.	Falta de apoyo para la comunicación sobre formas de riesgos	No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16
		Ausencia de evaluaciones de impacto de riesgos.		No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12
Biométrico	Acceso no autorizado	Cámaras de vigilancia insuficientes o mal configuradas	Actividades no controladas sobre los sistemas de vigilancia	Falta de seguridad en la recepción de visitantes	3	4	12
		Falta de seguridad en la recepción de visitantes.					
	Gestión de Riesgos	Deficiencias en la identificación y clasificación de activos.	Falta de apoyo para la comunicación sobre formas de riesgos	Tener a la vistas datos que son muy sensibles o que en la institución sean muy confidenciales	3	3	9
		Falta de procesos formales de gestión de riesgos.		No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16

		Ausencia de evaluaciones de impacto de riesgos.		No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12
Firewall	Hardware y equipos	Robo o vandalismo de hardware.	Robo de utensilios de acceso	Falta de sistemas de detección de intrusos físicos	4	4	16
		Fallas o averías en los equipos	Fallas mecánicas	Fallas en los dispositivos físicos	3	4	12
		Fallas o averías en los discos duros					
		Ausencia de Sistemas de monitorización de hardware	Aprovechamiento de brechas por mal funcionamiento	Deficiencias en la identificación y clasificación de activos	3	3	9
	Autenticación y Autorización	Contraseñas débiles o predeterminadas.	Usuarios que distribuyen su de claves de acceso	Fácil de vulnerar debido a las claves débiles o predeterminadas	4	4	16
		Insuficiente gestión de usuarios.		podría caer en un ataque de ingeniería social.	4	4	16
		Fallos en la implementación de políticas de acceso.		Entidades físicas como cibernéticas accederían sin permiso por falta de políticas de acceso.	3	4	12

	Configuración del Sistema	Falta de actualizaciones y parches de seguridad.	Ataques sobre puertos abiertos	Brechas de seguridad no parchadas y tener versiones de sistemas muy depreciadas se podría aprovechar para atacar las vulnerabilidades de esa versión.	4	4	16
		Malas Configuraciones de permisos		Datos como claves o datos sensibles podrían ser utilizados de mala forma.	3	3	9
		Falta de cifrado de datos sensibles		Malas Configuraciones de permisos	4	5	20
	Malware y Virus	Falta de Sistemas de detección y prevención de malware.	Aprovechamiento de brechas por mal funcionamiento	Fácil acceso a intrusos desde algún archivo o página infectada	4	5	20
		Descuidos en la actualización de bases de datos antivirus.		Descuidos en la actualización de bases de datos antivirus	3	4	12
		Ausencia de filtros efectivos de correo electrónico	Aprovechamiento de brechas por mal funcionamiento	Poder estar revisando correos spam que podría estar infectado	3	3	9

				de cualquier tipo.			
		Ausencia de Sistemas de detección temprana de DDoS.		Insuficientes medidas de mitigación contra ataques DDoS	3	5	15
	Ataques de Red	Vulnerabilidades en la configuración de la red.	Ataques cibernéticos en constante evolución	Insuficiente segmentación de red	4	4	16
		Falta de detección de intrusiones.		Provocar una brecha para que puedan intervenir al servidor	3	4	12
		Insuficiente segmentación de red.		No tener una buena cobertura entre cada segmento de la red	3	4	12
		Falta de monitoreo de actividad de red		Propenso a ciberataques de todo tipo a la falta y monitoreos a la red	3	4	12

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

CAPÍTULO IV

TRATAMIENTO DE RIESGO

4.1 Priorización de riesgos.

Con base en la evaluación de impacto y probabilidad, se procederá a la priorización de los riesgos identificados. Se dará mayor atención a aquellos riesgos que presenten mayores niveles de impacto y probabilidad, estableciendo así una jerarquía para la implementación de medidas de mitigación.

Para una gestión eficiente del tratamiento de riesgos se puede mitigar, aceptar, transferir o evitar el mismo, estas estrategias se seleccionan en función de la evaluación de riesgos, los objetivos y tolerancias al riesgo de la organización. La combinación de estas estrategias en un enfoque integral puede ayudar a las organizaciones a gestionar de manera efectiva la incertidumbre y proteger sus activos y objetivos.

Tabla 13. Estrategias para la gestión de riesgos

Estrategia	Descripción
Mitigar el riesgo	Mitigar implica tomar acciones para reducir la probabilidad de que ocurra un riesgo o disminuir su impacto en caso de que ocurra.
Aceptar el riesgo	Aceptar el riesgo significa reconocer conscientemente la existencia del riesgo y decidir no tomar medidas adicionales para mitigarlo. Esto puede deberse a que el costo de mitigación es demasiado alto o la probabilidad es baja.
Transferir el riesgo	Transferir el riesgo implica trasladar la responsabilidad del riesgo a otra entidad, generalmente a través de contratos, seguros u otros acuerdos.
Evitar el riesgo	Evitar el riesgo implica tomar medidas para eliminar la posibilidad de que ocurra el evento de riesgo.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

Bajo el contexto expuesto, se catalogan riesgos aceptables aquellos con una valoración inferior o igual a 2 y se reordenan de la siguiente manera:

Tabla 14. Valoración del impacto de los riesgos.

Riesgo	Probabilidad (1-5)	Impacto (1-5)	Probabilidad x Impacto
Falta de cifrado de datos sensibles	4	5	20
Falta de Sistemas de detección y prevención de malware	4	5	20
Acceso a la red del Data Center sin autorización	4	5	20
Falta de sistemas de detección de intrusos físicos	4	4	16
Contraseñas débiles o predeterminadas	4	4	16
Falta de actualizaciones y parches de seguridad	4	4	16
Falta de procesos formales de gestión de riesgos	4	4	16
Vulnerabilidades en la configuración de la red	4	4	16
Falta de concienciación y formación en seguridad	4	4	16

Políticas débiles de manejo de contraseñas	4	4	16
Insuficientes medidas de mitigación contra ataques DDoS	3	5	15
Falta de seguridad en la recepción de visitantes	3	4	12
Infraestructura eléctrica vulnerable a cortocircuitos	3	4	12
Sistemas de energía inestables	3	4	12
Falta de generadores de respaldo	3	4	12
Fallas en los discos duros	3	4	12
Fallos en la implementación de políticas de acceso	3	4	12
Configuraciones incorrectas de cortafuegos	3	4	12
Registros de auditoría insuficientes o mal gestionados	3	4	12
Ausencia de evaluaciones de impacto de riesgos	3	4	12
Descuidos en la actualización de bases de datos antivirus	3	4	12

Insuficiente segmentación de red	3	4	12
Falta de monitoreo de actividad de red	3	4	12
Falta de redundancia en servicios críticos	3	4	12
Falta de Sistemas de extinción de incendios	2	5	10
Sobrecargas eléctricas	3	3	9
Fallas en los equipos Desktop	3	3	9
Insuficiente gestión de usuarios	3	3	9
Malas Configuraciones de permisos	3	3	9
Deficiencias en la identificación y clasificación de activos	3	3	9
Falta de detección de intrusiones	3	3	9
Ausencia de filtros efectivos de correo electrónico	3	3	9

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

4.2 Asignación de controles de seguridad a los riesgos.

Cada riesgo, de acuerdo a su prioridad, será asociado a controles de seguridad específicos tipificados en la norma ISO 27002, estos

controles podrían incluir medidas físicas, tecnológicas, y procedimientos operativos diseñados como actividades sugeridas, con el objetivo de reducir la probabilidad de ocurrencia o mitigar el impacto en caso de que se materialice el riesgo.

Dada la importancia de los activos sobre los cuales se podrían materializar los riesgos, existe mayor viabilidad para reducir la probabilidad de ocurrencia de los riesgos, por ellos las actividades sugeridas derivadas de los controles pertinentes se plantarían con ese enfoque.

4.3 Plan de tratamiento de riesgos.

Con la asignación de controles, se desarrollará un plan de tratamiento de riesgos detallado. Este plan incluirá la descripción de cada riesgo, los controles asociados, actividades sugeridas y el riesgo residual El objetivo es garantizar que la implementación de medidas de mitigación sea efectiva y sostenible a lo largo del tiempo.

Tabla 15. Tabla de tratamiento de riesgos

Riesgo	Probabilidad (1-5)	Impacto (1-5)	Probabilidad x Impacto	Control	Actividad Sugerida	P	I	Riesgo Residual
Falta de sistemas de detección de intrusos físicos	4	4	v	7.2 Entrada física, 7.3 Seguridad	Implementación de sistema de videovigilancia y alarmas	2	4	8

				de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física	que monitoreen 24/7 las oficinas y datacenter			
Falta de implementación de sistemas de inventarios de equipos	4	4	16	8.1 Dispositivos de punto final de usuario	Realizar evaluaciones regulares de vulnerabilidades en todos los sistemas. Utilizar herramientas automatizadas para escaneos de seguridad.	2	4	8
Fallas en los equipos físicos de las desktops	3	4	12	7.13 Mantenimiento de equipos	Implementar herramientas de monitoreo para evaluar la salud y el rendimiento de los discos duros. Configurar alertas para notificar a los administradores sobre posibles problemas antes de que ocurran fallas críticas.	1	4	4
Dejar una brecha de seguridad que puede ser aprovechada por una atacante	4	4	16	8.1 Dispositivos de punto final de usuario	Realizar evaluaciones regulares de vulnerabilidades en todos los sistemas. Utilizar herramientas automatizadas para escaneos de seguridad.	2	4	8
Podría infectarse dando acceso total a toda la máquina ya si poder	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante	2	5	10

acceder a toda la institución					de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.			
Descuidos en la actualización de bases de datos antivirus	3	4	12	8.1 Dispositivos de punto final de usuario	Desarrollar políticas claras y detalladas que establezcan la frecuencia y los procedimientos para la actualización de bases de datos antivirus. Asegurarse de que estas políticas estén alineadas con las mejores prácticas y las recomendaciones del proveedor de antivirus.	1	4	4
Dar camino libre a troyanos y otros malware que podrían estar en las páginas u archivos a trabajar.	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.		5	5
Poder estar revisando correos spam que podría estar infectado de cualquier tipo.	3	4	12	8.9 Gestión de la configuración	Configurar firewalls siguiendo el principio de menor privilegio, permitiendo únicamente el tráfico necesario para el funcionamiento de las aplicaciones y servicios.	1	4	4

					Regularmente revisar y ajustar las reglas del firewall según las necesidades actuales.			
Falta de sistemas de detección de intrusos físicos o robo en los exteriores de la institución	4	4	16	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física, 7.9 Seguridad de los activos fuera de las instalaciones	Implementación de sistema de videovigilancia y alarmas que monitoreen 24/7 las oficinas y datacenter. No dejar el equipo y los medios de almacenamiento retirados de las instalaciones desatendidos en público y sin seguridad.	2	4	8
Fallos al tratar de guardar y leer informacion	3	4	12	7.13 Mantenimiento de equipos	Implementar herramientas de monitoreo para evaluar la salud y el rendimiento de los discos duros. Configurar alertas para notificar a los administradores sobre posibles problemas antes de que ocurran fallas críticas.	1	4	4
Deficiencias en la identificación y clasificación de activos	3	3	9	7.14 Eliminación segura o	Involucrar a los responsables de los diferentes departamentos y áreas de la	1	3	3

				reutilización de equipos	organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.			
Dejar quizás desactualizadas con parches que ayudan a la seguridad del quipo.	4	4	16	5.9 Inventario de información y otros activos asociados	Realizar evaluaciones regulares de vulnerabilidades en todos los sistemas. Utilizar herramientas automatizadas para escaneos de seguridad.	2	4	8
Poder estar revisando correos spam que podría estar infectado de cualquier tipo.	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.	2	5	10
Descuidos en la actualización de bases de datos antivirus	3	4	12	8.1 Dispositivos de punto final de usuario	Desarrollar políticas claras y detalladas que establezcan la frecuencia y los procedimientos para la actualización de bases de datos antivirus. Asegurarse de que estas políticas estén alineadas con las mejores prácticas	1	4	4

					y las recomendaciones del proveedor de antivirus.			
Falta de Sistemas de detección y prevención de malware	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.	2	5	10
Poder estar revisando correos spam que podría estar infectado de cualquier tipo.	3	4	12	8.9 Gestión de la configuración	Configurar firewalls siguiendo el principio de menor privilegio, permitiendo únicamente el tráfico necesario para el funcionamiento de las aplicaciones y servicios. Regularmente revisar y ajustar las reglas del firewall según las necesidades actuales.	1	4	4
Falta de seguridad en la recepción de visitantes	3	4	12	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física	Monitoreo y control de la atención a visitantes por medios físicos y digitales (personal en recepción y monitoreo por cámara)	1	4	4

Daño a los equipos o mucho peor perdida por la falta de equipos prendidos o equipos dañados.	3	4	12	7.8 Ubicación y protección del equipo	Utilizar dispositivos de protección contra sobretensiones para prevenir daños a equipos electrónicos sensibles. Instalar supresores de sobretensiones en puntos clave de la infraestructura eléctrica.	1	4	4
Falta de detección de intrusiones	3	3	9	7.4 Supervisión de la seguridad física, 8.15 Registro, 8.16 Actividades de seguimiento, 8.21 Seguridad de los servicios de red	Configurar los sistemas de detección de intrusiones de manera personalizada para adaptarse a las características específicas de la red y los sistemas de la organización. Ajustar las reglas y las firmas para mejorar la precisión de la detección.	1	3	3
Fallas en los equipos físicos de los servidores	3	4	12	7.13 Mantenimiento de equipos	Implementar herramientas de monitoreo para evaluar la salud y el rendimiento de los discos duros. Configurar alertas para notificar a los administradores sobre posibles problemas antes de que ocurran fallas críticas.	1	4	4

Deficiencias en la identificación y clasificación de activos	3	3	9	7.14 Eliminación segura o reutilización de equipos	Involucrar a los responsables de los diferentes departamentos y áreas de la organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.	1	3	3
Fácil de vulnerar debido a las claves débiles o predeterminadas	4	4	16	8.5 Autenticación segura	Implementar un sistema de gestión de contraseñas que facilite la creación y almacenamiento seguro de contraseñas. Utilizar herramientas que permitan la generación de contraseñas fuertes. Fomentar el uso de autenticación multifactor (MFA) para agregar una capa adicional de seguridad.	2	4	8
podría caer en un ataque de ingeniería social.	3	3	9	8.3 Restricción de acceso a la información	Implementar soluciones de Gestión Centralizada de Identidades (IAM) para administrar de manera eficiente los accesos y privilegios de los usuarios. Utilizar IAM para centralizar la gestión de	1	3	3

					cuentas de usuario y sus respectivos privilegios.			
Entidades físicas como cibernéticos podrían acceder sin ningún permiso debido a las faltas de políticas de acceso.	3	4	12	8.2 Derechos de acceso privilegiado	Revisar y actualizar regularmente las políticas de acceso para asegurar que estén alineadas con los requisitos de seguridad actuales y las necesidades de la organización. Asegurar que las políticas reflejen cambios en la estructura organizativa y en los sistemas de información.	1	4	4
Brechas de seguridad no parchadas y tener versiones de sistemas muy depreciadas se podría aprovechar para atacar las vulnerabilidades de esa versión.	4	4	16	8.1 Dispositivos de punto final de usuario	Realizar evaluaciones regulares de vulnerabilidades en todos los sistemas. Utilizar herramientas automatizadas para escaneos de seguridad.	2	4	8
Malas Configuraciones de permisos	3	3	9	8.9 Gestión de la configuración	Aplicar el principio de menor privilegio, asignando a los usuarios solo los permisos necesarios para realizar sus funciones. Evitar asignar permisos excesivos o innecesarios que puedan aumentar el riesgo de accesos no autorizados.	1	3	3
Datos como claves o datos sensibles podrían	4	5	20	5.17 Información de	Usar algoritmos que sean menos propensos a ser cifrados.	2	5	10

ser utilizados de mala forma.				autenticación, 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales, 8.3 Restricción de acceso a la información, 8.12 Prevención de fuga de datos, 8.24 Uso de criptografía				
Falta de procesos formales de gestión de riesgos	4	4	16	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	Realizar análisis de riesgos para evaluar la probabilidad e impacto de cada riesgo identificado. Utilizar métodos de evaluación de riesgos reconocidos. .	2	4	8
Tener a la vistas datos que son muy sensibles o	3	3	9	7.14 Eliminación	Involucrar a los responsables de los	1	3	3

que en la institución sean muy confidenciales				segura o reutilización de equipos	diferentes departamentos y áreas de la organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.			
No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	Realizar análisis de riesgos para evaluar la probabilidad e impacto de cada riesgo identificado. Utilizar métodos de evaluación de riesgos reconocidos. .	2	4	8
No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la	Realizar un análisis exhaustivo para identificar amenazas potenciales y vulnerabilidades asociadas a los activos críticos. Utilizar información histórica y expertos en	1	4	4

				información, 5.37 Procedimientos operativos documentados	seguridad para comprender los posibles escenarios de riesgo.			
Fácil acceso a intrusos desde algún archivo o página infectada	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.	2	5	10
Falta de Sistemas de detección y prevención de malware	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.	2	5	10
Insuficiente segmentación de red	3	4	12	7.12 Seguridad del cableado	Crear y mantener un mapa detallado de la infraestructura de red de la organización. Identificar puntos de conexión entre segmentos y evaluar la	1	4	4

					necesidad de restricciones adicionales.			
Propenso a ciberataques de todo tipo a la falta y monitoreos a la red	3	4	12	8.8 Gestión de vulnerabilidades técnicas	Seleccionar e implementar herramientas de monitoreo de red que se adapten a las necesidades específicas de la organización. Asegurarse de que las herramientas sean capaces de registrar eventos significativos y proporcionar alertas.	1	4	4
Se perderá la fluides del contenido debido a que no hay un buen manejo de la carga	3	4	12	7.8 Ubicación y protección del equipo	Utilizar dispositivos de protección contra sobretensiones para prevenir daños a equipos electrónicos sensibles. Instalar supresores de sobretensiones en puntos clave de la infraestructura eléctrica.	1	4	4
Fácil de vulnerar debido a las claves débiles o predeterminadas	4	4	16	8.5 Autenticación segura	Implementar un sistema de gestión de contraseñas que facilite la creación y almacenamiento seguro de contraseñas. Utilizar herramientas que permitan la generación de contraseñas fuertes. Fomentar el uso de autenticación multifactor (MFA) para agregar una capa adicional de seguridad.	2	4	8

Entidades físicas como cibernéticos podrían acceder sin ningún permiso debido a las faltas de políticas de acceso.	3	4	12	8.2 Derechos de acceso privilegiado	Revisar y actualizar regularmente las políticas de acceso para asegurar que estén alineadas con los requisitos de seguridad actuales y las necesidades de la organización. Asegurar que las políticas reflejen cambios en la estructura organizativa y en los sistemas de información.	1	4	4
Brechas de seguridad no parchadas y tener versiones de sistemas muy depreciadas se podría aprovechar para atacar las vulnerabilidades de esa versión.	4	4	16	8.1 Dispositivos de punto final de usuario	Realizar evaluaciones regulares de vulnerabilidades en todos los sistemas. Utilizar herramientas automatizadas para escaneos de seguridad.	2	4	8
Datos como claves o datos sensibles podrían ser utilizados de mala forma.	4	5	20	5.17 Información de autenticación, 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales, 8.3 Restricción de acceso a la información,	Usar algoritmos que sean menos propensos a ser cifrados.	2	5	10

				8.12 Prevención de fuga de datos, 8.24 Uso de criptografía				
Malas Configuraciones de permisos	3	3	9	8.9 Gestión de la configuración	Aplicar el principio de menor privilegio, asignando a los usuarios solo los permisos necesarios para realizar sus funciones. Evitar asignar permisos excesivos o innecesarios que puedan aumentar el riesgo de accesos no autorizados.	1	3	3
Falta de procesos formales de gestión de riesgos	4	4	16	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	Realizar análisis de riesgos para evaluar la probabilidad e impacto de cada riesgo identificado. Utilizar métodos de evaluación de riesgos reconocidos. .	2	4	8
No tener una buena cobertura entre cada segmento de la red	3	4	12	7.12 Seguridad del cableado	Crear y mantener un mapa detallado de la infraestructura de red de la organización.	1	4	4

					Identificar puntos de conexión entre segmentos y evaluar la necesidad de restricciones adicionales.			
Propenso a ciberataques de todo tipo a la falta de monitoreos a la red	3	4	12	8.8 Gestión de vulnerabilidades técnicas	Seleccionar e implementar herramientas de monitoreo de red que se adapten a las necesidades específicas de la organización. Asegurarse de que las herramientas sean capaces de registrar eventos significativos y proporcionar alertas.	1	4	4
Falta de seguridad en la recepción de personas no autorizadas para el acceso al área determinado	3	4	12	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física	Monitoreo y control de la atención a visitantes por medios físicos y digitales (personal en recepción y monitoreo por cámara)	1	4	4
Estar propenso a un incendio sin las debidas precauciones	2	5	10	7.11 Utilidades de apoyo	Realizar evaluaciones regulares de riesgos de incendios para identificar cambios en el entorno que puedan afectar la seguridad contra incendios. Actualizar los planes y	1	5	5

					medidas de seguridad según sea necesario.			
Falta de seguridad en la recepción de visitantes	3	4	12	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física	Monitoreo y control de la atención a visitantes por medios físicos y digitales (personal en recepción y monitoreo por cámara)	1	4	4
Estar propenso a un incendio sin las debidas precauciones	2	5	10	7.11 Utilidades de apoyo	Realizar evaluaciones regulares de riesgos de incendios para identificar cambios en el entorno que puedan afectar la seguridad contra incendios. Actualizar los planes y medidas de seguridad según sea necesario.	1	5	5
Se perderá la fluides del contenido debido a que no hay un buen manejo de la carga	3	4	12	7.8 Ubicación y protección del equipo	Utilizar dispositivos de protección contra sobretensiones para prevenir daños a equipos electrónicos sensibles. Instalar supresores de sobretensiones en puntos clave de la infraestructura eléctrica.	1	4	4
provocar daños en los equipos a largo plazo	3	4	12	7.11 Utilidades de apoyo	Contar con sistemas para respaldo de energía eléctrica UPS + banco de	1	4	4

					baterías que brinden soporte hasta por 12 horas y un generador que permita continuidad de las actividades (con reserva de combustible de hasta por 7 días)			
Provocar daños a los equipos directamente a sus integrados	3	3	9	7.8 Ubicación y protección del equipo	Implementar sistemas de alimentación ininterrumpida (UPS) para proporcionar energía temporal durante interrupciones eléctricas. Asegurar que los UPS sean dimensionados adecuadamente para soportar la carga crítica durante el tiempo necesario.	1	3	3
Tener a la vistas datos que son muy sensibles o que en la institución sean muy confidenciales	3	3	9	7.14 Eliminación segura o reutilización de equipos	Involucrar a los responsables de los diferentes departamentos y áreas de la organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.	1	3	3
No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16	5.36 Cumplimiento de políticas,	Realizar análisis de riesgos para evaluar la probabilidad e impacto de cada riesgo	2	4	8

				reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	identificado. Utilizar métodos de evaluación de riesgos reconocidos. .			
No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	Realizar un análisis exhaustivo para identificar amenazas potenciales y vulnerabilidades asociadas a los activos críticos. Utilizar información histórica y expertos en seguridad para comprender los posibles escenarios de riesgo.	1	4	4
Falta de seguridad en la recepción de visitantes	3	4	12	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la	Monitoreo y control de la atención a visitantes por medios físicos y digitales (personal en recepción y monitoreo por cámara)	1	4	4

				seguridad física				
Estar propenso a un incendio sin las debidas precauciones	2	5	10	7.11 Utilidades de apoyo	Realizar evaluaciones regulares de riesgos de incendios para identificar cambios en el entorno que puedan afectar la seguridad contra incendios. Actualizar los planes y medidas de seguridad según sea necesario.	1	5	5
Estar propenso a un incendio sin las debidas precauciones	3	4	12	7.8 Ubicación y protección del equipo	Utilizar dispositivos de protección contra sobretensiones para prevenir daños a equipos electrónicos sensibles. Instalar supresores de sobretensiones en puntos clave de la infraestructura eléctrica.	1	4	4
Provocar daños a equipos a largo plazo	3	4	12	7.11 Utilidades de apoyo	Contar con sistemas para respaldo de energía eléctrica UPS + banco de baterías que brinden soporte hasta por 12 horas y un generador que permita continuidad de las actividades (con reserva de combustible de hasta por 7 días)	1	4	4
Ausencia de evaluaciones de impacto de riesgos	3	4	12	5.36 Cumplimiento de políticas, reglas y estándares	Realizar un análisis exhaustivo para identificar amenazas potenciales y vulnerabilidades asociadas a los activos	1	4	4

				para la seguridad de la información, 5.37 Procedimientos operativos documentados	críticos. Utilizar información histórica y expertos en seguridad para comprender los posibles escenarios de riesgo.			
Provocar daños a equipos a largo plazo	3	4	12	7.11 Utilidades de apoyo	Contar con sistemas para respaldo de energía eléctrica UPS + banco de baterías que brinden soporte hasta por 12 horas y un generador que permita continuidad de las actividades (con reserva de combustible de hasta por 7 días)	1	4	4
Tener a la vistas datos que son muy sensibles o que en la institución sean muy confidenciales	3	3	9	7.14 Eliminación segura o reutilización de equipos	Involucrar a los responsables de los diferentes departamentos y áreas de la organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.	1	3	3
No tener una buena gestión de riesgo para	4	4	16	5.36 Cumplimiento de	Realizar análisis de riesgos para evaluar la probabilidad e impacto	2	4	8

toma de buenas decisiones				políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	de cada riesgo identificado. Utilizar métodos de evaluación de riesgos reconocidos. .			
No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	Realizar un análisis exhaustivo para identificar amenazas potenciales y vulnerabilidades asociadas a los activos críticos. Utilizar información histórica y expertos en seguridad para comprender los posibles escenarios de riesgo.	1	4	4
Falta de seguridad en la recepción de visitantes	3	4	12	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión	Monitoreo y control de la atención a visitantes por medios físicos y digitales (personal en recepción y monitoreo por cámara)	1	4	4

				de la seguridad física				
Tener a la vistas datos que son muy sensibles o que en la institución sean muy confidenciales	3	3	9	7.14 Eliminación segura o reutilización de equipos	Involucrar a los responsables de los diferentes departamentos y áreas de la organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.	1	3	3
No tener una buena gestión de riesgo para toma de buenas decisiones	4	4	16	5.36 Cumplimiento de políticas, reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	Realizar análisis de riesgos para evaluar la probabilidad e impacto de cada riesgo identificado. Utilizar métodos de evaluación de riesgos reconocidos. .	2	4	8
No poder clara lo que está ocurriendo ni en qué sección es el problema	3	4	12	5.36 Cumplimiento de políticas,	Realizar un análisis exhaustivo para identificar amenazas potenciales y	1	4	4

				reglas y estándares para la seguridad de la información, 5.37 Procedimientos operativos documentados	vulnerabilidades asociadas a los activos críticos. Utilizar información histórica y expertos en seguridad para comprender los posibles escenarios de riesgo.			
Falta de sistemas de detección de intrusos físicos	4	4	16	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física	Implementación de sistema de videovigilancia y alarmas que monitoreen 24/7 las oficinas y datacenter	2	4	8
Fallas en los dispositivos físicos	3	4	12	7.13 Mantenimiento de equipos	Implementar herramientas de monitoreo para evaluar la salud y el rendimiento de los discos duros. Configurar alertas para notificar a los administradores sobre posibles problemas antes de que ocurran fallas críticas.	1	4	4
Deficiencias en la identificación y clasificación de activos	3	3	9	7.14 Eliminación segura o	Involucrar a los responsables de los diferentes departamentos	1	3	3

				reutilización de equipos	y áreas de la organización en el proceso de identificación y clasificación de activos. Asegurarse de que los responsables comprendan la importancia de la clasificación para la seguridad de la información.			
Fácil de vulnerar debido a las claves débiles o predeterminadas	4	4	16	8.5 Autenticación segura	Implementar un sistema de gestión de contraseñas que facilite la creación y almacenamiento seguro de contraseñas. Utilizar herramientas que permitan la generación de contraseñas fuertes. Fomentar el uso de autenticación multifactor (MFA) para agregar una capa adicional de seguridad.	2	4	8
podría caer en un ataque de ingeniería social.	4	4	16	7.2 Entrada física, 7.3 Seguridad de oficinas, salas e instalaciones, 7.4 Supervisión de la seguridad física	Implementación de sistema de videovigilancia y alarmas que monitoreen 24/7 las oficinas y datacenter	2	4	8

Entidades físicas como cibernéticos podrían acceder sin ningún permiso debido a las faltas de políticas de acceso.	3	4	12	8.2 Derechos de acceso privilegiado	Revisar y actualizar regularmente las políticas de acceso para asegurar que estén alineadas con los requisitos de seguridad actuales y las necesidades de la organización. Asegurar que las políticas reflejen cambios en la estructura organizativa y en los sistemas de información.	1	4	4
Brechas de seguridad no parchadas y tener versiones de sistemas muy depreciadas se podría aprovechar para atacar las vulnerabilidades de esa versión.	4	4	16	8.1 Dispositivos de punto final de usuario	Realizar evaluaciones regulares de vulnerabilidades en todos los sistemas. Utilizar herramientas automatizadas para escaneos de seguridad.	2	4	8
Datos como claves o datos sensibles podrían ser utilizados de mala forma.	3	3	9	8.9 Gestión de la configuración	Aplicar el principio de menor privilegio, asignando a los usuarios solo los permisos necesarios para realizar sus funciones. Evitar asignar permisos excesivos o innecesarios que puedan aumentar el riesgo de accesos no autorizados.	1	3	3
Malas Configuraciones de permisos	4	5	20	5.17 Información de autenticación, 5.31	Usar algoritmos que sean menos propensos a ser cifrados.	2	5	10

				Requisitos legales, estatutarios, reglamentarios y contractuales, 8.3 Restricción de acceso a la información, 8.12 Prevención de fuga de datos, 8.24 Uso de criptografía				
Fácil acceso a intrusos desde algún archivo o página infectada	4	5	20	8.7 Protección contra malware	Implementar soluciones antivirus y antimalware que cuenten con actualización constante de la base de datos de firmas, capacidad heurística, la detección comportamental, y la capacidad para adaptarse a nuevas amenazas.	2	5	10
Descuidos en la actualización de bases de datos antivirus	3	4	12	8.1 Dispositivos de punto final de usuario	Desarrollar políticas claras y detalladas que establezcan la frecuencia y los procedimientos para la actualización de bases de datos antivirus. Asegurarse de que estas políticas estén alineadas con las mejores prácticas	1	4	4

					y las recomendaciones del proveedor de antivirus.			
Poder estar revisando correos spam que podría estar infectado de cualquier tipo.	3	3	9	5.14 Transferencia de información	Implementar soluciones antispam robustas que utilicen tecnologías avanzadas para identificar y bloquear correos electrónicos no deseados. Configurar los filtros para adaptarse a las necesidades específicas de la organización.	1	3	3
Insuficientes medidas de mitigación contra ataques DDoS	3	5	15	8.7 Protección contra malware	Asegurarse de contar con capacidad de ancho de banda adicional para absorber el tráfico durante un ataque DDoS. Coordinar con proveedores de servicios de Internet para implementar medidas de mitigación a nivel de red.	1	5	5
Insuficiente segmentación de red	4	4	16	8.20 Seguridad de redes	Mantener los dispositivos de red actualizados con los últimos parches de seguridad. Realizar pruebas de parches antes de implementarlos en la producción.	2	4	8
Provocar una brecha para que puedan intervenir al servidor	3	4	12	8.7 Protección contra malware	Crear y mantener un mapa detallado de la infraestructura de red de la organización. Identificar puntos de	1	4	4

					conexión entre segmentos y evaluar la necesidad de restricciones adicionales.			
No tener una buena cobertura entre cada segmento de la red	3	4	12	8.8 Gestión de vulnerabilidades técnicas	Seleccionar e implementar herramientas de monitoreo de red que se adapten a las necesidades específicas de la organización. Asegurarse de que las herramientas sean capaces de registrar eventos significativos y proporcionar alertas.	1	4	4
Propenso a ciberataques de todo tipo a la falta de monitoreos a la red	3	4	12	8.8 Gestión de vulnerabilidades técnicas	Seleccionar e implementar herramientas de monitoreo de red que se adapten a las necesidades específicas de la organización. Asegurarse de que las herramientas sean capaces de registrar eventos significativos y proporcionar alertas.	1	4	4

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza.

CAPÍTULO V

RESULTADOS ESPERADOS

5.1 Análisis del actual funcionamiento del Data Center en función de ISO 27001.

Con la premisa de preservar la confidencialidad pertinente sobre la infraestructura, y por la sensibilidad de la información que esta representa, se derivaron riesgos altamente relevantes que pueden hacerse presentes en diferentes data centers de una institución de educación superior pública en Ecuador; permitiendo con ello mantener la viabilidad del presente trabajo, sin que estos puedan asociarse directamente y en forma única con la institución objeto, preservando su anonimato y previniendo que el presente documento sea utilizado para la vulneración de alguna brecha de seguridad, y en su lugar plasmar

una solución coherente, eficiente y eficaz para el análisis y gestión de riesgos.

Bajo este contexto, Uno de los principales problemas que enfrenta el funcionamiento de un data center es la falta de una evaluación detallada de los riesgos específicos asociados a la infraestructura tecnológica. La norma ISO 27001 establece requisitos específicos para la identificación y evaluación de riesgos, lo que resulta crucial para garantizar la confidencialidad, integridad y disponibilidad de los datos almacenados en el data center. En este sentido, la falta de una evaluación detallada de los riesgos podría comprometer la efectividad de los controles de seguridad implementados y aumentar la exposición a amenazas y vulnerabilidades, por lo cual en base a los capítulos 3 y 4 se extrajo la información expuesta en el siguiente gráfico, sobre la relevancia de los controles de la norma ISO 27001 con mayor impacto sobre la infraestructura.

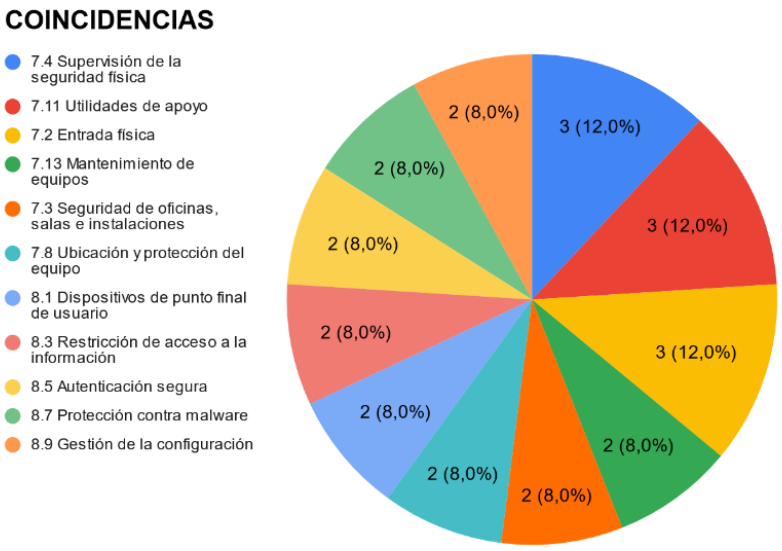

Figura 5.1. Controles con mayores coincidencias.

De acuerdo con los posibles riesgos para la infraestructura del Data Center de una Institución de Educación Superior.

Fuente: Luis Miguel Andrade y Luis Daniel Montaleza

Se aprecia que los controles con mayor impacto son los concernientes son los controles físicos y controles tecnológicos, destacándose aquellos concernientes a la seguridad física, el acceso y las utilidades de apoyo, indicando que el factor prioritario a controlar todo aquello involucrado a preservar el mantener la continuidad del negocio mediante las utilidades de apoyo y el acceso debido a las diferentes instancias del data center, con el objetivo de impedir fuga de información y acceso no autorizado que permita vulnerar la disponibilidad de los servicios, la confidencialidad de la información e incluso integridad de los datos y componentes físicos.

Otro problema que enfrenta el funcionamiento del data center es la falta de una revisión y mejora continua del sistema de gestión de seguridad de la información. La norma ISO 27001 establece requisitos específicos para la revisión y mejora continua del sistema de gestión de seguridad de la información, lo que resulta crucial para garantizar la efectividad de los controles de seguridad implementados y la mitigación de riesgos. La falta de una revisión y mejora continua del sistema de gestión de seguridad de la información podría comprometer la efectividad de los controles de seguridad implementados y aumentar la exposición a amenazas y vulnerabilidades; y si bien no lo expone el grafico 1, si se evidencia en la Tabla 15 Tabla de tratamiento de riesgos.

5.2 Análisis del funcionamiento posterior de la propuesta de controles.

Después de la implementación de los controles sugeridos, se observa una mejora sustancial en el funcionamiento del Centro de Datos en términos de seguridad. Un análisis detallado de la efectividad de cada medida revela reducciones significativas en los riesgos residuales asociados a las amenazas identificadas. A continuación, se presenta un resumen del impacto positivo de la propuesta de controles:

Falta de cifrado de datos sensibles: La adopción de algoritmos más seguros ha contribuido a la reducción del riesgo residual a 10,

proporcionando una capa adicional de seguridad para la confidencialidad de los datos almacenados.

Falta de Sistemas de detección y prevención de malware: La implementación de soluciones antivirus actualizadas ha demostrado ser eficaz, disminuyendo el riesgo residual a 10 y fortaleciendo la protección contra amenazas de malware.

Acceso a la red del Data Center sin autorización: La aplicación de controles como limitar el acceso y utilizar tecnologías de seguridad ha llevado a una disminución del riesgo residual a 10, garantizando una mayor integridad de la red.

Falta de sistemas de detección de intrusos físicos: La instalación de sistemas de videovigilancia y alarmas ha mejorado la seguridad física, reduciendo el riesgo residual a 8 y brindando una mayor capacidad de respuesta ante posibles intrusos.

Contraseñas débiles o deficientes: La implementación de un sistema de gestión de contraseñas y la promoción de la autenticación multifactor han contribuido a reducir el riesgo residual a 8, fortaleciendo la seguridad de las credenciales de usuario.

Falta de actualizaciones y parches de seguridad: La realización de evaluaciones regulares y el uso de herramientas automatizadas para escaneos de seguridad han llevado a una disminución del riesgo residual a 8, garantizando la actualización adecuada de los sistemas.

Falta de procesos formales de gestión de riesgos: La implementación de análisis de riesgos y métodos de evaluación reconocidos ha contribuido a documentar métricas pertinentes y reducir el riesgo residual a 8, mejorando la gestión integral de riesgos.

Vulnerabilidades en la configuración de la red: El mantenimiento regular de dispositivos de red y la realización de pruebas de parches antes de su implementación en producción han resultado en una disminución del riesgo residual a 8, fortaleciendo la seguridad de la red.

Falta de concienciación y formación en seguridad: La implementación de medidas como la segregación de redes y restricciones adicionales ha contribuido a reducir el riesgo residual a 8, mejorando la concienciación y la seguridad en el manejo de la red.

Políticas débiles de manejo de contraseñas: La exigencia de contraseñas fuertes y la aplicación de técnicas de almacenamiento seguro han reducido el riesgo residual a 8, fortaleciendo las políticas de manejo de contraseñas.

En general, el análisis del funcionamiento posterior de la propuesta de controles revelaría mejoras significativas en la seguridad del Data Center, destacando la efectividad de las implementadas y su impacto positivo en la mitigación de riesgos, mediante la adopción de algoritmos de cifrado más seguros, la implementación de soluciones antivirus actualizadas, controles de acceso y tecnologías de seguridad como

medidas para disminuir el riesgo asociado a la confidencialidad de datos sensibles y prevenir amenazas de malware, fortaleciendo la integridad de la red, dada su importancia para la gestión continua y la revisión del sistema de seguridad de la información procurando así mantener la eficacia de los controles en un entorno dinámico.

5.3 Análisis de la diferencia.

En el contexto del análisis diferencial, se examinará la disparidad entre el estado anterior y posterior a la implementación de los controles propuestos en el Centro de Datos de una Institución de Educación Superior. Este análisis se erige como una evaluación crítica, abordando las transformaciones sustantivas en términos de seguridad y gestión de riesgos.

Inicialmente, el escenario precontroles delinea una preocupación fundamental relacionada con la falta de una evaluación minuciosa de los riesgos específicos ligados a la infraestructura tecnológica del Data Center. La ausencia de este escrutinio pormenorizado podría potencialmente socavar la efectividad de los controles de seguridad y exponer la infraestructura a amenazas y vulnerabilidades.

Posteriormente, la fase de implementación de controles, tal como se describe en el tratamiento de riesgos, revelaría mejoras sustanciales en diversas áreas críticas. La adopción de algoritmos de cifrado más

seguros atenúa el riesgo residual asociado a la confidencialidad de datos sensibles. Simultáneamente, la implementación de soluciones antivirus actualizadas, así como la aplicación de controles de acceso y tecnologías de seguridad, contribuyen a la disminución del riesgo en aspectos vinculados a la prevención de malware y la integridad de la red. Estos avances, respaldados por la instauración de mecanismos de gestión continua y revisión del sistema de seguridad de la información, constituyen hitos notables que refuerzan la postura de la institución frente a riesgos potenciales.

Sin embargo, es imperativo subrayar que el análisis posterior no solo resalta las áreas de mejora, sino que también plasma la necesidad constante de una revisión rigurosa y continua. Este énfasis en la mejora continua se alinea con los preceptos de la norma ISO 27001, siendo esencial para mantener la adaptabilidad y eficacia de los controles de seguridad en un entorno dinámico.

El análisis diferencial entre el estado previo y posterior a la implementación de controles en el Data Center de la institución revela una transición positiva hacia una postura más segura y resiliente. No obstante, este análisis resalta la importancia continua de la vigilancia y adaptación, consolidando la seguridad de la infraestructura informática como una empresa en constante evolución y perfeccionamiento.

La implementación de controles en el Data Center genera mejoras sustanciales, reduciendo significativamente los riesgos clave, como la falta de cifrado, vulnerabilidades de red y contraseñas débiles, que tendrían alto impacto sobre la continuidad de los servicios y con ello a la reputación de la institución, ya que brindarían acceso no autorizado a la infraestructura desde una perspectiva lógica. Con esto se enfatiza la importancia de abordar proactivamente los riesgos de seguridad en un contexto donde la protección de la información se vuelve cada vez más crítica.

CONCLUSIONES

1. El análisis de riesgos es un componente clave para desarrollar estrategias de mitigación y mejores prácticas que garanticen la confidencialidad, integridad y disponibilidad de los datos almacenados en los Data Centers, a través de los controles de seguridad pertinentes como elementos clave para ello.

2. La seguridad de la información en los Data Centers es un aspecto crítico que requiere un análisis detallado de los riesgos específicos asociados a la infraestructura tecnológica, tomando en cuenta que el análisis del funcionamiento de los Data Center en relación con ISO 27001 proporciona una visión clara de brechas de seguridad existentes, permitiendo una toma de decisiones informada para la implementación de medidas correctivas.

3. La integración de un marco completo destinado al análisis y gestión de riesgos en los Centros de Datos puede desempeñar un papel crucial en la identificación y formulación de estrategias de mitigación personalizadas según las necesidades y características específicas de la infraestructura informática. En este contexto, la orientación hacia la norma ISO 27001 ha demostrado ser un fundamento robusto para el

análisis y manejo de riesgos en el centro de datos, ofreciendo una guía efectiva y práctica para la organización.

4. La adopción la familia de las normas ISO 27000 puede proporcionar un conjunto de mejores prácticas en seguridad de la información específicas para entornos críticos como los Data Centers, contribuyendo a la mejora de la gestión de riesgos y la seguridad de la información, ya que la implementación de controles basados en la norma ISO 27001 es fundamental para fortalecer la seguridad de la información en estos entornos, identificando áreas de mejora y garantizando un mayor nivel de cumplimiento de estándares internacionales.

RECOMENDACIONES

1. Se recomienda como práctica deseable la orientación hacia el monitoreo y evaluación periódica del cumplimiento de los controles de seguridad implementados, con el fin de adaptarse a los cambios en el entorno de amenazas y tecnológico.

2. Establecer un plan de capacitación continua para el personal del data center, con el objetivo de garantizar la comprensión y adhesión a las prácticas de seguridad de la información basadas en ISO 27001.

3. Se debe considerar la implementación de mecanismos de detección y respuesta automática ante incidentes para fortalecer la postura de seguridad del data center.

4. Realizar auditorías internas regulares para verificar la efectividad de los controles de seguridad y garantizar el cumplimiento continuo de los requisitos de ISO 27001.

5. Explorar la posibilidad de obtener certificaciones de conformidad con la norma ISO 27001, lo que podría mejorar la credibilidad y confianza en la seguridad de la información del data center.

BIBLIOGRAFÍA

[1] E. Commission, D.-G. for Research, Innovation, M. Breque, L. De Nul, y A. Petridis, *Industry 5.0 – Towards a sustainable, human-centric and resilient European industry*. Publications Office of the European Union, 2021. doi: doi/10.2777/308407.

[2] «ESET Security Report 2023: el panorama de la seguridad en las empresas de América Latina». Accedido: 14 de octubre de 2023. [En línea]. Disponible en: https://www.welivesecurity.com/es/informes/eset-security-report-2023-seguridad-empresas-america-latina/

[3] «Fiscalía General del Estado | Ola B. ahora es investigado por presunto acceso no consentido a un sistema informático». Accedido: 14 de octubre de 2023. [En línea]. Disponible en: https://www.fiscalia.gob.ec/ola-b-ahora-es-investigado-por-presunto-acceso-no-consentido-a-un-sistema-informatico/

[4] D. Buendia, «Acciones de la Super de Bancos frente a Ciberataque de entidad controlada», Superintendencia de Bancos. Accedido: 14 de octubre de 2023. [En línea]. Disponible en: https://www.superbancos.gob.ec/bancos/acciones-de-la-super-de-bancos-frente-a-ciberataque-de-entidad-controlada/

[5] «Banco Pichincha sufrió ataque informático que afectó parte de sus servicios». Accedido: 14 de octubre de 2023. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

[6] V. F. Barrezueta Bermeo, «Guía de gestión de seguridad de la información para el Gobierno Provincial de Tungurahua», Master's Thesis, Pontificia Universidad Católica del Ecuador, 2023.

[7] L. ALMAGRO, «MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad», *Internet (https://www. oas. org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP. pdf)*.

[8] M. Amutio Gómez y J. Candau, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información», 2012.

[9] C. Mosquera Riva, «Gestión de riesgo del data center de la PUCESE basada en estándares internacionales», PhD Thesis, Ecuador-PUCESE-Escuela de Sistemas y Computación, 2016.

[10] «ISO 27000 punto por punto - Glosario de términos ISO 27001», Norma ISO 27001. Accedido: 25 de abril de 2024. [En línea]. Disponible en: https://normaiso27001.es/referencias-normativas-iso-27000/

[11] «ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements». Accedido: 5 de noviembre de 2023. [En línea].

Disponible en: https://www.iso.org/obp/ui#iso:std:iso-iec:27001:ed-3:v1:en
[12] O. Ñañez Campos, «Modelo gestión de riesgos para la seguridad de la información, Universidad Nacional Toribio Rodríguez de Mendoza-Chachapoyas», 2021.
[13] M. A. Espinoza, «Importancia de los modelos para el gobierno de la seguridad de la información en las empresas. Una revisión sistemática de la literatura», *Revista ESPACIOS*, vol. 40, n.º 25, jul. 2019, Accedido: 5 de noviembre de 2023. [En línea]. Disponible en: https://www.revistaespacios.com/a19v40n25/19402505.html
[14] E. Samaniego Mena y J. Ponce Ordóñez, *Libro Fundamentos de seguridad informática*. 2021.
[15] L. Molina Tapia, «Data Center Urbano: alternativa de almacenamiento intangible de datos y regeneración urbana», 2023.
[16] A. Wierman, Z. Liu, I. Liu, y H. Mohsenian-Rad, «Opportunities and challenges for data center demand response», en *International Green Computing Conference*, 2014, pp. 1-10. doi: 10.1109/IGCC.2014.7039172.