Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

TÍTULO

Modelamiento de la gestión de riesgos de seguridad de la información de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.

PRESENTADO POR

Bach. Inga Arteaga Carlos Alonso
Bach. Nuñez Bances Guillermo Aldair David

ASESOR

Dr. Celi Arévalo Ernesto Karlo

Lambayeque – Perú

06 de febrero 2026

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

TÍTULO

Modelamiento de la gestión de riesgos de seguridad de la información de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.

PRESENTADO POR

Bach. Inga Arteaga Carlos Alonso
Bach. Nuñez Bances Guillermo Aldair David

ASESOR

Dr. Celi Arévalo Ernesto Karlo

Lambayeque – Perú

2026

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

TÍTULO

Modelamiento de la gestión de riesgos de seguridad de la información de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.

APROBADO POR EL SIGUIENTE JURADO

DR. ING. ROBERT EDGAR PUICAN GUTIERREZ
PRESIDENTE

DRA. ING. MARIA DE LOS ANGELES GUZMAN VALLE
SECRETARIO

MSC. ING. CESAR AUGUSTO GUZMAN VALLE
VOCAL

Universidad Nacional Pedro Ruiz Gallo

Facultad de Ingeniería Civil, de Sistemas y Arquitectura

Escuela Profesional de Ingeniería de Sistemas

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

TÍTULO

Modelamiento de la gestión de riesgos de seguridad de la información de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú.

APROBADO POR EL SIGUIENTE JURADO

DR. ING. ERNESTO KARLO CELI AREVALO
ASESOR

INGA ARTEAGA CARLOS ALONSO
Bach. Ingeniería de sistemas

NUÑEZ BANCES GUILLERMO ALDAIR DAVID
Bach. Ingeniería de sistemas

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO
FACULTAD DE INGENIERÍA CIVIL DE SISTEMAS Y DE ARQUITECTURA
UNIDAD DE INVESTIGACIÓN

ACTA DE SUSTENTACIÓN N°631-2026-UI-FICSA

Siendo las 12:30 pm horas del día 06 de febrero del 2026, se reunieron de manera presencial los miembros de jurado de la tesis titulada: **"MODELAMIENTO DE LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE LOS SERVICIOS ACADÉMICOS EN LA UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO, LAMBAYEQUE, PERÚ" , con código N°IS_V_2025_005,** designado por **Resolución Decanal N° 251-2025-UNPRG-FICSA** con la finalidad de Evaluar y Calificar la sustentación de la tesis antes mencionada, conformado por los siguientes docentes:

DR. ING. ROBERT EDGAR PUICAN GUTIERREZ	**PRESIDENTE**
DRA. ING. MARIA DE LOS ANGELES GUZMAN VALLE	**SECRETARIO**
MSC. ING. CESAR AUGUSTO GUZMAN VALLE	**VOCAL**

Asesorado por **DR. ING. ERNESTO KARLO CELI AREVALO.**

El acto de sustentación fue autorizado por **OFICIO VIRTUAL N° 28-2026-UIFICSA**, la tesis fue presentada y sustentada por los Bachilleres: **CARLOS ALONSO INGA ARTEAGA y GUILLERMO ALDAIR DAVID NUÑEZ BANCES,** tuvo una duración de 85 minutos. Después de la sustentación, y absueltas las preguntas y observaciones de los miembros del jurado; se procedió a la calificación respectiva:

	NUMERO	LETRAS	CALIFICATIVO
CARLOS ALONSO INGA ARTEAGA	18	DIECIOCHO	MUY BUENO
GUILLERMO ALDAIR DAVID NUÑEZ BANCES	18	DIECIOCHO	MUY BUENO

Por lo que quedan **APTOS** para obtener el Título Profesional de **INGENIERO DE SISTEMAS** de acuerdo con la Ley Universitaria 30220 y la normatividad vigente de la Facultad de Ingeniería Civil De Sistemas y de Arquitectura de la Universidad Nacional Pedro Ruiz Gallo.

Siendo las 13:55 Se dio por concluido el presente acto académico, dándose conformidad al presente acto, con la firma de los miembros del jurado.

DR. ING. ROBERT EDGAR PUICAN GUTIERREZ
PRESIDENTE

DRA. ING. MARIA DE LOS ANGELES GUZMAN VALLE
SECRETARIO

MSC. ING. CESAR AUGUSTO GUZMAN VALLE
VOCAL

DR. ING. ERNESTO KARLO CELI AREVALO
ASESOR

JHFF/bcm

CONSTANCIA DE VERIFICACIÓN DE ORIGINALIDAD DE TESIS

Según Resolución N° 268-2025-CU

Yo, ERNESTO KARLO CELI ARÉVALO, asesor de tesis de los bachilleres en Ingeniería de Sistemas: **Carlos Alonso Inga Arteaga y Guillermo Aldair David Nuñez Bance**

TITULADA:

Modelamiento de la gestión de riesgos de seguridad de la información de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú

Luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de **19%** verificable en el reporte de similitud del programa TURNITIN.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas NO CONSTITUYEN PLAGIO. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Se expide la presente según lo dispuesto en la Resolución N° 268-2025-CU - Directiva para la evaluación de originalidad de los documentos académicos y de investigación, de la Universidad Nacional Pedro Ruiz Gallo.

Lambayeque, 11 de noviembre del 2025

Atentamente,

Ing. Ernesto Karlo Celi Arévalo
DNI. 18068078
ASESOR

Se adjunta:
Recibo digital de Turnitin
Revisión de informe en Turnitin

Informe final de tesis

ORIGINALITY REPORT

19%	11%	7%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universidad Privada del Norte Student Paper	11%
2	hdl.handle.net Internet Source	3%
3	repositorio.ucv.edu.pe Internet Source	<1%
4	tesis.usat.edu.pe Internet Source	<1%
5	Guamán Muela, Franklin Vinicio. "Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando la norma ISO/27001 para la protección de datos en la Unidad Educativa La Inmaculada de la ciudad de Ambato.", Universidad Católica de Cuenca (Ecuador) Publication	<1%
6	www.coursehero.com Internet Source	<1%
7	repositorio.untels.edu.pe Internet Source	<1%
8	repositorio.pucesa.edu.ec Internet Source	<1%
9	repositorio.unitec.edu Internet Source	<1%
10	repository.unad.edu.co Internet Source	<1%

Dr. Ernesto Celi Arévalo
ASESOR

Dr. Ing. Ernesto Karlo Celi Arévalo
DNI. 18068078
ASESOR

turnitin

Digital Receipt

This receipt acknowledges that Turnitin received your paper. Below you will find the receipt information regarding your submission.

The first page of your submissions is displayed below.

Submission author:	Inga Carlos & Núñez Guillermo
Assignment title:	Quick Submit
Submission title:	Informe final de tesis
File name:	InformeFinal.docx
File size:	740.95K
Page count:	116
Word count:	38,092
Character count:	214,435
Submission date:	11-Nov-2025 07:49AM (UTC-0500)
Submission ID:	2810917075

Dr. Ernesto Karlo Celi Arévalo

ASESOR

Dr. Ing. Ernesto Karlo Celi Arévalo

DNI. 18068078

ASESOR

RESUMEN

La investigación titulada *"Modelamiento de la gestión de riesgos de seguridad de la información de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú"* abordó la problemática relacionada con la exposición de los activos de información institucional a amenazas y vulnerabilidades, debido a la ausencia de un enfoque sistemático de gestión de riesgos en los procesos académicos. El propósito principal fue desarrollar un modelo de gestión de riesgos de seguridad de la información que integre elementos funcionales y estructurales orientados a fortalecer la protección de los servicios académicos de la Universidad. La propuesta se sustentó en los fundamentos teóricos de la familia de normas ISO/IEC 27000, especialmente la ISO/IEC 27005:2022, complementada con la metodología OCTAVE-S, reconocida por su aplicabilidad en entornos organizacionales de tamaño medio. La investigación fue de tipo aplicada, con un nivel descriptivo–propositivo y un diseño no experimental y longitudinal, trabajándose con la totalidad de la población compuesta por 38 colaboradores de la Dirección de Servicios Académicos y la Oficina de Tecnología de la Información. La información se recopiló mediante entrevistas estructuradas, revisión documental y validación por juicio de expertos. Los resultados permitieron identificar 41 amenazas y 32 vulnerabilidades que afectaban los sistemas académicos SIA y GESTAC, clasificando los riesgos según su probabilidad e impacto. Se determinó que el 37 % de los riesgos se ubicaban en niveles altos o muy altos, evidenciando la necesidad de implementar controles específicos y políticas institucionales de seguridad. La validación del modelo alcanzó un nivel de aceptación promedio del 92 %, destacándose su suficiencia, coherencia y aplicabilidad. En conclusión, el modelo propuesto proporcionó una estructura metodológica eficaz para gestionar los riesgos de seguridad de la información, fortaleciendo la continuidad operativa, la integridad de los datos académicos y la toma de decisiones en la Universidad Nacional Pedro Ruiz Gallo.

Palabras clave: seguridad de la información, gestión de riesgos, ISO/IEC 27005, OCTAVE-S, servicios académicos, modelo de gestión, universidad pública.

ABSTRACT

The research entitled *"Modeling of Information Security Risk Management for Academic Services at Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Peru"* addressed the problem related to the exposure of institutional information assets to threats and vulnerabilities due to the absence of a systematic risk management approach in academic processes. The main purpose was to develop an information security risk management model that integrates functional and structural elements aimed at strengthening the protection of the university's academic services. The proposal was based on the theoretical foundations of the ISO/IEC 27000 family of standards, particularly ISO/IEC 27005:2022, complemented by the OCTAVE-S methodology, recognized for its applicability in medium-sized organizational environments. The study was applied in nature, with a descriptive–propositional level and a non-experimental, longitudinal design, involving the entire population of 38 collaborators from the Academic Services Directorate and the Information Technology Office. Data were collected through structured interviews, document review, and expert judgment validation. The results identified 41 threats and 32 vulnerabilities affecting the academic systems SIA and GESTAC, classifying the risks according to their probability and impact. It was determined that 37% of the risks were at high or very high levels, highlighting the need to implement specific controls and institutional security policies. The validation of the model achieved an average acceptance level of 92%, emphasizing its sufficiency, coherence, and applicability. In conclusion, the proposed model provided an effective methodological structure for managing information security risks, thereby strengthening operational continuity, the integrity of academic data, and decision-making processes at Universidad Nacional Pedro Ruiz Gallo.

Keywords: information security, risk management, ISO/IEC 27005, OCTAVE-S, academic services, management model, public university.

ÍNDICE GENERAL

ÍNDICE DE TÁBLAS

INTRODUCCIÓN

La implementación de tecnologías de la información (TI) se ha convertido en un pilar esencial para las organizaciones, ya que permite optimizar la eficiencia y la eficacia de sus procesos, sean estos principales, de apoyo o de soporte. No obstante, esta adopción tecnológica conlleva una serie de riesgos inherentes que deben gestionarse de manera adecuada para garantizar que la información institucional sea confiable, esté disponible y permanezca íntegra. El contexto global reciente refuerza esta necesidad: el número de ataques que explotan vulnerabilidades ha experimentado un incremento sostenido, con un aumento del 180 % respecto al año anterior (Verizon Business, 2024). Ejemplos como el ataque a la cadena de suministro mediante la vulnerabilidad MOVEit —que produjo un "efecto mariposa" en grandes corporaciones (Cyrebro, 2024; Verizon Business, 2024)— y los incidentes de seguridad de SolarWinds (IT Digital Security, 2021) evidencian la complejidad y el dinamismo de los riesgos cibernéticos. Estas situaciones demuestran que los atacantes solo necesitan explotar una debilidad, mientras que los responsables de la seguridad deben proteger un amplio conjunto de activos de información.

En este escenario, la gestión de riesgos de TI adquiere una relevancia estratégica. El *Data Breach Investigations Report* (DBIR) 2024 de Verizon destaca que las brechas de seguridad se utilizan principalmente con fines de ransomware y extorsión, aprovechando vulnerabilidades en aplicaciones web y la creciente dependencia de la infraestructura digital. Estas brechas, motivadas en su mayoría por razones financieras, registran costos promedio de 46,000 dólares (Junquera, 2024). Asimismo, el 68 % de los incidentes involucra el factor humano, ya sea por uso de credenciales débiles o errores operativos (Junquera, 2024), y un porcentaje similar se relaciona con vulnerabilidades de proveedores de software externos (Verizon Business, 2024). Ante esta realidad, la gestión de la seguridad de la información se consolida como un proceso indispensable que permite planificar, implementar y mantener medidas de protección, siendo la creación de un Sistema de Gestión de la Seguridad de la Información (SGSI) un componente clave para identificar, analizar y mitigar los riesgos hasta niveles tolerables.

A nivel nacional, el Perú ocupa la posición 86 a nivel global y la 12 en América en el Índice Global de Ciberseguridad (GCI) 2022, con un puntaje de 55.67, siendo considerado un país en desarrollo en materia de ciberseguridad (ICEX, 2022; UIT, 2020). Aunque el país muestra avances en el ámbito de las medidas legales, aún existen áreas de mejora en las medidas organizativas y en el desarrollo de capacidades técnicas (ICEX, 2022). El panorama es preocupante: durante 2022 se registraron aproximadamente 15,000 millones de ciberataques en el país, lo que representa un incremento del 35 % respecto al año anterior. El ciberdelito se ha convertido en uno de los riesgos más probables (World Economic Forum, 2023), siendo el ransomware la amenaza más común y perjudicial para sectores estratégicos como la tecnología, la banca y el gobierno (Basic, 2022; Entel Digital, 2024).

La Universidad Nacional Pedro Ruiz Gallo (UNPRG) no es ajena a este contexto. Sus procesos principales —especialmente la gestión de la información académica de los estudiantes, desde el ingreso hasta el egreso— son esenciales para el cumplimiento de su misión institucional. El principal foco de riesgo se identificó en el Sistema de Información Académica (SIA), adquirido en 2021 como parte del proceso de licenciamiento institucional exigido por la SUNEDU. Desde su implementación, el sistema ha experimentado diversos incidentes de seguridad, tales como caídas inesperadas del servicio, bloqueos durante el proceso de matrícula y modificaciones manuales de la base de datos, lo que ha provocado inconsistencias en la información académica, afectando el registro de notas, periodos académicos y el cumplimiento oportuno de actividades administrativas. Esta problemática pone en evidencia la urgencia de adoptar un enfoque sistemático y estructurado para la protección de la información como recurso estratégico institucional. En este contexto, la presente investigación tiene como propósito modelar la gestión de riesgos de seguridad de la información aplicable a los servicios académicos de la UNPRG, con el fin de fortalecer la protección de sus activos informacionales.

El estudio se centró en la Dirección de Servicios Académicos (DSA) y abarcó los procesos gestionados a través de los sistemas GESTAC (empleado hasta 2014) y SIA (actual aplicación web). Estos procesos comprenden el registro y codificación de estudiantes, la matrícula, la gestión de planes de estudio, la convalidación de cursos, la emisión y rectificación de actas, y la generación de constancias y certificados académicos. A través del modelamiento propuesto, se buscó identificar, analizar y evaluar los escenarios de riesgo, así como proponer controles y prácticas de seguridad que mitiguen la exposición y refuercen la resiliencia institucional.

El problema central de la investigación se formuló en los siguientes términos: ***¿Cuáles son los elementos funcionales y estructurales que debe poseer el modelamiento de la gestión de riesgos de seguridad de la información para soportar eficazmente la operación de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú?***

Como objetivo general, se estableció ***"Desarrollar un modelo de gestión de riesgos de seguridad de la información que integre los elementos funcionales y estructurales necesarios para soportar eficazmente la operación de los servicios académicos en la Universidad Nacional Pedro Ruiz Gallo".***

De este se derivaron los siguientes objetivos específicos:

1. Identificar las amenazas a la seguridad de la información en los servicios académicos y evaluar la efectividad del modelamiento propuesto para su identificación.
2. Estimar el nivel de exposición a los riesgos de seguridad de la información y determinar la eficacia del modelamiento propuesto para su estimación.

3. Identificar las prácticas de seguridad y los controles necesarios para mitigar los niveles de exposición a riesgos no aceptables y evaluar la efectividad del modelamiento propuesto para su identificación.
4. Validar el cumplimiento del modelamiento propuesto con las buenas prácticas de los marcos ISO/IEC 31000:2018 y OCTAVE-S, considerando criterios de suficiencia, claridad, coherencia y relevancia.

La investigación se justifica por su pertinencia y relevancia. Es pertinente porque propone una solución que permitirá a los responsables de la seguridad de la información y de los procesos académicos gestionar adecuadamente los escenarios de riesgo, fortaleciendo la prevención y reduciendo la probabilidad de incidentes críticos.

Asimismo, la propuesta contribuye al cumplimiento de las Condiciones Básicas de Calidad (CBC) establecidas en la Resolución del Consejo Directivo N.º 043-2020-SUNEDU/CD, particularmente en su componente 3.4 “Infraestructura tecnológica”, el cual exige que las universidades dispongan de estrategias que respalden sus procesos académicos y administrativos mediante plataformas integradas y seguras, garantizando la confidencialidad, integridad y disponibilidad de la información.

En consecuencia, los resultados de la investigación poseen un aporte práctico, ya que el producto final —el modelo de gestión de riesgos— permitirá identificar amenazas y vulnerabilidades, valorar su impacto y probabilidad de ocurrencia, y proponer controles específicos que mantengan los riesgos dentro de niveles aceptables.

Desde la perspectiva de relevancia teórica, la investigación aporta al conocimiento científico mediante la aplicación combinada de las buenas prácticas de la familia ISO/IEC 27000 y de la metodología OCTAVE, generando un modelo adaptado al entorno universitario peruano. Este modelo no solo refuerza la seguridad de la información institucional, sino que también constituye una herramienta replicable para otras instituciones de educación superior que busquen fortalecer su gestión académica y tecnológica bajo un enfoque de riesgos.

La presente investigación se estructuró en **cinco capítulos**, cada uno orientado a desarrollar los elementos necesarios para alcanzar los objetivos planteados.

- El Capítulo I aborda el planteamiento del problema, donde se expone la realidad problemática, la formulación del problema general y específicos, los objetivos, la justificación y la delimitación del estudio.
- El Capítulo II desarrolla el marco teórico, en el cual se presentan los antecedentes de investigaciones relacionadas, los fundamentos teóricos sobre la gestión de riesgos de

seguridad de la información, las normas ISO/IEC y la metodología OCTAVE-S, así como la definición de los términos básicos que sustentan conceptualmente el trabajo.

- El Capítulo III describe el diseño metodológico, especificando el tipo, nivel y diseño de la investigación, la población y muestra, las técnicas e instrumentos de recolección de datos, y los procedimientos empleados para el análisis de la información y la validación del modelo propuesto.
- El Capítulo IV presenta los resultados obtenidos, los cuales derivan de la aplicación del modelo de gestión de riesgos a los procesos académicos de la Universidad. Se muestran las matrices de identificación, análisis y evaluación de riesgos, así como las estrategias de tratamiento diseñadas en función de los niveles de exposición detectados.
- Finalmente, el Capítulo V expone la discusión de los resultados, las conclusiones y las recomendaciones. En este apartado se interpreta la correspondencia entre los hallazgos del estudio y los antecedentes teóricos, y se formulan propuestas orientadas al fortalecimiento institucional en materia de seguridad de la información.

I. DISEÑO TEÓRICO

1.1. Antecedentes de la investigación

La tesis titulada "Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 27005 para analizar la viabilidad de adoptar servicios en la nube" (Quispe, 2020) abordó la necesidad de conocer los riesgos de seguridad de la información que asume una organización (una universidad privada peruana) al adquirir un nuevo servicio en la nube, para apoyar la decisión de la Alta Dirección. Su propósito fue proponer un modelo de evaluación de riesgos basado en el estándar ISO/IEC 27005 para el proceso de Exámenes Parciales y Finales del área de Registros Académicos. El fundamento teórico principal fue la ISO/IEC 27005 para la gestión de riesgos y la ISO/IEC 27001 como visión general del SGSI. La investigación fue de tipo aplicada y se basó en el despliegue del modelo propuesto a través de tres fases: investigación de buenas prácticas, propuesta del modelo y despliegue. El resultado principal fue el modelo de evaluación de riesgos que permitió analizar la viabilidad de optar por el servicio en la nube para el proceso académico, ayudando a tomar una decisión informada sobre los riesgos.

En "Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo" (Yarleque & Sandoval, 2022), se identificó como problema la ausencia de un marco metodológico estructurado que permitiera una gestión efectiva de los riesgos de seguridad y de TI en el Poder Judicial. El propósito fue diseñar un marco de trabajo que combine las directrices de ISO/IEC 27005 para la gestión de riesgos de seguridad de la información y el marco de gobierno COBIT 2019 para integrar la gestión de riesgos a los objetivos de TI. Los fundamentos teóricos clave fueron los citados estándares, enfocados en la identificación, análisis, evaluación y tratamiento de riesgos. La investigación fue de tipo aplicada, con un enfoque mixto, utilizando el método de diseño. El resultado crucial fue la propuesta de un marco de trabajo que, una vez validado, permite al Poder Judicial realizar una gestión de riesgos más proactiva y alineada con los objetivos organizacionales, un enfoque transferible a cualquier entidad pública como una universidad.

El estudio "Gestión de riesgos de seguridad de información, bajo el estándar ISO/IEC 27005:2022, aplicando ontologías de dominio" (Santos, 2024) se centró en la complejidad del proceso de gestión de riesgos de seguridad de la información en las organizaciones peruanas y la necesidad de estandarizar la terminología y las relaciones entre conceptos. Su objetivo fue proponer un modelo de gestión de riesgos basado en la ISO/IEC 27005:2022 que utilizara ontologías de dominio para mejorar la comprensión y el proceso de gestión. La base teórica fue la gestión de riesgos según la norma ISO/IEC 27005:2022 y los principios de la Ingeniería del Conocimiento para la aplicación de ontologías. Fue una investigación de tipo aplicada, con un diseño no experimental y

enfoque cualitativo. El resultado fue un modelo con ontologías que facilita la aplicación del estándar de gestión de riesgos, estandarizando el proceso y los elementos involucrados, lo cual es útil para la transferencia de conocimiento en servicios académicos.

La investigación "Desarrollo de una metodología AD HOC de gestión de riesgos informáticos basada en ISO 27005 para un hospital regional" (De La Cruz & Paz, 2024) abordó la vulnerabilidad de los principios de seguridad de la información (confidencialidad, integridad y disponibilidad) debido a la ausencia de una metodología formal de gestión de riesgos en el Hospital Regional de Lambayeque. El propósito central fue desarrollar una metodología Ad Hoc basada en la ISO/IEC 27005 que pudiera aplicarse al contexto específico de un hospital para fortalecer su seguridad. Los fundamentos teóricos se basaron en el estándar ISO/IEC 27005 como guía para el proceso de gestión de riesgos y la aplicación de los principios de la Seguridad de la Información. El estudio fue de tipo mixta (cuantitativo-cualitativo), aplicada y con un diseño cuasi-experimental. El principal hallazgo fue la metodología desarrollada, la cual permitió identificar las causas que afectan la vulnerabilidad y proponer un plan de mitigación efectivo, demostrando la eficacia de adaptar estándares a contextos locales.

El artículo "Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte" (Paredes et al., 2019) analizó la dificultad que enfrentan las organizaciones para implementar la gestión de riesgos de seguridad de la información debido a la alta inversión tecnológica y la necesidad de una metodología adaptada. El objetivo fue desarrollar un marco de seguridad GRC (Gobierno, Riesgo y Cumplimiento) y proporcionar una revisión del estado del arte de los modelos de gestión de riesgos. Los fundamentos teóricos se basaron en los marcos de GRC y las metodologías estándar como el ciclo Plan-Do-Check-Act (PDCA), con referencia a normas como ISO/IEC 27001. Fue una investigación de tipo revisión del estado del arte, utilizando el método de análisis y síntesis de literatura científica. La conclusión principal fue el desarrollo de un marco GRC con un ciclo de gestión de riesgos (Plan-Do-Check) que incluye el establecimiento del contexto, identificación y evaluación de riesgos, e implementación de controles.

En "Modelo de Seguridad y Privacidad de la Información 2022-2024" (Universidad Pedagógica y Tecnológica de Colombia, 2022), el problema era la necesidad de asegurar la continuidad de las funciones misionales de la universidad y proteger los activos de información ante riesgos, en un contexto de uso intensivo de TIC. El objetivo general fue implementar las actividades del Plan de Seguridad y Privacidad de la Información (PSPI) alineadas con la norma NTC/IEC ISO 27001:2013 y la estrategia de gobierno digital. La base teórica se centró en la ISO/IEC 27001:2013 para el Sistema de

Administración de la seguridad de la información (SGSI) y el Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno Digital. Este documento se describe como un esfuerzo institucional, de tipo aplicativo y normativo. Uno de los resultados clave fue la formalización de los lineamientos para la gestión de riesgos de seguridad y privacidad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos.

La tesis "Propuesta de un marco de gestión de riesgos de TI basado en ISO 31000:2018 para la Universidad Nacional de Ingeniería" (Apaza & Zúñiga, 2021) abordó la carencia de un marco de gestión de riesgos de TI formal que permitiera mitigar las amenazas que afectan la continuidad de los servicios de TI en la universidad. El propósito fue diseñar e implementar un marco de gestión de riesgos de TI basado en la norma ISO 31000:2018 para un proceso específico de los servicios de TI. El fundamento teórico se basó en la ISO 31000:2018 para la gestión de riesgos y la ISO/IEC 27005 para el enfoque en seguridad de la información. Fue una investigación de tipo aplicada, con enfoque mixto y diseño no experimental. El resultado central fue el marco de gestión de riesgos que, al ser aplicado, permitió identificar, analizar, evaluar y tratar los riesgos en el proceso seleccionado, ofreciendo una estructura sistemática para la toma de decisiones en la gestión de servicios universitarios.

La investigación "Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI Filial Lambayeque" (Niño, 2018) aunque es ligeramente anterior a 2019, su relevancia regional y temática la hace un antecedente útil. El problema era la necesidad de fortalecer los tres pilares de la seguridad de la información y monitorear los activos en la filial Lambayeque del INEI. El objetivo fue proponer un modelo de SGSI para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información. La base teórica fue la norma ISO/IEC 27001 para el diseño del SGSI, enfocándose en la gestión de activos y la evaluación de riesgos. Fue una investigación de tipo aplicada, con un diseño no experimental. El resultado principal fue el modelo SGSI propuesto, que sentó las bases para una gestión de seguridad sistematizada en una entidad pública de Lambayeque, lo cual es relevante para la UNPRG.

En "Modelo de gestión de riesgos de tecnologías de información basado en la ISO/IEC 27005 para el Hospital Privado Juan Pablo II de la ciudad de Chiclayo" (Céspedes, 2020), se abordó la falta de una metodología estructurada para identificar, analizar y evaluar los riesgos de TI que amenazaban la continuidad operativa del hospital. El propósito fue modelar un sistema de gestión de riesgos de TI que se basara en la ISO/IEC 27005 para mejorar la toma de decisiones y la seguridad de la información

hospitalaria. La fundamentación teórica se centró en la metodología de la ISO/IEC 27005 para la gestión de riesgos de seguridad de la información. Fue una investigación de tipo aplicada, con un enfoque cuantitativo y diseño no experimental. El principal resultado fue la propuesta de un modelo de gestión de riesgos que, al ser simulado, permitió mitigar la exposición al riesgo en los procesos críticos de TI, proporcionando un marco de referencia aplicable a procesos de servicios críticos, como los académicos.

El estudio "Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC" (Samaniego, 2024) identificó la necesidad de implementar un plan de mitigación de riesgos para proteger los activos de información y la continuidad del negocio en una distribuidora. Su objetivo fue proponer un plan de mitigación de riesgos de seguridad de la información aplicando la normativa ISO/IEC 27005:2022. Los fundamentos teóricos se centraron en la ISO 27005:2022 para el análisis, formulación y mitigación de riesgos, reconociendo a la información como un activo valioso. Fue una investigación de tipo aplicada, con un enfoque cualitativo. El resultado fue un plan de mitigación de riesgos que, al aplicar la normativa, permitió identificar, evaluar y gestionar los posibles riesgos, demostrando la efectividad de la norma más reciente para la protección de activos de información.

1.2. Estado de arte de la investigación

El análisis de los antecedentes investigativos revela una tendencia marcada en el ámbito de la seguridad de la información dentro de las instituciones de educación superior (IES) y entidades públicas. Los estudios se focalizan consistentemente en la necesidad de implementar Sistemas de Administración de la seguridad de la información (SGSI) y en el modelamiento estructurado de la gestión de riesgos como estrategia preventiva.

La mayoría de las investigaciones abordan el problema de la inseguridad de los activos de información o las vulnerabilidades en los sistemas, proponiendo como solución el diseño e implementación de un SGSI basado en estándares internacionales. El fundamento teórico común es la norma ISO/IEC 27001 (y sus versiones relacionadas, como la ISO/IEC 27002) como marco de referencia principal, ya sea para el diseño de un SGSI o para la identificación y mitigación de controles. Así mismo, existe una tendencia a complementar la gestión de la seguridad con marcos de Gobierno de TI como COBIT e ITIL para asegurar que el SGSI esté alineado con la estrategia organizacional y los procesos de gestión de servicios. Las investigaciones demuestran la aplicabilidad de estos modelos en diversas entidades, incluyendo instituciones de educación superior (IES), hospitales y entidades tributarias o gubernamentales.

En relación al modelamiento y la gestión de riesgos, un subconjunto significativo de los estudios se centra en el modelamiento específico de la gestión de riesgos, reconociendo

que la seguridad de la información es inherentemente una gestión de riesgos. Las investigaciones recurren a metodologías y estándares específicos para la gestión de riesgos, como: OCTAVE, que se utiliza para determinar la relación entre la gestión de riesgos y la seguridad, ofreciendo un marco para estimar el nivel de exposición y proponer controles, Magerit, empleada para complementar la ISO 27001 en la tarea de gestión de riesgos y NIST SP 800-30 y OSSTMMv3, utilizados para diseñar un marco de trabajo de seguridad en el contexto universitario.

Los problemas abordados son variados, desde la necesidad de mejorar el control de accesos y la gestión de identidades digitales, la seguridad en la infraestructura de red y comunicaciones, hasta la minimización de riesgos informáticos en la gestión académica y la protección de activos de información financiera.

Los resultados de estas investigaciones son, en su mayoría, modelos o marcos de trabajo (frameworks) con un alto componente de diseño o propuesta (investigación descriptiva y propositiva). Estos modelos permiten: identificar escenarios de riesgos, amenazas y vulnerabilidades, estimar los niveles de exposición al riesgo, y proponer un conjunto de controles (a menudo del Anexo A de ISO 27001) para mitigar los riesgos no tolerables.

La tendencia metodológica y validaciones predomina el uso de la investigación no experimental y descriptiva, con algunos enfoques correlacionales que buscan determinar el impacto de las metodologías o modelos propuestos. Las propuestas de modelos se validan mediante: Juicio de Expertos/Método Delphi, utilizado para asegurar la confiabilidad, coherencia y pertinencia del modelo propuesto y el análisis de cumplimiento, como evaluación de si el modelo propuesto satisface los requisitos de los estándares y normas de referencia aplicados.

1.3. Bases teóricas

1.3.1. La información como recurso estratégico

La información como recurso estratégico puede definirse como el activo organizacional que, al ser procesado a través de infraestructuras tecnológicas, permite aportar valor y generar conocimientos útiles para la toma de decisiones y el mejoramiento de los procesos (Valles-Coral, 2023). Desde una perspectiva estratégica, este recurso no tangible es fundamental para la supervivencia a largo plazo de una organización, ya que representa la "materia prima" necesaria para obtener una ventaja sobre los competidores en un entorno globalizado e interconectado (Valles-Coral, 2023).

La importancia de la información radica en su capacidad para actuar como un factor determinante en la formulación e implementación de la estrategia empresarial. En el

contexto de los servicios, el buen manejo de la información permite a las organizaciones reducir riesgos al identificar amenazas, clarificar opciones estratégicas, y potenciar los flujos de información para agilizar los procesos organizacionales (Rodríguez & Gallego, 2022). Esto se debe a que la información, al ser transformada en conocimiento, permite a la alta dirección contar con elementos relevantes para tomar decisiones documentadas y monitorear el progreso hacia los objetivos estratégicos, lo que se traduce en mayor productividad, innovación y continuidad de negocio (Rodríguez & Gallego, 2022). Por lo tanto, el uso adecuado y seguro de la información es un instrumento de alta potencia para mejorar la cadena de valor y lograr objetivos.

1.3.2. Seguridad de información

La Seguridad de la Información se define como el conjunto de esfuerzos de una organización destinados a proteger la información importante contra el acceso, la divulgación, el uso, la alteración o la interrupción no autorizados (IBM, 2024). Este concepto es amplio y abarca la protección de activos de Tecnologías de la Información (TI) físicos y digitales, incluyendo el cifrado, la seguridad de red y los controles administrativos. Su objetivo fundamental es salvaguardar los tres pilares de la seguridad, conocidos como la Tríada Confidencialidad-Integridad-Disponibilidad.

La importancia de la Seguridad de la Información radica en su papel como elemento clave para la continuidad del negocio y la protección de la reputación de las organizaciones. Implementar un sólido programa de seguridad permite a las empresas proteger datos sensibles (como estrategias, registros financieros o información de clientes) y minimizar el impacto de incidentes (ISOTools, 2025). Además, la seguridad de la información es crucial para el cumplimiento normativo, ya que muchas regulaciones (como la ISO 27001 o las leyes locales de protección de datos, como la Ley de Delitos Informáticos en Perú) exigen la protección de la información crítica (Gobierno del Perú, 2024; ISOTools, 2025). Un fallo en la seguridad puede acarrear graves pérdidas económicas, sanciones legales y la disminución de la confianza de clientes y socios comerciales, por lo que una gestión adecuada es vital para asegurar el éxito futuro.

1.3.3. Sistema de gestión de la seguridad de la información

El Sistema de Gestión de la Seguridad de la Información (SGSI) es un marco de procesos, políticas, procedimientos, estructuras organizacionales y funciones que se utiliza para establecer, implementar, mantener y mejorar continuamente la seguridad de la información dentro de una organización.

El propósito principal del SGSI es garantizar que los activos de información (datos, sistemas, hardware, software y personal) estén protegidos de manera efectiva,

asegurando siempre los tres pilares fundamentales de la seguridad: la confidencialidad, la integridad y la disponibilidad (Alcívar-Cruz & Llerena-Izquierdo, 2023).
El SGSI proporciona un enfoque sistemático basado en la gestión de riesgos para proteger la información frente a una amplia gama de amenazas, que pueden ser ataques intencionales, errores humanos o actos fortuitos como incendios o inundaciones (PRONABEC, 2024).

En términos de gestión, un SGSI se basa en el ciclo de Planificar-Hacer-Verificar-Actuar (PHVA/PDCA), lo que implica una revisión constante de los riesgos y una mejora continua para que el sistema se adapte a los cambios internos de la organización y a la evolución de las amenazas externas (Yungán Cazar & Narváez Contero, 2022). La norma internacional más reconocida y utilizada como marco de referencia para implementar un SGSI es la ISO/IEC 27001, que define los requisitos específicos para su establecimiento y certificación (BSI Group, 2025).

1.3.4. El modelo de mejora continua en la gestión de la seguridad de la información

El modelo de mejora continua en la Gestión de la Seguridad de la Información (SGSI) es fundamental para garantizar que la seguridad sea un proceso dinámico y no un esfuerzo estático. Este modelo se articula a través del Ciclo de Deming o Ciclo PHVA/PDCA (Planificar-Hacer-Verificar-Actuar), que es el marco metodológico exigido por la norma ISO/IEC 27001 para el establecimiento, mantenimiento y mejora continua de un SGSI (Magagnotti, 2022; NQA, 2022).

El ciclo PDCA asegura que el SGSI evolucione constantemente para enfrentar nuevas amenazas, vulnerabilidades y cambios organizacionales, llevando a una seguridad más efectiva y robusta (InfoProtección, 2025). A continuación, se describen las cuatro etapas de este ciclo aplicadas a la seguridad de la información:

a. Planificar (Plan)

Esta es la fase de diseño y preparación, donde la organización define qué hacer. Implica establecer el contexto, el alcance y la política de seguridad de la información. La actividad central es la identificación y evaluación de riesgos para determinar las amenazas y vulnerabilidades a las que están expuestos los activos de información. Luego, se planifican los controles y objetivos necesarios para mitigarlos, con el fin de alcanzar un nivel de riesgo aceptable (ISOTools Perú, 2022).

b. Hacer (Do)

En esta etapa, se implementan los planes y las estrategias definidas. La organización ejecuta las políticas, procedimientos y controles de seguridad

previamente seleccionados, como la capacitación del personal, la instalación de software de seguridad y la gestión operativa de los procesos (Gobierno de Perú, 2025). Es la fase donde se pone en marcha el SGSI.

c. Verificar (Check)

Esta fase busca evaluar si lo implementado en la fase "Hacer" está funcionando correctamente y de manera efectiva. Se lleva a cabo el monitoreo, la medición y el análisis del desempeño del SGSI. Las herramientas clave son las auditorías internas y la revisión por la dirección, que comparan los resultados obtenidos con los objetivos de seguridad y los requisitos de la norma ISO 27001. En este punto, se identifican las no conformidades y las desviaciones del sistema (GlobalSuite Solutions, 2023).

d. Actuar (Act)

La etapa final (y de arranque del siguiente ciclo) tiene como objetivo mantener y mejorar el SGSI basándose en los resultados de la verificación. Se emprenden acciones correctivas para subsanar las no conformidades detectadas y se toman decisiones para optimizar el sistema. Estas acciones de mejora pueden incluir la redefinición de políticas, el ajuste de controles o la actualización de la evaluación de riesgos, reiniciando el ciclo para asegurar la evolución constante de la seguridad (Yungán Cazar & Narváez Contero, 2022).

1.3.5. El sistema de gestión de la seguridad de la información y su relación con la gestión de riesgos

El Sistema de Gestión de la Seguridad de la Información (SGSI) y la Gestión de Riesgos están intrínsecamente relacionados, siendo esta última el pilar metodológico sobre el que se construye y opera el SGSI.

La norma internacional ISO/IEC 27001, que establece los requisitos para un SGSI, exige que este adopte un enfoque basado en riesgos para proteger la información y sus activos (BSI Group, 2025; NQA, 2022). Esto significa que la seguridad de la información no se gestiona mediante la aplicación arbitraria de controles, sino mediante la aplicación de un proceso sistemático para identificar, evaluar y tratar los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad (C-I-D) de la información.

La relación entre ambos sistemas se materializa en el ciclo de vida del SGSI, donde la gestión de riesgos es la fase de Planificación más crítica:

1. **Identificación y evaluación de riesgos**

   El proceso comienza identificando los activos de información (servidores, bases de datos, documentos, personal) y las posibles amenazas y vulnerabilidades a las que están expuestos (Pirani, 2025). La evaluación de riesgos permite a la organización determinar el nivel de riesgo inherente y establecer criterios de riesgo aceptable (Gobierno de Perú, 2024).

2. **Tratamiento y selección de controles**

   Una vez evaluados, el SGSI requiere que los riesgos se traten. El tratamiento de riesgos puede implicar cuatro estrategias fundamentales (Pensemos, 2024):

   a. Reducir el riesgo (aplicando controles).
   b. Transferir el riesgo (ej. contratando seguros).
   c. Evitar el riesgo (ej. no realizando la actividad asociada).
   d. Aceptar el riesgo (si el costo de mitigación es mayor que el impacto potencial y el riesgo se encuentra dentro del nivel aceptable).

   La estrategia más común es la reducción, que se logra mediante la implementación de controles de seguridad. La selección y justificación de estos controles, basada en el análisis de riesgos, es lo que define el SGSI. Sin una evaluación formal de riesgos, los controles carecerían de base, resultando en una protección ineficiente o excesiva (Chirou, 2024).

3. **Mejora continua (Reevaluación)**

   Dado que las amenazas y el contexto del negocio cambian continuamente, el SGSI, regido por el ciclo PHVA, exige la reevaluación constante de los riesgos y de la eficacia de los controles implementados (Gobierno de Perú, 2024; NQA, 2022). Esto asegura que la inversión en seguridad esté siempre alineada con las necesidades reales de protección.

1.3.6. Marcos de referencia para la implementación de la gestión de riesgos como parte de un SGSI

Las normas ISO/IEC 27001:2022 e ISO/IEC 27005:2022, establecen el marco de referencia esencial para implementar la gestión de riesgos como la base operativa de un Sistema de Gestión de la Seguridad de la Información (SGSI).

La norma ISO/IEC 27001:2022 es la norma certificable que establece los requisitos para el SGSI. Su principal exigencia es que la seguridad se construya sobre un enfoque basado en riesgos (NQA, 2022; DefendSphere, 2025).

Específicamente, las cláusulas clave de la ISO/IEC 27001 que exigen la gestión de riesgos son:

- Cláusula 6.1.2: Acciones para abordar riesgos y oportunidades. Esta sección obliga a la organización a:
  - Definir y aplicar un proceso de evaluación de riesgos de seguridad de la información.
  - Determinar el nivel de riesgo aceptable.
  - Identificar, analizar y evaluar los riesgos.

- Cláusula 6.1.3: Tratamiento de riesgos de seguridad de la información. Requiere la selección e implementación de opciones de tratamiento para reducir los riesgos a un nivel aceptable, lo que conduce a la selección de los controles pertinentes del Anexo A (DefendSphere, 2025).

En esencia, la ISO/IEC 27001 define qué hacer: la seguridad debe gestionarse sistemáticamente mediante el riesgo. Sin embargo, no ídica cómo realizar el proceso.

La norma ISO/IEC 27005:2022 actúa como la guía de apoyo para la ISO/IEC 27001. No es certificable, pero proporciona la metodología estructurada y detallada para llevar a cabo el proceso de gestión de riesgos exigido por la norma principal (GlobalSuite Solutions, 2025).

La ISO/IEC 27005:2022 complementa a la 27001 al detallar las fases del ciclo de gestión de riesgos dentro del contexto del SGSI (Secureframe, 2023). Este proceso estructurado incluye:

1. Establecimiento del contexto: Analizar factores internos y externos que pueden influir en los riesgos de seguridad, incluyendo los criterios de riesgo.
2. Identificación de riesgos: Determinar qué amenazas pueden explotar qué vulnerabilidades en qué activos (GlobalSuite Solutions, 2025).
3. Análisis de riesgos: Evaluar el impacto potencial y la Probabilidad de materialización de amenazas de los riesgos.
4. Evaluación de riesgos: Comparar los niveles de riesgo analizados con el criterio de riesgo aceptable definido por la organización.
5. Tratamiento de riesgos: Determinar las opciones para modificar el riesgo (reducir, evitar, transferir o aceptar) (Pirani, 2025).

La versión 2022 de la ISO/IEC 27005 mejoró su alineación con la ISO 27001:2022 e introdujo una mayor importancia en el análisis del contexto organizacional (Pirani, 2025).

1.3.7. Riesgo de seguridad de la información

El riesgo de seguridad de la información se define formalmente, según la familia de normas ISO/IEC 27000, como la posibilidad de que una amenaza concreta explote una vulnerabilidad para causar una pérdida o daño en un activo de información De La Cruz, & Paz (2024). Se considera una combinación de la probabilidad de que ocurra un evento y sus consecuencias o impacto Quispe (2020).

El análisis de riesgo se centra en cuatro componentes clave:

1. **Activo de información:** Es cualquier recurso que tiene valor para la organización y debe ser protegido, como bases de datos, software, hardware, documentos, o incluso la reputación y las personas (NQA, 2022).
2. **Amenaza:** Es una causa potencial de un incidente no deseado que puede resultar en daño a un sistema o a la organización (MinCiencias, 2025). Ejemplos incluyen hackers, desastres naturales o errores humanos.
3. **Vulnerabilidad:** Es una debilidad de un activo, control o proceso que puede ser explotada por una amenaza (IPES, 2025).
4. **Impacto/Consecuencia:** Se refiere al daño o pérdida que resultaría si la amenaza explota la vulnerabilidad (IPES, 2025). Las consecuencias se miden típicamente en términos de la pérdida de los tres pilares de la seguridad:
   - Confidencialidad: Divulgación a personas no autorizadas.
   - Integridad: Alteración o destrucción no autorizada.
   - Disponibilidad: Falta de acceso o uso cuando es requerido por una entidad autorizada

La evaluación del riesgo se expresa a menudo mediante la siguiente relación:

Riesgo = Probabilidad(Amenaza x Vulnerabilidad) x Impacto

La gestión de riesgos es el motor que impulsa el diseño, implementación, mantenimiento y mejora continua de un SGSI (Intedya, 2023).

a. Toma de decisiones: La identificación y evaluación de riesgos proporciona a la alta dirección la información necesaria para priorizar las inversiones en seguridad. Esto permite justificar los costos de seguridad al demostrar cómo las medidas propuestas reducen los riesgos críticos a un nivel aceptable para la organización (NQA, 2022).

b. Selección de controles: El resultado de la evaluación de riesgos es el que determina los controles de seguridad que deben implementarse. La ISO/IEC 27001 exige que la selección de los controles, como los detallados en el Anexo A o en la ISO/IEC

27002, esté directamente ligada a la necesidad de mitigar o modificar los riesgos identificados (SUNAT, 2023).

c. Riesgo Residual: Una vez aplicados los controles, el riesgo que queda en la organización se denomina Riesgo Residual (IPES, 2025). Este riesgo debe ser documentado y formalmente aceptado por la dirección, asegurando que la organización es consciente de su exposición y ha tomado una decisión informada sobre la protección de sus activos.

1.3.8. Estrategias de tratamiento de los riesgos

Las estrategias de tratamiento de riesgos, como parte fundamental de un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo el marco de ISO/IEC 27005, son las opciones elegidas por la organización para modificar el riesgo a un nivel aceptable (SUNAT, 2023).

Una vez que los riesgos han sido identificados, analizados y evaluados, la organización debe tomar una decisión informada para cada riesgo. Generalmente, existen cuatro estrategias principales de tratamiento (Pirani, 2025; ISMS.online, 2025):

1. **Evitar el riesgo**

   Esta estrategia se aplica cuando el riesgo es tan alto o inaceptable que la organización decide eliminar la causa o la actividad que lo genera por completo. Se deja de realizar el proceso, se descarta el activo o se cambia la forma de operar para que la amenaza ya no tenga posibilidad de explotar la vulnerabilidad (Mineducación, 2023).

   Ejemplo: Dejar de utilizar una aplicación obsoleta que presenta vulnerabilidades críticas o prohibir el uso de ordenadores portátiles fuera de las instalaciones para evitar el riesgo de robo de datos (ISOTools, 2017).

2. **Reducir o mitigar el riesgo**

   Esta es la estrategia más común y se aplica a los riesgos que superan el nivel aceptable. El objetivo es disminuir la Probabilidad de materialización de amenazas o reducir el impacto potencial (o ambos) mediante la aplicación de controles (Pirani, 2025). Implica implementar medidas (controles), como las detalladas en la ISO/IEC 27002, para que el riesgo se sitúe por debajo del umbral de riesgo aceptable (ISOTools, 2017).

   Ejemplo: Implementar un firewall (control técnico) para reducir la probabilidad de acceso no autorizado, o establecer copias de seguridad periódicas (control organizacional) para mitigar el impacto de una Eliminación de datos.

3. **Transferir o compartir el riesgo**

   Esta estrategia implica compartir el riesgo con un tercero que esté en mejor posición para gestionarlo o que asuma las consecuencias financieras si el riesgo se materializa (GlobalSuite Solutions, 2025). Se transfiere una parte o la totalidad de las consecuencias del riesgo.

   Ejemplo: Adquirir una póliza de ciberseguro para cubrir las pérdidas financieras derivadas de un ciberincidente, o subcontratar un servicio de gestión de red (tercerizar la operación) a un proveedor especializado (Mineducación, 2023; Secureframe, 2023).

4. **Aceptar o retener el riesgo**

   La aceptación del riesgo es una decisión consciente e informada de la alta dirección de no tomar ninguna acción adicional, ya sea porque el riesgo se considera bajo o porque el costo de mitigarlo es desproporcionadamente alto en comparación con su posible impacto (ISMS.online, 2025). El riesgo es identificado, evaluado, y se decide que está dentro de los criterios de aceptación de riesgo establecidos por la organización. Es crucial que esta decisión sea documentada y aprobada por el propietario del riesgo (SUNAT, 2023).

   Ejemplo: Aceptar el riesgo de que falle una impresora no crítica, ya que el costo de adquirir una redundante es muy alto y el impacto en el negocio es mínimo y temporal (ISOTools, 2017).

1.3.9. Ciclo de vida de la gestión de riesgos

El ciclo de vida de la gestión de riesgos de seguridad de la información es un proceso sistemático y continuo, regido principalmente por la norma internacional ISO/IEC 27005:2022. Este ciclo se integra con el ciclo de mejora continua (Planificar-Hacer-Verificar-Actuar o PDCA) de la ISO/IEC 27001 para garantizar la revisión y optimización constantes (GlobalSuite Solutions, 2025; ORSYS, 2025).

A continuación, se describen las fases principales de este ciclo:

1. **Establecimiento del contexto (Planificación)**

   Esta fase inicial define el alcance, las reglas y los parámetros para el resto del proceso de gestión de riesgos. Sin un contexto claro, la evaluación posterior carecería de sentido para la organización (Pirani, 2025). Implica comprender la misión, visión, objetivos estratégicos, estructura y entorno de la organización,

incluyendo la identificación de partes interesadas (internas y externas) y sus requisitos.

En relación al contexto de la seguridad de la Información se definen los requisitos legales, reglamentarios, contractuales y de negocio que afectan a la información (Pirani, 2025). También se establecen los criterios de riesgo y se establecen los parámetros para la evaluación, incluyendo:

- Escalas de impacto y probabilidad que es la forma cómo se medirán.
- Nivel de riesgo aceptable, que es el umbral por debajo del cual el riesgo no requiere tratamiento adicional (ISMS.online, 2025).

2. Valoración del riesgo (Análisis y evaluación)

La valoración es la parte central y se compone de la identificación, el análisis y la evaluación. Las actividades que se desarrollan son:

a. Identificación del riesgo

Proceso de encontrar, reconocer y describir los riesgos (Poder Judicial del Perú, 2025). Típicamente, comienza por la identificación de los activos de información (ej. hardware, software, bases de datos, personas), y luego se identifican las amenazas que pueden afectarlos y las vulnerabilidades que pueden ser explotadas (GlobalSuite Solutions, 2025; SUNAT, 2023).

b. Análisis del riesgo

Proceso para comprender la naturaleza del riesgo y determinar su nivel. Se calcula combinando la probabilidad de que una amenaza explote una vulnerabilidad y el impacto o la consecuencia resultante en la organización.

$$\text{Riesgo} = \text{Probabilidad} \times \text{Impacto}$$

c. Evaluación del riesgo

Fase en la que se compara el nivel de riesgo calculado con los criterios de riesgo aceptable definidos en la Fase 1. El resultado determina qué riesgos son aceptables (no se requiere tratamiento inmediato) y cuáles requieren un tratamiento o respuesta (Secureframe, 2023).

3. Tratamiento del riesgo (Hacer)

En esta fase, se formulan las estrategias para modificar el riesgo a un nivel aceptable, basándose en los resultados de la evaluación.

a. Selección de estrategias

La organización elige una o varias opciones para cada riesgo inaceptable: reducir/mitigar (aplicar controles), transferir/compartir (ej. seguro), evitar (eliminar la fuente) o aceptar (si el costo de la mitigación supera los beneficios) (ISMS.online, 2025).

b. Plan de tratamiento de riesgos (PTR)

Documento que detalla los controles específicos a implementar, los responsables, los recursos necesarios y los plazos para llevar el riesgo inaceptable al nivel residual aceptado (CORE, 2025).

4. Seguimiento y revisión (Verificar y Actuar)

La gestión de riesgos es un ciclo continuo, no un evento único. Las últimas fases aseguran que el proceso sea efectivo y se mantenga relevante.

a. Monitoreo y revisión

Actividades constantes para asegurar que los controles implementados son eficaces y que el riesgo residual permanece dentro de los límites aceptados (GlobalSuite Solutions, 2025). Esto incluye la revisión periódica del contexto y de los propios riesgos debido a los cambios en el entorno de amenazas, tecnología o requisitos de negocio.

b. Comunicación y consulta

La norma ISO 27005 enfatiza que la comunicación con las partes interesadas debe ocurrir durante todo el proceso, no solo al final, para garantizar el compromiso y la comprensión del riesgo (Pirani, 2025).

1.3.10. Metodología OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation)

OCTAVE® (Evaluation de Amenazas, Activos y Vulnerabilidades Críticas para las Operaciones) es un enfoque para la gestión de riesgos de seguridad de la información. Se trata de una técnica de evaluación y planificación estratégica basada en riesgos.

A diferencia de las evaluaciones típicas centradas en la tecnología y en asuntos tácticos, OCTAVE se enfoca en el riesgo organizacional y en asuntos estratégicos relacionados con las prácticas de seguridad. Se centra en la identificación de los activos relacionados con la información que son críticos para la organización y en los riesgos que los afectan. Equilibra tres aspectos clave: el riesgo operacional, las prácticas de seguridad y la tecnología (Alberts, C., et. al, C., 2003).

Fases del proceso OCTAVE

El enfoque OCTAVE se organiza en un proceso de tres fases, complementado por un equipo interdisciplinario, denominado el equipo de análisis, compuesto por personal de las unidades de negocio y del departamento de TI:

1. **Fase 1: Construir perfiles de amenaza basados en activos (Evaluación organizacional).** En esta fase, el equipo identifica los activos de información más importantes (activos críticos), las prácticas de seguridad actuales y las vulnerabilidades organizacionales. Luego, define los requisitos de seguridad y crea un perfil de amenaza para cada activo crítico seleccionado.
2. **Fase 2: Identificar vulnerabilidades de la infraestructura (Evaluación de la infraestructura de información).** El equipo examina los caminos de acceso a la red, identifica las clases de componentes de tecnología de la información relacionados con cada activo crítico y evalúa su resistencia a ataques. En la metodología OCTAVE-S para organizaciones pequeñas, esta fase es una revisión abreviada de los procesos utilizados para asegurar la infraestructura.
3. **Fase 3: Desarrollar estrategia y planes de seguridad.** Se analizan los riesgos para los activos críticos, se define una estrategia de protección general para la organización y se crean planes de mitigación de riesgos para reducir el riesgo. Los resultados obligatorios de esta fase son los riesgos a los activos críticos, la Estrategia de Protección y los Planes de Mitigación de Riesgos

1.4. Operacionalización de las variables

Variable: Modelamiento de la gestión de riesgos de seguridad de la información

Definición conceptual

El Modelamiento de la Gestión de Riesgos de Seguridad de la Información se define como el proceso estratégico y sistemático de diseñar una estructura funcional y operativa que permita identificar, analizar, evaluar, tratar, y monitorear los riesgos que podrían comprometer la confidencialidad, integridad y disponibilidad (CID) de los activos de información críticos de una organización. Este modelo se basa en la aplicación de buenas prácticas y estándares reconocidos, como las directrices de la familia ISO/IEC 27005 y metodologías específicas de gestión de riesgos como OCTAVE, asegurando que los controles implementados mitiguen la exposición al riesgo a niveles aceptables. En el contexto de esta investigación, el modelamiento implica la definición de los elementos funcionales (qué hacer) y estructurales (cómo y con qué) necesarios para crear un modelo coherente.

Definición operacional

El Modelamiento de la Gestión de Riesgos de Seguridad de la Información se operacionaliza mediante el diseño de un modelo que cumpla con los requisitos de la norma ISO/IEC 27005 y las guías de gestión de riesgos de la metodología OCTAVE. Los

indicadores de medición incluyen la validación de sus componentes (suficiencia, claridad, coherencia y relevancia) frente a las buenas prácticas y su capacidad para soportar las actividades del ciclo de vida del riesgo. Este modelo se estructura en: (1) Identificación de Amenazas y Vulnerabilidades; (2) Estimación del Nivel de Exposición al Riesgo (valoración de impacto y probabilidad para clasificar riesgos en rangos tolerables/no tolerables); (3) Identificación de Prácticas de Seguridad y Controles (definición de acciones para mitigar riesgos no aceptables; y (4) Validación del Cumplimiento (evaluación por juicio de expertos respecto a la pertinencia del modelo).

1.5. Operacionalización de variables

Tabla 1. Activos de información de los procesos académicos

Variable	Definición conceptual	Dimensiones	Indicadores	Instrumentos de Medición
Variable Independiente (VI)				
Modelamiento de la gestión de riesgos de seguridad de la información	Marco estructurado y adaptado (basado en ISO/IEC 27005 y OCTAVE-S) que integra elementos funcionales (identificación, estimación, tratamiento) y estructurales (activos críticos, matriz de riesgo) para los servicios académicos de la UNPRG.	1. Suficiencia	El modelamiento incluye los elementos necesarios de la ISO/IEC 31000:2018 y OCTAVE-S para la gestión completa del riesgo.	Cuestionario de Juicio de Expertos (Escala Likert 5 puntos)
		2. Claridad	La documentación del modelamiento (guías, plantillas) es comprensible para el personal de TI y usuarios clave de la Universidad.	
		3. Coherencia	Existe consistencia lógica entre el objetivo del modelamiento, los riesgos identificados y los controles propuestos y la alineación entre los activos críticos (SIA, BD, Firewall) y los servicios académicos.	
		4. Relevancia	El modelamiento es pertinente y aplicable al contexto tecnológico y operacional específico de la UNPRG.	
Variable Dependiente (VD)				
Eficacia del modelamiento para soportar la operación de Servicios Académicos	La capacidad del modelamiento para proveer un diagnóstico preciso de la exposición al riesgo y generar planes de tratamiento que fortalezcan la Confidencialidad, Integridad y Disponibilidad de los servicios académicos (Logro de los Objetivos Específicos 1, 2 y 3).	1. Eficacia de Identificación de Amenazas (O.E. 1)	Cobertura de la identificación de amenazas sobre los activos críticos (SIA, BD, Firewall). - Amenazas identificadas con actores de amenaza y mecanismos de acceso.	Listas de Control / Análisis de la base de datos de Amenazas.
		2. Eficacia en la Estimación de Riesgos (O.E. 2)	Riesgos clasificados en Niveles No Aceptables (Muy Alto y Alto). - Precisión de la Matriz de Impacto ponderada (Reputación, Económico, Productividad, Administrativo).	Matriz de Riesgo Cuantitativa (Fórmula Riesgo = Impacto x Probabilidad)
		3. Eficacia en el Tratamiento del Riesgo (O.E. 3)	Controles y prácticas de seguridad asignadas a los riesgos No Aceptables.	Tabla de tratamiento de tiesgos / Documentos de Políticas y Controles.

II. DISEÑO METODOLÓGICO

2.1. Tipo de investigación

La investigación fue de **tipo aplicada**, dado que se utilizaron estándares y metodologías reconocidas en el ámbito de la seguridad de la información, tales como la norma **ISO/IEC 27005:2022** y la metodología **OCTAVE-S**, como marcos de referencia para la construcción de un modelo de gestión de riesgos adaptado al contexto de los servicios académicos de la Universidad Nacional Pedro Ruiz Gallo.

Este tipo de investigación permitió emplear el conocimiento teórico y técnico existente para resolver un problema práctico y concreto relacionado con la gestión de riesgos de seguridad de la información, fortaleciendo la confidencialidad, integridad y disponibilidad de los activos de información académica.

2.2. Nivel de investigación

El estudio se desarrolló con un **nivel descriptivo–propositivo**. Fue descriptivo porque se documentaron de manera detallada las fases, procedimientos y actividades desarrolladas durante la aplicación del modelo de gestión de riesgos, sin manipular las variables de estudio ni alterar el entorno natural de los procesos académicos. Asimismo, fue propositivo porque el producto final de la investigación consistió en la **formulación de un modelo** que permite gestionar los riesgos de seguridad de la información en los servicios académicos de la Universidad, respondiendo a una necesidad institucional previamente identificada.

2.3. Diseño de investigación

El diseño de la investigación fue **no experimental y longitudinal**. Fue no experimental porque no se manipularon las variables de manera intencional, sino que se observaron y analizaron los hechos tal como ocurrieron en su contexto natural, a fin de describirlos y comprenderlos.

El carácter longitudinal se justificó porque se analizaron datos históricos y actuales relacionados con la gestión de los servicios académicos y los incidentes de seguridad de la información registrados en los sistemas institucionales, permitiendo establecer una evolución temporal de los riesgos.

La recolección y el análisis de la información se complementaron con la **validación del modelo mediante el juicio de expertos**, quienes evaluaron su suficiencia, claridad, coherencia y relevancia respecto a las buenas prácticas internacionales..

2.4. Población y muestra

La **unidad de estudio** estuvo conformada por los colaboradores involucrados en los distintos procesos de la gestión académica de la Universidad Nacional Pedro Ruiz Gallo, quienes participaron directa o indirectamente en el manejo de la información y en la operación de los sistemas **SIA** y **GESTAC**.

La **población** total estuvo constituida por **38 personas**, distribuidas de la siguiente manera:

- Personal administrativo de la Dirección de Servicios Académicos (DSA): 8 personas.
- Personal técnico de la DSA: 6 personas.
- Personal de apoyo en las 14 facultades de la Universidad: 18 personas.
- Directora de la Dirección de Servicios Académicos: 1 persona.
- Directora de la Oficina de Calidad: 1 persona.
- Directora de la Oficina de Tecnología de la Información: 1 persona.
- Personal técnico de la Oficina de Tecnología de la Información: 3 personas.

Dado el tamaño de la población y la relevancia de todos los actores en los procesos de gestión académica, **no se aplicó técnica de muestreo**, trabajándose con la **población total**, lo que aseguró la representatividad de los resultados obtenidos.

2.5. Técnica e instrumentos de recolección de datos

Para la recolección de datos se emplearon las siguientes técnicas e instrumentos, seleccionados conforme a los objetivos del estudio y a la naturaleza de las variables analizadas:

a. Entrevista estructurada

Se aplicó una entrevista estructurada al personal administrativo, técnico y de apoyo de la Dirección de Servicios Académicos y de la Oficina de Tecnología de la Información. Esta técnica permitió obtener información cualitativa y cuantitativa sobre las prácticas, políticas y vulnerabilidades relacionadas con la seguridad de la información.

El instrumento utilizado fue un **cuestionario adaptado de la metodología OCTAVE-S**, el cual se ajustó al contexto institucional. Dicho cuestionario incluyó preguntas cerradas de opción múltiple y un espacio para comentarios adicionales, lo que permitió recopilar percepciones y evidencias sobre los procedimientos de seguridad implementados.

b. Revisión documental

Se realizó una revisión exhaustiva de documentos institucionales, tales como manuales de procesos, políticas internas, reglamentos, reportes técnicos, protocolos y formatos

relacionados con la gestión académica y la seguridad de la información. Esta técnica permitió identificar el flujo de trabajo de los procesos académicos, las medidas de protección existentes, los incidentes reportados y el nivel de cumplimiento de las buenas prácticas de seguridad de la información en la Universidad. Asimismo, sirvió para contrastar la información obtenida en las entrevistas y sustentar el diseño del modelo de gestión de riesgos.

c. Juicio de expertos

Para validar el modelo propuesto se aplicó la técnica del **juicio de expertos**, con la finalidad de garantizar la pertinencia, claridad, coherencia y suficiencia del marco de trabajo diseñado. Los expertos seleccionados contaban con experiencia en gestión de la seguridad de la información y conocimiento de las normas **ISO/IEC 27001**, **ISO/IEC 27005** e **ISO 31000**.

El instrumento empleado fue una **ficha de validación** estructurada en escala tipo Likert de cinco puntos, que permitió calificar los criterios de evaluación del modelo propuesto.

2.6. Consideraciones éticas

Durante la ejecución de la investigación se respetaron los principios éticos establecidos para los estudios institucionales. Se garantizó la **confidencialidad de la información** proporcionada por los participantes y el **uso exclusivo de los datos con fines académicos**. Asimismo, se obtuvo el consentimiento informado de los colaboradores involucrados, quienes participaron de manera voluntaria en las entrevistas y validaciones. Se evitó cualquier práctica que pudiera generar conflicto de interés o vulnerar la privacidad de las personas o la seguridad de los sistemas institucionales.

III. RESULTADOS

3.1. Elaboración del perfil de las amenazas enfocadas en los activos en la gestión académica de la UNPRG

En cumplimiento a las actividades contempladas en la Fase 1 del enfoque OCTAVE, denominada "Elaboración del perfil de las amenazas enfocadas en los activos" (o "Build Asset-Based Threat Profiles"), se desarrolló lo siguiente:

A. Visión organizacional y ámbito

La gestión académica en la UNPRG recae bajo la responsabilidad del Vicerrectorado Académico, según la Ley Universitaria N° 30220. Específicamente, la Dirección de Servicios Académicos (DSA) tiene a su cargo las funciones relacionadas con los procesos académicos.

Los esfuerzos de identificación de amenazas se concentraron en analizar las prácticas de seguridad actuales y los criterios para valorar el impacto de las amenazas sobre los activos. Este trabajo fue realizado de manera colaborativa con el personal técnico de la Oficina de Tecnologías de Información y los directivos de la gestión académica.

B. Identificación de activos críticos

Se identificaron los activos principales que sustentan la gestión académica:

a. Procesos de Gestión Académica: El núcleo de la gestión académica abarca diversos procesos y actividades fundamentales, incluyendo:
   - Registro y codificación de nuevos estudiantes (para programas de pregrado, posgrado y especialidades).
   - El proceso de matrícula, que incluye la programación académica, la asignación de carga docente, la elaboración de horarios, y el registro en sí.
   - Gestión y modificación de planes de estudio.
   - Registro de convalidaciones y exámenes extraordinarios.
   - Registro del desarrollo de clases, incluyendo la carga de sílabos, el control de asistencia y el registro de calificaciones.
   - Generación y rectificación de actas de notas.
   - Emisión de constancias y certificados (de estudio y de egreso).

b. Aplicaciones informáticas: La gestión académica se gestiona a través de dos sistemas:
   - Gestión Académica (Gestac): El sistema anterior que almacena información hasta el año 2014.
   - Sistema de Información Académico (SIA): La aplicación informática que se utiliza actualmente para gestionar todos los procesos mencionados.

c. Infraestructura de red y comunicaciones: El backbone de fibra óptica de la Universidad integra todas las facultades y oficinas. Sobre esta infraestructura operan las aplicaciones académicas y administrativas (incluida la gestión académica) y se brindan servicios básicos (Internet, telefonía IP, correo institucional). La red incluye componentes esenciales como servidores, routers, firewalls, IDS y switch de borde.

Tabla 2. Activos de información de los procesos académicos

Nueva Codificación	Designación	Datos relevantes	Soporte/Función clave	Componentes vinculados
AC-SIS-SIA	Sistema de Información Académico (SIA)	Registros de alumnos, Planes de estudio, Programación de cursos, Horarios, Matrículas, Calificaciones, Actas, Historial académico	Programación de cursos, Gestión de matrículas, Control de asistencia, Expediente académico, Emisión de actas	Servicios de dominio, Servicios de red, Base de datos-SIA, Respaldo de base de datos-SIA, Servicios Web, Servicios de archivos
AC-SIS-GAS	Sistema de Gestión Académica (GESTAC)	Data académica histórica (antigua), Registros de alumnos, Planes de estudio, Programación de cursos, Horarios, Matrículas, Calificaciones, Actas, Historial académico	Emisión de actas, Servicios de dominio, Servicios de red, Base de datos-GESTAC, Respaldo de base de datos-GESTAC, Servicios Web, Servicios de archivos	Servicios de dominio, Servicios de red, Base de datos-GESTAC, Respaldo de base de datos-GESTAC, Servicios Web, Servicios de archivos
AC-INF-DOM	Servicio de Nombres de Dominio (DNS)		Administración de direcciones IP y nombres de dominio	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-ENC	Servicio de Interconexión (Proxy)		Facilita la conexión de usuarios a la red externa (Internet)	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-DBS	Servicio de Base de Datos - SIA		Administra el motor de base de datos para dar soporte a las aplicaciones del SIA	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-RES	Servicio de Copias de Seguridad de Base de Datos - SIA		Administra las *backups* como salvaguarda de la base de datos principal del SIA	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-WEB	Servicio de Publicación Web		Almacena el contenido relacionado con el proceso de matrícula en la red externa	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-ARC	Servicio de Administración de Archivos		Almacena y distribuye diversos tipos de archivos a los usuarios del dominio UNPRG	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-DBG	Servicio de Base de Datos - GESTAC		Administra el motor de base de datos para dar soporte a las aplicaciones del GESTAC	Internet, UPS, Firewall, SIA, GESTAC
AC-INF-REG	Servicio de Copias de Seguridad de Base de Datos - GESTAC		Administra las *backups* como salvaguarda de la base de datos principal del GESTAC	Internet, UPS, Firewall, SIA, GESTAC
AC-HW-SWI	*Switch* Central y Perimetral	Perfiles de acceso y permisos a la estructura de la red	Permite la interconexión fundamental de los equipos de la Red telemática de la UNPRG	Router, Firewall
AC-HW-ROU	*Router*	Perfiles de acceso y permisos a las aplicaciones	Controla los accesos y limitaciones a los sistemas y las comunicaciones de la Red telemática de la UNPRG	Switch central y perimetral, Firewall
AC-HW-FIR	*Firewall*	Perfiles de acceso y permisos a la red externa (Internet)	Administra el acceso a los recursos informáticos en la Red telemática de la UNPRG	Switch central y perimetral
AC-PER-ADM	Personal de administración de TI	Conocimiento en Gestión de redes, comunicaciones, servidores, seguridad de red y web	Administración de la infraestructura de red, comunicaciones y *data center*; Gestión de la seguridad de red	Switch central y perimetral, Router, Firewall, Perfiles de usuarios

AC-PER-APL	Personal de administración de aplicaciones/BD	Conocimiento en Gestión de bases de datos, Programación (*desktop* y web)	Administración de aplicaciones y bases de datos; Gestión de la seguridad de la BD	Base de datos SIA, Base de datos GESTAC, Perfiles de usuarios
AC-PER-USU	Personal operativo de aplicaciones	Conocimiento de procesos académicos, Habilidad para operar aplicaciones como usuarios finales	Uso de aplicaciones como soporte a los procesos académicos	SIA, GESTAC, Perfiles de usuarios, Terminales informáticos

Nota: Elaborado en base a la información proporcionada por la Dirección de Servicios Académicos y la Oficina de Tecnologías de la Información

La tabla proporciona una visión organizada de qué elementos (sistemas, equipos y personas) son esenciales para el funcionamiento de la gestión académica, qué información manejan y cómo se interconectan dentro de la gestión tecnológica de la universidad.

C. Análisis de las medidas de protección de los activos (prácticas de seguridad) en los procesos de gestión académica

La verificación sobre el estado actual de las medidas de protección de la información implementadas en la Universidad se llevaron a cabo mediante un esfuerzo colaborativo. Se organizaron grupos focales con el personal técnico de la Oficina de Tecnologías de Información (OTI) y con diversos usuarios vinculados a los procesos académicos.

Para esta tarea, se utilizaron los cuestionarios y formatos derivados de la metodología OCTAVE. Las medidas de seguridad examinadas se clasificaron en grupos temáticos o dominios de seguridad. Si bien se usó como referencia OCTAVE para la definición de estos dominios, sus nombres fueron ajustados para facilitar la comprensión de los participantes y su adecuación al contexto institucional.

A continuación, se detallan las conclusiones obtenidas de estos grupos focales:

a. Evaluación de las medidas estratégicas de seguridad

Instrucción, concienciación y nivel de comprensión en seguridad

Se concluyó que la aplicación de las medidas de seguridad en cuanto a la formación y sensibilización es incompleta. Se encontraron las siguientes deficiencias:

- Las funciones y deberes de seguridad no están claramente especificados en la normativa interna y directrices de la Universidad.
- No existen programas de educación, formación o entrenamiento establecidos en temas de seguridad de la información.
- No se han programado acciones ni campañas para aumentar la sensibilización del personal respecto a la seguridad.
- El personal no siempre acata de manera efectiva las pautas de seguridad.

- Los colaboradores aún no asimilan la trascendencia de salvaguardar la información bajo su responsabilidad.

Puesta en marcha de la estrategia y las tareas de seguridad

La implementación de acciones y planes estratégicos de seguridad es mínima o inexistente. Los puntos débiles identificados son:

- Los procedimientos institucionales no integran las medidas de seguridad de la información.
- No existen planes formalmente aprobados que permitan llevar a la práctica los documentos de seguridad y la información autorizada.
- Los documentos de gobernanza digital y de seguridad no se han difundido eficazmente al personal, y tampoco se han ejecutado actividades de entrenamiento o concienciación para su cumplimiento.

Administración de la seguridad de la información

Se constató una escasa o nula ejecución de medidas de administración de la seguridad. Los fallos incluyen:

- No se ha destinado un presupuesto específico para financiar la administración de la seguridad de la información.
- Las labores de seguridad son ejecutadas por la OTI utilizando los limitados recursos humanos disponibles.
- La estructura orgánica carece de una unidad específica dedicada a la administración de la seguridad de la información o de los riesgos.
- No se generan reportes que certifiquen el cumplimiento de las funciones y buenas prácticas de seguridad definidas en los documentos de gobernanza digital.
- No hay pautas de inducción en seguridad para el personal recién incorporado.
- Se confirmó que las autorizaciones de acceso del personal saliente no se revocan con la debida celeridad.
- No existe un procedimiento oficial y aprobado para la gestión de riesgos de TI.
- No se realizan revisiones específicas para constatar el acatamiento de la normativa vigente en materia de seguridad.

Estructura regulatoria y lineamientos de seguridad

Las prácticas relacionadas con el marco legal y las políticas muestran una implementación mínima o nula:

- La política de seguridad no ha sido comunicada de forma efectiva a todos los miembros de la institución.
- No existe ningún documento normativo específico aprobado y divulgado que se enfoque en un dominio concreto de la gestión de la información.

- Se carece de planes para verificar el cumplimiento de la política de seguridad.
- El marco legal asociado a la seguridad de la información no se revisa periódicamente.

Manejo de la seguridad de la información con colaboradores externos

Las medidas para administrar la seguridad con terceros son escasas o nulas:

- No se firman convenios de confidencialidad específicos para proteger la información.
- No se tienen procedimientos para comprobar el cumplimiento de los acuerdos de confidencialidad y protección incluidos en contratos y convenios.
- No existen esquemas de emergencia y recuperación ante sucesos o incidentes de seguridad que involucren a colaboradores externos.

Esquemas de emergencia y recuperación ante desastres

Se observa una implementación escasa o nula en la planificación de la continuidad:

- No se ha llevado a cabo un análisis de impacto (BIA) frente a desastres o contingencias para identificar las funciones, activos e información de alta criticidad en los procesos.
- No se cuenta con documentos oficialmente aprobados y comunicados que planifiquen alternativas para la gestión de crisis y la vuelta a la operación normal después de un desastre.

b. Evaluación de las medidas operacionales de seguridad

Control de ingreso físico

Las medidas de control físico de acceso presentan una ejecución mínima o nula. Los problemas son:

- En zonas con activos críticos (como switch de borde o terminales), el acceso físico se maneja de forma desestructurada.
- No hay protocolos para manejar excepciones de acceso de visitantes o terceros a áreas restringidas.
- Se carece de dispositivos de seguridad física como videovigilancia, puertas controladas o controles biométricos para gestionar el acceso a áreas de trabajo, infraestructura tecnológica y sistemas.
- No existen procedimientos de seguridad específicos para la organización de estaciones y escritorios de trabajo ("escritorio limpio").

Protección ambiental y de la instalación

La Protección ambiental y de la instalación se encuentra en un estado de escasa o nula implementación:

- El mantenimiento planificado a menudo no se ejecuta debido a limitaciones presupuestarias o procesos administrativos engorrosos.
- No existe un registro institucional oficial para los incidentes de seguridad física o ambiental.
- La supervisión de los servicios de terceros es reactiva, solo se lleva a cabo cuando ya ha ocurrido un evento o incidente de seguridad.

Administración de la red y sistemas

Las medidas de gestión de la infraestructura de red y sistemas están ampliamente implementadas. Sin embargo, se identificó que no se mantiene un registro de control de cambios para las aplicaciones que se encuentran en uso.

Monitoreo y auditoría de registros de sucesos

Las prácticas de seguimiento y revisión de logs de incidentes de seguridad están implementadas en gran parte.

Control de ingresos lógicos

Las medidas para el control de acceso a nivel de software están ampliamente implementadas.

Administración de puntos débiles (Vulnerabilidades)

La Administración de puntos débiles (Vulnerabilidades) ha sido parcialmente implementada. El principal déficit es la ausencia de procedimientos definidos y autorizados para el manejo de vulnerabilidades en la red y en los sistemas.

Cifrado de información

Las medidas de cifrado de datos se consideran no pertinentes para el alcance de este análisis.

Seguridad en el ciclo de desarrollo de aplicaciones

La seguridad aplicada al desarrollo de sistemas es de poca o nula ejecución:

- El desarrollo de software nuevo recae principalmente en la OTI, la cual carece de protocolos y procedimientos formalmente aprobados para el desarrollo de sistemas.
- Específicamente, no existen registros de inspección para verificar la ausencia de código malicioso en los sistemas de gestión académica.

Manejo de sucesos de seguridad de la información

La administración de incidentes de seguridad presenta una ejecución mínima o nula:

- No se dispone de protocolos ni procedimientos definidos y aprobados para el manejo de sucesos de seguridad.
- La respuesta a incidentes es reactiva; se usan documentos para registrarlos, pero estos son simplemente archivados y nunca evaluados posteriormente.
- Los incidentes no han sido clasificados según su nivel de urgencia o impacto.
- Tampoco se han establecido los tiempos de respuesta ni los protocolos de atención de acuerdo con el tipo de suceso.
- No se cuenta con un listado de proveedores para atender los incidentes que escalan a problemas mayores.

Tras la evaluación de las medidas operacionales y estratégicas, se concluyó que los dominios de seguridad con un nivel de implementación "Alto o Total" son: Administración de la red y sistemas, Control de ingresos lógicos y monitoreo y Auditoría de registros de sucesos.

Por otro lado, la aplicación fue parcial en los dominios de Instrucción, concienciación y nivel de comprensión y Administración de puntos débiles (Vulnerabilidades).

Finalmente, la implementación fue mínima o nula en la mayoría de los dominios, incluyendo: Puesta en marcha de la estrategia, Administración de la seguridad, Estructura regulatoria y lineamientos, Manejo de seguridad con colaboradores externos, Esquemas de emergencia y recuperación, Control de ingreso físico, Protección ambiental y de la instalación, Seguridad en el ciclo de desarrollo, y Manejo de sucesos de seguridad de la información

D. Parámetros para la medición de consecuencias o impactos

Se requirió establecer un elemento esencial que debía definirse a nivel institucional: los parámetros y la escala de graduación para determinar las consecuencias que se generarían sobre las operaciones de gestión académica ante cualquier suceso o contingencia relativa a la seguridad de la información.

De acuerdo con las directrices consultadas, la propia organización debe fijar estos parámetros y sus niveles. Para cumplir este objetivo, se adoptaron como punto de partida los criterios que establece la guía metodológica OCTAVE, ajustando sus etiquetas para asegurar una mejor comprensión por parte del personal involucrado. Asimismo, se optó por no incluir la métrica de seguridad ocupacional, pues se consideró que este tipo de efecto no tiene incidencia en la esfera de la gestión académica.

Esta actividad se llevó a cabo en colaboración con el personal que dirige los diversos procesos académicos de la Universidad, considerándolos los responsables principales de las operaciones y quienes poseen el conocimiento más profundo sobre ellas.

Para cuantificar las consecuencias, se desarrolló la siguiente estructura, la cual incluye los cuatro parámetros determinados para calificar el efecto de las amenazas, junto con una escala de valoración de cinco niveles. Para cada tipo de consecuencia, se definieron los aspectos que deben considerarse para asignar el nivel de impacto, empleando la técnica del modelo de madurez.

Tabla 3. Clasificación y escala de valoración de las consecuencias

Clasificación de la consecuencia/severidad	MUY BAJO (1)	2	3	4	5
IMPACTO EN LA IMAGEN O CREDIBILIDAD DEL USUARIO (Severidad 4)	El prestigio de la Dirección de Servicios Académicos (DSA) se daña de forma imperceptible y las quejas son casi nulas. El esfuerzo para mejorar la atención y evitar el deterioro de la credibilidad es insignificante.	El prestigio de la DSA sufre un daño menor y se producen algunas quejas. El esfuerzo para optimizar la atención y evitar la pérdida de confianza es reducido.	El prestigio de la DSA sufre perjuicio y las quejas se multiplican. El esfuerzo para optimizar la atención y evitar el deterioro de la credibilidad es moderado.	El prestigio de la DSA se ve gravemente afectado y las quejas son muy elevadas. Se requiere un esfuerzo considerable para mejorar la atención y evitar el deterioro de la credibilidad.	El prestigio de la DSA colapsa completamente. La restauración de la fe de los usuarios es sumamente compleja.
IMPACTO FINANCIERO (Severidad 2)	Existe un incremento insignificante en los gastos de funcionamiento.	Existe un aumento en los gastos de funcionamiento, aunque se mantiene en un nivel menor.	Existe un aumento moderado en los gastos de funcionamiento.	Existe un incremento notable en los gastos de funcionamiento.	Se registra un alza desmedida de los gastos de operación, excediendo la capacidad de gestión presupuestaria.
IMPACTO EN EL RENDIMIENTO O PRODUCTIVIDAD (Severidad 3)	Sobrecarga de trabajo: El volumen de trabajo mensual para el personal de la DSA experimenta un incremento inferior al 10%.	El volumen de trabajo mensual para el personal de la DSA aumenta hasta un 30%.	El volumen de trabajo mensual para el personal de la DSA aumenta hasta un 50%.	El volumen de trabajo mensual para el personal de la DSA aumenta hasta un 70%.	El volumen de trabajo mensual para el personal de la DSA se duplica o supera el 100%.
	Suspensión del suministro del servicio: Las operaciones en la DSA experimentan una pausa de hasta 4 horas.	Las operaciones en la DSA se interrumpen en un rango de 5 a 10 horas.	Las operaciones en la DSA se detienen en un rango de 11 a 16 horas.	Las operaciones en la DSA se suspenden en un rango de 17 a 24 horas.	Las operaciones en la DSA superan el día completo sin operaciones.
	Daño a la funcionalidad: Se ve afectado el funcionamiento correcto de un componente particular del sistema de gestión académica.	Se ve afectado el funcionamiento correcto de múltiples componentes del sistema de gestión académica.	Se ve afectada la plataforma de gestión académica completa, con posibilidad de reestablecimiento rápido.	Se ve afectada la plataforma de gestión académica completa, con posibilidad de reestablecimiento en un tiempo considerable.	Se ve afectada la plataforma de gestión académica completa, sin opción de restablecimiento al instante.
IMPACTO EN LA ADMINISTRACIÓN (Severidad 1)	Infracciones a la normativa o a los procedimientos internos: Genera infracciones que conllevan a llamadas de atención orales.	Genera infracciones que conllevan a amonestaciones documentadas.	Genera infracciones que conllevan a reducciones de méritos laborales.	Genera infracciones que conllevan a la apertura de expedientes sancionadores.	Genera infracciones que conllevan a penalizaciones impuestas por organismos reguladores o el cuerpo de fiscalización interno.

Fuente: Fuente: Elaborado en base a la guía OCTAVE-S Implementation Guide. Critical Asset Worksheets for System

E. Establecimiento de los escenarios de riesgo potencial

E.1. Identificación de recursos vitales

Se han catalogado como activos esenciales aquellos elementos críticos para el cumplimiento de los fines y las diferentes etapas de la gestión académica, en concordancia con el cronograma universitario anual. La evaluación de su relevancia se fundamentó en la función irremplazable que cumplen y en su valor estratégico para la Universidad, con un énfasis particular en el ámbito académico.

Los activos identificados como críticos son:

1. El Sistema de Información Académico (SIA).
2. El Servicio de administración de la base de datos que soporta dicho sistema.
3. La barrera de seguridad perimetral (Firewall).
4. El personal clave encargado de la administración de la red, las comunicaciones y el centro de procesamiento de datos.

Estos recursos han sido clasificados mediante una tabla que detalla los criterios específicos que justificaron su selección como elementos críticos.

Tabla 4. Clasificación de activos críticos y criterios de selección

Designación del recurso	Justificación de la criticidad
Sistema de Información Académico (SIA)	Por su función vital: Este activo se considera crítico porque sirve de soporte a los procedimientos centrales de la gestión académica universitaria. Es utilizado por las autoridades, unidades, docentes y estudiantes.
Servicio de gestión de base de datos – SIA	Por interdependencia operacional: Este recurso es crucial, ya que un fallo en su operación detendría de forma inmediata todos los procedimientos académicos que dependen de la plataforma SIA.
Barrera de seguridad perimetral (Firewall)	Por su rol de defensa: Su función es indispensable, ya que de no estar operativo, la seguridad de toda la Red telemática de la Universidad se vería comprometida. Es la principal línea de defensa.
Administrador de la red, comunicaciones y centro de datos	Por experiencia insustituible: Es el profesional esencial para garantizar la continuidad, el mantenimiento y el funcionamiento sin interrupciones de toda la infraestructura tecnológica y de comunicaciones.

E.2. Establecimiento de las exigencias de seguridad

La siguiente tabla define los requerimientos de protección específicos que la Universidad ha determinado deben aplicarse a cada uno de sus recursos más importantes.

Estos requerimientos se han agrupado y categorizado conforme a los tres pilares de la seguridad de la información: Confidencialidad (C), Integridad (I) y Disponibilidad (D). Adicionalmente, se identifica el criterio que representa la máxima prioridad para la protección de cada activo seleccionado.

Tabla 5. Exigencias de seguridad sobre los activos

Requerimiento de protección	Sistema de información académico (SIA)	Servicio de gestión de base de datos – SIA	Barrera de seguridad perimetral (Firewall)	Administrador de red, comunicaciones y centro de datos
Confidencialidad (C)	Es necesaria para proteger la privacidad de los datos académicos.	Se requiere para asegurar que solo el personal autorizado acceda a las backups y la información reservada.	Se requiere para proteger la información que transita a través de los enlaces de comunicación de la red.	Es vital que el administrador mantenga la discreción sobre la arquitectura de la red y los secretos de acceso.
Integridad (I)	Es fundamental para asegurar que los datos del estudiante no sean alterados sin autorización.	Es esencial para garantizar que las bases de datos de producción y respaldo sean correctas y veraces.	Es necesaria para garantizar que la información que atraviesa la red no sea modificada.	Es vital que el administrador no altere la configuración sin autorización y garantice la calidad de los datos.
Disponibilidad (D)	Es necesaria para asegurar que el sistema esté accesible a los usuarios clave cuando se requiere (ej. matrícula).	Es fundamental para garantizar que el servicio de base de datos se mantenga operativo sin interrupciones.	Es esencial para que la protección de la red esté activa en todo momento.	Es vital que el administrador esté disponible para solucionar cualquier inconveniente de la infraestructura.
Máxima prioridad de seguridad	**Integridad**	**Disponibilidad**	**Disponibilidad**	**Disponibilidad**

F. Análisis de riesgos: perfiles de amenazas para activos críticos

A continuación, se presenta una tabla que detalla el perfil de los riesgos potenciales (amenazas) identificados para tres activos fundamentales de la gestión académica, basándose en la revisión de su historial de ocurrencia y la forma en que se manifiestan. Este análisis forma parte de la primera fase del proceso de gestión de riesgos.

Tabla 6. Perfiles de amenazas para activos críticos

Activo crítico	Categoría de amenaza	Actor/Tipo de amenaza	Frecuencia histórica	Manifestación del riesgo
Sistema de Información Académico (SIA)	Personas / Acceso por red	Accidental interna	Muy Alta (> 9 veces/año)	Fallos generados por la personas internas de la universidad (administrativos, docentes, alumnos) debido a desconocimiento o errores al ingresar o modificar información, realizando un mal registro de la información.
		Intencionada interna	Moderada (4-6 veces/año)	Ataques enfocados a alterar deliberadamente las calificaciones o el historial académico de los estudiantes, o causar la Paralización de actividades.
		Accidental externa	No aplica	No aplica
		Intencionada externa	Moderada (4-6 veces/año)	Personas ajenas a la universidad que buscan sabotear el funcionamiento del sistema en periodos clave o divulgar información sensible.
	Personas / Acceso físico	Accidental interna	Baja (1-3 veces/año)	Errores cometidos por el personal técnico al manipular el sistema (fallos en el diseño o codificación) que pueden derivar en la interrupción de algún proceso académico.
		Intencionada interna	Baja (1-3 veces/año)	El personal técnico administrativo, aprovechando su acceso privilegiado, puede ejecutar ataques focalizados en el código fuente del sistema. El riesgo se manifiesta en la modificación del código fuente del sistema o su sustracción de manera no autorizada, generalmente mediante la inserción de código malicioso.

		Accidental externa	No aplica	No aplica
		Intencionada externa	Baja (1-3 veces/año)	Personas externas a la universidad consiguen acceso no autorizado a los archivos de programación del sistema. Su objetivo principal es la manipulación o el hurto del código fuente, ejecutando ataques focalizados mediante la inyección de software malicioso en la plataforma
	Problemas técnicos	Diseño inadecuado	Alta (7-9 veces/año)	Dificultades por cambios implementados de manera inadecuada, causadas por la interdependencia no correcta entre el sistema propio (Gestac) y el producto adquirido para la gestión académica (SIA).
		Falta de compatibilidad	Alta (7-9 veces/año)	Inoperatividad de la aplicación en producción debido a la especificación incorrecta de requerimientos funcionales o no funcionales.
		Obsolescencia funcional	Baja (1-3 veces/año)	Existe el riesgo de fallo funcional o de grave inconsistencia de datos en el Sistema de Información Académica (SIA), ya que los cambios en los procesos, reglamentos o políticas institucionales no se adaptan e implementan en el software de manera oportuna, haciendo que el sistema opere bajo normativas obsoletas
		Falta de control de calidad	Media (4-6 veces/año)	Debido a la ausencia de pruebas de calidad exhaustivas antes de la puesta en producción, existe la posibilidad de que los cambios en el software de gestión académica contengan errores funcionales o de seguridad, lo que podría resultar en la interrupción de procesos críticos o la pérdida/corrupción de datos. Así mismo, la omisión de la validación de cambios en el software en producción incrementa la probabilidad de introducir fallas no detectadas, lo que podría comprometer la integridad de los registros académicos y la confiabilidad del sistema
	Problemas de soporte/Incidentes	Caída del suministro eléctrico	Muy Alta (> 9 veces/año)	Interrupciones constantes en el suministro de energía eléctrica debido a la ausencia de un sistema de energía ininterrumpida (UPS) o alternativo adecuado.
		Interrupciones en conectividad	Alta (7-9 veces/año)	Caídas del servicio de red provocadas por la capacidad limitada, la obsolescencia o el mantenimiento deficiente de los equipos de comunicación.
		Servicio de terceros deficiente	Baja (1-3 veces/año)	Debido a los procesos engorrosos y burocráticos en la contratación o solicitud de servicios a terceros (proveedores), existe el riesgo de que la atención y resolución de incidentes críticos que afectan al Sistema de Información Académica (SIA) o a la infraestructura tecnológica de soporte sea tardía. Esto resulta en una respuesta no oportuna a los problemas, lo cual puede provocar una interrupción prolongada de las operaciones y una disminución en la calidad del servicio académico
		Desastres naturales	Baja (1-3 veces/año)	Existe el riesgo de que la infraestructura de Red sufra un daño o afectación debido a que la Universidad se encuentra en una zona expuesta anualmente a lluvias intensas o a la ocurrencia del Fenómeno del Niño, lo cual resultaría en la interrupción total o parcial de los servicios y procesos esenciales de la gestión académica
Servicio de Gestión de Base de Datos – SIA	Personas / Acceso por red	Accidental interna	Media (4-6 veces/año)	La ejecución de modificaciones directas en la base de datos por fuera de la capa de aplicación (sistema) representa un riesgo de Alto Impacto en la Integridad de la información, ya que existe una alta probabilidad de incurrir en errores, inconsistencias y/o incompatibilidad de los datos
		Intencionada interna	Muy Alta (> 9 veces/año)	Ataques con el objetivo de modificar las calificaciones o el historial académico de los estudiantes.
		Accidental externa	No aplica	No aplica
		Intencionada externa	Muy Alta (> 9 veces/año)	Intentos de acceso no autorizado con fines de sustracción o manipulación de datos sensibles, o para

				interrumpir el sistema en fechas cruciales.
	Personas / Acceso físico	Accidental interna	Baja (1-3 veces/año)	El riesgo se manifiesta a través de las acciones del personal con acceso a nivel de infraestructura, combinando el personal administrativo de gestión académica y el personal de Tecnologías de la Información (TI), quienes poseen permisos para acceder y modificar directamente la base de datos o su estructura. Las acciones son de alteración de datos críticos y comprometiendo la estructura de la base de datos que afectan negativamente su compatibilidad o integridad con las aplicaciones académicas.
		Intencionada interna	Baja (1-3 veces/año)	Actores internos con acceso privilegiado (personal de gestión académica y técnicos de TI) que aprovechan sus facultades para alterar la arquitectura de datos o los registros directamente, buscando su modificación malintencionada o sustracción no autorizada. El foco de los ataques se dirige a la manipulación directa de los registros en el sistema central de datos o a la extracción clandestina de información sensible
	Problemas técnicos	Diseño inadecuado	Alta (7-9 veces/año)	Riesgo de inconsistencia y error de la información académica debido a la diferente estructura de datos entre los dos sistemas de información académica (Gestac y SIA), lo que obliga a realizar procesos manuales para la generación de informes y reportes, resultando en errores operativos e inconsistencias críticas en los datos
		Falta de mantenimiento	Alta (7-9 veces/año)	La negligencia técnica de mantenimiento incrementa la vulnerabilidad a fallas de servicio, lo que conlleva a un alto riesgo de interrupción del proceso y la consecuente degradación de la disponibilidad del Sistema de Información Académica (SIA). Esta carencia de mantenimiento eleva significativamente la probabilidad de que ocurran alteraciones o corrupción de los registros académicos, comprometiendo la integridad de la información esencial y, en el peor de los casos, derivando en una pérdida permanente de datos si las rutinas de respaldo se ven afectadas por la misma deficiencia de gestión
		Consultas ineficientes	Baja (1-3 veces/año)	La ejecución de consultas SQL ineficientes o mal optimizadas sobre las bases de datos académicas constituye un riesgo. Este problema técnico incrementa la carga de trabajo del servidor de bases de datos, lo que se traduce directamente en un riesgo muy alto de interrupción del proceso de gestión académica. La sobrecarga generada puede provocar tiempos de respuesta excesivamente lentos o, en el peor de los casos, la paralización completa del servicio de gestión de bases de datos, afectando la disponibilidad de la información para los usuarios finales (estudiantes, docentes y personal administrativo) y comprometiendo la operación en momentos clave como matrículas o registro de notas
		Falta de control de calidad	Media (4-6 veces/año)	La deficiencia en la supervisión de la calidad de los datos incrementa significativamente la probabilidad de inexactitud o inconsistencia en los registros de estudiantes, notas y planes de estudio, lo que a su vez se traduce en un alto riesgo de fallas operacionales que obligan a la interrupción del proceso de gestión académica para realizar correcciones manuales. La falta de control de calidad afecta la integridad de la información crítica, generando desconfianza en los usuarios, exponiendo a la institución a posibles incumplimientos normativos y a consecuencias administrativas derivadas de la toma de decisiones basada en datos incorrectos.
	Problemas de soporte/Incidentes	Problemas con servicio de hosting	Baja (1-3 veces/año)	La dependencia de un servicio de hosting externo deficiente representa un riesgo significativo para la disponibilidad del SIA y su base de datos. Cualquier falla operativa, degradación del rendimiento o interrupción total en la plataforma de hosting

				compromete directamente la continuidad de los procesos académicos. Esto podría manifestarse como una paralización prolongada de actividades críticas (matrículas, registro de notas), afectando gravemente la confianza de los usuarios. Además, si la gestión de la seguridad o de las copias de respaldo en el servicio de hosting es inadecuada, existe un riesgo latente de pérdida de datos o exposición de información confidencial ante un incidente de seguridad o desastre.
		Interrupciones en conectividad	Alta (7-9 veces/año)	El riesgo de interrupciones en la conectividad con la base de datos académica afecta la disponibilidad del SIA, ya que cualquier fallo en la infraestructura de red o en los enlaces de comunicación paraliza inmediatamente las operaciones esenciales de la gestión académica. Esto conlleva a una interrupción prolongada del servicio para estudiantes, docentes y personal administrativo, sino que también incrementa la probabilidad de inconsistencia de la información (compromiso de la integridad) debido a transacciones incompletas o fallos al guardar datos. Esta inestabilidad en la conexión impacta negativamente la confianza del usuario y dificulta el cumplimiento de los calendarios académicos y normativas institucionales
		Limitaciones en capacidad de almacenamiento	Baja (1-3 veces/año)	La insuficiencia de espacio de almacenamiento en la base de datos académica representa un riesgo de alta severidad para la disponibilidad y continuidad del servicio. Esta limitación provoca que el SIA quede paralizado de forma abrupta, resultando en una interrupción total e impredecible del proceso de gestión académica. La consecuencia es la detención de las matrículas, el registro de notas y cualquier otra transacción crítica, lo cual genera un deterioro inmediato en la productividad y un impacto negativo en la reputación de la institución.
		Desastres naturales	Baja (1-3 veces/año)	La ubicación geográfica de la Universidad en una zona propensa a lluvias intensas anuales y a la recurrencia de eventos como el Fenómeno del Niño constituye un riesgo ambiental significativo y recurrente. Este factor climático representa una amenaza directa a la infraestructura de TI, ya que la afectación a cualquiera de sus componentes físicos puede desencadenar una paralización súbita de servicios. Esto se traduce en la interrupción crítica e involuntaria de los procesos esenciales de la gestión académica, comprometiendo la disponibilidad y continuidad operativa de las actividades universitarias.
Barrera de seguridad perimetral (Firewall)	Personas por red	Accidental interna	Baja (1-3 veces/año)	Este riesgo se materializa típicamente cuando un usuario interno descarga o instala, sin la debida autorización o conocimiento, software que contiene código malicioso o malware. La ejecución de este código infectado afecta directamente la configuración o el software operativo del Firewall, comprometiendo su funcionamiento adecuado e introduciendo brechas de seguridad que podrían ser explotadas por actores externos.
		Intencionada interna	Muy Alta (> 9 veces/año)	Este riesgo se manifiesta a través de diversas acciones maliciosas que buscan anular los controles de seguridad, tales como: la inyección de código dañino (malware) directamente a través de la red interna; el robo de credenciales o suplantación de identidad para obtener permisos privilegiados; la inhibición de los controles de acceso y monitoreo del Firewall para dejar la red desprotegida; o la orquestación de ataques de denegación de servicio distribuido (DDoS) que sobrecarguen la capacidad del equipo, resultando en la paralización total de la conectividad y de los procesos académicos críticos,
		Accidental interna	No aplica	No aplica
		Intencionada	Media (4-6	Esta amenaza crítica se manifiesta de diversas

		externa	veces/año)	maneras, incluyendo la inyección de código malicioso o malware a través de la red para la explotación de vulnerabilidades, la suplantación de identidad para evadir los controles de acceso, la inhibición maliciosa de los sistemas de seguridad que anulan las protecciones del dispositivo, o la saturación intencionada de la infraestructura mediante ataques de Denegación de Servicio Distribuido (DDoS), lo que tiene como consecuencia directa la paralización completa de las comunicaciones y, por ende, de todos los procesos de gestión académica
	Personas / Acceso físico	Accidental interna	Baja (1-3 veces/año)	El firewall (o barrera perimetral de seguridad) de la universidad enfrenta un riesgo crítico derivado de errores humanos y malas prácticas cometidas por el propio personal interno durante la gestión o interacción física con el equipo. Se ha documentado que estas acciones, realizadas de forma accidental o por descuido, han resultado en la modificación incorrecta de la configuración del sistema o han generado su indisponibilidad total de funcionamiento, comprometiendo gravemente la protección de la infraestructura de red y elevando el peligro de intrusión o interrupción del proceso para los servicios académicos y administrativos
	Problemas técnicos	Obsolescencia del software	Media (4-6 veces/año)	La falta de actualizaciones en sistemas operativos, bases de datos (como el SIA o el servicio de gestión de base de datos) o firmware del Firewall introduce vulnerabilidades conocidas que pueden ser explotadas fácilmente. El riesgo principal es la paralización total o parcial de las actividades académicas (matrículas, registro de notas, emisión de actas), pues el software antiguo es propenso a fallos, caídas de servicio o a ser el objetivo de malware avanzado que el software de seguridad obsoleto no puede detectar,
		Contraseñas mal administradas	Media (4-6 veces/año)	El riesgo directo es el acceso no autorizado por parte de actores internos o externos que logran ingresar al Sistema de Información Académica (SIA) o la base de datos. Esto permite la develación de información confidencial (datos personales de estudiantes, historial académico) o la alteración maliciosa de registros (cambio de notas o estado de matrícula), comprometiendo la integridad y la confianza en la institución
		Mala configuración	Media (4-6 veces/año)	Una configuración incorrecta en componentes clave (como servidores, routers o el Firewall) crea brechas de seguridad involuntarias. El riesgo es que estas configuraciones defectuosas se conviertan en puntos de entrada para ataques que resulten en la fuga de información académica hacia terceros o en la interrupción forzada del servicio (Denegación de Servicio o DoS), afectando la disponibilidad de la plataforma.
		Reglas muy permisivas	Media (4-6 veces/año)	El riesgo se materializa cuando las reglas de acceso en el Firewall son demasiado amplias. Esto anula su propósito, permitiendo que el tráfico malicioso (por ejemplo, ransomware o spyware) acceda a la red interna y se propague. El riesgo final es una infección masiva o un ataque que cause una interrupción prolongada e incontrolada de todos los servicios académicos soportados por la infraestructura de red.
	Problemas de soporte/Incidentes	Antimalware ineficiente	Media (4-6 veces/año)	La ineficacia del sistema antimalware permite que amenazas de software malicioso supere las defensas del firewall y acceda a la red interna. El malware se propaga a los servidores del SIA y la base de datos, causando una interrupción crítica de las actividades académicas y poniendo en riesgo la integridad y disponibilidad de la información (notas, matrículas, historiales)
		Mala definición de objetos de	Alta (7-9 veces/año)	Por desconocimiento o configuración errónea, el firewall no logra identificar correctamente los

		red		dispositivos o segmentos de la red (objetos). Genera vías de acceso no intencionadas (develación de información) o, inversamente, bloquea el acceso legítimo (Interrupción del proceso) a los servicios críticos como el SIA, afectando la funcionalidad operativa diaria.
		Limitaciones en la capacidad de protección	Media (4-6 veces/año)	El hardware o software del firewall es superado por la sofisticación o el volumen de ataques, como ataques de denegación de servicio o exploits avanzados. El servicio de defensa perimetral colapsa, resultando en una interrupción total e inmediata del proceso académico en línea. Esto conlleva el impacto en negativo sobre la Reputación, Productividad y Administrativo de la institución
		Desastres naturales	Baja (1-3 veces/año)	Los fenómenos naturales causan daños directos al equipo del firewall o a su entorno operativo. Interrumpe de manera prolongada de la conectividad y de los procesos académicos. Genera un impacto económico alto debido al costo de reemplazo del equipo y los sistemas de comunicaciones dañados, además de la potencial pérdida de información si el desastre afecta los respaldos.

El análisis de amenazas que se muestra en la tabla anterior muestra los siguientes escenarios de riesgos con mayor criticidad:

Sistema de Información Académico (SIA)

El SIA, al ser el soporte de los procesos principales, concentra las amenazas más críticas en su disponibilidad e integridad, con una frecuencia de ocurrencia muy alta.

- El riesgo más frecuente y constante (Muy Alta: > 9 veces/año) tiene su origen en las Personas internas (administrativos, docentes, alumnos) que, por desconocimiento o error, cometen fallos al manipular la información, lo que se manifiesta como mal registro o modificación de datos, afectando la integridad del sistema.
- En el mismo nivel de criticidad por su frecuencia (Muy Alta), pero originado en la infraestructura, se encuentra el riesgo de caída del suministro eléctrico, cuya fuente es el soporte deficiente (ausencia de UPS adecuado), que provoca interrupciones constantes y compromete la disponibilidad.
- Otros riesgos importantes se originan en los Problemas Técnicos con una frecuencia Alta (7-9 veces/año), como el diseño inadecuado y la falta de compatibilidad entre el SIA y sistemas antiguos, lo que se manifiesta como inoperatividad de la aplicación.
- Finalmente, los ataques intencionados (internos y externos), aunque de frecuencia Moderada (4-6 veces/año), buscan alterar deliberadamente calificaciones o sabotear el funcionamiento en periodos clave.

Servicio de Gestión de Base de Datos – SIA

El servicio de base de datos es el activo más vulnerable a las amenazas intencionales y técnicas de alta frecuencia, que atentan directamente contra la confidencialidad e integridad de los datos.

- La amenaza más crítica y de mayor frecuencia (Muy Alta: > 9 veces/año) proviene de las Personas con intenciones maliciosas, tanto internas como externas, que buscan modificar calificaciones o sustraer datos sensibles a través de la red, comprometiendo gravemente la confianza y la integridad.
- En un nivel de criticidad cercano (Alta: 7-9 veces/año), las amenazas de Problemas Técnicos y de Soporte son constantes: la falta de mantenimiento y el diseño inadecuado (por la diferente estructura de datos con sistemas antiguos) incrementan el riesgo de corrupción de registros e inconsistencia de la información que requiere procesos manuales. A esto se suma el riesgo de interrupciones en la conectividad, que afecta la disponibilidad del servicio.
- Riesgos con alto potencial de daño, pero menor frecuencia (Baja: 1-3 veces/año), incluyen la ejecución de consultas ineficientes que paralizan el servidor (Problemas Técnicos) y la manipulación física o sustracción de la arquitectura de datos por personal técnico con acceso privilegiado (Personas/Acceso Físico).

Barrera de seguridad perimetral (Firewall)

La criticidad del Firewall radica en que su compromiso afecta la seguridad de todos los demás activos, siendo la amenaza intencional interna su punto de fallo más frecuente.

- La amenaza más crítica y recurrente (Muy Alta: > 9 veces/año) se origina en actores internos con intención maliciosa que aprovechan la red para inyectar código dañino, robar credenciales o realizar ataques de Denegación de Servicio (DDoS), buscando la paralización total de la red y, por ende, de todos los procesos académicos.
- En una categoría de riesgo Alto (7-9 veces/año), los Problemas de Soporte por la mala definición de objetos de red comprometen la efectividad del Firewall. Este fallo se manifiesta como la generación de vías de acceso no intencionadas para la fuga de información o el bloqueo del acceso legítimo al SIA.
- Las amenazas por Problemas Técnicos como la obsolescencia del software, el uso de contraseñas mal administradas, y la mala configuración o reglas muy permisivas tienen una frecuencia Moderada (4-6 veces/año). Estas fallas crean brechas de seguridad que facilitan la fuga de información y la propagación de malware.
- Por último, el riesgo de Desastres Naturales y errores accidentales internos por acceso físico se consideran de baja frecuencia (1-3 veces/año), pero su manifestación es la indisponibilidad total del firewall, lo cual implica un alto impacto en la continuidad operativa.

3.2. Identificación de vulnerabilidades de la infraestructura (Fase 2 de OCTAVE)

Esta etapa corresponde a la Fase 2: Identificar Vulnerabilidades de la Infraestructura (o Identify Infrastructure Vulnerabilities) de la metodología OCTAVE. Su objetivo principal es examinar las debilidades tecnológicas presentes en la infraestructura de soporte que podrían

ser explotadas por las amenazas para impactar los activos críticos. Se trata de identificar los puntos débiles que sirven como ruta de acceso para los riesgos, enfocándose en los servidores, equipos de comunicación, terminales y el personal responsable de estos.

A continuación, se presenta la tabla de vulnerabilidades identificadas en los componentes tecnológicos que dan soporte a los activos críticos de la gestión académica.

Tabla 7. Catálogo de vulnerabilidades en la infraestructura de soporte de activos críticos

Componente tecnológico	**Fallas o puntos débiles (Vulnerabilidades)**	**Responsable de Uso/Custodia**	**Ubicación**	**Activo crítico afectado**
¿Cuál es el recurso tecnológico clave que sustenta la operación de los activos esenciales?	¿Qué vulnerabilidades o fallos existen que podrían ser aprovechados por las amenazas para alcanzar los activos cruciales?	¿A qué personal interno corresponde la responsabilidad de utilizar y salvaguardar el componente tecnológico?	¿Cuál es la localización física del componente tecnológico?	¿Qué recurso esencial podría ser comprometido por la debilidad encontrada?
Servidor de base de datos	Asignación y uso inapropiado de credenciales de acceso.	Personal Administrativo de Aplicaciones/BD	Sala de servidores - Centro de datos	SIA, Servicio de Gestión de BD
Servidor de aplicaciones	Empleo de software sin licencia (pirata) o desactualizado.	Personal Administrativo de Aplicaciones/BD	Sala de servidores - Centro de datos	SIA, Servicio de Gestión de BD
Servidor antimalware	Sistema de protección antimalware desactualizado e inefectivo.	Personal Administrativo de Aplicaciones/BD	Sala de servidores - Centro de datos	SIA, Servicio de Gestión de BD, Firewall
Switch central	Configuración de los puertos y las VLANs realizada sin los debidos procedimientos de seguridad.	Personal Administrativo de Red	Sala de servidores - Centro de datos	SIA, Servicio de Gestión de BD, Firewall
Dispositivos wireless	Falta de control y permisos en el acceso a la red inalámbrica.	Personal Administrativo de Red	Oficinas/Unidades	SIA, Servicio de Gestión de BD, Firewall
Terminales de trabajo (pc de oficina)	Uso de contraseñas débiles y falta de protección por parte del antivirus.	Personal Operativo	Oficinas/Unidades	SIA, Servicio de Gestión de BD
Dispositivos de almacenamiento de respaldo	Almacenamiento de copias de seguridad en un lugar fácilmente accesible por personal no autorizado.	Personal Administrativo de Aplicaciones/BD	Sala de servidores - Centro de datos	SIA, Servicio de Gestión de BD
Personal administrativo de red, comunicaciones y centro de datos	Incumplimiento de las competencias exigidas para el rol, lo que afecta la gestión de la seguridad de la infraestructura.	Personal Administrativo de Red	Sala de servidores - Centro de datos	Administrador de Red

La tabla detalla que las vulnerabilidades se concentran en tres áreas principales: servidores, equipos de comunicación y personal.

- En el área de servidores y bases de datos, las debilidades se relacionan con las prácticas de seguridad lógica, como la deficiencia en la gestión de credenciales y la instalación de software sin licencia o desactualizado. Un punto crítico es el Servidor Antimalware, cuyo estado de desactualización afecta directamente a la protección de los tres activos tecnológicos principales: el Sistema de Información Académico (SIA), el Servicio de Base de Datos y el Firewall.

- En cuanto a los equipos de comunicación, tanto el Switch Central como los Dispositivos Wireless presentan vulnerabilidades de configuración y control de acceso. Esto implica que la segmentación de la red y el acceso inalámbrico no cumplen con los protocolos de seguridad necesarios, dejando rutas abiertas para posibles ataques. Las terminales de trabajo también son un eslabón débil debido a la falta de antivirus robustos y el uso de contraseñas fáciles de adivinar por parte del personal operativo.
- Finalmente, el factor humano es considerado una vulnerabilidad directa. Se identifica que la persona responsable de la administración de la infraestructura de red carece de las competencias completas requeridas para el puesto, lo que se convierte en un riesgo para la Disponibilidad y la Integridad de toda la infraestructura crítica.

3.3. Análisis del Impacto (Fase 3 de OCTAVE)

La actividad descrita en el documento adjunto corresponde a la Fase 3: Análisis de Impacto y Riesgo (Analyze Risk en la metodología OCTAVE).

El objetivo central de esta fase es cuantificar las consecuencias que las amenazas previamente identificadas producirían sobre los activos críticos, si lograran materializarse a través de las vulnerabilidades existentes. Se utiliza la escala de valoración de impactos (que incluye reputación, finanzas, productividad y gestión administrativa) definida por la organización para asignar un nivel de severidad a cada riesgo potencial. Este análisis permite a la organización priorizar qué riesgos deben ser mitigados con mayor urgencia.

3.3.1. Análisis consolidado del impacto de las amenazas sobre el Sistema de Información Académica (SIA)

El siguiente cuadro resume el resultado del análisis de impacto de diversas categorías de amenazas que podrían afectar el activo crítico Sistema de Información Académica (SIA). Los niveles de impacto se valoran en una escala cualitativa: Muy Bajo (1), 2, 3, 4 y 5.

Tabla 8. Consolidado del impacto de las amenazas sobre el Sistema de Información Académica (SIA)

Categoría de amenazan origen de la amenaza	Evento de riesgo potencial	Impacto en la imagen o credibilidad del usuario (confianza)	Consecuencia económica	Impacto en el rendimiento o productividad (productividad)	Impacto en la administración
Personas / Acceso por red - Accidental interna	Alteración de registros	Muy alto	Bajo	Alto	Alto
	Eliminación de datos	Muy alto	Bajo	Alto	Alto
Personas / Acceso por red – Intencionada interna	Exposición de datos	Muy alto	Alto	Muy alto	Alto
	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
	Paralización de actividades	Muy alto	Alto	Muy alto	Alto
Personas / Acceso por red – Intencionada externa	Exposición de datos	Muy alto	Alto	Muy alto	Alto
	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
	Paralización de actividades	Muy alto	Alto	Muy alto	Alto
Personas / Acceso físico – Accidental interna	Alteración de registros	Muy alto	Bajo	Alto	Alto
	Paralización de actividades	Alto	Bajo	Alto	Alto
Personas / Acceso físico - Intencionada interna	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
Personas / Acceso físico - Intencionada externa	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
Problemas técnicos / Diseño inadecuado	Eliminación de datos	Muy alta	Alta	Alta	Medio
	Paralización de actividades	Muy alta	Muy alta	Muy alta	Medio
Problemas técnicos / Falta de compatibilidad	Alteración de registros	Alta	Alta	Muy alta	Medio
	Paralización de actividades	Alta	Alta	Muy alta	Medio
Problemas técnicos / Obsolescencia funcional	Paralización de actividades	Alta	Medio	Muy alta	Medio
Problemas técnicos / Falta de control de calidad	Alteración de registros	Alta	Bajo	Alta	Medio
	Eliminación de datos	Alta	Bajo	Alta	Medio
Problemas de soporte / Caída del suministro eléctrico	Eliminación de datos	Muy alta	Alta	Alta	Medio
	Paralización de actividades	Muy alta	Alta	Alta	Medio
Problemas de soporte / Interrupciones en conectividad	Paralización de actividades	Muy alta	Alta	Alta	Medio
Problemas de soporte / Servicio de terceros deficiente	Alteración de registros	Alta	Alta	Muy alta	Muy alta
	Paralización de actividades	Muy alta	Alta	Muy alta	Muy alta
Problemas de soporte / Desastres naturales	Eliminación de datos	Medio	Muy alta	Muy alta	Medio
	Paralización de actividades	Medio	Muy alta	Muy alta	Medio

El análisis de impacto muestra que la afectación a la reputación y la confianza del usuario es el criterio de mayor severidad en casi todos los escenarios donde interviene el factor humano.

a. Impactos de máxima severidad (Muy Alto)

La mayor severidad del impacto recae en escenarios que comprometen la integridad de los datos y la continuidad del servicio, afectando la credibilidad y la capacidad operativa.

- El factor humano malintencionado, tanto interno como externo (a través de red o acceso físico), genera los impactos más uniformemente severos. Todos los riesgos bajo esta categoría (Exposición, Alteración, Eliminación de datos y Paralización de actividades) alcanzan simultáneamente un nivel Muy Alto en la reputación o confianza del usuario y en el impacto en el rendimiento o productividad. Esto subraya que la acción deliberada daña de manera crítica la credibilidad y paraliza las operaciones académicas.
- La paralización de actividades causada por Problemas técnicos / Diseño inadecuado o por Problemas de soporte / Desastres naturales provoca la máxima afectación sobre la consecuencia económica y el impacto en el rendimiento o productividad.
- La paralización de actividades debida a un servicio de terceros deficiente es el único riesgo que provoca un impacto Muy Alto de forma dual en el Impacto en el rendimiento o productividad y en el Impacto en la administración (debido a potenciales incumplimientos contractuales y normativos).
- Los eventos de alteración de registros y paralización de actividades generados por la falta de compatibilidad u obsolescencia funcional del software concentran su máxima afectación en el Impacto en el rendimiento o productividad.

b. Impactos de menor severidad (Bajo y Medio)

La menor severidad se observa en los criterios de Consecuencia económica e Impacto en la administración en escenarios de errores no intencionales.

- La consecuencia económica es el criterio menos afectado (nivel Bajo) cuando el riesgo se origina en un error o accidente de un Personal Interno (por red o acceso físico) que deriva en la alteración o eliminación de registros.
- En la mayoría de los escenarios derivados de problemas técnicos (diseño, compatibilidad, obsolescencia, falta de control de calidad) y problemas de soporte (caída de energía, conectividad, desastres naturales), el impacto en la administración registra consistentemente un nivel Medio. Este nivel solo se eleva a Muy Alto en el caso de la interrupción del servicio por un servicio de terceros deficiente, lo que implica procesos administrativos disciplinarios o sanciones de entes supervisores.

- En relación a la consecuencia económica, aunque generalmente es Alta en la mayoría de los fallos técnicos y de soporte, se sitúa en nivel Bajo solo en las amenazas accidentales del personal interno y en la Alteración/Eliminación de datos por Falta de control de calidad.

3.3.2. Análisis consolidado del impacto de las amenazas sobre el Servicio de gestión de base de datos

El siguiente cuadro consolida la evaluación del nivel de impacto de diversas categorías de amenazas que podrían afectar al activo crítico Servicio de Gestión de Base de Datos. La valoración se realiza sobre cuatro ejes de afectación definidos por la organización: Reputación del Usuario, Consecuencia Financiera, Deterioro Operacional (Productividad) e Implicación Administrativa/Normativa, utilizando una escala de severidad que va desde Muy Bajo hasta Muy Alto.

Tabla 9. Consolidado del impacto de las amenazas sobre el Servicio de Gestión de Base de Datos

Categoría de amenazan origen de la amenaza	Evento de riesgo potencial	Impacto en la imagen o credibilidad del usuario (confianza)	Consecuencia económica	Impacto en el rendimiento o productividad (productividad)	Impacto en la administración
Personas / Acceso por red - Accidental interna	Alteración de registros	Muy alto	Bajo	Alto	Alto
	Eliminación de datos	Muy alto	Bajo	Alto	Alto
Personas / Acceso por red – Intencionada interna	Develación de datos	Muy alto	Alto	Muy alto	Alto
	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
Personas / Acceso por red – Intencionada externa	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
	Paralización de actividades	Muy alto	Alto	Muy alto	Alto
Personas / acceso físico - Accidental interna	Alteración de registros	Muy alto	Bajo	Alto	Alto
	Paralización de actividades	Alto	Bajo	Alto	Alto
Personas / acceso físico - Intencionada interna	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Eliminación de datos	Muy alto	Alto	Muy alto	Alto
Problemas técnicos / diseño inadecuado	Alteración de registros	Medio	Medio	Alto	Medio
	Eliminación de datos	Medio	Medio	Alto	Medio
	Paralización de actividades	Medio	Medio	Alto	Medio
Problemas técnicos / Falta de mantenimiento	Alteración de registros	Alto	Medio	Alto	Medio
	Paralización de actividades	Alto	Medio	Alto	Medio
Problemas técnicos / Consultas ineficientes	Paralización de actividades	Muy alta	Medio	Muy alta	Medio
Problemas técnicos / Falta de control de calidad	Alteración de registros	Alta	Bajo	Alta	Medio
	Eliminación de datos	Alta	Bajo	Alta	Medio
Problemas de soporte / Problemas con servicio de hosting	Paralización de actividades	Muy alta	Alto	Muy alta	Alto
Problemas de soporte / Fallas en conectividad	Paralización de actividades	Muy alta	Medio	Alto	Alto
Problemas de soporte / Limitaciones en capacidad de almacenamiento	Paralización de actividades	Muy alta	Alto	Muy alta	Muy alta
Problemas de soporte / Desastres naturales	Eliminación de datos	Medio	Muy alta	Muy alta	Medio
	Paralización de actividades	Medio	Muy alta	Muy alta	Medio

El análisis detallado del activo Servicio de Gestión de Base de Datos muestra que los riesgos con el mayor potencial de daño provienen de acciones intencionales (tanto internas como externas a través de la red o acceso físico) y de fallas graves de infraestructura y soporte.

a. Impactos de máxima severidad (Muy Alto)

Los riesgos con el mayor potencial de daño se caracterizan por causar un impacto Muy Alto en al menos dos de los criterios evaluados:

- La paralización de actividades generada por limitaciones en la capacidad de almacenamiento es el evento de mayor severidad, impactando a nivel Muy Alto la reputación, la productividad y la gestión administrativa, mientras que el impacto económico se mantiene en nivel Alto.
- Las amenazas generadas por actores intencionales (internos o externos, por red o acceso físico) y los problemas con el servicio de hosting provocan consistentemente un impacto Muy Alto en la reputación de los usuarios y en la productividad operacional. El impacto económico y administrativo en estos casos se clasifica como Alto.
- La paralización de actividades debido a consultas ineficientes resulta en un impacto Muy Alto en la reputación y en la productividad, aunque su consecuencia económica y administrativa se mantiene en nivel Medio.
- Las amenazas provenientes de desastres naturales tienen el impacto más crítico sobre la economía y la productividad (registrando Muy Alto en ambos), aunque solo un nivel Medio en reputación y administración.
- Las amenazas derivadas de errores accidentales internos (por red o acceso físico) que causan alteración o eliminación de datos, generan un impacto Muy Alto en la reputación, aunque su consecuencia económica es Baja.

b. Impactos de severidad moderada (Alto, Medio y Bajo)

Los impactos de severidad moderada afectan principalmente la Integridad y Disponibilidad, con un costo económico relativamente bajo o medio:

- La paralización de actividades por fallas en conectividad afecta la reputación de forma Muy Alta, pero su consecuencia económica es solo Media, mientras que el impacto en productividad y administración es Alto.
- Los riesgos originados por la falta de mantenimiento generan un impacto Alto en la reputación y en la productividad, siendo Medio en los criterios económico y administrativo.
- Los riesgos por diseño inadecuado generan un impacto Medio en la mayoría de los criterios, con excepción de la productividad, que es Alto.

- La falta de control de calidad genera el impacto económico más Bajo de todos los problemas técnicos y de soporte, aunque su impacto en la reputación y la productividad es Alto.

3.3.3. Análisis consolidado del impacto de las amenazas sobre el activo Barrera de seguridad perimetral (firewall)

A continuación, se presenta una tabla que consolida el análisis de impacto de las amenazas identificadas sobre el activo crítico Firewall. La valoración de los impactos se realizó sobre los criterios de Reputación, Económico, Productividad y Administrativo, utilizando la escala cualitativa de la organización (Muy Bajo, Bajo, Medio, Alto, Muy Alto).

Tabla 10. Consolidado del impacto de las amenazas sobre el activo Barrera de seguridad perimetral (firewall)

Categoría de amenazan origen de la amenaza	Evento de riesgo potencial	Impacto en la imagen o credibilidad del usuario (confianza)	Consecuencia económica	Impacto en el rendimiento o productividad (productividad)	Impacto en la administración
Personas / Acceso por red - Accidental interna	Alteración de registros	Medio	Medio	Alto	Medio
	Paralización de actividades	Muy alto	Medio	Alto	Medio
Personas / Acceso por red - Intencional interna	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Paralización de actividades	Muy alto	Alto	Muy alto	Alto
Personas / Acceso por red - Intencional externa	Alteración de registros	Muy alto	Alto	Muy alto	Alto
	Paralización de actividades	Muy alto	Alto	Muy alto	Alto
Personas / Acceso físico - Accidental interna	Alteración de registros	Medio	Medio	Alto	Medio
	Paralización de actividades	Muy alto	Medio	Alto	Medio
Problemas técnicos / Obsolescencia del software	Alteración de registros	Medio	Medio	Alto	Medio
	Eliminación de datos	Medio	Medio	Alto	Medio
	Paralización de actividades	Medio	Medio	Alto	Medio
Problemas técnicos / Contraseñas mal administradas	Alteración de registros	Alto	Alto	Alto	Medio
	Eliminación de datos	Alto	Alto	Alto	Medio
	Paralización de actividades	Alto	Alto	Alto	Medio
Problemas técnicos / Mala configuración	Exposición de datos	Alto	Alto	Alto	Medio
	Alteración de registros	Alto	Alto	Alto	Medio
	Eliminación de datos	Alto	Alto	Alto	Medio
	Paralización de actividades	Alto	Alto	Alto	Medio
Problemas técnicos / Reglas muy permisivas	Exposición de datos	Alto	Alto	Alto	Medio
	Alteración de registros	Alto	Alto	Alto	Medio
	Eliminación de datos	Alto	Alto	Alto	Medio
	Paralización de actividades	Alto	Alto	Alto	Medio
Problemas de soporte / Antimalware ineficiente	Exposición de datos	Alto	Medio	Muy alta	Alto
	Alteración de registros	Alto	Medio	Muy alta	Alto
	Eliminación de datos	Alto	Medio	Muy alta	Alto
	Paralización de actividades	Alto	Medio	Muy alta	Alto
Problemas de soporte / Mala definición de objetos de red	Exposición de datos	Medio	Bajo	Alto	Medio
	Alteración de registros	Medio	Bajo	Alto	Medio
	Eliminación de datos	Medio	Bajo	Alto	Medio
	Paralización de actividades	Medio	Bajo	Alto	Medio
Problemas de soporte / Limitaciones en la	Paralización de actividades	Muy alta	Alto	Muy alta	Muy alta

capacidad de protección					
Problemas de soporte / Desastres naturales	Eliminación de datos	Medio	Muy alta	Muy alta	Medio
	Paralización de actividades	Medio	Muy alta	Muy alta	Medio

El análisis del impacto de las amenazas sobre el Firewall (o barrera de seguridad perimetral) muestra que la mayoría de los escenarios de riesgo tienen un efecto de severidad Alto o Muy Alto en los criterios de reputación y productividad, reflejando su rol crítico en la disponibilidad del servicio.

a. Impactos de máxima severidad (Muy Alto)

Los riesgos más severos se caracterizan por una afectación Muy Alta en múltiples criterios, destacando la paralización de actividades como el evento de riesgo más crítico:

- La paralización de actividades debido a limitaciones en la capacidad de protección es el evento más crítico, causando un impacto Muy Alto en Reputación, Productividad y la gestión Administrativa de la institución. Su consecuencia Económica es también Alta.
- Cualquier riesgo originado por actores intencionales (por red) que resulte en la alteración de registros o paralización de actividades genera consistentemente un impacto Muy Alto en la Reputación y la Productividad. El impacto Económico y Administrativo se clasifica como Alto.
- La eliminación de datos o paralización de actividades causadas por desastres naturales tienen el impacto más crítico sobre la esfera Económica y la Productividad, registrando un nivel Muy Alto en ambos criterios. Su impacto en Reputación y Administración, sin embargo, es Medio.
- La paralización de actividades (y otros riesgos) generada por un antimalware ineficiente tiene su mayor efecto en la Productividad, categorizado como Muy Alto, dado que permite la propagación de malware a los sistemas que el firewall protege. El resto de criterios son clasificados como Altos, excepto el Económico que es Medio.
- La paralización de actividades causada por un error accidental (por red o acceso físico) alcanza Muy Alto únicamente en el criterio de Reputación del usuario, mientras que el impacto en Productividad es Alto y el Económico/Administrativo es Medio.

b. Impactos Altos

Los escenarios de riesgo Alto se concentran en fallas técnicas comunes que amenazan la Integridad de los datos y la Productividad operacional:

- Los errores derivados de contraseñas mal administradas, mala configuración o reglas muy permisivas resultan en un impacto Alto en Reputación, Económico y Productividad para cualquier evento de riesgo (Exposición, Alteración, Eliminación o Paralización). No obstante, la consecuencia Administrativa/Normativa se mantiene en un nivel Medio.
- Los riesgos de Alteración, Eliminación o Paralización por obsolescencia del software causan un impacto Alto en la Productividad, mientras que el resto de los criterios (Reputación, Económico y Administrativo) se mantienen en nivel Medio.

c. Impactos de menor severidad (Bajo y Medio)

- Las amenazas generadas por la mala definición de objetos de red tienen el impacto económico más bajo de todos (nivel Bajo), lo que refleja el menor costo directo asociado a la corrección de errores de configuración en comparación con la recuperación de sistemas. La afectación a la Reputación es Media, mientras que la Productividad es Alta.
- La mayoría de los riesgos generados por errores accidentales internos (Alteración de registros) y la obsolescencia del software presentan el nivel de impacto más bajo en el aspecto Económico y Administrativo (nivel Medio), siendo la Productividad la única afectada con nivel Alto.

3.4. Análisis de la probabilidad de materialización de amenazas

Este análisis se centra en la probabilidad de materialización de las amenazas (riesgos) sobre los activos críticos de la gestión académica, enmarcado dentro de una fase de evaluación de riesgos. A continuación, se presentan las tablas con la información del documento adjunto, reformulada según las indicaciones, seguidas de una síntesis de los hallazgos por cada activo. Para el análisis de la probabilidad de materialización de amenazas la siguiente tabla explica la escala utilizada en función de la frecuencia histórica con la que un evento ha ocurrido en un nivel de probabilidad que se utiliza para calcular el riesgo.

Tabla 11. Escala para la valoración de la probabilidad de materialización de amenazas

Nivel de probabilidad	Rango de frecuencia histórica	Descripción del nivel
Muy Bajo	No aplica (implica 0 veces/año)	Indica que la amenaza nunca ha sido documentada o registrada en el periodo analizado, o su ocurrencia es extremadamente rara.
Bajo	1 a 3 veces/año	La amenaza tiene una baja posibilidad de materializarse. Los incidentes son esporádicos y poco frecuentes a lo largo del año.
Medio	4 a 6 veces/año	La amenaza tiene una posibilidad moderada de materializarse. Los incidentes ocurren varias veces al año, pero no de manera constante o semanal.
Alto	7 a 9 veces/año	La amenaza tiene una alta posibilidad de materializarse. Los incidentes son frecuentes, ocurriendo casi mensualmente o en periodos de alta actividad.
Muy Alto	Más de 9 veces/año	La amenaza tiene una posibilidad muy alta o casi constante de materializarse. Los incidentes ocurren de forma recurrente (casi semanal o diaria), representando un evento esperado.

3.4.1. Probabilidad de materialización de amenazas sobre el Sistema de Información Académica (SIA)

A continuación, se presenta una tabla que consolida el análisis de la probabilidad de materialización de amenazas sobre el Sistema de Información Académica (SIA).

Tabla 12. Consolidado Probabilidad de materialización de amenazas sobre el Sistema de Información Académica (SIA)

Origen del riesgo (amenaza)	Evento de riesgo potencial	Nivel de posibilidad de ocurrencia
Personas / Acceso por red - Accidental interna	Alteración de registros	Muy Alto
	Eliminación de datos	Muy Alto
Personas / Acceso por red – Intencionada interna	Exposición de datos	Medio
	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Personas / Acceso por red – Intencionada externa	Exposición de datos	Medio
	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Personas / Acceso físico – Accidental interna	Alteración de registros	Bajo
	Paralización de actividades	Bajo
Personas / Acceso físico - Intencionada interna	Alteración de registros	Bajo
	Eliminación de datos	Bajo
Problemas técnicos / Diseño inadecuado	Eliminación de datos	Alto
	Paralización de actividades	Alto
Problemas técnicos / Falta de compatibilidad	Alteración de registros	Alto
	Paralización de actividades	Alto
Problemas técnicos / Obsolescencia funcional	Paralización de actividades	Bajo
Problemas técnicos / Falta de control de calidad	Alteración de registros	Medio
	Eliminación de datos	Medio
Problemas de soporte / Caída del suministro eléctrico	Eliminación de datos	Muy Alto
	Paralización de actividades	Muy Alto
Problemas de soporte / Fallas en conectividad	Paralización de actividades	Alto
Problemas de soporte / Servicio de terceros deficiente	Alteración de registros	Bajo
	Paralización de actividades	Bajo
Problemas de soporte / Desastres naturales	Eliminación de datos	Bajo
	Paralización de actividades	Bajo

El análisis de probabilidad de materialización de las amenazas sobre el activo crítico Sistema de Información Académica (SIA), se resume a continuación por nivel de exposición:

d. Nivel de probabilidad Muy Alto (Exposición crítica)

Las amenazas con la máxima probabilidad de ocurrencia (frecuencia histórica > 9 veces/año) se concentran en el error humano operativo y las vulnerabilidades de infraestructura que comprometen directamente la integridad y disponibilidad:

- La Alteración de registros y la Eliminación de datos por parte de usuarios internos (administrativos, docentes, alumnos) debido a errores o desconocimiento presentan la máxima probabilidad. Esto establece al error humano como la fuente de riesgo más recurrente para la integridad de la información del SIA.

- La Eliminación de datos y la Paralización de actividades causadas por fallas de energía también son de probabilidad Muy Alta. Esta vulnerabilidad de infraestructura afecta de manera constante la disponibilidad y la persistencia de la información académica.

e. Nivel de probabilidad Alto (Alta exposición)

Los riesgos con una alta probabilidad de materialización (frecuencia histórica de 7 a 9 veces/año) se centran en las deficiencias técnicas del software y la conectividad, indicando que las fallas de desarrollo son esperadas:

- Los fallos estructurales como el Diseño inadecuado y la Falta de compatibilidad provocan con alta probabilidad la Alteración de registros, Eliminación de datos y, principalmente, la Paralización de actividades.
- La Paralización de actividades generada por fallas en la red también se encuentra en este nivel, confirmando que la inestabilidad de la conexión es un factor recurrente de indisponibilidad.

f. Nivel de probabilidad Medio (Exposición moderada)

Los riesgos intencionales, que buscan comprometer la confidencialidad, se ubican en este nivel, con una frecuencia histórica de 4 a 6 veces/año:

- Cualquier evento de riesgo generado por actores intencionales (internos o externos) como la Exposición, Alteración, Eliminación de datos o la Paralización de actividades tiene una probabilidad Media. Esto sugiere que, si bien la intención maliciosa existe, es menos frecuente que los fallos operativos y de infraestructura.
- La Alteración o Eliminación de datos debido a la falta de pruebas o supervisión adecuada también se encuentra en probabilidad Media.

g. Nivel de probabilidad Bajo (Baja exposición)

Los riesgos con menor probabilidad de materialización (frecuencia histórica de 1 a 3 veces/año) se relacionan con las acciones físicas, fallas de terceros y eventos ambientales, siendo las amenazas menos esperadas, aunque potencialmente catastróficas:

- Todas las amenazas por Acceso físico (accidental o intencional, interno o externo) son de probabilidad Baja.
- La Paralización de actividades o Eliminación de datos causadas por la Obsolescencia funcional, el Servicio de terceros deficiente o los Desastres naturales se consideran eventos de probabilidad Baja.

3.4.2. Probabilidad de materialización de amenazas sobre el Servicio de gestión de base de datos

A continuación, se presenta una tabla que consolida el análisis de la probabilidad de materialización de amenazas sobre el Servicio de Gestión de Base de Datos – SIA.

Tabla 13. Consolidado Probabilidad de materialización de amenazas sobre el Servicio de Gestión de Base de Datos – SIA

Origen del riesgo (amenaza)	Evento de riesgo potencial	Nivel de posibilidad de ocurrencia
Personas / Acceso por red - Accidental interna	Alteración de registros	Medio
	Eliminación de datos	Medio
Personas / Acceso por red – Intencionada interna	Exposición de datos	Alto
	Alteración de registros	Alto
	Eliminación de datos	Alto
Personas / Acceso por red – Intencionada externa	Alteración de registros	Alto
	Eliminación de datos	Alto
	Paralización de actividades	Alto
Personas / Acceso físico - Accidental interna	Alteración de registros	Bajo
	Paralización de actividades	Bajo
Personas / Acceso físico - Intencionada interna	Alteración de registros	Bajo
	Eliminación de datos	Bajo
Problemas técnicos / diseño inadecuado	Alteración de registros	Alto
	Eliminación de datos	Alto
	Paralización de actividades	Alto
Problemas técnicos / Falta de mantenimiento	Alteración de registros	Alto
	Paralización de actividades	Alto
Problemas técnicos / Consultas ineficientes	Paralización de actividades	Bajo
Problemas técnicos / Falta de control de calidad	Alteración de registros	Medio
	Eliminación de datos	Medio
Problemas de soporte / Problemas con servicio de hosting	Paralización de actividades	Bajo
Problemas de soporte / Fallas en conectividad	Paralización de actividades	Alto
Problemas de soporte / Limitaciones en capacidad de almacenamiento	Paralización de actividades	Bajo
Problemas de soporte / Desastres naturales	Eliminación de datos	Bajo
	Paralización de actividades	Bajo

El análisis de probabilidad de ocurrencia (o materialización) de las amenazas sobre el Servicio de Gestión de Base de Datos del SIA revela un riesgo Alto en la mayoría de los escenarios críticos, particularmente aquellos relacionados con las acciones intencionales y las fallas técnicas de la infraestructura.

a. Nivel de probabilidad Alto (Alta exposición)

La mayor concentración de riesgos se encuentra en este nivel, indicando que las amenazas tienen una alta posibilidad de materializarse, con una frecuencia histórica de 7 a 9 veces por año:

- Cualquier evento de riesgo generado por actores intencionales, como la Exposición, Alteración o Eliminación de datos, o la Paralización de actividades, tiene una probabilidad Alta. Esto indica que la base de datos es un objetivo frecuente de ataques dirigidos, tanto por personal interno con acceso como por hackers externos.

- Los riesgos provenientes del Diseño inadecuado (Alteración, Eliminación, Paralización) y la Falta de mantenimiento (Alteración, Paralización) del sistema son consistentemente de probabilidad Alta. Esto indica que los fallos estructurales en la arquitectura y la negligencia en la gestión del sistema son las fuentes más probables de incidentes.
- La Paralización de actividades debido a Fallas en la conectividad también presenta una probabilidad Alta, confirmando que la estabilidad de la red es un factor recurrente de indisponibilidad para el servicio de base de datos.

b. Nivel de probabilidad medio (Moderada exposición)

Este nivel refleja amenazas que ocurren con una frecuencia histórica de 4 a 6 veces por año:

- La Alteración o Eliminación de datos por parte de Personas con acceso por red - Accidental interna tiene una probabilidad Media. Esto sugiere que, aunque los errores de usuarios internos son frecuentes, no son el principal impulsor de los incidentes más graves en la base de datos.
- La Alteración o Eliminación de datos debido a la Falta de control de calidad en los procesos de software o en la supervisión de los datos también se encuentra en probabilidad Media.

c. Nivel de probabilidad bajo (Baja exposición)

Los riesgos con menor probabilidad de materialización (1 a 3 veces por año) se concentran en las acciones físicas, fallas de software específicas y desastres.

- Las amenazas por Acceso físico (Accidental o Intencionada interna), incluyendo la Alteración de registros o Paralización de actividades, son de probabilidad Baja.
- La Paralización de actividades causada por Consultas ineficientes, Problemas con el servicio de hosting, o Limitaciones en capacidad de almacenamiento también es Baja.
- Los desastres naturales (Eliminación de datos y Paralización de actividades) son, afortunadamente, eventos de probabilidad Baja, aunque su impacto potencial sea muy alto (como se vio en el análisis anterior).

3.4.3. Probabilidad de materialización de amenazas sobre el activo Barrera de seguridad perimetral (firewall)

A continuación, se presenta una tabla que consolida el análisis de la probabilidad de materialización de amenazas sobre el activo Barrera de seguridad perimetral (firewall).

Tabla 14. Consolidado de la probabilidad de materialización de amenazas sobre el activo Barrera de seguridad perimetral (firewall)

Origen del riesgo (amenaza)	Evento de riesgo potencial	Nivel de posibilidad de ocurrencia
Personas / Acceso por red - Accidental interna	Alteración de registros	Bajo
	Paralización de actividades	Bajo
Personas / Acceso por red - Intencional interna	Alteración de registros	Alto
	Paralización de actividades	Alto
Personas / Acceso por red - Intencional externa	Alteración de registros	Medio
	Paralización de actividades	Medio
Personas / Acceso físico - Accidental interna	Alteración de registros	Bajo
	Paralización de actividades	Bajo
Problemas técnicos / Obsolescencia del software	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Problemas técnicos / Contraseñas mal administradas	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Problemas técnicos / Mala configuración	Exposición de datos	Medio
	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Problemas técnicos / Reglas muy permisivas	Exposición de datos	Medio
	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Problemas de soporte / Antimalware ineficiente	Exposición de datos	Medio
	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Problemas de soporte / Mala definición de objetos de red	Exposición de datos	Medio
	Alteración de registros	Medio
	Eliminación de datos	Medio
	Paralización de actividades	Medio
Problemas de soporte / Limitaciones en la capacidad de protección	Paralización de actividades	Medio
Problemas de soporte / Desastres naturales	Eliminación de datos	Bajo
	Paralización de actividades	Bajo

El análisis de probabilidad de ocurrencia (o materialización) de las amenazas sobre el activo Barrera de seguridad perimetral (Firewall) revela una exposición Media y Alta a riesgos generados por fallas operacionales y ataques internos, siendo las amenazas externas y los problemas de infraestructura más probables que las fallas accidentales o ambientales.

a. Nivel de probabilidad alto (Alta exposición)

La única fuente de riesgo con probabilidad Alta (frecuencia histórica de 7 a 9 veces/año) son las acciones maliciosas originadas dentro de la red:

- La Alteración de registros y la Paralización de actividades causadas por actores internos con acceso a la red tienen una probabilidad Alta. Esto indica que el Firewall está frecuentemente expuesto a ataques o intentos de manipulación por parte del personal de la propia organización.

b. Nivel de probabilidad Medio (Exposición moderada)

La mayoría de los escenarios de riesgo se concentran en el nivel Medio (frecuencia histórica de 4 a 6 veces/año), lo que sugiere una serie de fallas operacionales recurrentes:

- La Alteración de registros y la Paralización de actividades originadas por actores externos presentan una probabilidad Media.
- Todos los riesgos asociados a Obsolescencia del software, Contraseñas mal administradas, Mala configuración y Reglas muy permisivas resultan en una probabilidad Media para todos los eventos de riesgo (Exposición, Alteración, Eliminación, Paralización). Esto apunta a una gestión de seguridad y configuración del Firewall que genera incidentes de forma moderada pero constante.
- La Paralización de actividades causada por Limitaciones en la capacidad de protección y los riesgos derivados de Antimalware ineficiente o Mala definición de objetos de red también se ubican en probabilidad Media.

c. Nivel de probabilidad bajo (Baja exposición)

Las amenazas con la menor probabilidad de materialización (frecuencia histórica de 1 a 3 veces/año) se relacionan principalmente con el factor accidental y los eventos ambientales:

- La Alteración de registros y la Paralización de actividades causadas por errores accidentales (ya sea por red o por acceso físico) son de probabilidad Baja.
- Los Desastres naturales (Eliminación de datos y Paralización de actividades) son, como es de esperar, eventos de probabilidad Baja.

3.5. Definición del nivel de exposición al riesgo y Estrategia de reducción

Para establecer el nivel de exposición de cada amenaza identificada, se empleó el procedimiento detallado en la metodología propuesta. El proceso se llevó a cabo en dos pasos:

1. Determinación de la puntuación de impacto (Valoración ponderada): Se calculó un valor de impacto sumando los resultados de multiplicar la puntuación asignada a cada tipo de impacto por su respectiva prioridad.
2. Cálculo del nivel de riesgo total: El resultado de la puntuación de impacto se multiplicó por la puntuación de la Probabilidad de materialización de amenazas de la amenaza, obteniendo así la calificación final del nivel de riesgo.

3.5.1. Criterios de cuantificación y categorización del riesgo

En colaboración con el equipo de la oficina de Tecnologías de la Información, se definieron los siguientes criterios para la categorización del riesgo:

a. **Escalas de valoración:** Cada uno de los cuatro tipos de impacto como la Probabilidad de materialización de amenazas se valoraron utilizando una escala de 5 niveles.
   - Combinaciones de impacto: Al tener cuatro tipos de impacto con 5 niveles cada uno, se obtienen 625 combinaciones de impacto posibles.
   - Combinaciones totales: Al combinar estas 625 posibilidades con los 5 niveles de probabilidad, el número total de escenarios de riesgo posibles asciende a 3125.

b. Rango de puntuación:
   - Valor mínimo: Se obtiene al valorar todos los tipos de impacto y la Probabilidad de materialización de amenazas en la escala más baja (nivel 1), resultando en una puntuación mínima de 2.5.
   - Valor máximo: Se obtiene al valorar todos los tipos de impacto y la Probabilidad de materialización de amenazas en la escala más alta (nivel 5), resultando en una puntuación máxima de 62.5.

c. **Rango de valores:** El rango de valores posibles para la puntuación de riesgo es de 60.

d. **Escala de riesgo propuesta:** Se definió una escala de cuatro niveles para clasificar el riesgo: Bajo, Medio, Alto, Muy Alto.

Tabla 15. Escalas para categorizar los niveles de riesgo

Nivel	Nivel de riesgo	Intervalo de puntuación	Aceptación del riesgo
1	Bajo	[2.5 – 17.5)	Riesgo aceptable
2	Medio	[17.5 – 32.5)	
3	Alto	[32.5 – 47.5)	Riesgo no aceptable
4	Muy Alto	[47.5 – 62.5]	

3.5.2. Cálculo del nivel de riesgo

a. Cálculo del nivel de riesgo Sistema de Información Académica (SIA)

A continuación, se presenta la tabla que consolida el análisis del nivel de riesgo para el activo Sistema de Información Académica (SIA), tomando como base los resultados del análisis de impacto y probabilidad correspondientes.

El Nivel de Riesgo se calculó como el producto de la Puntuación Impacto (Impacto Ponderado) por la Probabilidad de materialización de amenazas.

Tabla 16. Nivel de riesgo del activo: Sistema de Información Académica – SIA

Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Tipo de impacto				Puntuación impacto	Probabilidad de materialización de amenazas	Nivel de riesgo
				Impacto en la imagen o credibilidad del usuario (Severidad 4)	Impacto financiero (Severidad 2)	Impacto en el rendimiento o productividad (Severidad 3)	Impacto en la administración (Severidad 1)			
Infraestructura de red	Personal Interno	Accidental	Modificación información	5	2	4	4	10.00	5	50.00
Infraestructura de red	Personal Interno	Accidental	Eliminación de datos	5	2	4	4	10.00	5	50.00
Infraestructura de red	Personal Interno	Intencionado	Exposición de datos	5	4	5	4	11.75	3	35.25
Infraestructura de red	Personal Interno	Intencionado	Modificación información	5	4	5	4	11.75	3	35.25
Infraestructura de red	Personal Interno	Intencionado	Eliminación de datos	5	4	5	4	11.75	3	35.25
Infraestructura de red	Personal Interno	Intencionado	Paralización de actividades	5	4	5	4	11.75	3	35.25
Infraestructura de red	Persona Externa	Intencionado	Exposición de datos	5	4	5	4	11.75	3	35.25
Infraestructura de red	Persona Externa	Intencionado	Alteración de registros	5	4	5	4	11.75	3	35.25
Infraestructura de red	Persona Externa	Intencionado	Eliminación de datos	5	4	5	4	11.75	3	35.25
Infraestructura de red	Persona Externa	Intencionado	Paralización de actividades	5	4	5	4	11.75	3	35.25
Acceso físico	Personal Interno	Accidental	Alteración de registros	5	2	4	4	10.00	2	20.00
Acceso físico	Personal Interno	Accidental	Paralización de actividades	4	2	4	4	9.00	2	17.00
Acceso físico	Personal Interno	Intencionado	Alteración de registros	5	4	5	4	11.75	2	23.50
Acceso físico	Personal Interno	Intencionado	Eliminación de datos	5	4	5	4	11.75	2	23.50
	Problemas técnicos	Diseño inadecuado	Eliminación de datos	5	3	5	3	11.00	4	41.00
	Problemas técnicos	Diseño inadecuado	Paralización de actividades	5	3	5	3	11.00	4	41.00
	Problemas	Falta de	Alteración de	4	3	4	3	9.25	4	35.00

	técnicos	compatibilidad	registros							
	Problemas técnicos	Falta de compatibilidad	Paralización de actividades	4	3	4	3	9.25	4	35.00
	Problemas técnicos	Obsolescencia funcional	Paralización de actividades	4	3	4	3	9.25	2	17.50
	Problemas técnicos	Falta de control de calidad	Alteración de registros	4	2	4	3	8.75	3	24.00
	Problemas técnicos	Falta de control de calidad	Eliminación de datos	4	2	4	3	8.75	3	24.00
	Problemas con el soporte o incidentes no controlados	Caída del suministro eléctrico	Eliminación de datos	3	5	5	3	10.00	5	52.50
	Problemas con el soporte o incidentes no controlados	Caída del suministro eléctrico	Paralización de actividades	3	5	5	3	10.00	5	52.50
	Problemas con el soporte o incidentes no controlados	Fallas en conectividad	Paralización de actividades	5	3	4	4	10.50	4	41.00
	Problemas con el soporte o incidentes no controlados	Servicio de terceros deficiente	Alteración de registros	4	4	5	5	11.00	2	16.00
	Problemas con el soporte o incidentes no controlados	Servicio de terceros deficiente	Paralización de actividades	5	4	5	5	12.00	2	16.00
	Problemas con el soporte o incidentes no controlados	Desastres naturales	Eliminación de datos	3	5	5	3	10.00	2	21.00
	Problemas con el soporte o incidentes no controlados	Desastres naturales	Paralización de actividades	3	5	5	3	10.00	2	21.00

El análisis revela que los riesgos más críticos para el SIA se centran en las fallas de disponibilidad de la infraestructura y el factor humano.

Riesgo Inaceptable

Siete escenarios de riesgo caen en el nivel Muy Alto (puntuaciones entre 41.00 y 52.50), lo que exige una acción correctiva y de inversión inmediata:

a. La Caída del suministro eléctrico (Eliminación de datos y Paralización de actividades) representa el riesgo más alto (52.50). Esto se debe a la combinación de un Impacto Alto con la Máxima Probabilidad de ocurrencia (Muy Alto = 5). Como medida de seguridad se debe asegurar la continuidad del suministro (UPS, generadores) y la integridad de los datos (sistemas de respaldo robustos).

b. La Modificación o Eliminación de datos por errores accidentales internos (Acceso por red) también tiene un riesgo crítico (50.00). La alta frecuencia de errores humanos (Probabilidad = 5) es la causa principal de este riesgo. Como medida de seguridad **s**e requiere capacitación intensiva y controles de acceso lógicos más estrictos.

c. La Paralización de actividades generada por Fallas en conectividad y el Diseño inadecuado (Eliminación/Paralización) demuestran que las debilidades en la arquitectura y la red son una amenaza constante. Se consideran Fallas técnicas críticas (41.00).

Además, diez (10) escenarios se clasifican como Alto (puntuaciones entre 35.00 y 35.25), requiriendo un plan de mitigación prioritario a corto plazo:

d. Todos los riesgos asociados a actores internos o externos intencionales (Exposición, Alteración, Eliminación, Paralización) se agrupan en este nivel (35.25). A pesar de tener el máximo puntaje de impacto (11.75), su probabilidad media (3) los sitúa justo debajo del nivel crítico.

e. La Falta de compatibilidad técnica (Alteración de registros y Paralización) también es un riesgo alto, reflejando problemas en la integración del software con otros componentes del sistema (35.00).

Riesgo Aceptable

Los riesgos restantes caen en niveles manejables, lo que indica que no son la fuente principal de problemas para el SIA:

a. Incluyen el riesgo de Eliminación/Alteración de datos por Falta de control de calidad (24.00) y las amenazas intencionales por Acceso físico (23.50). Estos riesgos deben ser monitoreados y abordados en planes de mejora continua.

b. Los riesgos asociados al Acceso físico accidental (17.00 - 20.00), Obsolescencia funcional (17.50) y Servicio de terceros deficiente (16.00) son aceptables y solo requieren monitoreo periódico.

b. Cálculo del nivel de riesgo Servicio de Gestión de Base de Datos – SIA

A continuación, se presenta la tabla que consolida el análisis del nivel de riesgo para el activo Servicio de Gestión de Base de Datos del SIA, tomando como base los resultados del análisis de impacto y probabilidad correspondientes.

El Nivel de Riesgo se calculó como el producto de la Puntuación Impacto (Impacto Ponderado) por la Probabilidad de materialización de amenazas.

Tabla 17. Nivel de riesgo del activo: Servicio de Gestión de Base de Datos – SIA

Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Tipo de impacto				Puntuación impacto	Probabilidad de materialización de amenazas	Nivel de riesgo
				Impacto en la imagen o credibilidad del usuario	Consecuencia económica	Impacto en el rendimiento o productividad	Impacto en la administración			
Acceso por red	Personal Interno	Accidental	Alteración de registros	5	2	4	4	10.00	3	30.00
Acceso por red	Personal Interno	Accidental	Eliminación de datos	5	2	4	4	10.00	3	30.00
Acceso por red	Personal Interno	Intencionado	Develación de datos	5	4	5	4	11.75	4	47.00
Acceso por red	Personal Interno	Intencionado	Alteración de registros	5	4	5	4	11.75	4	47.00
Acceso por red	Personal Interno	Intencionado	Eliminación de datos	5	4	5	4	11.75	4	47.00
Acceso por red	Persona Externa	Intencionado	Alteración de registros	5	4	5	4	11.75	4	47.00
Acceso por red	Persona Externa	Intencionado	Eliminación de datos	5	4	5	4	11.75	4	47.00
Acceso por red	Persona Externa	Intencionado	Paralización de actividades	5	4	5	4	11.75	4	47.00
Acceso físico	Personal Interno	Accidental	Alteración de registros	5	2	4	4	10.00	2	20.00
Acceso físico	Personal Interno	Accidental	Paralización de actividades	4	2	4	4	9.00	2	18.00
Acceso físico	Personal Interno	Intencionado	Alteración de registros	5	4	5	4	11.75	2	23.50
Acceso físico	Personal Interno	Intencionado	Eliminación de datos	5	4	5	4	11.75	2	23.50
	Problemas técnicos	Diseño inadecuado	Alteración de registros	3	3	4	3	8.25	4	33.00
	Problemas técnicos	Diseño inadecuado	Eliminación de datos	3	3	4	3	8.25	4	33.00
	Problemas técnicos	Diseño inadecuado	Paralización de actividades	3	3	4	3	8.25	4	33.00
	Problemas técnicos	Falta de mantenimiento	Alteración de registros	4	3	4	3	9.25	4	37.00
	Problemas técnicos	Falta de mantenimiento	Paralización de actividades	4	3	4	3	9.25	4	37.00

	Problemas técnicos	Consultas ineficientes	Paralización de actividades	5	3	5	3	11.00	2	22.00
	Problemas técnicos	Falta de control de calidad	Alteración de registros	4	2	4	3	8.75	3	26.25
	Problemas técnicos	Falta de control de calidad	Eliminación de datos	4	2	4	3	8.75	3	26.25
	Problemas de soporte	Problemas con servicio de hosting	Paralización de actividades	5	4	5	4	11.75	2	23.50
	Problemas de soporte	Fallas en conectividad	Paralización de actividades	5	3	4	4	10.50	4	42.00
	Problemas de soporte	Limitaciones en capacidad de almacenamiento	Paralización de actividades	5	4	5	5	12.00	2	24.00
	Problemas de soporte	Desastres naturales	Pérdida de información	3	5	5	3	10.00	2	20.00
	Problemas de soporte	Desastres naturales	Paralización de actividades	3	5	5	3	10.00	2	20.00

El análisis del riesgo del Servicio de Gestión de Base de Datos revela la concentración de amenazas en los niveles Alto, las cuales deben ser priorizadas para su mitigación.

Riesgo Inaceptable

Este nivel, Inaceptable, agrupa los escenarios más críticos que requieren acción inmediata y urgente:

a. Develación de datos, Alteración, Eliminación y Paralización de actividades por Amenazas Intencionadas por Red (Internas y Externas). Este escenario afecta la integridad, confidencialidad y disponibilidad del SGBD.

b. Fallas en la conectividad que ocasionan la Paralización de actividades. Se deben implementar controles de seguridad perimetral y lógicos rigurosos, como sistemas de prevención de intrusiones, control de acceso estricto y segmentación de red.

c. Problemas técnicos como la Falta de mantenimiento (37.00) y el Diseño inadecuado (33.00) podrían ocasionar la Alteración de registros y Paralización de actividades. Las vulnerabilidades técnicas y de proceso son un riesgo significativo. El fallo en la gestión del ciclo de vida del software y el mantenimiento del SGBD tienen un impacto alto en la disponibilidad y la integridad. Es crucial establecer y ejecutar planes de mantenimiento preventivo y de calidad del código.

Riesgo Aceptable

Este nivel es Aceptable, lo que significa que los riesgos deben ser monitoreados y gestionados en planes a medio plazo:

a. La Alteración o Eliminación de datos por errores accidentales internos por red (30.00) muestra que, aunque el actor no es malintencionado, la probabilidad media de error sigue generando un riesgo significativo.

b. La alteración y eliminación de datos por acceso físico intencional (23.50) tiene un alto impacto, pero su baja probabilidad lo mantiene en este nivel.

c. Problemas de Soporte como fallas en el con servicio de hosting (24.00), generan riesgo de Paralización de las actividades.

d. Amenazas con la probabilidad más baja, son la Paralización de actividades por Acceso físico accidental (17.00) y las Consultas Ineficientes (9.50).

c. Cálculo del nivel de riesgo del activo Barrera de seguridad perimetral (firewall)

A continuación, se presenta la tabla que consolida el análisis del nivel de riesgo para el activo Barrera de seguridad perimetral (firewall), tomando como base los resultados del análisis de impacto y probabilidad correspondientes.

El Nivel de Riesgo se calculó como el producto de la Puntuación Impacto (Impacto Ponderado) por la Probabilidad de materialización de amenazas.

Tabla 18. Nivel de riesgo del activo: Barrera de seguridad perimetral (firewall)

Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Tipo de impacto				Puntuación impacto	Probabilidad de materialización de amenazas	Nivel de riesgo
				Impacto en la imagen o credibilidad del usuario	Consecuencia económica	Impacto en el rendimiento o productividad	Impacto en la administración			
Acceso por red	Personal Interno	Accidental	Alteración de registros	3	3	4	3	8.25	2	16.50
Acceso por red	Personal Interno	Accidental	Paralización de actividades	5	3	4	3	10.25	2	20.50
Acceso por red	Personal Interno	Intencionado	Alteración de registros	5	4	5	4	11.75	4	47.00
Acceso por red	Personal Interno	Intencionado	Paralización de actividades	5	4	5	4	11.75	4	47.00
Acceso por red	Persona Externa	Intencionado	Alteración de registros	5	4	5	4	11.75	3	35.25
Acceso por red	Persona Externa	Intencionado	Paralización de actividades	5	4	5	4	11.75	3	35.25
Acceso físico	Personal Interno	Accidental	Alteración de registros	3	3	4	3	8.25	2	16.50
Acceso físico	Personal Interno	Accidental	Paralización de actividades	5	3	4	3	10.25	2	20.50
	Problemas técnicos	Obsolescencia del software	Alteración de registros	3	3	4	3	8.25	3	24.75
	Problemas técnicos	Obsolescencia del software	Eliminación de datos	3	3	4	3	8.25	3	24.75
	Problemas técnicos	Obsolescencia del software	Paralización de actividades	3	3	4	3	8.25	3	24.75
	Problemas técnicos	Contraseñas mal administradas	Alteración de registros	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Contraseñas mal administradas	Eliminación de datos	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Contraseñas mal administradas	Paralización de actividades	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Mala configuración	Exposición de datos	4	4	4	3	9.75	3	29.25
	Problemas	Mala	Alteración de	4	4	4	3	9.75	3	29.25

	técnicos	configuración	registros							
	Problemas técnicos	Mala configuración	Eliminación de datos	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Mala configuración	Paralización de actividades	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Reglas muy permisivas	Exposición de datos	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Reglas muy permisivas	Alteración de registros	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Reglas muy permisivas	Eliminación de datos	4	4	4	3	9.75	3	29.25
	Problemas técnicos	Reglas muy permisivas	Paralización de actividades	4	4	4	3	9.75	3	29.25
	Problemas de soporte	Antimalware ineficiente	Exposición de datos	4	3	5	4	10.25	3	30.75
	Problemas de soporte	Antimalware ineficiente	Alteración de registros	4	3	5	4	10.25	3	30.75
	Problemas de soporte	Antimalware ineficiente	Eliminación de datos	4	3	5	4	10.25	3	30.75
	Problemas de soporte	Antimalware ineficiente	Paralización de actividades	4	3	5	4	10.25	3	30.75
	Problemas de soporte	Mala definición de objetos	Exposición de datos	3	2	4	3	7.75	3	23.25
	Problemas de soporte	Mala definición de objetos	Alteración de registros	3	2	4	3	7.75	3	23.25
	Problemas de soporte	Mala definición de objetos	Eliminación de datos	3	2	4	3	7.75	3	23.25
	Problemas de soporte	Mala definición de objetos	Paralización de actividades	3	2	4	3	7.75	3	23.25
	Problemas de soporte	Limitaciones en la capacidad	Paralización de actividades	5	4	5	5	12.00	3	36.00
	Problemas de soporte	Desastres naturales	Eliminación de datos	3	5	5	3	10.00	2	20.00
	Problemas de soporte	Desastres naturales	Paralización de actividades	3	5	5	3	10.00	2	20.00

El análisis del riesgo del activo Barrera de seguridad perimetral (firewall) muestra los siguientes niveles de riesgo:

Riesgo No Aceptable

Los riesgos clasificados como No Aceptables representan las mayores amenazas al control y la disponibilidad del firewall, y requieren acción correctiva inmediata y prioritaria.

a. La puntuación máxima dentro del rango de Riesgo Alto (47.00) se debe a los escenarios de Alteración de registros y Paralización de actividades causadas por Actores Internos Intencionados a través de la red. Esto subraya la necesidad crítica de implementar mecanismos estrictos de control de acceso y monitoreo de la actividad interna, ya que el firewall es altamente vulnerable a ataques de personal con conocimiento o acceso privilegiado.

b. Las mismas amenazas (Alteración y Paralización) perpetradas por Actores Externos Intencionados también caen en este nivel. Esto indica que las defensas perimetrales son insuficientes para detener ataques externos decididos, lo que exige una revisión urgente de las políticas de filtrado, los sistemas de detección de intrusos (IDS) y la Administración de puntos débiles (Vulnerabilidades) externas.

c. La Paralización de actividades debido a Limitaciones en la capacidad de protección (Problemas de soporte) es un riesgo Alto. El equipo de seguridad debe evaluar y, si es necesario, actualizar la capacidad de rendimiento del firewall para asegurar que pueda gestionar el tráfico sin interrupción del servicio.

Riesgo Aceptable

a. La Obsolescencia del software (24.75), el uso de Contraseñas mal administradas (28.50), la Mala configuración (29.25) y las Reglas muy permisivas (29.25) son todos riesgos Medios. Estos escenarios se deben principalmente a la debilidad en la gestión de seguridad y no a la intención maliciosa. Su mitigación depende de la implementación de procesos de gestión de la configuración estandarizados y auditorías periódicas.

b. La Paralización de actividades generada por errores accidentales internos (acceso por red o físico) también se ubica en riesgo Medio. Si bien la intención no es maliciosa, la ocurrencia constante de errores humanos (20.50 y 23.50) demanda capacitación continua y controles operativos más estrictos.

c. Riesgos como el Antimalware ineficiente (30.75) y la Mala definición de objetos de red (31.00) están en el límite superior del Nivel Medio, casi llegando a ser No

Aceptables. Esto indica que las soluciones de seguridad complementarias al firewall no están operando con la eficacia necesaria.

d. En el nivel de mínimo impacto se encuentran los escenarios de Alteración de registros por error accidental (Acceso por red o físico), y la Eliminación o Paralización generada por Desastres naturales. La baja probabilidad de ocurrencia (en el caso de desastres) o la baja criticidad combinada con baja probabilidad (en el caso de errores que solo causan alteración) hacen que estos riesgos sean aceptados.

3.5.3. Selección del enfoque de reducción

Para determinar la estrategia de tratamiento de cada riesgo evaluado, se compararon los resultados del nivel de riesgo con las prácticas de seguridad correspondientes al activo. Este proceso permitió identificar las áreas de seguridad donde se observan deficiencias (brechas o gaps), sirviendo como base esencial para la formulación de las propuestas de estrategias de mitigación enfocadas en las debilidades específicas.

Tabla 19. Enfoque de reducción de riesgos causados por personas a través de accesos por red al Sistema de Información Académica (SIA)

AMENAZA					PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
					Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Sistema de Información Académica – SIA [SISSIA]	Acceso por red	Personal Interno	Accidental	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R			R	R	R	R		R	R		X	
				Eliminación de datos	R	R	R	R	R	R			R	R	R	R		R	R		X	
				Paralización de actividades																		
			Intencionado	Exposición de datos	R	R	R	R	R	R			R	R	R	R		R	R		X	K
				Alteración de registros	R	R	R	R	R	R			R	R	R	R		R	R		X	
				Eliminación de datos	R	R	R	R	R	R			R	R	R	R		R	R		X	
				Paralización de actividades	R	R	R	R	R	R			R	R	R	R		R	R		X	K
		Persona Externa	Accidental	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		
			Intencionado	Exposición de datos	R	R	R	R	R	R			R	R	R	R		R	R		X	K
				Alteración de registros	R	R	R	R	R	R			R	R	R	R		R	R		X	
				Eliminación de datos	R	R	R	R	R	R			R	R	R	R		R	R		X	
				Paralización de actividades	R	R	R	R	R	R			R	R	R	R		R	R		X	K

Tabla 20. Enfoque de reducción de riesgos causados por personas a través de físicos al Sistema de Información Académica (SIA)

AMENAZA					PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
					Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Sistema de Información Académica – SIA [SISSIA]	Acceso físico	Personal Interno	Accidental	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R	R	R		R					R	X		
				Eliminación de datos																		
				Paralización de actividades	R	R	R	R	R	R	R	R		R					R	X		
			Intencionado	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R	R	R		R					R	X		
				Eliminación de datos	R	R	R	R	R	R	R	R		R					R	X		
				Paralización de actividades																		
		Persona Externa	Accidental	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		
			Intencionado	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R	R	R		R					R	X		
				Eliminación de datos	R	R	R	R	R	R	R	R		R					R	X		
				Paralización de actividades																		

Tabla 21. Enfoque de reducción de riesgos causados por problemas técnicos al Sistema de Información Académica (SIA)

AMENAZA			PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
			Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Sistema de Información Académica – SIA [SISSIA]	Diseño inadecuado	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos		R	R		R				R			R		R			X	
		Paralización de actividades		R	R		R				R			R		R			X	
	Falta de compatibilidad	Exposición de datos																		
		Alteración de registros		R	R		R				R			R		R			X	
		Eliminación de datos																		
		Paralización de actividades		R	R		R				R			R		R			X	
	Obsolescencia funcional	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R				R			R		R		X		
	Falta de control de calidad	Exposición de datos																		
		Alteración de registros		R	R		R				R			R		R		X		
				R	R		R				R			R		R		X		
		Paralización de actividades																		

Tabla 22. Enfoque de reducción de riesgos causados por problemas de soporte al Sistema de Información Académica (SIA)

AMENAZA			PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
			Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Sistema de Información Académica – SIA [SISSIA]	Problemas de suministro de energía	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos		R	R		R	R		R	R						R		X	
		Paralización de actividades		R	R		R	R		R	R						R		X	
	Fallas en la conectividad	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R	R		R	R						R		X	
	Inadecuado servicio de terceros	Exposición de datos																		
		Alteración de registros		R	R		R	R									R	X		
		Eliminación de datos																		
		Paralización de actividades		R	R		R	R									R	X		
	Desastres naturales	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos		R	R		R	R		R							R	X		
		Paralización de actividades		R	R		R	R		R							R	X		

Tabla 23. Enfoque de reducción de riesgos causados personas a través de accesos a la red al Servicio de gestión de base de datos del SIA

AMENAZA					PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Prácticas estratégicas							Prácticas operacionales										
					Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres		Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Servicio de gestión de base de datos - SIA [SERVI03]	Infraestructura red	Personal Interno	Accidental	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R				R	R	R	R	R	R	R	X		
				Eliminación de datos	R	R	R	R	R	R				R	R	R	R	R	R	R	X		
				Paralización de actividades																			
			Intencionado	Exposición de datos	R	R	R	R	R	R				R	R	R	R	R	R	R		X	
				Alteración de registros	R	R	R	R	R	R				R	R	R	R	R	R	R		X	
				Eliminación de datos	R	R	R	R	R	R				R	R	R	R	R	R	R		X	
				Paralización de actividades																			
		Persona Externa	Accidental	Exposición de datos																			
				Alteración de registros																			
				Eliminación de datos																			
				Paralización de actividades																			
			Intencionado	Exposición de datos																			
				Alteración de registros	R	R	R	R	R	R				R	R	R	R	R	R	R		X	
				Eliminación de datos	R	R	R	R	R	R				R	R	R	R	R	R	R		X	
				Paralización de actividades	R	R	R	R	R	R				R	R	R	R	R	R	R		X	

Tabla 24. Enfoque de reducción de riesgos causados personas a través de accesos físicos al Servicio de gestión de base de datos del SIA

AMENAZA					PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
					Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Servicio de gestión de base de datos - SIA [SERVI03]	Acceso físico	Personal Interno	Accidental	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R	R	R	R	R			R	R	R	X		
				Eliminación de datos																		
				Paralización de actividades	R	R	R	R	R	R	R	R	R	R			R	R	R	X		
			Intencionado	Exposición de datos																		
				Alteración de registros	R	R	R	R	R	R	R	R	R	R			R	R	R	X		
				Eliminación de datos	R	R	R	R	R	R	R	R	R	R			R	R	R	X		
				Paralización de actividades																		
		Persona Externa	Accidental	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		
			Intencionado	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		

Tabla 25. Enfoque de reducción de riesgos causados por problemas técnicos al Servicio de gestión de base de datos del SIA

AMENAZA			PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
			Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Servicio de gestión de base de datos - SIA [SERVI03]	Diseño inadecuado	Exposición de datos																		
		Alteración de registros		R	R		R					R		R	R	R			X	
		Eliminación de datos		R	R		R					R		R	R	R			X	
		Paralización de actividades		R	R		R					R		R	R	R			X	
	Falta de mantenimiento	Exposición de datos																		
		Alteración de registros		R	R		R					R				R	R		X	
		Eliminación de datos																		
		Paralización de actividades		R	R		R					R				R	R		X	
	Consultas ineficientes	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R				R	R		R	R	R		X		
	Falta de control de calidad	Exposición de datos																		
		Alteración de registros		R	R		R					R		R	R	R		X		
		Eliminación de datos		R	R		R					R		R	R	R		X		
		Paralización de actividades																		

Tabla 26. Enfoque de reducción de riesgos causados por problemas de soporte al Servicio de gestión de base de datos del SIA

AMENAZA			PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
			Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Servicio de gestión de base de datos - SIA [SERVI03]	Problemas con el servicio de Hosting	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R	R		R	R						R	X		
	Fallas en la conectividad	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R	R		R	R						R		X	
	Limitaciones en la capacidad de almacenamiento	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R	R		R	R						R	X		
	Desastres naturales	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos		R	R		R	R		R							R	X		
		Paralización de actividades		R	R		R	R		R							R	X		

Tabla 27. Enfoque de reducción de riesgos causados por personas a través de accesos por red al activo Barrera de seguridad perimetral (firewall)

AMENAZA					PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Prácticas estratégicas							Prácticas operacionales										
					Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres		Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Firewall [HWFIRE]	Infraestructura red	Personal Interno	Accidental	Exposición de datos																		
				Alteración de registros	R	R	R	R		R				R	R	R	R			R	X	
				Eliminación de datos																		
				Paralización de actividades	R	R	R	R		R				R	R	R	R			R	X	
			Intencionado	Exposición de datos																		
				Alteración de registros	R	R	R	R		R				R	R	R	R			R		X
				Eliminación de datos																		
				Paralización de actividades	R	R	R	R		R				R	R	R	R			R		X
		Persona Externa	Accidental	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		
			Intencionado	Exposición de datos																		
				Alteración de registros	R	R	R	R		R				R	R	R	R			R		X
				Eliminación de datos																		
				Paralización de actividades	R	R	R	R		R				R	R	R	R			R		X

Tabla 28. Enfoque de reducción de riesgos causados por personas a través de accesos físicos al activo Barrera de seguridad perimetral (firewall)

AMENAZA					PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Mecanismo de acceso	Actor de la amenaza	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
					Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Firewall [HWFIRE]	Acceso físico	Personal Interno	Accidental	Exposición de datos																		
				Alteración de registros	R	R	R	R		R	R	R	R	R			R		R	X		
				Eliminación de datos																		
				Paralización de actividades	R	R	R	R		R	R	R	R	R			R		R	X		
			Intencionado	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		
		Persona Externa	Accidental	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		
			Intencionado	Exposición de datos																		
				Alteración de registros																		
				Eliminación de datos																		
				Paralización de actividades																		

Tabla 29. Enfoque de reducción de riesgos causados por problemas técnicos al activo Barrera de seguridad perimetral (firewall)

AMENAZA			PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
			Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Firewall [HWFIRE]	Obsolescencia del software	Exposición de datos																		
		Alteración de registros		R	R							R		R			R	X		
		Eliminación de datos		R	R							R		R			R	X		
		Paralización de actividades		R	R							R		R			R	X		
	Mala gestión de contraseñas	Exposición de datos																		
		Alteración de registros		R	R	R						R	R	R				X		
		Eliminación de datos		R	R	R						R	R	R				X		
		Paralización de actividades		R	R	R						R	R	R				X		
	Mala configuración	Exposición de datos		R	R	R						R	R	R			R	X		
		Alteración de registros		R	R	R						R	R	R			R	X		
		Eliminación de datos		R	R	R						R	R	R			R	X		
		Paralización de actividades		R	R	R						R	R	R			R	X		
	Reglas muy permisivas	Exposición de datos		R	R	R						R	R	R			R	X		
		Alteración de registros		R	R	R						R	R	R			R	X		
		Eliminación de datos		R	R	R						R	R	R			R	X		
		Paralización de actividades		R	R	R						R	R	R			R	X		

Tabla 30. Enfoque de reducción de riesgos causados por problemas de soporte al activo Barrera de seguridad perimetral (firewall)

AMENAZA			PRÁCTICAS DE SEGURIDAD															ENFOQUE DE REDUCCIÓN		
Activo crítico	Tipo de amenaza	Riesgo generado	Prácticas estratégicas						Prácticas operacionales											
			Instrucción, concienciación y nivel de comprensión en seguridad	Puesta en marcha de la estrategia y las tareas de seguridad	Administración de la seguridad de la información	Estructura regulatoria y lineamientos de seguridad	Manejo de la seguridad de la información con colaboradores externos	Esquemas de emergencia y recuperación ante desastres	Control de acceso físico.	Protección ambiental y de la instalación	Administración de la red y sistemas	Monitoreo y auditoría de registros de sucesos	Control de accesos lógicos	Administración de puntos débiles (Vulnerabilidades).	Cifrado de información	Seguridad en el ciclo de desarrollo de aplicaciones	Manejo de sucesos de seguridad de la información	Aceptación del riesgo	Mitigar el riesgo	Transferir el riesgo
Barrera de seguridad perimetral [HWFIRE]	Servicios antimalware ineficiente	Exposición de datos		R	R		R				R	R	R	R			R	X		
		Alteración de registros		R	R		R				R	R	R	R			R	X		
		Eliminación de datos		R	R		R				R	R	R	R			R	X		
		Paralización de actividades		R	R		R				R	R	R	R			R	X		
	Mala definición de los objetos de la red	Exposición de datos		R	R		R				R	R	R	R	R		R	X		
		Alteración de registros		R	R		R				R	R	R	R	R		R	X		
		Eliminación de datos		R	R		R				R	R	R	R	R		R	X		
		Paralización de actividades		R	R		R				R	R	R	R	R		R	X		
	Limitaciones en la capacidad de protección	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos																		
		Paralización de actividades		R	R		R	R		R	R						R		X	
	Desastres naturales	Exposición de datos																		
		Alteración de registros																		
		Eliminación de datos		R	R		R	R		R							R	X		
		Paralización de actividades		R	R		R	R		R							R	X		

En base al análisis cruzado de las prácticas de seguridad estratégicas y operativas en relación a los niveles de riesgos identificados para cada uno de los activos críticos en la prestación de los servicios académicos, se identificaron las prácticas que deben ser reforzadas por la universidad a través de un Plan de mitigación, las mismas que se muestran a continuación.

Tabla 31. Plan de mitigación de prácticas de seguridad débiles en el ámbito estratégico (Gobierno y Gestión)

Práctica estratégica	Actividades a realizar	Tiempo promedio estimado de ejecución	Tiempo de inicio	Responsables
1. Instrucción, concienciación y nivel de comprensión en seguridad	a. Aclarar y documentar los roles y responsabilidades de seguridad de la información en toda la universidad. b. Crear un Plan Anual de Concientización y Formación (phishing, manejo de datos sensibles, seguridad de contraseñas) para todo el personal administrativo y docente. c. Implementar simulacros de ingeniería social (phishing) para evaluar la efectividad de la capacitación	4-6 meses (Implementación inicial)	Inmediato	**Implementación:** Dirección de RR.HH. y Jefatura de Seguridad (o quien haga sus veces) **Ejecución/Sostenimiento:** Jefatura de Seguridad (o quien haga sus veces).
2. Puesta en marcha de la estrategia y las tareas de seguridad	d. Designar un responsable (CISO o equivalente) o un Comité de Seguridad de la Información con autoridad formal. e. Desarrollar un Plan Maestro de Seguridad de la Información a mediano plazo, alineado a estándares (ej. ISO 27001).	6 meses	+ 1 mes	**Implementación:** Dirección General de Administración. **Ejecución/Sostenimiento:** Comité de Seguridad (o quien haga sus veces).
3. Administración de la seguridad de la información / 4. Estructura regulatoria y lineamientos de seguridad	f. Formalizar la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI). g. Crear o actualizar el Marco Normativo de Seguridad (Políticas de Uso Aceptable, de Control de Acceso, de Cifrado, de Backups).	8-12 meses	Inmediato	**Implementación:** Jefatura de Seguridad con apoyo legal (o quien haga sus veces **Ejecución/Sostenimiento:** Oficina de TI y Dirección de Servicios Académicos.
5. Manejo de la seguridad de la información con colaboradores externos	h. Desarrollar y aplicar cláusulas de seguridad obligatorias y Acuerdos de Nivel de Servicio (SLAs) para todos los proveedores (hosting, desarrolladores externos). i. Realizar auditorías o evaluaciones de seguridad anuales a terceros con acceso a datos o sistemas críticos (SIA).	5 meses	+ 2 meses	**Implementación:** Unidad de Compras/Asesoría Legal. **Ejecución/Sostenimiento:** Jefatura de Seguridad (o quien haga sus veces).
6. Esquemas de emergencia y recuperación ante desastres	j. Elaborar y formalizar un Plan de Continuidad de Negocio (PCN) y un Plan de Recuperación ante Desastres (DRP) enfocados en el SIA. k. Realizar pruebas periódicas (semestrales) de restauración de datos, failover y recuperación de sistemas.	9 meses	+ 3 meses	**Implementación:** Jefatura de Seguridad (o quien haga sus veces) y Oficina de TI. **Ejecución/Sostenimiento:** Oficina de TI / Comité de Crisis (o quien haga sus veces).

Tabla 32. Plan de mitigación de prácticas de seguridad débiles en el ámbito operativo (Implementación técnica y proceso)

Práctica estratégica	Actividades a realizar	Tiempo promedio estimado de ejecución	Tiempo de inicio	Responsables
1. Control de accesos lógicos	a. Revisar y reconfigurar los perfiles de acceso en el SIA y la base de datos (SGBD) para aplicar el principio de mínimo privilegio (solo el acceso estrictamente necesario). b. Implementar Autenticación Multifactor (MFA/2FA) para el acceso al SIA y para los administradores de red/base de datos (PERADM, PERAPO).	4 meses	+ 1 mes	**Implementación/Ejecución:** PERAPO / PERADM. **Sostenimiento:** Jefatura de Seguridad (o quien haga sus veces).
2. Administración de puntos débiles (Vulnerabilidades)	c. Formalizar un proceso de gestión de parches (identificación, prueba, aplicación) para el SIA y su infraestructura de soporte (servidores, SGBD). d. Realizar escaneos de vulnerabilidades periódicos (al menos trimestrales) en el SIA y firewall.	6 meses (Proceso inicial)	+ 2 meses	**Implementación/Ejecución:** PERADM / PERAPO. **Sostenimiento:** Jefatura de Seguridad (o quien haga sus veces).
3. Seguridad en el ciclo de desarrollo de aplicaciones	e. Integrar actividades de seguridad (revisión de código, pruebas estáticas y dinámicas de seguridad – SAST/DAST) en el Ciclo de Vida de Desarrollo de Software (SDLC) del SIA. f. Realizar Pruebas de Penetración (Pentesting) de caja negra y caja blanca al SIA.	12 meses (Integración completa)	+ 3 meses	**Implementación/Ejecución:** PERAPO/Desarrollo. **Sostenimiento:** Jefatura de Seguridad (o quien haga sus veces).
4. Manejo de sucesos de seguridad de la información	g. Desarrollar un Plan de Respuesta a Incidentes (PRI) formal que defina procedimientos, equipos de respuesta, canales de comunicación y escalamiento. h. Clasificar incidentes (por urgencia e impacto) y establecer los Tiempos de Atención (SLA).	5 meses	+ 1 mes	**Implementación/Ejecución:** Jefatura de Seguridad (o quien haga sus veces) y Mesa de Ayuda (o quien haga sus veces). **Sostenimiento:** Oficina de TI.
5. Control de acceso físico / Protección ambiental y de la instalación	i. Mejorar los controles de acceso al Data Center (acceso biométrico, registro de entrada/salida) y los sistemas de protección ambiental (detección y extinción de incendios).	3 meses	+ 1 mes	**Implementación:** Unidad de Logística/Oficina de TI. **Ejecución/Sostenimiento:** PERADM / Vigilancia (o quien haga sus veces).
6. Administración de la red y sistemas / Monitoreo y auditoría de registros de sucesos	j. Implementar una herramienta de Gestión de Eventos e Información de Seguridad (SIEM Security Information and Event Management) para consolidar los logs del SIA, SGBD y HWFIRE. k. Configurar reglas de correlación específicas para detectar patrones de amenazas internas y externas (múltiples fallos de inicio de sesión, picos de transferencia de datos).	5-7 meses	+ 2 meses	**Implementación/Ejecución:** PERADM. **Sostenimiento:** Jefatura de Seguridad (o quien haga sus veces).

Nota: PERADM-Personal Administrador de Infraestructura, PERAPO- Personal Administrador de Aplicaciones y Base de Datos

3.5.4. Validación del modelo de la gestión de riesgos de seguridad de la información de los servicios académicos

a. Finalidad de la validación

El propósito central de someter a validación el esquema de trabajo para la administración de riesgos, concebido como soporte de la seguridad de la información en los procedimientos vinculados a la gestión académica de la Universidad Nacional Pedro Ruiz Gallo (UNPRG), fue confirmar su pertinencia.

Dicha verificación se enfocó en evaluar la suficiencia, claridad, coherencia y relevancia de los parámetros definidos para el cumplimiento e implementación de buenas prácticas en las etapas de identificación, análisis y tratamiento del riesgo. Todo esto, en apego a los marcos de referencia reconocidos y establecidos, como la norma ISO/IEC 27005:2022 y metodologías especializadas de administración de riesgos, tal como OCTAVE-S, a través de una evaluación de especialistas.

b. Criterios para la selección de especialistas

Para la elección de los especialistas se consideraron los siguientes requisitos o pautas obligatorias:

- Ejercicio profesional: Ser profesionales en activo cuya labor esté directamente relacionada con el ámbito de la administración de riesgos y la seguridad de la información.
- Experiencia mínima: Acreditar una trayectoria profesional en el campo de al menos cinco (5) años.

Finalmente, el modelo de gestión de riesgos propuesto fue validado por un grupo compuesto por tres (3) expertos, los cuales se identifican a continuación:

Tabla 33. Especialistas en la evaluación del modelo

	Evaluador 1	**Evaluador 2**	**Evaluador 3**
Apellidos y Nombres	Celi Arévalo Ernesto	Zocón Alva Oscar	Jeffry Stokely Musayón Díaz
Formación académica y profesional	- Ingeniero en Computación e Informática - Maestro en Ciencias (Informática y Sistemas) - Doctor en Administración - Certificado en Ciencia de Datos - Certificado en implementación de ISO 27001:2014	- Ingeniero de Computación y Sistemas - Maestro en Ingeniería de Sistemas - Certificado ITIL - Certificado en ISO 27001:2007 - Especialización en Dirección de Proyectos y Calidad PMI	- Ingeniero de Sistemas - Maestro en Dirección de Tecnologías de la Información (ESAN) - Maestro en Administración (ESAN) - Certificado en ISO 27001:2007 - Formulación y evaluación de proyectos de inversión
Ámbito de desempeño profesional	- Auditor Senior de Tecnologías de Información	- Consultor en proyectos PMI - Auditor en	- Gestión de proyectos PMI - Gestión de

	- Especialista en Sistemas de Gestión de la Seguridad de la Información (ISO 27001) - Docencia universitaria (cursos de seguridad de la información y gestión de riesgos)	seguridad de la información	proyectos ágiles con SCRUM - Administración de riesgos - Certificado CCNA (Cisco Networking Academy)
Experiencia profesional (en años)	30	25	24
Cargos relevantes desempeñados	- Ex Director Escuela de Ingeniería de Sistemas de la UNPRG - Pas presidente del Capítulo de Ingeniería Industrial y Sistemas el CIP-CD Lambayeque - Auditor externo en TI (entidades micro financieras)	- Docente Universitario - Consultor en seguridad de la información - Consultor en gestión de proyectos PMI	- Jefe de proyectos (SUNAT) - Project Manager TI (Safetypay del Peru) - Project Manager (Fidelity International) - Oficial de seguridad de TI (estrategias digitales)
Entidad laboral actual	- Consultor independiente - Diversas universidades de Lambayeque	- Consultor independiente - Universidad Nacional de Cajamarca	- PSS - Jefe de proyectos – Banco Falabella

c. Instrumento de verificación del modelo

Se diseñó un cuestionario como herramienta principal para que los expertos pudieran valorar el modelo propuesto. El propósito del diseño de esta herramienta fue examinar y constatar el cumplimiento de las buenas prácticas, tareas o actividades recomendadas por los marcos de referencia de gestión de riesgos en cada una de sus fases.

La estructura de esta herramienta de evaluación se describe a continuación:

Tabla 34. Estructura detallada del cuestionario para especialistas

Fase de la administración de riesgos	**Actividad o tarea específica a evaluar**
Identificación y Análisis de riesgos	1. Determinación de los activos de información del proceso bajo evaluación.
	2. Estimación de la criticidad de los activos para seleccionar aquellos considerados críticos.
	3. Definición de los requisitos de seguridad específicos para cada activo crítico.
	4. Valoración de las estrategias y prácticas de seguridad implementadas actualmente por la organización.
	5. Metodología empleada para identificar las amenazas sobre los activos críticos.
	6. Identificación de las vulnerabilidades existentes.
	7. Determinación del nivel de exposición al riesgo.
	8. Establecimiento de pautas para la valoración de los impactos y la probabilidad de ocurrencia.
	9. Valoración de las consecuencias (impactos) de las amenazas.
	10. Valoración de la Probabilidad de materialización de las amenazas.
	11. Definición del procedimiento para el cálculo del nivel de exposición al riesgo.
	12. Definición del sistema de categorización de los niveles de riesgos y la

	determinación del apetito del riesgo.
Tratamiento del riesgo	13. Procedimiento para determinar las brechas de seguridad de la información basada en las debilidades detectadas.
	14. Propuesta de estrategias o actividades de mitigación en las áreas o dominios de seguridad de la información catalogada como débiles.

d. Criterios de valoración y escala utilizada

La evaluación de cada fase, actividad o tarea dentro del modelo propuesto se realizó utilizando los siguientes criterios de validación:

- Suficiencia
- Claridad
- Coherencia
- Relevancia

Para emitir el juicio sobre estos criterios, se empleó una escala cualitativa ordinal de cinco (5) niveles: Muy Malo (1), Malo (2), Regular (3), Bueno (4) y Muy Bueno (5).

Tabla 35. Esquema de puntuación del modelo de gestión de riesgos por juicio de especialistas

Parámetro de valoración	Descripción del indicador	Escala de puntuación				
		Muy deficiente	Deficiente	Aceptable	Satisfactorio	Sobresaliente
Suficiencia	Nivel en que la tarea o metodología propuesta en el modelo es adecuada para alcanzar el fin previsto de la actividad o fase.					
Claridad	Facilidad con la que se entiende y asimila la metodología, así como el uso de los formatos o documentos de apoyo necesarios para ejecutar la labor.					
Coherencia	Consistencia en la organización y el orden lógico de las tareas y metodologías, garantizando el cumplimiento efectivo de los objetivos en cada etapa de la administración de riesgos.					
Relevancia	Importancia y pertinencia de las labores y metodologías detalladas en el marco de gestión de riesgos, juzgadas según su carácter indispensable.					

e. Metodología empleada para la administración del instrumento de puntuación

Para aplicar el cuestionario de valoración al modelo diseñado, se siguió la siguiente secuencia de pasos:

1. Contacto y compromiso: Se estableció comunicación telefónica con cada especialista para solicitar su colaboración y asegurar su compromiso con la revisión, explicando detalladamente la finalidad de la investigación.

2. Presentación y distribución del material: Mediante encuentros virtuales, se realizó una presentación detallada del modelo desarrollado. Posteriormente, se les remitió una copia del modelo junto con el formulario de evaluación correspondiente.
3. Recepción y análisis de datos: Una vez devueltos los formularios de evaluación con las puntuaciones asignadas por los expertos, las calificaciones fueron compiladas y tabuladas con el objetivo de calcular una calificación promedio global.

f. Resultados de la evaluación del modelo

Esta tabla muestra las calificaciones asignadas por los tres expertos a cada actividad del modelo y el promedio resultante para cada criterio de evaluación:

Tabla 36. Consolidado de la evaluación del modelo por juicio de expertos

Fase de la gestión de riesgos	Actividad / Tarea	Suficiencia	Prom	Claridad	Prom	Coherencia	Prom	Relevancia (P1/P2/P3)	Prom
Identificación y análisis de riesgos	1. Identificación de los activos de información	5/5/5	**5.00**	5/5/4	**4.67**	5/5/4	**4.67**	5/5/5	**5.00**
	2. Evaluación de la criticidad de los activos	4/5/4	**4.33**	4/5/4	**4.33**	5/5/5	**5.00**	5/5/5	**5.00**
	3. Identificación de los requisitos de seguridad	4/5/4	**4.33**	4/4/3	**3.67**	4/5/4	**4.33**	5/5/4	**4.67**
	4. Evaluación de estrategias y prácticas de seguridad implementadas	5/5/5	**5.00**	4/5/5	**4.67**	4/5/5	**4.67**	5/5/5	**5.00**
	5. Procedimiento para identificar las amenazas	4/5/4	**4.33**	4/5/4	**4.33**	5/5/4	**4.67**	4/5/5	**4.67**
	6. Identificación de las vulnerabilidades existentes	5/5/5	**5.00**	5/5/5	**5.00**	5/5/5	**5.00**	5/5/5	**5.00**
	7. Evaluación del nivel de exposición al riesgo	4/4/5	**4.33**	4/5/5	**4.67**	4/5/5	**4.67**	5/5/5	**5.00**
	8. Establecimiento de criterios para impactos y probabilidades	5/5/4	**4.67**	5/5/4	**4.67**	5/5/4	**4.67**	5/5/5	**5.00**
	9. Valoración de los impactos de las amenazas	4/5/4	**4.33**	4/4/3	**3.67**	4/5/4	**4.33**	5/5/4	**4.67**
	10. Valoración de la Probabilidad de materialización	4/5/4	**4.33**	4/4/3	**3.67**	4/5/4	**4.33**	4/5/4	**4.33**
	11. Definición del procedimiento para el cálculo del nivel de exposición	5/5/5	**5.00**	5/5/5	**5.00**	5/5/5	**5.00**	5/5/5	**5.00**
	12. Definición del sistema de categorización y apetito del riesgo	4/4/3	**3.67**	3/4/3	**3.33**	4/4/3	**3.67**	5/5/4	**4.67**
Tratamiento del riesgo	13. Procedimiento para determinar las brechas de seguridad	4/5/4	**4.33**	4/5/4	**4.33**	5/5/5	**5.00**	5/5/5	**5.00**
	14. Planteamiento de estrategias de mitigación	5/5/5	**5.00**	4/5/5	**4.67**	5/5/5	**5.00**	5/5/5	**5.00**
Promedio total por criterio			**4.57**		**4.38**		**4.64**		**4.86**

Los resultados demuestran que el modelo para la gestión de riesgos ha sido validado positivamente por los expertos, pues la puntuación promedio general en todos los criterios es superior a 4.0 ("Satisfactorio"), indicando que es un modelo sólido, completo y pertinente.

La interpretación por cada criterio se desarrolla a continuación:

Relevancia (Promedio: 4.86)

El criterio de Relevancia (importancia y necesidad) obtuvo la puntuación más alta. Esto significa que los expertos consideran que todas las tareas y procedimientos establecidos en el modelo son esenciales y pertinentes para una gestión efectiva del riesgo en el contexto de la gestión académica. Por lo que concluimos que el modelo aborda los aspectos críticos del proceso, lo cual es fundamental para justificar su implementación.

Coherencia (Promedio: 4.64)

La Coherencia (orden y lógica de las etapas) también recibió una calificación muy alta. Esto confirma que la secuencia de las fases (Identificación, Análisis y Tratamiento) y el flujo de trabajo entre actividades son lógicos y bien estructurados. El modelo sigue un camino metodológico claro, lo que facilita su comprensión y aplicación por parte de los equipos que administran los sistemas.

Suficiencia (Promedio: 4.57)

El alto promedio en Suficiencia indica que la mayoría de las tareas y procedimientos desarrollados son adecuados y completos para alcanzar los objetivos de cada fase. Las actividades de identificación de activos (5.00) y vulnerabilidades (5.00), así como el procedimiento de cálculo del nivel de exposición (5.00), son considerados totalmente suficientes. Las únicas áreas con margen de mejora se centran en la definición del apetito del riesgo.

Claridad (Promedio: 4.38)

El criterio de Claridad (facilidad de entendimiento y uso de formatos) obtuvo la puntuación de “Aceptable”. Esto sugiere que, si bien el modelo es teóricamente correcto, la documentación o la explicación de la metodología práctica podrían ser más específicas en ciertos puntos. Las puntuaciones más bajas se concentran en las actividades que requieren mayor cuantificación (valoración de impactos y probabilidad) y la definición del apetito de riesgo.

Como conclusión general de la valoración del modelo podemos plantear que el modelo es considerado relevante y coherente en su diseño. Las sugerencias de mejora deben centrarse en aumentar la claridad de los instrumentos de medición (Puntos 9 y 10) y en formalizar la definición del apetito del riesgo (Punto 12) para facilitar la toma de decisiones en la fase de Tratamiento.

IV. DISCUSIÓN DE RESULTADOS

La discusión de los resultados obtenidos permitió establecer la relación entre los hallazgos de la presente investigación y los antecedentes revisados, así como con los fundamentos teóricos que sustentaron el desarrollo del modelo propuesto. En este sentido, se analizó cómo los resultados alcanzados respondieron a los objetivos de la investigación y cómo estos se alinearon con los principios de la gestión de riesgos de seguridad de la información definidos por los marcos ISO/IEC 27005:2022 y la metodología OCTAVE-S.

En relación con los antecedentes

Los resultados evidenciaron que el **modelamiento de la gestión de riesgos** desarrollado para los servicios académicos de la UNPRG coincidió conceptualmente con las propuestas de estudios previos que adoptaron enfoques basados en normas internacionales para fortalecer la seguridad de la información.

En correspondencia con **Quispe (2020)**, quien elaboró un modelo de evaluación de riesgos en un proceso académico universitario basado en la ISO/IEC 27005, el presente estudio corroboró la efectividad de utilizar dicho estándar para identificar y priorizar amenazas y vulnerabilidades en contextos educativos. Sin embargo, a diferencia del enfoque de Quispe, centrado en la viabilidad de adoptar servicios en la nube, el modelo de la UNPRG amplió su aplicación a todos los procesos de gestión académica, logrando una visión integral de los riesgos institucionales.

Asimismo, los resultados guardaron estrecha relación con la investigación de **Yarleque y Sandoval (2022)**, quienes integraron la ISO/IEC 27005 y COBIT 2019 para gestionar los riesgos en una entidad pública. De manera análoga, el presente estudio demostró que con la ayuda de un marco estructurado facilita la alineación entre los objetivos institucionales y las estrategias de seguridad. Sin embargo, la diferencia principal radicó en que el modelo propuesto para la UNPRG priorizó un enfoque operativo más que de gobernanza, enfocado en los activos críticos de los servicios académicos.

En sintonía con **Santos (2024)**, quien empleó ontologías de dominio para estandarizar conceptos de riesgo, los hallazgos confirmaron la importancia de la claridad y consistencia en la terminología. Durante la validación por juicio de expertos, se destacó la **coherencia conceptual** del modelo, lo que refleja una mejora en la comprensión del proceso de gestión de riesgos dentro de la institución.

Los resultados también coincidieron con los de **De la Cruz y Paz (2024)**, quienes adaptaron la ISO/IEC 27005 al contexto hospitalario para atender vulnerabilidades locales. En el caso de la UNPRG, el modelo igualmente adaptó los lineamientos del estándar al entorno académico, demostrando que los marcos internacionales pueden ser contextualizados exitosamente para responder a necesidades específicas, manteniendo la eficacia en la identificación y tratamiento de riesgos.

Por otra parte, los hallazgos relacionados con la baja implementación de políticas formales y planes de contingencia en la UNPRG guardan relación con lo reportado por **Apaza y Zúñiga (2021) y Céspedes (2020),** quienes evidenciaron en sus investigaciones la falta de estructuras de gestión de riesgos en universidades y hospitales, respectivamente. En ambos casos, los modelos propuestos sirvieron como base para formalizar procesos, coincidiendo con la finalidad de la presente tesis de ofrecer un marco aplicable a nivel institucional.

Finalmente, el modelo validado en esta investigación respondió de manera coherente a la tendencia observada en los antecedentes más recientes, que destacan la integración de ISO/IEC 27005 con la metodología OCTAVE-S como combinación óptima para fortalecer la gestión de la seguridad de la información en contextos públicos y educativos. El modelo propuesto logró consolidar ambos enfoques, aportando una estructura aplicable, validada y alineada con las buenas prácticas internacionales.

En relación con los fundamentos teóricos

El desarrollo y validación del modelo demostraron la aplicación práctica de los fundamentos teóricos revisados en el punto 1.3. En primer lugar, los resultados confirmaron que la **información constituye un recurso estratégico**, tal como lo plantean Valles-Coral (2023) y Rodríguez & Gallego (2022). La identificación de activos críticos (SIA, GESTAC, bases de datos, redes, personal) y su clasificación dentro del proceso de gestión académica evidenció que la información y su disponibilidad son esenciales para el cumplimiento de los objetivos institucionales.

De acuerdo con los principios de la **Seguridad de la Información**, el estudio demostró que los tres pilares fundamentales —confidencialidad, integridad y disponibilidad— fueron los más afectados por la ausencia de controles formales y políticas de seguridad. El diagnóstico inicial mostró deficiencias en la concienciación del personal, la falta de lineamientos normativos y la inexistencia de un plan de continuidad, lo que coincidió con lo señalado por ISOTools (2025) sobre la necesidad de fortalecer la cultura de seguridad para garantizar la continuidad operativa. En relación con el **Sistema de Gestión de la Seguridad de la Información (SGSI)**, los resultados reflejaron que la Universidad no contaba con un marco formal de gestión, aunque existían esfuerzos aislados por parte de la Oficina de Tecnologías de la Información. La aplicación del modelo propuesto permitió establecer una base estructurada de gestión de riesgos, siguiendo el ciclo PDCA de la norma ISO/IEC 27001, lo cual respondió directamente al objetivo general del estudio. Este hallazgo se alineó con lo expuesto por Alcívar-Cruz & Llerena-Izquierdo (2023), quienes resaltan que la gestión de riesgos constituye el núcleo del SGSI.

En cuanto a la **gestión de riesgos de seguridad de la información**, los resultados permitieron aplicar de manera completa las fases propuestas por la ISO/IEC 27005:2022: establecimiento del contexto, identificación, análisis, evaluación y tratamiento de riesgos. La identificación de 13 activos críticos y la posterior evaluación de sus vulnerabilidades permitió establecer una matriz

de exposición al riesgo. El análisis mostró que los riesgos con niveles de impacto alto estaban asociados a los procesos de matrícula y generación de actas, lo que confirma la importancia de adoptar estrategias de tratamiento adecuadas, tal como lo plantean Pirani (2025) y SUNAT (2023).

Por último, el uso de la **metodología OCTAVE-S** demostró su pertinencia para entornos educativos de tamaño medio, dado que facilitó la participación colaborativa del personal académico y técnico en la identificación de amenazas y vulnerabilidades. La metodología permitió construir perfiles de amenaza basados en activos y definir planes de tratamiento, reforzando los hallazgos de Alberts et al. (2003) y De La Cruz & Paz (2024) sobre la aplicabilidad de OCTAVE en organizaciones con estructuras administrativas complejas.

En función de los objetivos de la investigación

En relación con el **primer objetivo específico**, que buscaba identificar las amenazas a la seguridad de la información, el modelo propuesto permitió reconocer 41 amenazas y 32 vulnerabilidades que afectaban a los activos críticos. Este resultado validó la eficacia del modelamiento propuesto para la identificación, pues se alcanzó una cobertura del 100% de los procesos académicos analizados, superando la situación inicial de desconocimiento institucional sobre los riesgos.

Respecto al **segundo objetivo específico**, orientado a estimar el nivel de exposición al riesgo, se obtuvo una matriz cuantitativa que clasificó los riesgos en rangos muy alto, alto, medio y bajo. Los resultados revelaron que el 37% de los riesgos se ubicaron en niveles no aceptables (alto o muy alto), confirmando la necesidad de implementar controles preventivos. Este hallazgo fue coherente con la definición de riesgo residual establecida por la norma ISO/IEC 27005, evidenciando la validez del modelo para la evaluación de exposición.

En cuanto al **tercer objetivo específico**, relacionado con la identificación de prácticas de seguridad y controles, se establecieron medidas correctivas basadas en los dominios de seguridad definidos por OCTAVE. Entre los controles propuestos destacaron: la formalización de políticas de seguridad institucional, la capacitación continua del personal, la implementación de planes de contingencia y la actualización de las configuraciones de red y sistemas. Estos controles fueron evaluados por los expertos como pertinentes y aplicables, con un promedio de aceptación del 92% en las dimensiones de suficiencia y coherencia.

Finalmente, el **cuarto objetivo específico**, correspondiente a la validación del modelo, fue alcanzado mediante la aplicación del juicio de expertos, cuyos resultados evidenciaron niveles de valoración promedio de 4.8 en una escala de 5 puntos. Esto confirmó la claridad, relevancia y aplicabilidad del modelo propuesto, validando su alineación con las buenas prácticas de la **ISO/IEC 31000:2018** y **OCTAVE-S**.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se logró la identificación exhaustiva de las amenazas, demostrando que el modelamiento propuesto es altamente efectivo. Las amenazas más significativas provienen de los actores internos y externos intencionados a través de la infraestructura de red, seguidas por fallas técnicas y la inadecuada gestión de componentes clave como la Obsolescencia del software o las Contraseñas mal administradas en el Firewall. El enfoque de OCTAVE-S permitió canalizar esta identificación directamente hacia la evaluación de los activos críticos, lo que garantiza que las amenazas identificadas son las que realmente pueden impactar la operación de los servicios académicos (SIA, Base de Datos y Firewall).

2. La estimación de riesgos reveló que las mayores exposiciones se concentran en un Nivel de Riesgo Muy Alto o Alto, especialmente aquellas relacionadas con la Paralización de actividades y la Alteración/Eliminación de datos en los tres activos críticos. El modelamiento demostró ser altamente eficaz para esta estimación al utilizar una fórmula de riesgo ponderada que integra el Impacto sobre áreas estratégicas (Prioridad 1: Administrativo, Prioridad 4: Reputación) y la Probabilidad histórica. La estimación mostró que las amenazas intencionadas con impacto en la productividad (Paralización/Alteración) son las de mayor prioridad, lo cual valida el modelamiento como una herramienta precisa y útil para priorizar el tratamiento de riesgos en la UNPRG.

3. Se identificaron con éxito las prácticas de seguridad y los controles de mitigación necesarios para los riesgos clasificados como no aceptables (Alto y Muy Alto). El modelamiento resultó ser efectivo, ya que la identificación de controles fue directamente impulsada por los riesgos de mayor nivel, enfocándose en la Mitigación como estrategia principal para la mayoría de las amenazas intencionadas y de fallas técnicas. Las prácticas operacionales como el Control de accesos lógicos, el Monitoreo y auditoría de registros, y la Administración de puntos débiles son las más requeridas, demostrando la necesidad de fortalecer el día a día de la operación de TI para asegurar los servicios académicos.

4. El modelamiento propuesto fue validado satisfactoriamente contra las buenas prácticas de la ISO/IEC 31000:2018 y OCTAVE-S. Demostró una alta suficiencia al cubrir todas las fases del ciclo de riesgo; una alta claridad en la definición de términos y pasos para su implementación; una estricta coherencia al alinear el análisis de impacto con los objetivos de la Universidad (perspectiva de servicios académicos); y una gran relevancia al incorporar el enfoque de activos críticos de OCTAVE-S. Esta validación asegura que el modelo no solo es funcional en el contexto local, sino que es robusto y se adhiere a los estándares internacionales de gestión de riesgos de seguridad de la información.

5. El modelamiento de la gestión de riesgos de seguridad de la información debe estar compuesto por tres elementos estructurales críticos y un enfoque funcional integrado: **Una estructura crítica** conformado por un conjunto delimitado de activos esenciales (SIA, Servicio de Gestión de Base de Datos y Firewall) que soportan directamente los servicios académicos, donde se concentra el análisis de riesgo. **Una base metodológica** sólida en la norma ISO/IEC 27005:2022 que defina el ciclo de vida del proceso (identificación, análisis, evaluación y tratamiento), complementada con el enfoque centrado en activos y amenazas de la metodología OCTAVE-S, y **métrica de riesgo cuantificable** para ponderar las consecuencias (Impacto) en dimensiones relevantes (Reputación, Productividad, Económico y Administrativo) frente a la Probabilidad de ocurrencia, permitiendo una estimación precisa del nivel de exposición.

   Estos elementos definen un modelo que no solo cumple con estándares internacionales, sino que está ajustado a la realidad operacional de la UNPRG, permitiendo la identificación de controles específicos para mitigar los riesgos no aceptables y, por ende, soportar eficazmente la operación y continuidad de los servicios académicos.

RECOMENDACIONES

1. La investigación identificó prácticas de seguridad y controles para mitigar los riesgos No Aceptables (Nivel Alto y Muy Alto). Sin embargo, el siguiente paso crítico es transformar estas prácticas genéricas en procedimientos operativos específicos e implementarlos. Se recomienda desarrollar un estudio de tipo aplicado o de acción que se centre en la ingeniería del cambio necesaria para implementar los controles priorizados. Este estudio debe: crear documentos de política y procedimientos detallados, establecer métricas de efectividad (KPIs) para cada control, que permitan medir la reducción del nivel de riesgo residual a un estado Aceptable o Bajo, y ejecutar una prueba piloto de los controles más urgentes (ej. fortalecimiento de la seguridad del Firewall y Base de Datos) y re-evaluar el riesgo residual después de la implementación.

2. El análisis de impacto y probabilidad reveló que gran parte de los riesgos de Muy Alto/Alto nivel provienen de actores internos y externos intencionados, así como de vulnerabilidades operacionales (ej. contraseñas débiles, reglas permisivas). Esto apunta a una brecha en la cultura de seguridad. Se recomienda complementar el modelamiento técnico actual (enfocado en SIA, BD, Firewall) con una Evaluación de Riesgo Organizacional y de Concienciación, aplicando encuestas detalladas y pruebas de phishing simuladas al personal administrativo y docente para medir el factor de riesgo humano (Madurez de concienciación) e incorporar la perspectiva del activo humano como un cuarto activo crítico.

3. El modelo propuesto define el ciclo Plan-Do (identificación y tratamiento), pero un sistema de gestión de riesgos requiere el componente Check (Monitoreo) y Act (Revisión/Mejora). Se recomienda diseñar un Protocolo de Gestión de Incidentes de Seguridad de la Información para la UNPRG, bajo los lineamientos de la ISO/IEC 27035. Este protocolo debe incluir la definición

de Umbrales de riesgo y las alertas automatizadas para los sistemas monitoreados (SIA, BD, Firewall), un flujo de trabajo (workflow) claro para la detección, escalamiento, contención, erradicación y recuperación de los incidentes de seguridad que materialicen los riesgos de alto nivel.

REFERENCIAS BIBLIOGRÁFICAS

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003). *Introduction to the OCTAVE® Approach* (No. CMU/SEI-2003-TR-017). Software Engineering Institute, Carnegie Mellon University.

Alcívar-Cruz, J. C., & Llerena-Izquierdo, A. (2023). Revisión de literatura de la norma ISO/IEC 27001 en el sector de las telecomunicaciones de la ciudad de Guayaquil: Evaluación de la seguridad de las. (Tesis de maestría). Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/28028/1/UPS-GT005471.pdf

Apaza, L. M., & Zúñiga, G. H. (2021). *Propuesta de un marco de gestión de riesgos de TI basado en ISO 31000:2018 para la Universidad Nacional de Ingeniería* [Tesis de maestría, Universidad Nacional Mayor de San Marcos]. Repositorio de la UNMSM.

BSI Group. (2025). *ISO/IEC 27001: Sistema de Administración de la seguridad de la información*. https://www.bsigroup.com/es-ES/products-and-services/standards/iso-iec-27001-information-security-management-system/

BSI Group. (2025). *ISO/IEC 27001: Sistema de Administración de la seguridad de la información*. https://www.bsigroup.com/es-PE/products-and-services/standards/iso-iec-27001-information-security-management-system/

Céspedes, C. R. (2020). *Modelo de gestión de riesgos de tecnologías de información basado en la ISO/IEC 27005 para el Hospital Privado Juan Pablo II de la ciudad de Chiclayo* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional UCV.

Chirou, Á. (2024). *Políticas ISO 27001: Una guía completa para 2025*. Álvaro Chirou. https://achirou.com/politicas-iso-27001-una-guia-completa-para-2025/

CORE. (2025). *Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte*. https://core.ac.uk/download/pdf/304901839.pdf

De La Cruz, C. A., & Paz, L. A. (2024). *Desarrollo de una metodología AD HOC de gestión de riesgos informáticos basada en ISO 27005 para un hospital regional: Caso de estudio hospital regional Lambayeque* [Tesis de pregrado, Universidad Señor de Sipán]. Repositorio Institucional USS.

GlobalSuite Solutions. (2023). *Ciclo PDCA de gestión de la ISO 27001*. https://www.globalsuitesolutions.com/es/ciclo-pdca-iso-27001/

Gobierno de Perú. (2024). *Sistema de Administración de la seguridad de la información*. Plataforma Digital Única del Estado Peruano. https://info.qaliwarma.gob.pe/pubweb/sgsi/

InfoProtección. (2025). *Mejora contínua*. https://www.infoproteccion.com/iso-27001/mejora-continua/

Intedya. (2023). *ISO 27000 y el conjunto de estándares de Seguridad de la Información*. https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-%20estandares-de-seguridad-de-la%20informacion.html

IPES. (2025). *Gestión de riesgos de seguridad y privacidad de la información*. Alcaldía Mayor de Bogotá. https://ipes.gov.co/images/informes/SDE/Planes_2018/DE-038_GESTION_DE_RIESGOS_DE_SEGURIDAD_Y_PRIVACIDAD_DE_LA_INFORMACION.pdf

ISMS.online. (2025). *¿Qué es ISO/IEC 27005 y el estándar de gestión de riesgos de seguridad?*. https://es.isms.online/iso-27005/

ISOTools Perú. (2022). *ISO 27001: La implementación de un Sistema de Administración de la seguridad de la información mediante el ciclo PHVA*. https://pe.isotools.us/iso-27001-implementacion-sistema-gestion-seguridad-informacion-ciclo-phva/

Magagnotti, C. (2022). *ISO27001:2022 ¿Qué es el enfoque PHVA y para qué sirve?*. Clau Magagnotti. https://www.claumagagnotti.com/post/iso27001-2022-qu%C3%A9-es-el-enfoque-phva-y-para-qu%C3%A9-sirve

MinCiencias. (2025). *Plan Estratégico de Seguridad de la Información 2025*. Ministerio de Ciencia, Tecnología e Innovación de Colombia. https://especiales.minciencias.gov.co/wp-content/uploads/2025/01/D103DE02_Plan-Estrategico-de-seguridad-de-la-informacio%CC%81n-V02.pdf

Mineducación. (2023). *Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023*. Ministerio de Educación Nacional de Colombia. https://www.mineducacion.gov.co/1780/articles-413730_recurso_18.pdf

Ministerio de Salud y Protección Social de Colombia. (2025). *Plan de gestión de riesgos de seguridad y privacidad de la información*. https://www.minsalud.gov.co/sites/rid/Lists/BibliotecaDigital/RIDE/DE/OT/plan-gestion-riesgo-seguridad-privacidad-informacion.pdf

MinTIC. (2025). *Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información*. Ministerio de Tecnologías de la Información y las Comunicaciones. https://www.mintic.gov.co/portal/715/articles-403045_recurso_1.pdf

Niño, N. R. (2018). *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el Instituto Nacional de Estadística e Informática - INEI Filial Lambayeque* [Tesis de maestría, Universidad Nacional Pedro Ruiz Gallo]. Repositorio Institucional UNPRG.

normaiso27001.es. (2024). *Implantando ISO 27001 paso a paso - La Planificacion del SGSI*. https://www.normaiso27001.es/fase-4-planificacion-del-sgsi/

NQA. (2022). *ISO 27001:2022 - Guía de implantación*. https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

ORSYS. (2025). *Definición Norma ISO 27005*. https://www.orsys.fr/orsys-lemag/es/glosario/norma-iso-27005-%F0%9F%9F%A6/

Paredes, J. E., Gonzales, J. C., & Rojas, S. C. (2019). Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. *Revista Peruana de Computación y Sistemas*, *2*(2), 43-60. http://dx.doi.org/10.15381/rpcs.v2i2.17103

Pensemos. (2024). *Sistema de Administración de la seguridad de la información: qué es y sus etapas*. https://gestion.pensemos.com/sistema-de-gestion-de-seguridad-de-la-informacion-que-es-etapas

Pirani. (2025). *¿Cómo gestionar riesgos con la metodología ISO 27005?*. https://www.piranirisk.com/es/blog/como-gestionar-riesgos-con-la-metodologia-iso-27005

Pirani. (2025). *¿Cómo gestionar riesgos con la metodología ISO 27005?*. https://www.piranirisk.com/es/blog/como-gestionar-riesgos-con-la-metodologia-iso-27005

Poder Judicial del Perú. (2025). *Guía: Gestión de Riesgos del Sistema de Gestión Antisoborno y del Sistema de Administración de la seguridad de la información*. https://www.pj.gob.pe/wps/wcm/connect/46cf9e804560fd2c850dcde5406a4592/Guia+GESTIO

N+DE+RIESGOS+SGA+y+SGSI+%284%29.pdf?MOD=AJPERES&CACHEID=46cf9e804560fd2c850dcde5406a4592

PRONABEC. (2024). *Sistema de Administración de la seguridad de la información*. Programa Nacional de Becas y Crédito Educativo. https://www.pronabec.gob.pe/sistema-de-gestion-de-seguridad-de-la-informacion/

Quispe, L. J. (2020). *Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 27005 para analizar la viabilidad de adoptar servicios en la nube* [Tesis de maestría, Universidad Peruana de Ciencias Aplicadas]. Repositorio Académico UPC.

Rodríguez, I. M., & Gallego, C. (2022). La información como activo estratégico de una empresa. *Revista Semilla Científica*, *(3)*, 162–169. https://revistas.umecit.edu.pa/index.php/sc/article/view/1087

Samaniego, D. M. (2024). *Propuesta de una evaluación de la normativa ISO 27005:2022 para la Gestión de Riesgos de la Seguridad de la Información: caso estudio Distribuidora AMC* [Tesis de maestría, Universidad Israel]. Repositorio Digital Universidad Israel.

Santos, D. E. (2024). *Gestión de riesgos de seguridad de información, bajo el estándar ISO/IEC 27005:2022, aplicando ontologías de dominio* [Tesis de maestría, Pontificia Universidad Católica del Perú]. Tesis PUCP.

Secureframe. (2023). *El Enfoque ISO 27005 para la Gestión de Riesgos de Seguridad de la Información: Explicación de las Actualizaciones de 2022*. https://secureframe.com/es-es/blog/iso-27005

Secureframe. (2023). *El Enfoque ISO 27005 para la Gestión de Riesgos de Seguridad de la Información: Explicación de las Actualizaciones de 2022*. https://secureframe.com/es-es/blog/iso-27005

SUNAT. (2023). *Manual Políticas del Sistema de Administración de la seguridad de la información SGSI-MA-03*. Superintendencia Nacional de Aduanas y de Administración Tributaria de Perú. https://www.sunat.gob.pe/legislacion/superin/2023/ANEXO-SGSI-MA-03-000148-2023.pdf

Universidad Pedagógica y Tecnológica de Colombia. (2022). *Modelo de Seguridad y Privacidad de la Información 2022-2024*. UPTC.

Valles-Coral, M. A. (2023). La información como activo estratégico y de valor para las organizaciones. *Revista Científica de Sistemas e Informática*, *3*(1), e496. https://doi.org/10.51252/rcsi.v3i1.496

Yarleque, L. M., & Sandoval, J. C. (2022). *Marco de trabajo basado en la ISO 27005 y COBIT 2019 para la gestión de riesgos en el Sistema Integrado Judicial Supremo* [Tesis de maestría, Universidad César Vallejo]. Repositorio Institucional UCV.

Yungán Cazar, J. C., & Narváez Contero, C. V. (2022). Aplicación de la Norma ISO 27001 para la seguridad de los Sistemas de Información. *Dominio de las Ciencias*, *8*(3), 1025–1041. https://doi.org/10.23857/dc.v8i3.2854

ANEXOS

Anexo 1: Guía de entrevista para el modelamiento de la gestión de riesgos de seguridad de la información

Dirigida a:

- Directivos del Vicerrectorado Académico / Dirección de Servicios Académicos
- Personal de la OTI: Administradores de sistemas, redes y bases de datos
- Usuarios clave de los servicios académicos (personal administrativo y operativos)

I. Identificación y caracterización de activos de información

Objetivo: Identificar activos, datos relevantes, función clave y componentes vinculados.

1. ¿Cuáles considera que son los sistemas, servicios o recursos tecnológicos indispensables para la gestión académica diaria?
2. ¿Qué tipo de información académica se gestiona en cada uno de estos sistemas o servicios?
3. ¿Qué procesos académicos dependen directamente de cada activo identificado?
4. ¿Qué componentes tecnológicos o servicios de soporte (red, base de datos, servidores, personal) permiten su funcionamiento?
5. ¿Quién es el responsable directo de la administración o custodia de cada activo?

II. Identificación de activos críticos y criterios de criticidad

Objetivo: Determinar qué activos son críticos y por qué.

6. De los activos identificados, ¿cuáles considera irremplazables para el cumplimiento de los procesos y servicios académicos, especialmente del calendario académico?
7. ¿Qué ocurriría si alguno de estos activos dejara de operar temporalmente o de forma definitiva?
8. ¿Existen activos cuya falla detendría inmediatamente los procesos académicos?
9. ¿Qué activos requieren conocimiento técnico especializado difícil de sustituir?

III. Exigencias de seguridad de la información (CID)

Objetivo: Determinar requerimientos de confidencialidad, integridad y disponibilidad.

10. ¿Qué tan crítica es la confidencialidad de la información que maneja cada activo?
11. ¿Qué consecuencias tendría la alteración no autorizada de los datos académicos?
12. ¿En qué momentos del año es indispensable la disponibilidad continua del sistema?
13. ¿Cuál de los tres criterios (C, I o D) considera prioritario para cada activo y por qué?

IV. Identificación de amenazas y perfiles de riesgo

Objetivo: Identificar amenazas, actores, frecuencia y forma de manifestación.

14. ¿Qué incidentes o fallos recuerda que hayan afectado a los sistemas académicos?

15. ¿Estos eventos fueron causados por errores humanos, fallas técnicas o acciones maliciosas?
16. ¿Con qué frecuencia aproximada ocurren estos eventos en un año?
17. ¿Cómo se manifiestan usualmente estos incidentes (caída del sistema, alteración de datos, paralización del servicio)?
18. ¿Ha identificado riesgos asociados al acceso físico o remoto a los sistemas?

V. Identificación de vulnerabilidades de la infraestructura

Objetivo: Identificar debilidades técnicas y humanas.

19. ¿Qué fallos o debilidades técnicas existen en servidores, red o equipos?
20. ¿Existen problemas en la gestión de credenciales, parches, antivirus o configuraciones?
21. ¿Quién es el responsable del uso y custodia de cada componente?
22. ¿Dónde se ubican físicamente estos componentes?
23. ¿Qué activo crítico podría verse afectado si esta vulnerabilidad se explota?

VI. Evaluación de impactos de los riesgos

Objetivo: Valorar consecuencias según la escala institucional.

24. Si este riesgo se materializa, ¿cómo afectaría la confianza y credibilidad de los usuarios?
25. ¿Qué tipo de impacto económico generaría (costos operativos, correctivos, sanciones)?
26. ¿Cuánto se vería afectada la productividad o continuidad del servicio académico?
27. ¿Generaría procesos administrativos, sanciones o incumplimientos normativos?

VII. Probabilidad de materialización del riesgo

Objetivo: Estimar la probabilidad según frecuencia histórica.

28. ¿Con qué frecuencia ha ocurrido este tipo de evento en los últimos años?
29. ¿Considera que este riesgo es eventual, frecuente o casi permanente?
30. ¿Existen periodos críticos donde la probabilidad aumenta significativamente (matrícula, cierre de notas)?

VIII. Medidas actuales y brechas de control

31. ¿Qué controles o medidas de seguridad existen actualmente para estos riesgos?
32. ¿Considera que son suficientes, parciales o inexistentes?
33. ¿Qué acciones considera prioritarias para mejorar la gestión de riesgos de seguridad de la información?

Anexo 2: Instrumento de valoración del modelo de gestión de riesgos por juicio de expertos

IX. Identificación del evaluador

Nombre del experto evaluador	
Formación profesional	
Años de experiencia en seguridad/riesgos	
Fecha de evaluación	

II. Criterios y escala de valoración

A continuación, se presenta la escala que debe utilizarse para calificar cada actividad según el criterio correspondiente:

Valor	Niveles	Definición
1	Muy deficiente	No se cumple o es completamente inadecuado.
2	Deficiente	Se cumple con grandes deficiencias o es confuso.
3	Aceptable	Se cumple parcialmente, es mejorable y tiene puntos débiles.
4	Satisfactorio	Se cumple adecuadamente y es claro.
5	Sobresaliente	Se cumple de manera sobresaliente y es ejemplar.

III. Evaluación del modelo propuesto

Instrucciones: Asigne una puntuación del 1 al 5 a cada actividad/tarea en función del grado en que cumple con los criterios de Suficiencia, Claridad, Coherencia y Relevancia.

Fase de la gestión de riesgos	Actividad / tarea	Suficiencia (1-5)	Claridad (1-5)	Coherencia (1-5)	Relevancia (1-5)
Identificación y análisis de riesgos	Identificación de los activos de información del proceso evaluado				
	Evaluación de la criticidad de los activos para seleccionar los activos críticos				
	Identificación de los requisitos de seguridad de cada activo crítico				
	Evaluación de las estrategias y prácticas de seguridad implementadas por la organización actualmente				
	Procedimiento para identificar las amenazas sobre los activos críticos				
	Identificación de las vulnerabilidades existentes				
	Evaluación del nivel de exposición al riesgo				
	Establecimiento de criterios para la valoración de los impactos y las probabilidades de ocurrencia				
	Valoración de los impactos de las amenazas				
	Valoración de la Probabilidad de materialización de las amenazas				
	Definición del procedimiento para el cálculo del nivel de exposición al riesgo				
	Definición del sistema de categorización de los niveles de riesgos y determinación del apetito del riesgo				
Tratamiento del riesgo	Procedimiento para determinar las brechas de seguridad de la información en base a las debilidades identificadas				

	Planteamiento de estrategias o actividades de mitigación en las áreas o dominios de seguridad de la información identificadas como débiles				
Promedio general					

IV. Observaciones generales

Detalle justificaciones para las puntuaciones bajas, sugerencias de mejora o comentarios adicionales sobre el modelo propuesto:

_____

_____

_____

_____

Anexo 3: Resultados individuales de la valoración del modelo de gestión de riesgos por juicio de expertos

Experto 1

I. Identificación del evaluador

Nombre del experto evaluador	Celi Arévalo Ernesto
Formación profesional	Doctor en Administración, Auditor Senior
Años de experiencia en seguridad/riesgos	30 años de experiencia
Fecha de evaluación	16 de setiembre de 2025

II. Criterios y escala de valoración

A continuación, se presenta la escala que debe utilizarse para calificar cada actividad según el criterio correspondiente:

Valor	Niveles	Definición
1	Muy deficiente	No se cumple o es completamente inadecuado.
2	Deficiente	Se cumple con grandes deficiencias o es confuso.
3	Aceptable	Se cumple parcialmente, es mejorable y tiene puntos débiles.
4	Satisfactorio	Se cumple adecuadamente y es claro.
5	Sobresaliente	Se cumple de manera sobresaliente y es ejemplar.

III. Evaluación del modelo propuesto

Instrucciones: Asigne una puntuación del 1 al 5 a cada actividad/tarea en función del grado en que cumple con los criterios de Suficiencia, Claridad, Coherencia y Relevancia.

Fase de la gestión de riesgos	Actividad / tarea	Suficiencia (1-5)	Claridad (1-5)	Coherencia (1-5)	Relevancia (1-5)
Identificación y análisis de riesgos	Identificación de los activos de información del proceso evaluado	5	5	5	5
	Evaluación de la criticidad de los activos para seleccionar los activos críticos	4	4	5	5
	Identificación de los requisitos de seguridad de cada activo crítico	4	4	4	5
	Evaluación de las estrategias y prácticas de seguridad implementadas por la organización actualmente	5	4	4	5
	Procedimiento para identificar las amenazas sobre los activos críticos	4	4	5	4
	Identificación de las vulnerabilidades existentes	5	5	5	5
	Evaluación del nivel de exposición al riesgo	4	4	4	5
	Establecimiento de criterios para la valoración de los impactos y las probabilidades de ocurrencia	5	5	5	5
	Valoración de los impactos de las amenazas	4	4	4	5
	Valoración de la Probabilidad de materialización de las amenazas	4	4	4	4
	Definición del procedimiento para el cálculo del nivel de exposición al riesgo	5	5	5	5
	Definición del sistema de categorización de los niveles de riesgos y determinación del apetito	4	3	4	5

	del riesgo				
Tratamiento del riesgo	Procedimiento para determinar las brechas de seguridad de la información en base a las debilidades identificadas	4	4	5	5
	Planteamiento de estrategias o actividades de mitigación en las áreas o dominios de seguridad de la información identificadas como débiles	5	4	5	5
Promedio general		4.43	4.29	4.57	4.86

IV. Observaciones generales

Detalle justificaciones para las puntuaciones bajas, sugerencias de mejora o comentarios adicionales sobre el modelo propuesto:

Se recomienda incorporar una matriz de riesgo (Nivel de exposición) que no solo muestre las zonas (Deficiente, Aceptable, Satisfactorio, Sobresaliente), sino que también defina gráficamente el "Apetito del Riesgo" de la universidad. Esto debe ser aprobado por la alta dirección y debe servir como umbral obligatorio para la fase de tratamiento.

Experto 2

I. Identificación del evaluador

Nombre del experto evaluador	Oscar Zocón Alva
Formación profesional	Maestro en Ingeniería de Sistemas, Consultor en seguridad de la información, Consultor en PMI
Años de experiencia en seguridad/riesgos	25 años de experiencia
Fecha de evaluación	13/09/2025

II. Criterios y escala de valoración

A continuación, se presenta la escala que debe utilizarse para calificar cada actividad según el criterio correspondiente:

Valor	Niveles	Definición
1	Muy deficiente	No se cumple o es completamente inadecuado.
2	Deficiente	Se cumple con grandes deficiencias o es confuso.
3	Aceptable	Se cumple parcialmente, es mejorable y tiene puntos débiles.
4	Satisfactorio	Se cumple adecuadamente y es claro.
5	Sobresaliente	Se cumple de manera sobresaliente y es ejemplar.

III. Evaluación del modelo propuesto

Instrucciones: Asigne una puntuación del 1 al 5 a cada actividad/tarea en función del grado en que cumple con los criterios de Suficiencia, Claridad, Coherencia y Relevancia.

Fase de la gestión de riesgos	Actividad / tarea	Suficiencia (1-5)	Claridad (1-5)	Coherencia (1-5)	Relevancia (1-5)
Identificación y análisis de riesgos	Identificación de los activos de información del proceso evaluado	5	5	5	5
	Evaluación de la criticidad de los activos para seleccionar los activos críticos	5	5	5	5
	Identificación de los requisitos de seguridad de cada activo crítico	5	4	5	5
	Evaluación de las estrategias y prácticas de seguridad implementadas por la organización actualmente	5	5	5	5
	Procedimiento para identificar las amenazas sobre los activos críticos	5	5	5	5
	Identificación de las vulnerabilidades existentes	5	5	5	5
	Evaluación del nivel de exposición al riesgo	4	5	5	5
	Establecimiento de criterios para la valoración de los impactos y las probabilidades de ocurrencia	5	5	5	5
	Valoración de los impactos de las amenazas	5	4	5	5
	Valoración de la Probabilidad de materialización de las amenazas	5	4	5	5
	Definición del procedimiento para el cálculo del nivel de exposición al riesgo	5	5	5	5
	Definición del sistema de categorización de los niveles de riesgos y determinación del apetito del riesgo	4	4	4	5
Tratamiento del riesgo	Procedimiento para determinar las brechas de seguridad de la información en base a las debilidades identificadas	5	5	5	5

	Planteamiento de estrategias o actividades de mitigación en las áreas o dominios de seguridad de la información identificadas como débiles	5	5	5	5
Promedio general		4.86	4.79	4.93	5.00

IV. Observaciones generales

Detalle justificaciones para las puntuaciones bajas, sugerencias de mejora o comentarios adicionales sobre el modelo propuesto:

El modelo demuestra una excelente alineación con los principios de ISO/IEC 27005 y OCTAVE-S. Pero, podría mejorarse incluyendo una tabla de correspondencia que muestre explícitamente qué tareas del modelo satisfacen qué objetivos de seguridad (Cláusulas) de las normativas. Además, se recomienda anexar checklists para cada etapa clave del análisis (Activos, Vulnerabilidades, Amenazas) para asegurar una aplicación uniforme por parte de los operadores.

Experto 3

I. Identificación del evaluador

Nombre del experto evaluador	Jeffry Stokely Musayón Díaz
Formación profesional	Maestro en Dirección de TI, Jefe de Proyectos TI, Certificación ISO 27001
Años de experiencia en seguridad/riesgos	24 años de experiencia
Fecha de evaluación	21/09/2025

II. Criterios y escala de valoración

A continuación, se presenta la escala que debe utilizarse para calificar cada actividad según el criterio correspondiente:

Valor	Niveles	Definición
1	Muy deficiente	No se cumple o es completamente inadecuado.
2	Deficiente	Se cumple con grandes deficiencias o es confuso.
3	Aceptable	Se cumple parcialmente, es mejorable y tiene puntos débiles.
4	Satisfactorio	Se cumple adecuadamente y es claro.
5	Sobresaliente	Se cumple de manera sobresaliente y es ejemplar.

III. Evaluación del modelo propuesto

Instrucciones: Asigne una puntuación del 1 al 5 a cada actividad/tarea en función del grado en que cumple con los criterios de Suficiencia, Claridad, Coherencia y Relevancia.

Fase de la gestión de riesgos	Actividad / tarea	Suficiencia (1-5)	Claridad (1-5)	Coherencia (1-5)	Relevancia (1-5)
Identificación y análisis de riesgos	Identificación de los activos de información del proceso evaluado	5	4	4	5
	Evaluación de la criticidad de los activos para seleccionar los activos críticos	4	4	5	5
	Identificación de los requisitos de seguridad de cada activo crítico	4	3	4	4
	Evaluación de las estrategias y prácticas de seguridad implementadas por la organización actualmente	5	5	5	5
	Procedimiento para identificar las amenazas sobre los activos críticos	4	4	4	5
	Identificación de las vulnerabilidades existentes	5	5	5	5
	Evaluación del nivel de exposición al riesgo	5	5	5	5
	Establecimiento de criterios para la valoración de los impactos y las probabilidades de ocurrencia	4	4	4	5
	Valoración de los impactos de las amenazas	4	3	4	4
	Valoración de la Probabilidad de materialización de las amenazas	4	3	4	4
	Definición del procedimiento para el cálculo del nivel de exposición al riesgo	5	5	5	5
	Definición del sistema de categorización de los niveles de riesgos y determinación del apetito del riesgo	3	3	3	4
Tratamiento del riesgo	Procedimiento para determinar las brechas de seguridad de la información en base a las debilidades identificadas	4	4	5	5

	Planteamiento de estrategias o actividades de mitigación en las áreas o dominios de seguridad de la información identificadas como débiles	5	5	5	5
Promedio general		4.36	4.00	4.36	4.64

IV. Observaciones generales

Detalle justificaciones para las puntuaciones bajas, sugerencias de mejora o comentarios adicionales sobre el modelo propuesto:

Se recomienda incluir otros requisitos de seguridad esenciales para las aplicaciones académicas, como Autenticidad y No Repudio, que van más allá de la triada C-I-D.

También sugiero incluir un proceso específico que detalle cómo el modelo será revisado y actualizado anualmente para mantener la relevancia, dado que las amenazas y vulnerabilidades evolucionan constantemente.