Acondicionamiento del EGSI v2 de la ESPE para el cumplimiento de la Ley Orgánica de Protección de Datos Personales.

Bombón Toca, Gerson Steven

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Trabajo de integración curricular previo a la obtención del título de Ingeniería en Tecnologías de la Información

Ing. Ron Egas, Mario Bernabé

27 de febrero de 2024

Copyleaks

Plagiarism and AI Content Detection Report

Tesis Acondicionamiento EGSI-ESPE a ...

Scan details

Scan time	Total Pages:	Total Words:
February 29th, 2024 at 22:52 UTC	70	17256

Plagiarism Detection

9.9%

Types of plagiarism		Words
Identical	2.7%	465
Minor Changes	1.8%	303
Paraphrased	5.5%	947
Omitted Words	0%	0

AI Content Detection

4.1%

Text coverage		Words
AI text	4.1%	702
Human text	95.9%	16554

Learn more

Firma:

MARIO BERNABE RON EGAS

.....

Ron Egas Mario Bernabé

C. C: 1704229747

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Certificación

Certifico que el trabajo de integración curricular: "**Acondicionamiento del EGSI v2 de la ESPE para el cumplimiento de la Ley Orgánica de Protección de Datos Personales**" fue realizado por el señor **Bombón Toca Gerson Steven,** el mismo que cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se lo sustente públicamente.

Sangolquí, 20 de marzo de 2024

Firma:

Firmado electrónicamente por:
MARIO BERNABE RON EGAS

……

Ron Egas Mario Bernabé

C. C: 1704229747

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Responsabilidad de Autoría

Yo, **Bombón Toca Gerson Steven**, con cédula de ciudadanía N° 1726525155 declaro que el contenido, ideas y criterios del trabajo de integración curricular: **Acondicionamiento del EGSI v2 de la ESPE para el cumplimiento de la Ley Orgánica de Protección de Datos Personales** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 20 de marzo de 2024

.....

Bombón Toca Gerson Steven

C.C.: 1726525155

Departamento de Ciencias de la Computación

Carrera de Tecnologías de la Información

Autorización de Publicación

Yo **Bombón Toca Gerson Steven**, con cédula de ciudadanía n° 1726525155, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Acondicionamiento del EGSI v2 de la ESPE para el cumplimiento de la Ley Orgánica de Protección de Datos Personales** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 20 de marzo de 2024

.....

Bombón Toca Gerson Steven

C.C.: 1726525155

Dedicatoria

Con profundo amor y gratitud, dedico este proyecto a mis pilares más importantes en mi vida, mis padres, René y Mirian. Por ser los mejores padres del mundo, por su incansable esfuerzo, amor y humildad que son el reflejo en el que me miro cada día, su comprensión y apoyo incondicional me han brindado la valentía necesaria para afrontar cada paso en mi camino hacia nuevas metas. A mi hermana Karely, te dedico también este logro como fuente de inspiración para que paso a paso conquistes también tus sueños. A mi pequeña familia, Diana y Renata, ustedes son mi refugio de paz y mi mayor motivación. Y finalmente a toda mi familia por su cariño incondicional me impulsa a seguir adelante con renovadas fuerzas, te lo prometí mami Majito y ahora lo estoy haciendo realidad, un abrazo para el angelito más hermoso del cielo.

Agradecimientos

En primer lugar, quiero expresar mi profunda gratitud a Dios por la salud y la vida que me regala cada día, permitiéndome avanzar y cumplir mis metas. A mis padres y familia, les agradezco infinitamente su apoyo, sus consejos sabios y por creer en mí siempre, incluso cuando yo mismo dudaba.

De igual manera, deseo agradecer al Ing. Mario Ron, mi tutor de tesis, por su invaluable guía, sus consejos oportunos y su comprensión durante todo el desarrollo de este proyecto. Agradezco también a todos los profesores que han sido pilares fundamentales en mi formación profesional, brindándome las herramientas y conocimientos necesarios para llegar hasta aquí.

Finalmente, no puedo dejar de expresar mi más sincero agradecimiento a la querida y prestigiosa Universidad de las Fuerzas Armadas ESPE, por brindarme la oportunidad de vivir experiencias invaluables y conocer personas que han dejado una huella profunda en mi vida. Gracias a esta institución, he podido crecer personal y profesionalmente, y estoy seguro de que los valores y conocimientos adquiridos me acompañarán en el camino futuro.

Tabla de Contenidos

Lista de tablas

Lista de figuras

Resumen

Actualmente la Universidad de las Fuerzas Armadas ESPE mediante la Unidad de Seguridad Integrada implementó el Esquema Gubernamental de la Seguridad de la Información (ESGI) v2, la cual debe ser actualizada realizando un acondicionamiento para incluir las reglas establecidas por la Ley Orgánica de Protección de Datos Personales mediante el uso de la norma ISO 27001(Estándar internacional para la gestión de seguridad de la información) y derivados.

La planificación del proyecto se basa en realizar un análisis exhaustivo a la Ley Orgánica de Protección de Datos Personales y al Reglamento General de Protección de Datos Personales para guiarnos hacia qué tipo de datos personales deben ser protegidos y cuales no por ser datos de uso público.

Se ha realizado el análisis de riesgos basándose en los procesos internos que manejen o almacenen estos datos personales sensibles, de los cuales obtuvimos sus principales activos de información, los cuales nos sirvió para poder identificar cuáles son las amenazas y vulnerabilidades existentes en la actualidad de cada activo.

En base a los resultados del análisis de riesgos se logró establecer varios controles y salvaguardas para cada vulnerabilidad presente, y gracias a este análisis se pudo desarrollar un plan de implementación de salvaguardas que reduzca el nivel de riesgo presente.

Palabras clave: Ley Orgánica de Protección de Datos Personales, Esquema Gubernamental de Seguridad de la Información, Gestión de riesgos, controles y salvaguardas, datos personales

Abstract

Currently the University of the Armed Forces ESPE through the Integrated Security Unit implemented the Governmental Scheme of Information Security (ESGI) v2, which must be updated by making a conditioning to include the rules established by the Organic Law for the Protection of Personal Data using ISO 27000 and derivatives.

The planning of the project is based on an exhaustive analysis of the Organic Law on Personal Data Protection and the General Regulation on Personal Data Protection to guide us towards which type of personal data should be protected and which type should not because it is public data.

The risk analysis has been carried out based on the internal processes that handle or store these sensitive personal data, from which we obtained their main information assets, which helped us to identify the threats and vulnerabilities currently existing in each asset. Based on the results of the risk analysis we were able to establish several controls and safeguards for each vulnerability present, and thanks to this analysis we were able to develop an implementation plan of safeguards to reduce the level of risk present.

Keywords: Organic Law on Personal Data Protection, Governmental Information Security Scheme, risk management, controls and safeguards, personal data.

Capítulo I

Introducción

Antecedentes

La Universidad de las Fuerzas Armadas - ESPE ha desarrollado el Esquema Gubernamental de Seguridad de la Información (EGSI) como un marco integral para gestionar la seguridad de la información en la institución. Aunque este esquema ha sido eficaz, la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP), en Ecuador ha introducido nuevos requisitos legales que exigen una adaptación del EGSI para garantizar el cumplimiento normativo.

La LOPDP impone desafíos adicionales al requerir una revisión exhaustiva del EGSI para abordar las nuevas implicaciones legales en la protección de la privacidad individual. La adaptación del EGSI no solo implica ajustes en políticas y procedimientos existentes, sino también la identificación y mitigación de posibles brechas para fortalecer la salvaguardia de la información personal.

La universidad enfrenta la necesidad de comprometerse activamente en el proceso de adaptación del EGSI a los estándares de la LOPDP. Este compromiso institucional no solo responde a las demandas legales, sino que también refuerza la posición de la ESPE como una institución educativa líder comprometida con la protección responsable de la información confidencial y personal.

Planteamiento del problema

La gestión, procesamiento, almacenamiento y transmisión de información en sus diversas formas, requiere la protección que exige la normativa vigente. Si la información no está protegida y es vulnerada de alguna manera, la responsabilidad recaerá en la Institución y en sus autoridades, quienes podrían ser sujetas a multas y otras sanciones

que la ley establece, según la normativa, las personas cuya información han confiado a la Institución o que, por fines de la relación contractual o procedimental, podrían sufrir vulneración a sus derechos constitucionales de privacidad de su información y, por tanto, podrían demandar a la Institución y pedir la reparación integral.

Justificación

La Universidad de las Fuerzas Armadas ESPE se encuentra inmersa en un proceso fundamental del acondicionamiento de su Esquema Gubernamental de Seguridad de la Información (EGSI) v2 para cumplir con la Ley Orgánica de Protección de Datos Personales.

Para adecuar el Entorno de Gestión de la Seguridad de la Información (EGSI) de la ESPE al cumplimiento de la Ley Orgánica de Protección de Datos Personales, se requiere la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI). Esto garantizará que la ESPE establezca controles apropiados en función de la confidencialidad, disponibilidad e integridad de la información, asegurando la protección de los datos personales de todas las partes involucradas. La adhesión a la normativa ISO 27001 permitirá demostrar de manera transparente a los usuarios las normas de seguridad aplicadas en la gestión de información, la gestión de riesgos de seguridad y la determinación de los niveles de protección requeridos. Mediante la implementación del SGSI, se logrará optimizar el funcionamiento de las diversas unidades de la ESPE que participan en la gestión de datos personales, mejorando la eficiencia y la seguridad en la manipulación de la información. Además, este enfoque también considerará la evaluación de riesgos y la implementación de los procedimientos de gestión necesarios para cumplir con la Ley Orgánica de Protección de Datos Personales.

Objetivos

Objetivo General

Realizar el acondicionamiento del EGSI de la ESPE para el cumplimiento de la Ley Orgánica de Protección de Datos Personales, en base de las normas ISO 27003, ISO 27001, ISO 27002, ISO 3100, con el fin proteger la información del personal relacionado con los procesos internos de la ESPE y evitar sanciones por parte de la Autoridad Nacional de Protección de datos personales.

Objetivos Específicos

- Establecer el estado del Arte.
- Análisis de la Ley Orgánica de protección de datos personales.
- Análisis de riesgos.
- Tratamiento de riesgos y definición de salvaguardas.
- Implantación de salvaguardas.

Alcance

Adaptar el Esquema Gubernamental de Seguridad de la Información (EGSI) v2 para cumplir con los requisitos de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador.

Considerando los objetivos específicos, se llevará a cabo una revisión exhaustiva del estado del arte, focalizándose en la descripción detallada de las disposiciones, normativas esenciales para la planificación del sistema de gestión. Los recursos y la información necesarios para esta revisión serán proporcionados por la Unidad de Seguridad Integral (USIN) y las unidades administrativas de la universidad. A

continuación, se presentan los objetivos específicos y las preguntas de investigación asociadas, que guiarán el desarrollo del proyecto en concordancia con el tema de nuestra tesis, como se detalla en la **Tabla 1.**

Tabla 1.

Objetivos y Preguntas

Objetivos Específicos	***Preguntas de investigación***
Establecer el estado del Arte	a. ¿Cómo ayudará el acondicionamiento con la LOPDP en el EGSI v2 a la Universidad de las Fuerzas Armadas “ESPE”? b. ¿De qué manera y en que se basará el acondicionamiento del EGSl?
Análisis de la Ley Orgánica de protección de datos personales	a. ¿Cuáles son los requisitos clave de la LOPDP a considerar en el acondicionamiento del EGSI de la ESPE? b. ¿Cómo impactará el cumplimiento de la LOPDP en las prácticas actuales de manejo de datos en la universidad?
Análisis de riesgos	a. ¿Cuáles son los riesgos específicos asociados con la gestión de datos en la ESPE en el contexto de la LOPDP? b. ¿Cómo afectarán estos riesgos a la seguridad de la información y la privacidad de los datos personales?

Objetivos Específicos	*Preguntas de investigación*
Tratamiento de riesgos y definición de salvaguardas	a. ¿Cuáles son las estrategias más efectivas para mitigar los riesgos identificados en el análisis previo? b. ¿Cómo se pueden definir e implementar salvaguardas adecuadas para proteger los datos personales en la universidad?
Implantación de salvaguardas	a. ¿Cuál es el proceso de implementación más eficiente y efectivo para incorporar las salvaguardas identificadas en el EGSI? b. ¿Cómo se garantizará la adopción efectiva de estas salvaguardas en todas las unidades administrativas de la ESPE?

Hipótesis

Se postula que el acondicionamiento del EGSI de la Universidad ESPE para cumplir con los requisitos establecidos por la LOPDP en Ecuador contribuirá significativamente a fortalecer la seguridad de la información y la protección de datos personales en la institución. Se espera que el análisis de la LOPDP, la identificación y tratamiento adecuado de riesgos y la implantación efectiva de salvaguardas mejoren las prácticas de manejo de datos en la universidad, asegurando el cumplimiento normativo y promoviendo un entorno confiable para la gestión de información sensible.

Metodología

Para el desarrollo de este trabajo se considera la metodología establecida en la norma ISO/IEC NTE 27003, en concordancia con las normas ISO 27001, 27002 y 27005.

ISO 27003

Norma internacional que representa una guía para implementar y diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) donde se detalla las especificaciones necesarias con la finalidad de obtener la aprobación de la Dirección de la organización y que el proceso de desarrollo cumpla con los requerimientos establecidos. (Instituto Ecuatoriano de Normalización, 2012)

Metodología PHVA

El ciclo PHVA, también conocido como ciclo de Deming o ciclo PDCA, es una metodología ampliamente utilizada para la mejora continua de procesos y sistemas. Se basa en cuatro etapas: Planificar, Hacer, Verificar y Actuar. Este ciclo se implementa de forma iterativa, lo que permite un aprendizaje constante y la búsqueda de mejoras incrementales.

Planificar

La etapa de planificación es fundamental para el éxito del ciclo PHVA. En esta etapa se definen los objetivos que se desean alcanzar, se identifican los procesos a mejorar y se establecen las acciones que se llevarán a cabo.

Hacer

En este paso ponen en práctica las acciones que se definieron en la etapa de planificación. Es importante que se documente el proceso de implementación para poder analizarlo posteriormente y realizar las mejoras necesarias.

Verificar

Aquí se evalúan los resultados de las acciones que se implementaron en la etapa de Hacer. Se comparan los resultados con los objetivos que se definieron en la etapa de planificación y se identifican las áreas de mejora.

Actuar

Se basa en implementar las mejoras que se identificaron en la etapa de Verificar. Se pueden realizar cambios en el proceso, en las acciones o en los objetivos. Esta etapa completa el ciclo y permite iniciar un nuevo ciclo de mejora continua.

Figura 1.

Metodología PHVA

Nota. Cuatro pasos fundamentales en la metodología PHVA. Tomado de Hernández, Mónica & Ortiz, Giannina. (2022).

Capítulo II

Fundamentación teórica y estado del arte

En el marco de este proyecto, es esencial abordar y tener en cuenta una diversidad de terminología y componentes que servirán como base para la investigación. Entre estos se incluyen aspectos como la ciberseguridad, mecanismos de protección, regulaciones, enfoques y criterios que se emplearán para realizar la iniciativa.

Normas y marcos de referencia

Para el presente acondicionamiento se tiene varias normas y marcos relevantes, las cuales les presentamos a continuación:

- ISO 27001: Es la norma principal de la serie ISO 27000 y contiene los requisitos del sistema de gestión de seguridad de la información. Este estándar brinda los requerimientos para el desarrollo y operación de SGSI incluyendo una lista de controles para el manejo y mitigación de los riesgos asociados a los activos de información. Se puede confirmar la eficacia de la implementación del SGSI mediante una auditoria o certificación (Fuentes Serrate, 2020)
- ISO 27002: Es un estándar internacional que proporciona orientación para las organizaciones que buscan establecer, implementar y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) centrado en la ciberseguridad. Mientras que ISO/IEC 27001 describe los requisitos para un SGSI, ISO/IEC 27002 ofrece mejores prácticas y objetivos de control relacionados con aspectos clave de ciberseguridad, incluido el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta a incidentes. El estándar sirve como modelo práctico para las organizaciones que buscan salvaguardar

eficazmente sus activos de información contra las amenazas cibernéticas. Siguiendo las directrices ISO/IEC 27002, las empresas pueden adoptar un enfoque proactivo para la gestión de riesgos de ciberseguridad y proteger la información crítica contra el acceso no autorizado y su pérdida (International Organization for Standardization, 2022a)

- ISO 27005: Según (International Organization for Standardization, 2008) esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Respalda los conceptos generales especificados en ISO/IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y terminologías descritos en ISO/IEC 27001 e ISO/IEC 27002 es importante para una comprensión completa de ISO/IEC 27005:2008. ISO/IEC 27005:2008 es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que intentan gestionar riesgos que podrían comprometer la seguridad de la información de la organización.
- ISO 31000: Es una norma internacional que proporciona principios y directrices para la gestión de riesgos. Describe un enfoque integral para identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos en toda una organización (International Organization for Standardization, 2022b).

  Dentro de los beneficios que indica el mismo autor, podemos encontrar los siguientes:

  - Principios, marco y proceso estándar de gestión de riesgos

- Guía para implementar prácticas de gestión de riesgos
- Herramientas para contextualizar la gestión de riesgos a cualquier organización
- Criterios para monitorear, revisar y mejorar continuamente la gestión de riesgos
- Fundación para integrar la gestión de riesgos en toda una organización

Sistema de Gestión de Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información es el elemento más importante de la norma ISO 27001, que unifica los criterios para la evaluación de los riesgos asociados al manejo de la información institucional. (Gobierno Electrónico de Ecuador, 2019)

Principios del SGSI

El Sistema de Gestión de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información:

Figura 2.

Principios de la S.I.

Nota. Pirámide de principios fundamentales de la triada CIA. Tomado de https://infosegur.wordpress.com/tag/disponibilidad/

- **Confidencialidad:** Se refiere a la protección de la información sensible contra accesos no autorizados, garantizando que solo personas autorizadas puedan acceder a ella.
- **Integridad:** Se centra en la precisión y fiabilidad de la información, asegurando que no se modifique ni se corrompa de manera no autorizada.
- **Disponibilidad:** Se relaciona con la accesibilidad y disponibilidad oportuna de la información cuando sea requerida por usuarios autorizados, evitando interrupciones no planificadas.

Beneficios del SGSI

Entre los beneficios relevantes de un SGSI podemos citar los siguientes:

- Establece una metodología de Gestión de la Seguridad estructurada y clara.

- Reduce el riesgo de pérdida, robo o integridad de la información sensible.
- Los riesgos y los controles son continuamente revisados.
- Se garantiza la confianza de los usuarios en los servicios institucionales.
- Facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras un incidente grave.
- Cumple con la legislación vigente sobre información personal, propiedad intelectual y otras.
- La imagen de la institución mejora.
- Aumenta la confianza y las reglas claras para los miembros de la institución.
- Reduce los costes y la mejora de los procesos y el servicio.
- Se incrementa la motivación y la satisfacción del personal.
- Aumenta la seguridad en base la gestión de procesos en lugar de una compra sistemática de productos y tecnologías. (Gobierno Electrónico de Ecuador, 2019)

Esquema Gubernamental de Seguridad de la Información (EGSI)

El marco gubernamental de seguridad de la información sigue los principios establecidos por la normativa ecuatoriana NTE INEN-ISO/IEC 27000 para la gestión de la seguridad de la información. El EGSI da directrices y puntos de control a seguir con la instauración de un sistema de gestión de seguridad de la información. Este sistema pretende asegurar la elaboración de procesos y procedimientos para proteger la información y activos informáticos de las Instituciones Públicas en Ecuador. (López et al., 2022)

En el cumplimiento del Acuerdo Ministerial N° 025 EGSI V2 (Gobierno Electrónico de Ecuador, 2019) controlado por la Secretaría Nacional de Administración Pública (SNAP), indica que la expedición del Esquema Gubernamental de Seguridad de la

Información es de manera obligatoria para todas las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, que se encuentra como Apéndice Al presente Acuerdo Ministerial, además indica como recomendación hacia cuyas instituciones utilizar como guía las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información.

Ley Orgánica de Protección de Datos Personales

El foco principal del presente proyecto se centra en la Ley Orgánica de Protección de Datos Personales, la cual respalda y fortalece la salvaguarda de información de carácter personal, facilitando así el acceso, la toma de decisiones y la seguridad de estos datos. En este contexto, nos enfocaremos en los artículos y normativas establecidas que tienen como objetivo mejorar los sistemas de información en el ámbito de los datos personales.

En (LOPDP, 2021) se puede encontrar todos los artículos que están sujetos a esta ley, la cual debemos poner en marcha para el acondicionamiento en el EGSI v2 de la ESPE, para que mediante controles y salvaguardas a la información sensible (datos personales) se pueda cumplir los lineamientos establecidos en el Reglamento General de Protección de Datos. Esta ley orgánica se divide en 12 capítulos los cuales vamos a describir a continuación:

Capítulos LOPDP

I. Ámbito de aplicación integral
II. Principios
III. Derechos
IV. Categorías especiales de datos
V. Transferencia o comunicación y acceso a datos personales por terceros

VI. Seguridad de datos personales

VII. Del responsable, encargo y delegado de protección de datos personales

VIII. De la responsabilidad proactiva

IX. Transferencia o comunicación internacional de datos personales

X. De los requerimientos directos y de la gestión de procedimiento administrativo

XI. Medidas correctivas, infracciones y régimen sancionatorio

XII. Autoridad de protección de datos personales

Definiciones relevantes

Estas explicaciones contribuirán a la comprensión de la LOPDP:

- **Información personal:** Información que permite identificar o hace identificable a una persona natural, ya sea de manera directa o indirecta. Ejemplos de esto incluyen tu nombre completo o tu número de cédula.
- **Titular:** Individuo natural (ser humano) cuyos datos están sujetos a ser procesados. Un ejemplo sería el titular de una cuenta de ahorros en un banco.
- **Procesamiento:** Cualquier operación o conjunto de operaciones llevadas a cabo en datos personales, ya sea de forma automatizada o manual, que incluye actividades como la recolección, almacenamiento, procesamiento, transferencia y destrucción, así como cualquier uso general de datos personales.
- **Aprobación:** Expresión voluntaria, específica, bien informada e inequívoca del titular para permitir el tratamiento de sus datos personales.

Marco Legal LOPDP

Según el objetivo del presente proyecto los capítulos más importantes para el acondicionamiento del ESGI v2 de la ESPE son los siguientes:

Art 1.- “Objeto y finalidad. -El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela” (LOPDP, 2021)

Art 2.- “Ámbito de aplicación material. -La presente ley se aplicará al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior. La ley no será aplicable a:...” (LOPDP, 2021)

Art. 10.- Principios:

Transparencia. - “El tratamiento de datos personales deberá ser transparente, por lo que toda información o comunicación relativa a este tratamiento deberá ser fácilmente accesible y fácil de entender y se deberá utilizar un lenguaje sencillo y claro.” (LOPDP, 2021)

Finalidad. - “Las finalidades del tratamiento deberán ser determinadas, explícitas, legítimas y comunicadas al titular: no podrán tratarse datos personales con fines distintos para los cuales fueron recopilados, a menos que concurra una de las causales que habiliten un nuevo tratamiento conforme los supuestos de tratamiento legítimo señalados en esta ley.” (LOPDP, 2021)

Seguridad de datos personales. - “Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, (…) para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto.” (LOPDP, 2021)

Art. 12.- Derecho a la Información. - “El titular de datos personales tiene derecho a ser informado conforme los principios de lealtad y transparente por cualquier medio…” (LOPDP, 2021)

Art. 13.- Derecho de acceso. – “El titular tiene derecho a conocer y a obtener, gratuitamente, del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin necesidad de presentar justificación alguna…”(LOPDP, 2021)

Art. 14.- Derecho de rectificación y actualización. – “El titular tiene el derecho a obtener del responsable del tratamiento la rectificación y actualización de sus datos personales inexactos o incompletos…”(LOPDP, 2021)

Art. 15.- Derecho de eliminación. – “El titular tiene derecho a que el responsable del tratamiento suprima sus datos personales…”(LOPDP, 2021)

Art. 25.- Categorías especiales de datos personales. - “Se considerarán categorías especiales de datos personales, los siguientes:

a) Datos sensibles;
b) Datos de niñas, niños y adolescentes;
c) Datos de salud; y,
d) Datos de personas con discapacidad y de sus sustitutos, relativos a la discapacidad.” (LOPDP, 2021)

Art. 33.- Transferencia o comunicación de datos personales. - “Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario, cuando la transferencia se encuentre configurada dentro

de una de las causales de legitimidad establecidas en esta Ley, y se cuente, además, con el consentimiento del titular.” (LOPDP, 2021)

Art. 37.- Seguridad de datos personales. - “El responsable o encargado del tratamiento de datos personales según sea el caso, deberá sujetarse al principio de seguridad de datos personales, para lo cual deberá tomar en cuenta las categorías y volumen de datos personales, el estado de la técnica, mejores prácticas de seguridad integral y los costos de aplicación de acuerdo a la naturaleza, alcance, contexto y los fines del tratamiento, así como identificar la probabilidad de riesgos.” (LOPDP, 2021)

Art. 65.- Medidas correctivas.- “En caso de incumplimiento de las disposiciones previstas en la presente Ley, su reglamento, directrices y lineamientos y regulaciones emitidas por la Autoridad de Protección de Datos Personales y normativas sobre la materia, o transgresión a los derechos y principios que componen al derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales dictará medidas correctivas con el objeto de evitar que se siga cometiendo la infracción y que la conducta se produzca nuevamente, sin perjuicio de la aplicación de las correspondientes sanciones administrativas.” (LOPDP, 2021)

Aspectos técnicos en los sistemas informáticos relacionados con la protección de datos

A continuación, vamos a describir aspectos y términos técnicos que describe (Remache Arias, 2019) los cuales son de importante relación con la protección de datos:

- **Dato:** La noción de "Dato", derivada del término latino "datum" que significa "lo que se da", se refiere a la información presentada en forma numérica o alfabética. Los datos en sí mismos no proporcionan información relevante, a menos que estén vinculados a alguna experiencia, como ocurre, por ejemplo, con el número

de cédula, una dirección de correo electrónico o el número de cuenta bancaria (Remache Arias, 2019).

- **Dato personal:** Dato que identifica o hace identificable a una persona natural, directa o indirectamente.
- **Tipos de datos personales:** Existen varias clasificaciones de los datos a continuación vamos a describir brevemente cada una y seleccionaremos cuál de estas definiciones encaja con esta investigación:
    - **Dato anónimo:** Se denomina dato anónimo al dato estadístico o general que carece de personalización y no permite la identificación de individuos.
    - **Dato nominativo:** es aquel que está vinculado a una persona específica. Se clasifica según la forma en que se accede a la identificación de la persona, dividiéndose en dos tipos:
        - **Directos:** identifican a la persona sin necesidad de ningún proceso adicional.
        - **Indirectos:** posibilitan la identificación, pero no de manera directa, sino mediante la agrupación de datos.

    El dato nominativo se categoriza de la siguiente manera:

    - **Dato nominativo sensible**: hace referencia a información que afecta o podría afectar la intimidad, como, por ejemplo, detalles de diagnósticos médicos.
    - **Dato nominativo no sensible:** comprende información personal que, aunque es privada, está destinada a ser pública, como el número de documento de identidad.

Como podemos evidenciar el tipo de dato que vamos a centralizar y tomar en cuenta en este proyecto son los datos nominativo-sensibles, ya que estos son los que se enfocan a los datos propios de la intimidad de una persona y por naturaleza se comprende que, debido a su naturaleza, estos datos deben mantenerse confidenciales, por lo tanto, se requiere una regulación que garantice su protección durante la recolección y gestión.

Metodología ISO/IEC 27003

La metodología basada en la Norma ISO/IEC NTE 27003 consta de 8 pasos los cuales (Fuentes Serrate, 2020) describe de la siguiente manera:

Paso 1: Inicio del Proyecto

En la primera fase, es crucial asegurar el compromiso y respaldo de la dirección general, así como seleccionar y capacitar al equipo inicial del proyecto. La dirección debe brindar apoyo operativo, técnico, presupuestario y de planificación temporal para agilizar el proceso. Se enfatiza que el respaldo de la dirección implica un compromiso constante, ya que la infraestructura establecida requerirá ajustes y mejoras continuas para garantizar la eficacia a lo largo del proyecto.

Paso 2: Alcance del SGSI

En este paso esencial (Fuentes Serrate, 2020) destaca la necesidad de definir el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), considerando las limitaciones y conexiones con otros sistemas y proveedores. Se enfatiza la importancia de identificar los requerimientos legales y de negocio, así como establecer una declaración de aplicabilidad que incluya exclusiones y justificaciones. La planificación debe considerar el contexto estratégico de la organización, teniendo en cuenta metas

actuales y futuras. Además, se destaca la recopilación y revisión de la documentación existente para evaluar medidas ya implementadas, con un enfoque en la elaboración de un inventario documental por parte de los responsables de departamento.

Paso 3: Evaluación de riesgos

Con independencia del tipo o tamaño de la empresa, todas las organizaciones son vulnerables a las amenazas que ponen en peligro la confidencialidad, integridad y disponibilidad de la información importante. Cuanto antes se adopten las medidas correctivas, la seguridad representará un menor coste y será más efectiva. Para poder realizar una identificación y selección de controles más sencillos que permitan una mejor gestión de los recursos humanos y financieros se debe conocer la fuente y naturaleza de las amenazas.

Esta etapa incluye:

- Aplicabilidad de los controles de la ISO/IEC 27002: diagnóstico preliminar.
- Identificación y evaluación de activos, datos a proteger.
- Identificación y evaluación de amenazas y vulnerabilidades.

Paso 4: Tratamiento y Administración del Riesgo

En este paso es básico conocer cómo la selección y la implantación de los controles permiten reducir los riesgos a un nivel aceptable por la organización. Esta gestión generalmente es una función de la:

- Política de seguridad inicial.
- Nivel de seguridad requerido.
- Resultados de la evaluación de riesgos.
- Reglamentación y legislación aplicable.
- Regulaciones y restricciones del negocio existentes.

En general existen cuatro opciones para el tratamiento del riesgo: reducir el riesgo, aceptar el riesgo, evitar el riesgo y transferencia del riesgo.

Paso 5: Programa de formación y Sensibilización para el personal

La organización debe garantizar que el personal con responsabilidades específicas en el Sistema de Gestión de Seguridad de la Información (SGSI) esté debidamente capacitado y cualificado para cumplir con sus funciones. Asimismo, es esencial concienciar al personal sobre la importancia de sus actividades en la seguridad de la información y cómo contribuyen a los objetivos del SGSI. Para lograr esto, se destaca la necesidad de implementar un programa integral de formación y sensibilización que "eduque" a todos los empleados, asegurándose de que comprendan y respeten las buenas prácticas de seguridad de la información.

Paso 6: Documentación e implantación del SGSI

La documentación de un SGSI es una exigencia necesaria y previa a la implantación del sistema y se articula en torno a dos puntos estratégicamente claves:

- La descripción de la estrategia de la organización, sus objetivos, la evaluación de riesgos y las medidas adoptadas para evitar o atenuar los mismos.
- El control y el seguimiento del funcionamiento del SGSI. Es usual plantear por lo menos cuatro niveles de documentación como muestra el cuadro siguiente:

Tabla 2.

Niveles de documentación en seguridad de la información

Nivel	***Documento Requerido***	***Contenido***
1	Manual de seguridad	Política, evaluación de riesgos, declaración de aplicabilidad

Nivel	*Documento Requerido*	*Contenido*
2	Procedimientos	Procesos: ¿Qué?, ¿Quién?, ¿Cuándo?, ¿Dónde?
3	Fichas de trabajo, formularios, etc.	Descripción de cómo se realiza el trabajo y actividades
4	Registros	Este nivel proporciona pruebas objetivas de conformidad con las exigencias del SGSI

Nota. Sistema de Gestión de Seguridad de la Información Norma ISO/IEC 27003

Paso 7: Ajustes y preparación para la Auditoria de Certificación

El Diagnóstico, esencial para las organizaciones que buscan la certificación ISO/IEC 27001, representa un paso crucial para validar si el sistema cumple con los requisitos necesarios para la implementación del marco de gestión. Este documento, que se convierte en un registro fundamental durante la auditoría de certificación, ofrece la justificación de la aplicabilidad de cada control ISO/IEC 27001 en el Sistema de Gestión de Seguridad de la Información (SGSI), indicando también el estado de implantación de cada control y su aplicabilidad en el SGSI.

Paso 8: Control y mejora continua

El control y la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) siguen el Ciclo de Deming (P-D-C-A) según la normativa establecida. Este proceso se lleva a cabo antes de la Auditoría de Certificación, basándose en los resultados del diagnóstico realizado previamente.

Estado del arte

Se llevó a cabo una revisión bibliográfica con el fin de enmarcar la indagación de instancias científicas pertinentes para la ejecución del proyecto. Se establecieron los propósitos y se proporcionó una exposición del problema objeto de investigación, junto con criterios de inclusión y exclusión.

Construcción y afinación de la cadena de búsqueda

Basándonos en el tema, los objetivos planteados y el alcance de este proyecto se define las siguientes palabras y conceptos clave para la cadena de búsqueda en los repositorios académicos:

- Ley orgánica de protección de datos personales
- Instituciones
- Acondicionamiento
- Ecuador
- Esquema gubernamental de seguridad de la información

A continuación, se establecerá una matriz para establecer sinónimos y acrónimos de estas palabras clave y así obtener más información.

Tabla 3.

Construcción de cadena de búsqueda literaria

Palabra Clave	***Texto alternativo***	***Conector***
Ley orgánica de protección de datos personales	(LOPDP OR protección de datos personales)	AND

Palabra Clave	*Texto alternativo*	*Conector*
Instituciones	(universidades OR institución educativa OR institución pública OR educación superior)	AND
Mejora	(mejora OR actualización)	AND
Ecuador	(Ecuador OR Latinoamérica)	
Esquema gubernamental de seguridad de la información	(EGSI OR SGSI)	AND

Nota. Conforme Google Académico nos otorgue los resultados se irá modificando la cadena de búsqueda para una mejor búsqueda de información

Selección de estudios primarios

En base a nuestra línea de investigación se aplicó varios filtros en la selección del material literario, con el fin de obtener artículos literarios que sean de nuestro apoyo, los filtros son los siguientes:

- Artículos publicados desde el 2019 a 2023, dando prioridad a artículos que sean del año 2021 en adelante, ya que el Gobierno Ecuatoriano dio vigencia a la LOPDP el 21 de mayo de 2021.
- Artículos que se fundamenten en Norma ISO/IEC 27001.
- Artículos únicamente en idioma español o inglés.
- Artículos que hablen netamente de protección de datos personales

Características de artículos a no tomar en cuenta:

- Artículos que sean escritos en idioma diferente a español o ingles
- Artículos que no hablen de datos personales
- Artículos que no mencionen la LOPDP del 2021 o no menciones el RGPD

Estrategia de extracción

A continuación, en la **Tabla 4** se puede ver los artículos que se ha seleccionado por parte del autor del proyecto, mencionando que estos artículos fueron seleccionados en base a su título, alcance, objetivos y respuesta a las preguntas de investigación planteadas.

Después de un análisis exhaustivo a la mayor parte de los resultados que brindo Google Académicos con variantes en la cadena de búsqueda, se han obtenido aproximadamente 50 bibliografías potenciales. De las cuales 5 estudios han ido acorde y apegado a nuestro objetivo. Los cuales son las siguientes:

Tabla 4.

Estudios primarios seleccionados

Código	***Título***
EP01	Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos.
EP02	Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador.
EP03	Consideraciones para la implementación del esquema gubernamental de seguridad de la información basado en la ley de protección de datos personales caso de estudio: instituto nacional de patrimonio cultural.
EP04	Sistema de información integrado en instituciones de educación superior en Ecuador.

Código	*Título*
EP05	Alcance de la protección de datos personales en el marco legal ecuatoriano.

Resumen de los estudios principales

EP01 - Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos (Mayorga Jácome et al., 2019)

En el presente articulo menciona la elaboración de un borrador del anteproyecto de LOPDP, ya que el articulo está redactado en el año 2019 y en cuyas instancias Ecuador no tenía una ley que abarque todas las normativas para cumplir con la protección de datos personales, el artículo es esencial ya que nos da a conocer un antes y después de la vigencia de la Ley Orgánica de Protección de Datos Personales en el país. Los actores destacan la importancia de un proceso previo de sensibilización y un tiempo prudencial para la implementación de la ley. Esto se debe a que la LOPDP representa un cambio importante en la legislación ecuatoriana.

Además, los autores recomiendan que la ley aborde los siguientes aspectos:

- Ponderación entre los derechos y el libre flujo de información.
- Medios y vías judiciales y administrativas.
- Determinación de las autoridades encargadas de la supervisión de la ley.
- Un tiempo prudencial para la implementación de la ley.
- Claridad en las definiciones y aspectos centrales de la regulación.
- Un régimen sancionatorio proporcional y lo suficientemente severo para garantizar el cumplimiento de la ley.

EP02 - Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador. (Vaca Escobar, 2020)

En este articulo el autor se centra en proporcionar directrices para el manejo adecuado de datos altamente confidenciales, específicamente en los Distritos de Educación del Ecuador. Presenta un modelo de gestión de seguridad lógica de la información que aborda la captura, almacenamiento y procesamiento de datos sensibles, garantizando la confidencialidad, integridad y disponibilidad de la información. Este modelo sigue el marco de referencia Planear, Hacer, Verificar y Actuar establecido por la normativa ISO 9001:2015, buscando la mejora continua.

También incluye documentos anexos como políticas de seguridad de la información, mecanismos de control y acuerdos de confidencialidad. Se detallan también los mecanismos de control definidos en la ISO 27001:2013, que ofrecen buenas prácticas para la preservación de la información.

En resumen, la tesis aborda la implementación de un modelo de gestión de seguridad lógica basado en estándares internacionales y experiencias de otros países, adaptado a la realidad específica de los Distritos de Educación en Ecuador.

EP03 - Consideraciones para la implementación del esquema gubernamental de seguridad de la información basado en la ley de protección de datos personales caso de estudio: instituto nacional de patrimonio cultural. (Jaramillo Burbano, 2022)

La investigación se enfoca en contribuir directamente al Instituto Nacional de Patrimonio Cultural (INPC) para la implementación de normativas emitidas por entes rectores. Esto pretende aumentar la seguridad de la información en el tratamiento de

datos personales en sistemas públicos y disponibles para la ciudadanía, como la Autorización de Movilización de Bienes Culturales, Registro de Profesionales, Servicios Especializados de Laboratorio, y el Sistema de Información del Patrimonio Cultural, entre otros. El autor proporcionará información valiosa, incluyendo consideraciones y procedimientos para establecer un esquema de seguridad de la información y tratamiento de datos personales a nivel gubernamental, siguiendo la normativa ecuatoriana. Esto contribuirá al fortalecimiento de la confianza en el manejo de información en sistemas de Gobierno Electrónico.

EP04 - Sistema de información integrado en instituciones de educación superior en Ecuador (Tenesaca Guamán et al., 2023).

La tesis se enfoca en el proceso de implementación de Sistemas de Información Integrados en las Instituciones de Educación Superior de Ecuador, destacando su influencia en decisiones cruciales. El objetivo principal consiste en analizar los factores que garantizan seguridad y restricciones al acceder a estos sistemas.

Los autores realizaron una revisión sistemática de 47 artículos para identificar las principales amenazas a la seguridad en el acceso a los SII.

Identificando las siguientes amenazas:

- **Amenazas internas:** Estas amenazas son causadas por personas autorizadas a acceder a los SII, como estudiantes, docentes y personal administrativo.
- **Amenazas externas:** Estas amenazas son causadas por personas no autorizadas a acceder a los SII, como piratas informáticos o ciberdelincuentes.

Para mitigar estas amenazas proponen los indicadores de seguridad siguientes:

- Responsabilidad del personal
- Cifrado
- Acceso

EP05 - Alcance de la protección de datos personales en el marco legal ecuatoriano. (Vivar Butiñá, 2022)

El estudio busca determinar el nivel de protección de los datos personales de los ecuatorianos en el marco legal actual del país. A pesar de la existencia de la Ley del Sistema Nacional de Registro de Datos Públicos, que busca garantizar la seguridad jurídica y la transparencia en la gestión de la información, se observa que, en la práctica, el acceso, procesamiento y almacenamiento de datos por parte de personas naturales o jurídicas puede dar lugar a la creación de duplicados de información traspasables nacional e internacionalmente. Aunque **el** Sistema Nacional de Registro de Datos Públicos **(**SINARDAP**)** establece procedimientos de alta calidad para la custodia de datos, enfrenta desafíos en la articulación efectiva de los procesos posteriores a la salida de la información. Esto genera preocupación sobre cuándo el acceso de terceros a estos datos podría afectar los derechos fundamentales de las personas, sin que la Ley de Protección de Datos defina claramente qué referencias personales se consideran sensibles y podrían vulnerar la intimidad y la privacidad.

Capítulo III

Análisis de la LOPDP en la ESPE

Introducción y perspectiva general

El presente capítulo se centra en el análisis de la LOPDP y su repercusión en los procesos de la ESPE. A través de diferentes actividades fundamentales, se abordará la documentación detallada de las implicaciones de la LOPDP en los procedimientos institucionales. La elaboración de un informe actualizado será esencial para evaluar la adhesión de la ESPE a las leyes y regulaciones pertinentes en materia de protección de datos y seguridad de la información. La perspectiva global de este capítulo incluirá una comparativa meticulosa entre los requisitos establecidos por la LOPDP y las prácticas actuales del EGSI-ESPE, con el objetivo de identificar posibles brechas de cumplimiento y áreas de mejora.

Descripción del Proyecto

Para proceder con el acondicionamiento del SGSI V2, se debe contar con la colaboración de la Dirección de la organización que debe aprobar mediante un proyecto institucional donde se detallen las actividades a realizar. Se deberá generar un caso de negocio que describa los objetivos, alcance y la estructura de la organización para llevar a cabo la implantación del proyecto.

Leyes y regulaciones

En el Ecuador, las leyes y regulaciones pertinentes en materia de protección de datos y seguridad de la información con sus respectivos marcos legales podemos verlos en el punto siguiente.

Marco legal

- **Constitución de la República del Ecuador**

Numeral 19 del artículo 66:" (…) El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley (…)";

Artículo 82:" El derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes";

Artículo 92: "(…) Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo, tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados (…) ";

Artículo 226:"(...)Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad

estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución (…)"; (*Constitución de la Republica del Ecuador.pdf*, s. f.)

- **Código Orgánico Integral Penal**

Artículo 178: "(...) Violación a la intimidad. - La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley (...)".

Artículo 179: "Revelación de secreto. - La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año."

Artículo. 229: "(...) Revelación ilegal de base de datos. - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de

instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años (...)". (*Código Orgánico Integral Penal*, s. f.)

- **Ley Orgánica del Sistema Nacional de Registro de Datos Públicos**

Artículo 4: "(…) Responsabilidad de la información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados es exclusiva de la o el declarante cuando esta o este provee toda la información (...) ";

Artículo 6, "(…) Son confidenciales los datos de carácter personal. El acceso a estos datos sólo será posible cuando quien los requiera se encuentre debidamente legitimado, conforme a los parámetros previstos en la Ley Orgánica de Protección de Datos Personales, su respectivo reglamento y demás normativa emitida por la Autoridad de Protección de Datos Personales (...)". (*Ley Orgánica del Sistema Nacional de Registro de Datos Públicos*, s. f.)

- **Ley Orgánica de Telecomunicaciones**

Artículo 78.- Seguridad de los Datos Personales: "(Sustituido por el lit. a del num. 2 de la Disp. Reformatoria Cuarta de la Ley s/n, R.O. 459-5S, 26-V-2021).- Las y los prestadores de servicios de telecomunicaciones deberán adoptar las medidas técnicas, organizativas y de cualquier otra índole adecuadas para preservar la seguridad de su red con el fin de garantizar la protección de los datos personales de conformidad con lo establecido en la

Ley Orgánica de Protección de Datos Personales". (*Ley Orgánica de Telecomunicaciones*, 2015)

- **Ley Orgánica de Protección de Datos Personales**

Numeral 4 del artículo 47 de la Ley Orgánica de Protección de Datos Personales, expresa: "El responsable del tratamiento de datos personales está obligado a: (…) 4) Implementar políticas de protección de datos personales afines al tratamiento de datos personales en cada caso en particular (…)";

Numeral 3 del artículo 67 de la norma ibidem, establece: "Se consideran infracciones leves las siguientes: (…) "No mantener disponibles políticas de protección de datos personales afines al tratamiento de datos personales (…)"; (LOPDP, 2021)

Regulaciones

La (LOPDP, 2021) del Ecuador, establece una serie de regulaciones que deben ser aplicadas por todas las instituciones, públicas y privadas, que traten datos personales. En el caso de las instituciones de educación pública, estas regulaciones se aplican a los datos personales de los estudiantes, docentes, personal administrativo y demás personas que se relacionan con la institución.

En la **Tabla 5** podemos ver cuáles son las principales regulaciones de la LOPDP:

Tabla 5.
Regulaciones principales de la LOPDP

Regulaciones	***Descripción***
Principios de protección de datos personales	Se deben respetar los principios de protección de datos personales establecidos en la LOPDP, como la legalidad, finalidad, proporcionalidad, libertad, veracidad y transparencia, seguridad y responsabilidad.
Bases legales para el tratamiento de datos personales	Solo se pueden tratar datos personales si tienen una base legal válida, como el consentimiento, la ejecución de un contrato o el cumplimiento de una obligación legal.
Derechos de los titulares de datos personales	Deben respetar los derechos de los titulares de datos personales, como el acceso, la rectificación, la cancelación, la oposición y la portabilidad.
Procedimientos para el ejercicio de los derechos de los titulares	Las instituciones de educación pública deben establecer procedimientos claros y sencillos para que los titulares de datos personales puedan ejercer sus derechos.
Seguridad de los datos personales	Se debe implementar medidas de seguridad adecuadas para proteger los datos personales que tratan.

Regulaciones	***Descripción***
Estructurar los roles de las personas que se encargan del tratamiento de los datos personales	Se debe estructurar los roles de las personas que se encargan del tratamiento de los datos personales, como el responsable, el encargado y el delegado.
Transferencia y comunicación de datos	Las instituciones solo pueden transferir o comunicar datos personales a terceros o internacionalmente, si y solamente, si cumplen los requisitos establecidos en la LOPDP y cumple con las normas de seguridad correspondientes.

Alcance en el EGSI

Se realizará una revisión y análisis de todas las políticas y procedimientos documentados en el ESGI vigente de la ESPE, para comparar con las regulaciones escritas en *3.3.2. Regulaciones,* con el objetivo de identificar los procesos o controles ya establecidos por la universidad y así crear o mejorar una política definida netamente hacia la protección de datos personales.

Para ellos se debe identificar los procesos críticos que manejen o manipulen datos personales, una vez identificados los procesos críticos, se hará un tratamiento a los activos que tratan estos procedimientos.

Este proceso se basa en la evaluación de vulnerabilidades y amenazas, que permite identificar los activos que son susceptibles de ser vulnerados. Una vez

identificadas las vulnerabilidades, se realiza un análisis y valoración de riesgos, que permite determinar la probabilidad e impacto de cada riesgo.

Los resultados de este análisis se utilizan para definir los controles de seguridad necesarios para mitigar los riesgos identificados. Estos controles se incluirán en el Plan de Implantación de Salvaguardas, que es el documento que define cómo se implementarán los controles de seguridad.

Adhesión de la organización

La ESPE tiene en vigencia la política específica para la aplicabilidad de la ley de protección de datos personales cuyo identificador es **USIN-PLT-V1-2023-038**. En este documento se establece los principios y procedimientos para la protección de los datos personales que maneja la Universidad actualmente.

La política cubre algunos puntos para cumplir con las leyes y regulaciones pertinentes en materia de protección de datos y seguridad de la información que los veremos en la **Tabla 6**.

Tabla 6.
Controles de datos personales ejecutados en la ESPE

Código	***Control***	***Descripción***
CI01	Estructura organizativa de la protección de datos personales	En la política establecida desarrolla y describe las obligaciones de los cargos siguientes: • Responsable del tratamiento de datos personales • Comité de Seguridad de la Información • Unidad de Seguridad Integrada • Delegado de protección de datos personales • Encargado del tratamiento de datos personales
CI02	Contenido del acuerdo de términos, condiciones y consentimiento	Describe los derechos y obligaciones a las que se encuentra sujeto el titular de datos personales y en la política lo adjuntan como *APÉNDICE A*

Código	*Control*	*Descripción*
CI03	Derecho de acceso y rectificación	Se reconoce a los titulares estos derechos sobre la información de sus datos personales, para lo cual deberán realizar una solicitud física o a través de canales virtuales establecidos por la Universidad y gestionados por los encargados de datos personales.

Nota. Controles Implementados tomados de la política específica para la aplicabilidad de la ley de protección de datos personales.

Capítulo IV

Análisis de Riesgos

Tratamiento de Datos

Para el presente capítulo de análisis, el primer paso fue analizar todos los datos que menciona la LOPDP y el Reglamento General de la LOPDP, de los cuales se creó la siguiente lista:

Tabla 7.

Listado de datos obtenidos de la ley

Núm.	***Datos de las personas***
1	Datos biométricos (huella digital)
2	Datos crediticios (becas)
3	etnia
4	identidad de género
5	identidad cultural
6	religión
7	ideología
8	filiación política
9	pasado judicial
10	condición migratoria
11	orientación sexual
12	salud
13	datos genéticos
14	datos relativos a las personas apátridas

Núm.	*Datos de las personas*
15	refugiados que requieren protección internacional
16	Datos cuyo tratamiento indebido pueda dar origen a discriminación atenten o puedan atentar contra los derechos y libertades fundamentales
17	rendimiento profesional
18	situación económica
19	preferencias personales
20	intereses
21	fiabilidad
22	ubicación
23	movimiento físico
24	Nombres y apellidos
25	Número de cédula
26	Dirección
27	Número de teléfono
28	Correo electrónico
29	Fecha de nacimiento
30	Estado civil
31	Cargas familiares
32	Datos familiares
33	Discapacidades
34	Calificaciones académicas

Núm.	*Datos de las personas*
35	Curriculum vitae

Nota. Estos datos no tienen ningún análisis, ningún filtro, están escritos acorde dicta la ley.

Análisis de datos

Ahora el proceso es realizar un análisis a estos datos, aplicar filtros, curar datos para que estos puedan ser la base para el posterior análisis de riesgos.

1. **Descomposición de datos complejos**

   Logramos observar que en el registro Núm. 16 de la Tabla 7, es un párrafo general que menciona sobre el cual tiene varios datos específicos, por lo cual vamos a desglosar en los siguientes datos:

- Datos relacionados con la discriminación
  - Datos relativos a la raza, el origen étnico o la nacionalidad.
  - Datos relativos al género, la identidad de género o la expresión de género.
  - Datos relativos a la discapacidad.
  - Datos relativos a la edad.
  - Datos relativos a la situación socioeconómica.
- Datos relacionados con los derechos y libertades fundamentales:
  - Datos relativos a la libertad de expresión.
  - Datos relativos a la libertad de reunión y asociación.
  - Datos relativos a la libertad de movimiento.
  - Datos relativos al derecho a la privacidad.
  - Datos relativos al derecho a la protección de datos personales.
- Otros datos que podrían usarse para discriminar:

- Datos relativos a los ingresos.
- Datos relativos al nivel educativo.
- Datos relativos al historial crediticio.
- Datos relativos a los antecedentes penales.
- Datos relativos a las opiniones políticas.

De todo el desglose que se obtuvo de este registro, se analizó cada uno de ellos para saber cuál de estos datos tienen relación con nuestro objetivo principal de proyecto, el cual se enfoca netamente en **datos personales.**

Para que no exista redundancia ni repeticiones con los demás datos ya establecidos en la lista, se obtuvo los siguientes nuevos registros:

- Ingresos
- Historial crediticio

Ya que los demás datos que pueda causar discriminación están incluidos en los demás registros.

2. Filtro de datos personales

El presente punto vamos a realizar un análisis de toda la lista para desechar datos de la lista que no contengan enfoque hacia datos netamente personales, clasificando en datos sensibles y no sensibles acorde a la LOPDP.

2.1. Datos Personales

- **Datos Sensibles**
  - Datos biométricos (huella digital)
  - Etnia
  - Identidad de género
  - Identidad cultural

        - Religión
        - Ideología
        - Filiación política
        - Antecedentes penales
        - Condición migratoria
        - Orientación sexual
        - Salud
        - Datos genéticos
        - Discapacidades
    - **Datos No Sensibles:**
        - Nombres y apellidos
        - Número de cédula
        - Dirección
        - Nro. de teléfono
        - Correo electrónico
        - Fecha de nacimiento
        - Estado civil
        - Cargas familiares
        - Datos familiares
        - Calificaciones académicas
        - Curriculum vitae

2.2. Datos NO personales

- **Becas:** dato no personal, puede ser indicio de datos sensibles como condición socioeconómica

- **Ingresos:** dato no personal, puede ser indicio de datos sensibles como condición socioeconómica
- **Rendimiento profesional**: dato no personal, puede ser indicio de datos sensibles como salud
- **Situación económica:** dato no personal, puede ser indicio de datos sensibles como ingresos
- **Preferencias personales**: dato no personal
- **Intereses:** dato no personal
- **Fiabilidad:** dato no personal
- **Ubicación:** dato no personal, puede ser indicio de datos sensibles como movimiento físico
- **Movimiento físico:** dato no personal, puede ser indicio de datos sensibles como ubicación
- **Historial Crediticio**: dato no personal, puede ser indicio de datos sensibles como datos crediticios

2.3. Lista Final de Datos Personales

Tabla 8.

Lista final de Datos Personales a controlar

Núm.	*Datos de las personas*
1	Datos biométricos
2	Etnia
3	Identidad de género

Núm.	*Datos de las personas*
4	Identidad cultural
5	Religión
6	Ideología
7	Filiación política
8	Antecedentes penales
9	Condición migratoria
10	Orientación sexual
11	Salud
12	Datos genéticos
13	Discapacidades
14	Nombres y apellidos
15	Número de Identificación
16	Dirección
17	Nro. de teléfono
18	Correo electrónico
19	Fecha de nacimiento
20	Estado civil
21	Calificaciones académicas
22	Curriculum vitae

Nota. Esta lista es el resultado del tratamiento de registros para enfocarla a nuestro objetivo de proyecto.

Procesos de tratamiento

En esta sección vamos a realizar el levantamiento de los procesos que manipulan y utilizan los datos personales que definimos en **Tabla 8.** Para lo cual primero se categorizó los datos personales que requieran una protección acorde indique la ley.

Después, se señala cuáles son los datos personales que corresponden a cada titular de la Universidad ESPE, para lo cual se definieron los siguientes titulares:

1. Estudiantes
2. Docentes
3. Funcionarios Administrativos
4. Proveedores
5. Personal externo relacionado

Y por último se identifica qué procesos trabajan o manipulan estos datos, para posteriormente analizarlos en una matriz.

Procesos Críticos

Para la definición de procesos críticos se realizó un análisis exhaustivo de las políticas declaradas y en vigencia de la ESGI de la ESPE, con lo que se logró establecer los siguientes procesos de negocio críticos que manejan datos personales, tanto sensibles como no sensibles:

Tabla 9.

Procesos críticos

ID	*Proceso*	*Descripción*
PRC-01	Admisiones y Matriculación	Gestiona el proceso de inscripción de los estudiantes de cada carrera y gestiona su matrícula de forma eficiente y transparente
PRC-02	Pagos	Gestiona el proceso de cobro de aranceles y otros servicios académicos de forma eficiente, transparente y segura.
PRC-03	Evaluación y Seguimiento Académico	Asegura la calidad del proceso educativo mediante la evaluación continua del aprendizaje de los estudiantes y el seguimiento de su rendimiento académico.
PRC-04	Gestión del Talento Humano	Gestión del personal de la ESPE
PRC-05	Gestión Administrativa	Gestionar el soporte administrativo a los demás procesos de la universidad
PRC-06	Gestión Medica Institucional	Gestión de todos los aspectos relacionados con la atención médica dentro de la institución

Acorde a estos procesos críticos se crea una *clasificación de datos* en donde vamos a seleccionar los datos personales que se utiliza en cada uno de los procesos críticos definidos en **Tabla 9,** que nos entrega como resultado la matriz que se puede visualizar en **Figura 3**.

Figura 3.

Matriz de Clasificación de Procesos

Núm.	Datos de las personas	Sensibilidad	Con protección	Titulares						Proceso de tratamiento
				Estudiantes	Docentes	Funcionarios Administrativos	Personal militar SA	Proveedores	Personal externo relacionado	
1	Datos biométricos	Sensible	SI		x	x	x			Gestión del Talento Humano
2	Etnia	Sensible	SI		x	x	x		x	Admisiones y Matriculación
3	Identidad de género	Sensible	SI							Admisiones y Matriculación
4	Identidad cultural	Sensible	SI	x	x	x	x		x	
5	Religión	Sensible	SI							
6	Ideología	Sensible	SI							
7	Filiación política	Sensible	SI							
8	Antecedentes penales	Sensible	SI		x	x	x		x	Gestión del Talento Humano
9	Condición migratoria	Sensible	SI				x			Admisiones y Matriculación Gestion Medica Institucional
10	Orientación sexual	Sensible	SI	x	x	x	x		x	Admisiones y Matriculación
11	Salud	Sensible	SI	x	x	x	x		x	Admisiones y Matriculación Gestion Medica Institucional
12	Datos genéticos	Sensible	SI	x	x	x	x			
13	Discapacidades	Sensible	SI	x	x	x	x		x	Admisiones y Matriculación Gestión del Talento Humano Gestion Medica Institucional
14	Nombres y apellidos	No sensible	NO	x	x	x	x	x	x	Admisiones y Matriculación Pagos Evaluación y Seguimiento Académico Gestión del Talento Humano Gestión Administrativa Gestion Medica Institucional
15	Número de Identificación	No sensible	NO	x	x	x	x	x	x	Admisiones y Matriculación Pagos Evaluación y Seguimiento Académico Gestión del Talento Humano Gestion Medica Institucional Gestión Administrativa
16	Dirección	No sensible	NO	x	x	x	x	x	x	Admisiones y Matriculación Gestión del Talento Humano Gestión Administrativa
17	Nro. de teléfono	No sensible	NO	x	x	x	x	x	x	Admisiones y Matriculación Pagos Gestión del Talento Humano Gestión Administrativa
18	Correo electrónico	No sensible	NO	x	x	x	x	x	x	Admisiones y Matriculación Pagos Gestión del Talento Humano
19	Fecha de nacimiento	No sensible	NO	x	x	x	x		x	Admisiones y Matriculación Gestión del Talento Humano Gestión Administrativa
20	Estado civil	No sensible	NO	x	x	x	x			Admisiones y Matriculación Gestión del Talento Humano Gestión Administrativa
21	Calificaciones académicas	No sensible	SI	x	x		x			Planificación Académica Admisiones y Matriculación Evaluación y Seguimiento Académico
22	Curriculum vitae	No sensible	NO		x	x		x	x	Gestión del Talento Humano

Nota. Matriz se encuentra adjunta en Apéndice A

Activos de procesos críticos

En base a la matriz de procesos **Tabla 9** se realiza un análisis total de todos los activos que tenemos descritos en el ESGI de la ESPE, los cuales los podemos encontrar las políticas vigentes ***ESPE EGSI – USIN – 4.1.1 Inventario de Activos***, dentro de este inventario podemos encontrar varias matrices las cuales apuntan a diferentes tipos de activos.

De todos estos activos, seleccionamos los siguientes para cada proceso de tratamiento:

Tabla 10.

Activos de la información

Proceso de tratamiento	***Activos de información***		
	ID	***Nombre***	***Descripción***
Admisiones y Matriculación	ACT-1	Bases de datos	Bases de datos en general de la universidad
	ACT-2	Banner	Sistema encargado de procesos estudiantiles y administrativos como: matriculas, gestión de notas y asistencia, etc.
	ACT-3	Directorio Activo AD	Windows Server 2019 datacenter/ Principal
Gestión del Talento Humano	ACT-4	SIFRHE	Módulo de Talento Humano del personal de la ESPE
	ACT-5	OnlyControl - biométrico, carnetización	Módulo para el control de asistencia del personal de la ESPE y Registro de carnetización
Pagos	ACT-6	Botón de Pagos	Módulo para registro de pagos en línea
Evaluación y Seguimiento Académico	ACT-7	Workflow	Sistema de gestión de procesos académicos, impedimentos, terceras matriculas, etc.

Proceso de tratamiento	*Activos de información*		
	ID	*Nombre*	*Descripción*
	ACT-8	ESPEMATICO	Sistema encargado de la gestión de formularios, certificados y documentación estudiantil
Gestión Administrativa	ACT-9	QUIPUX	Sistema de Gestión Documental Institucional utilizado para el registro, control, circulación y organización de los documentos digitales y/o físicos que se generan, reciben y tramitan en la Institución.
Diagnóstico Socioeconómico	ACT-10	InnovativaSalud	Sistema para la administración de fichas médicas del personal y estudiantes

Nota. Todos los activos fueron obtenidos del ESGI de la ESPE y su ID es su identificador para corroboración y consistencia con APÉNDICE A

Amenazas y Vulnerabilidades

Ya establecido los activos críticos de cada proceso que utiliza o realiza tratamiento de datos personales, vamos a establecer las amenazas y vulnerabilidades relacionadas para un posterior análisis y valoración de riesgo.

Amenazas

Cada activo tiene varias amenazas que lo rodean variando su tipo de origen, se han pulido y comparado las amenazas comunes que nos indica la ***ISO 27005 – Gestión***

de Riesgos y las dispuestas en el **ESGI – ESPE,** en **Tabla 11** podemos visualizar un ejemplo de las amenazas seleccionadas para el activo Bases de Datos tomado de Apéndice A.

Tabla 11.

Amenazas General

Activo	***Amenaza***
Bases de Datos	Evento natural (Inundación, tormenta eléctrica, sismo) Abuso de los derechos Suplantación de identidad

En base a la identificación de las amenazas, la evaluación de su proceso crítico y evaluación del activo, se identificará las vulnerabilidades correspondientes que presenta actualmente.

Vulnerabilidades

El análisis de vulnerabilidades se realiza individualizada para cada activo, considerando las amenazas propias según su proceso crítico. De este modo, se establece una correlación específica entre las amenazas y las vulnerabilidades reales que pueden afectar a cada activo.

Aquí mostramos un ejemplo de selección de vulnerabilidades para el Activo Bases de Datos:

Tabla 12.

Ejemplo de selección de Vulnerabilidades

Activo	***Amenaza***	***Vulnerabilidades***
Bases de Datos	Evento natural (Inundación, tormenta eléctrica, sismo)	centro de cómputo bajo nivel probable de inundación -- Protección hasta sismo grado 8)
	Abuso de los derechos	ausencia de procesos de auditoría capacidad para inhabilitar logs de auditoría Acceso a la base de datos como administrador
	Suplantación de identidad	No existe concienciación al personal de TI acerca de la Ingeniería social
	Mal funcionamiento del software	Mantenimiento no adecuado ni planificado de la BDD

De esta manera se relacionan las vulnerabilidades con las amenazas, dependiendo del activo y su proceso crítico, de esta manera se podrá realizar un análisis cualitativo de riesgos.

Análisis de Riesgos

Para determinar el impacto real de las vulnerabilidades en los objetivos de la institución, se realiza un análisis cualitativo de riesgos. Este análisis se enfoca en evaluar

las potenciales consecuencias de la explotación de cada vulnerabilidad, considerando el impacto en los diferentes procesos, activos y recursos de la organización.

El análisis cualitativo permite determinar la severidad de cada vulnerabilidad y su potencial impacto en el negocio. Y como resultado del análisis cualitativo, se define un posible impacto real de negocio para cada vulnerabilidad.

Esta información se utiliza como insumo para la evaluación de riesgos, que permite calcular la probabilidad de ocurrencia de un evento adverso y su impacto en varios ámbitos.

A continuación, podemos ver un ejemplo de cómo se establece el impacto a cada vulnerabilidad:

- Activo: Bases de Datos

Tabla 13.

Análisis de impacto

Activo	***Amenaza***	***Vulnerabilidades***	***Impacto***
Bases de Datos	Evento natural (Inundación, tormenta eléctrica, sismo)	centro de cómputo bajo nivel probable de inundación - Protección hasta sismo grado 8)	suspensión de servicio
	Abuso de los derechos	ausencia de procesos de auditoría	no pueden ser detectados ni corregidos, hallazgos y responsabilidades en vulneración de derechos de

Activo	*Amenaza*	*Vulnerabilidades*	*Impacto*
			los titulares de los datos y daño moral.
		capacidad para inhabilitar logs de auditoría	falta de evidencia probatoria de errores para determinar oportunidades de mejora y responsabilidades.
		Acceso a la base de datos como administrador	vulneración de derechos de los titulares de los datos y daño moral.
	Suplantación de identidad	No existe concienciación al personal de TI acerca de la Ingeniería social	vulneración de derechos de los titulares de los datos y daño moral.
	Mal funcionamiento del software	Mantenimiento no adecuado ni planificado de la BDD	suspensión de servicio

Este análisis de riesgos se debe realizar por cada una de las vulnerabilidades declaradas de cada activo, en este proyecto en total se obtuvieron **39 riesgos** entre todos los procesos críticos.

Evaluación de Riesgos

Para realizar la evaluación de riesgos se llevó a cabo un análisis cuantitativo que consideró tanto el impacto como la probabilidad de cada riesgo.

En cuanto al impacto, se elaboró la matriz (**Figura 4**) con parámetros de evaluación basándose en el objetivo principal del proyecto, por ende, se agrega los siguientes:

- Económico
- Daño Psicológico (al titular de los datos personales)
- Imagen Institucional
- Daño a la reputación personal del titular

Figura 4.

Matriz de Evaluación del Impacto de Riesgos

IMPACTO					
Categoría	Valor	Descripción			
		Económico	Daño psicológico	Imagen institucional	Daño a la reputación personal
Catastrófico	5	>= 50.000 USD	Daño psicológico grave al titular	Pérdida de mas de 20 puntos en el Ranking Universitario	Daño grave a la reputación del titular
Muy Alto	4	>= 5.000 USD <50.000 USD	Daño psicológico significativo al titular	Pérdida de mínima de 10 puntos en el Ranking	Daño significativo a la reputación del titular
Alto	3	>= 5.000 USD <20.000 USD	Daño psicológico subsanable al titular	Probable pérdida de puntos en el Ranking Universitario	Daño subsanable a la reputación del titular
Medio	2	>= 1.000 USD <5.000 USD	Daño psicológico leve al titular	Sin pérdida en el Ranking Universitario nacional	Daño leve a la reputación del titular
Bajo	1	< 1.000 USD	Sin daño psicológico al titular	Sin pérdida en el Ranking Universitario nacional	Sin daño a la reputación del titular

Nota. Adjunta en Apéndice A – Pestaña “Matrices de impacto y probabilidad”

Para evaluar la probabilidad de ocurrencia de cada riesgo, se creó la siguiente matriz específica que evaluó diferentes parámetros enfocándose en las probabilidades reales de riesgos.

Figura 5.

Matriz de Evaluación de Probabilidad de Riesgos

PROBABILIDAD				
Categoría	Valor	Descripción		
		Repeticiones anuales	Referencia estadística	Otros
Certeza	5	Menos de 1 evento cada seis meses	>90%	Impredecible pero continuo
Muy probable	4	1 evento por año	>=90%<70%	Impredecible poco continuo
Probable	3	1 evento cada 2 años	>=40%<70%	Impredecible
Casi probable	2	1 evento cada 3 años	>=10%<40%	No se puede identificar
Improbable	1	1 evento en mas de 3 años	<10%	Muy poco probable

Nota. Adjunta en Apéndice A – Pestaña “Matrices de impacto y probabilidad”

La combinación de las matrices de impacto y probabilidad permitió obtener una valoración integral de cada riesgo, lo que facilitó la priorización de las acciones de mitigación.

Finalmente, para obtener un valor cuantitativo total de cada riesgo, establecemos la matriz en **Figura 6** de Niveles de Riesgo y así poder categorizar si cada activo es de nivel Alto, Medio o Bajo

Figura 6.

Niveles de Riesgo

Nivel de Riesgo		
Niveles de riesgo	Rango	Color
Alto	Mayor de 12	
Medio	Entre 9 y 12	
Bajo	Menor que 9	

Ahora, veremos en **Figura 7** un ejemplo de cómo fue la evaluación de riesgos en cada activo, para el ejercicio tomamos el siguiente activo:

- Activo: Bases de Datos

Figura 7.

Evaluación de riesgo

Descripción del riesgo	Valoración									NIvel de Riesgo
	Impacto					Probabilidad				
	Ec	Psic	Imln	Rep	Total	RA	RE	OT	Total	
Evento natural (Inundación, tormenta eléctrica, sismo) por centro de cómputo bajo nivel probable de inundación -- Protección hasta sismo grado 8) causa la suspensión de servicio con probabilidad de 30%	3	3	4	2	3,00	4	2	5	3,67	11,00
Abuso de los derechos por ausencia de procesos de auditoría causa que no pueden ser detectados ni corregidos, hallazgos y responsabilidades en vulneración de derechos de los titulares de los datos y daño moral. con probabilidad de 95%	3	4	5	2	3,50	4	5	3	4,00	14,00
Abuso de los derechos por capacidad para inhabilitar logs de auditoría causa la falta de evidencia probatoria de errores para determinar oportunidades de mejora y responsabilidades. con probabilidad de 80%	3	3	3	4	3,25	3	4	5	4,00	13,00
Abuso de los derechos por Acceso a la base de datos como administrador causa la vulneración de derechos de los titulares de los datos y daño moral . con probabilidad de 90%	5	2	4	4	3,75	4	5	3	4,00	15,00
Suplantación de identidad por No existe concienciación al personal de TI acerca de la Ingeniería social causa la vulneración de derechos de los titulares de los datos y daño moral . con probabilidad de 90%	2	2	4	5	3,25	4	5	3	4,00	13,00
Mal funcionamiento del software por Mantenimiento no adecuado ni planificado de la BDD causa la suspensión de servicio con probabilidad de 80%	3	4	5	5	4,25	4	4	2	3,33	14,17

Nota. Matriz completa ubicada en Apéndice A – Pestaña “Análisis de Riesgos”

Resultados de la evaluación de riesgos

En resumen, para realizar la evaluación de riesgos se obtuvo utilizó los datos personales definidos en **Tabla 8**, para realizar un análisis de uso de datos y obteniendo cuales son los procesos críticos que los utilizan, los cuales fueron definidos en **Tabla 9**, después se estableció cuáles son los activos críticos en cada uno de estos procesos y partiendo de estos activos se colocó cuáles son sus respectivas amenazas y vulnerabilidades, con lo que posteriormente logramos obtener una calificación de cada uno de estos riesgos.

Después de un largo periodo de evaluación, a continuación, se va a visualizar cuales fueron los resultados en total, categorizando por el nivel de riesgo obtenido de cada uno.

Podemos visualizar la **Figura 8** que existen 39 riesgos identificables, de los cuales: 2 riesgos fueron catalogados de nivel BAJO representado el 5.13%, 13 de nivel MEDIO representando el 33.33% y 24 de nivel ALTO representando el 61.54% del total de riesgos. Esta matriz nos sirve para el paso posterior ya que decidiremos la estrategia para indicar que nivel de riesgos categorizaremos como riesgos asumibles y cuales como reducción de riesgo.

Figura 8.

Resultados de Evaluación de Riesgos

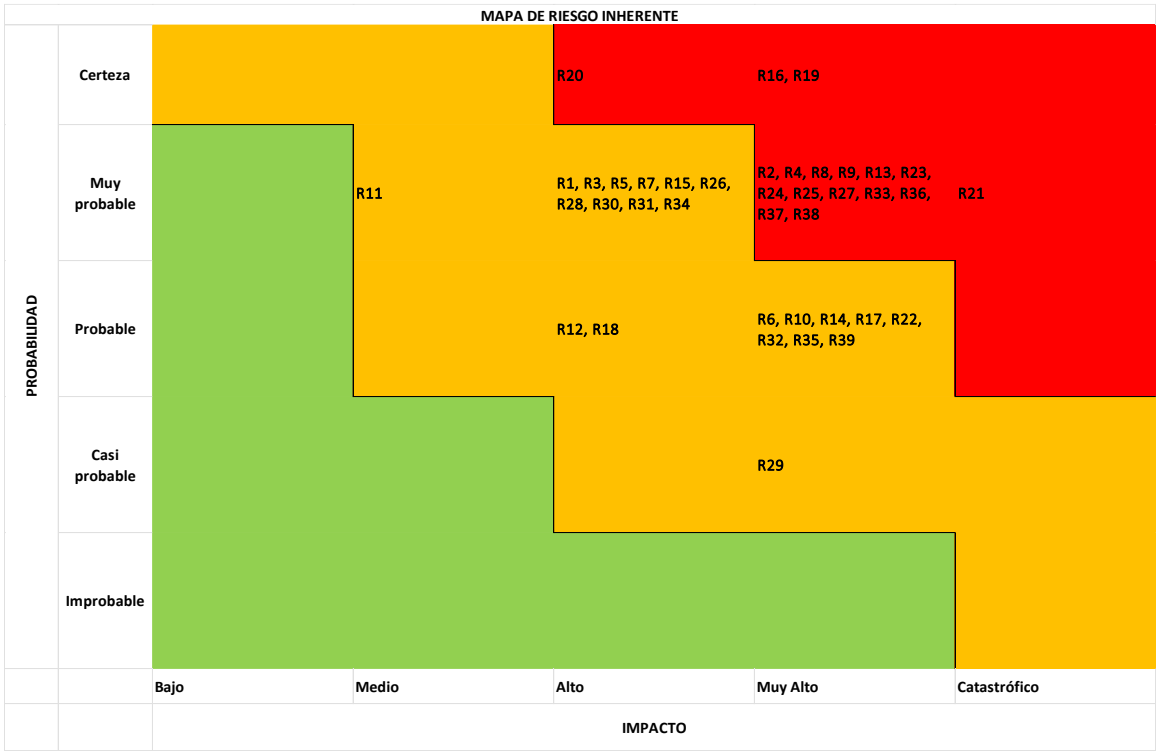
ACTIVOS	BAJO	MEDIO	ALTO	TOTAL GENERAL	PORCENTAJE
Bases de Datos	0	1	5	6	15,38%
Banner	1	2	3	6	15,38%
SIFRHE -	0	1	3	4	10,26%
OnlyControl - biométrico, carnetización	0	2	2	4	10,26%
Botón de Pagos	0	1	2	3	7,69%
Workflow	0	1	2	3	7,69%
ESPEMATICO	0	0	2	2	5,13%
Directorio Activo AD	1	3	1	5	12,82%
QUIPUX	0	1	2	3	7,69%
InnovativaSalud	0	1	2	3	7,69%
TOTAL	2	13	24	**39**	100,00%
Porcentaje	5,13%	33,33%	61,54%		100,00%

Mapa de Riesgo

En **Figura 9** podemos ver a detalle todos los riesgos ubicados según su puntuación en impacto y probabilidad.

Figura 9.

Mapa de Riesgos



Al observar la distribución de los riesgos en la matriz, se aprecia que la mayoría se ubican en las zonas media y alta. Este panorama es un mal indicio, ya que indica que la mayoría de los riesgos no son tolerables y podrían comprometen la seguridad de la información y los datos personales de los distintos titulares.

No obstante, se hace necesario un seguimiento especial para los riesgos específicos: R16, R19 y R21. Según su evaluación, estos riesgos se clasifican como catastróficos con certeza de explotación, lo que implica una alta probabilidad de ocurrencia y un impacto significativo en caso de materializarse.

Para los riesgos R16, R19 y R21, se recomienda implementar medidas de control adicionales para mitigar su impacto y reducir la probabilidad de ocurrencia.

Adicionalmente, se debe prestar atención a los riesgos ubicados en la zona roja (alta) de la matriz. Estos riesgos también requieren un tratamiento adecuado para salvaguardar el activo de cualquier compromiso.

Capítulo V

Tratamiento de Riesgos

Predominio de riesgos no asumibles

La mayoría de los riesgos (24) se encuentran en la categoría de riesgo alto, lo que representa un 61.54% del total. Esto indica que la mayoría de los activos representan una amenaza significativa para la seguridad de la información y también para los datos personales.

Áreas de atención

Existen algunos activos que requieren atención especial debido a su mayor nivel de riesgo:

- **Bases de Datos:** 6 riesgos en general y 5 riesgos catalogados como nivel alto.
- **Banner:** 6 riesgos en general y 3 riesgos catalogados como nivel alto.

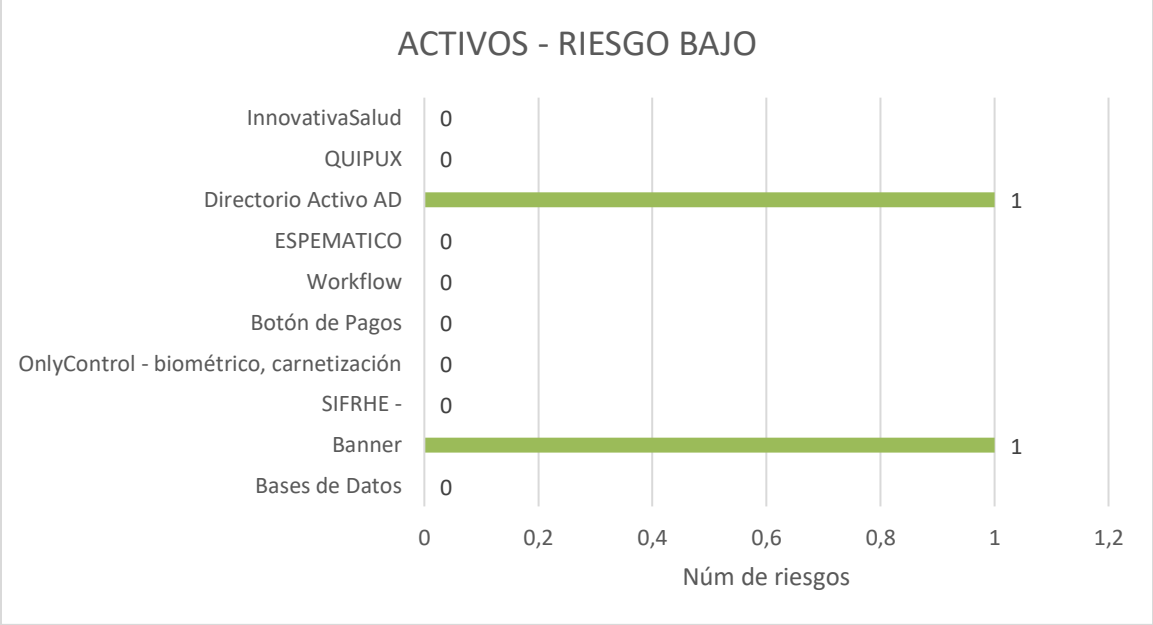
Riesgos Nivel Aceptable

Nivel Bajo

Los riesgos de nivel bajo en este proyecto se clasifican como riesgos asumibles. Esta categorización se basa en la evaluación exhaustiva de su impacto potencial, la cual ha determinado que no representan un peligro significativo para la seguridad de los datos personales de la institución.

Figura 10.

Número de riesgos bajos por cada activo



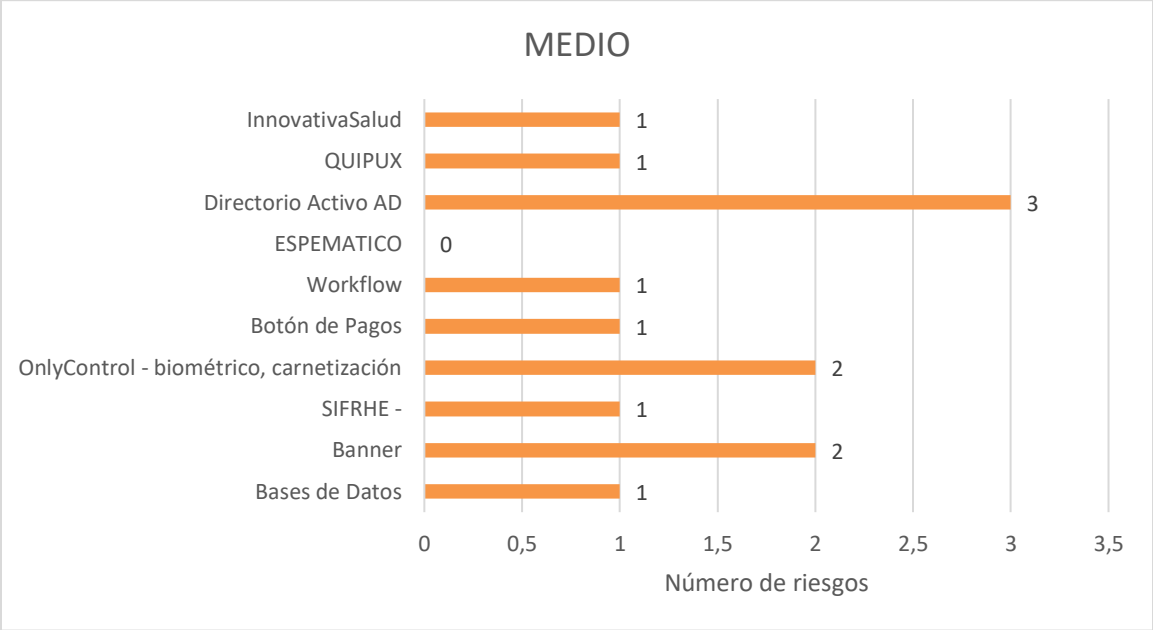
Podemos notar que en toda la evaluación de riesgos solo existieron 2 riesgos de bajo nivel, uno existe en el activo Directorio Activo y el otro en el activo Banner.

Nivel medio

Estos riesgos de nivel medio se caracterizan por un impacto limitado en la seguridad de la información y datos personales. Si bien podrían generar ciertos gastos, no se prevé que afecten de manera significativa el funcionamiento de la Universidad. Las consecuencias de estos riesgos son manejables y se pueden mitigar con la implementación de medidas de control adecuadas.

Figura 11.

Riesgos nivel medio



Aquí destacamos que solamente el activo Directorio Activo tiene 3 riesgos de nivel medio, siendo el más alto de este rango, y el que menos tiene riesgos de este nivel es el activo ESPEMATICO con 0 riesgos y los demás activos mantienen un promedio de 1 o 2 riesgos de este nivel.

Riesgos de Reducción

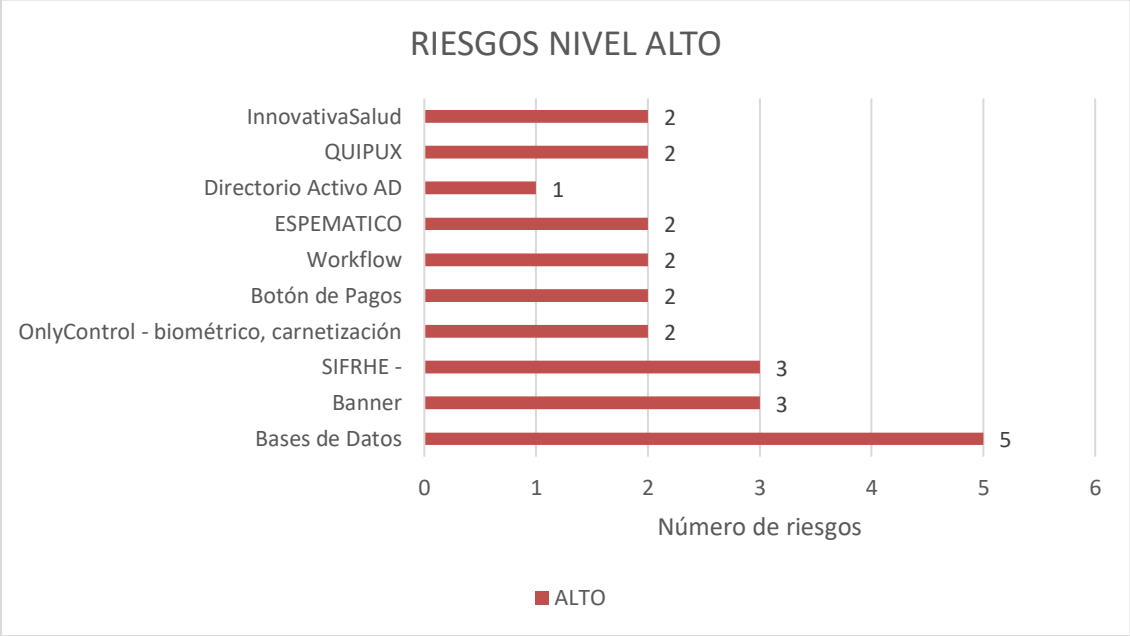
Nivel Alto

Estos riesgos de alto nivel representan una amenaza significativa para la seguridad de la información y datos personales de la ESPE. Estos riesgos se caracterizan por su potencial de causar interrupciones severas o el mal funcionamiento de los sistemas y activos de información, con consecuencias que pueden ser graves e incluso irreversibles.

Es crucial identificar y mitigar estos riesgos de manera proactiva para proteger la información confidencial, la integridad de los sistemas y la operación continua de la Universidad. La gestión eficaz de estos riesgos de alto nivel es fundamental para garantizar la seguridad y la disponibilidad de la información vital para la institución.

Figura 12.

Riesgos nivel alto



Un punto muy importante para destacar en este gráfico es que debemos tener un cuidado especial y realizar un análisis exhaustivo para proponer varios controles y salvaguardas para estos activos:

- Bases de Datos
- Banner
- SIFHRE

Ya que son los activos son más riesgos de nivel alto

De igual manera para todos los demás activos, hay que seleccionar el tratamiento adecuado para cada riesgo y poder disminuir el número de riesgos de nivel alto, ya que es muy importante tratar de cubrir todas las brechas de seguridad de la información y datos personales que pueda tener la universidad.

Estrategia de gestión de riesgos

Para el tratamiento de riesgos vamos a basarnos en las actividades que propone la ISO 27005. Donde menciona que la gestión de riesgos de seguridad de la información no se limita a la identificación y evaluación de los riesgos. Una vez que se han determinado los riesgos y su impacto potencial, es necesario definir un plan para su tratamiento. Este plan debe seleccionar e implementar controles específicos para cada riesgo, con el objetivo de reducir, aceptar/retener, evitar o transferir los riesgos a un nivel aceptable.

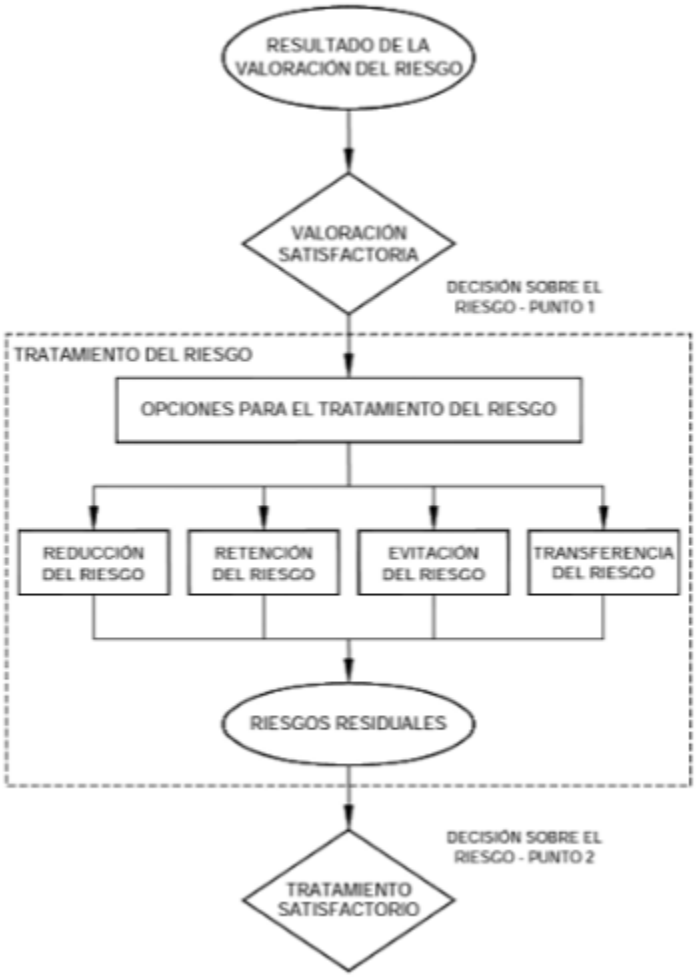
Existen cuatro opciones principales para el tratamiento del riesgo:

- **Reducción del riesgo:** Implementación de medidas para disminuir la probabilidad de ocurrencia o el impacto de un riesgo.
- **Aceptación del riesgo:** Decisión de asumir las consecuencias de un riesgo sin tomar medidas adicionales.
- **Evitación del riesgo:** Eliminación del riesgo mediante la eliminación de la fuente de este.
- **Transferencia del riesgo:** Transferencia de la responsabilidad del riesgo a otra parte, como a través de un seguro.

La **Figura 13** ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información.

Figura 13.

Actividades para tratamiento de riesgos



Nota. Mapa de flujo que se utiliza en la norma ISO 27005

Para este proyecto en base a los resultados de la evaluación de riesgos en **Figura 8** se optó, que los riesgos de nivel bajo y medio sean calificados como **Aceptación**, mientras que los riesgos de nivel alto como **Reducción.**

Figura 14.

Estrategia de riesgos

Estrategia de Tratamiento					
ACTIVOS	ASUMIR RIESGO		REDUCIR RIESGO	TOTAL GENERAL	Porcentaje
	BAJO	MEDIO	ALTO		
Bases de Datos	0	1	5	6	15,38%
Banner	1	2	3	6	15,38%
SIFRHE -	0	1	3	4	10,26%
OnlyControl - biométrico, carnetización	0	2	2	4	10,26%
Botón de Pagos	0	1	2	3	7,69%
Workflow	0	1	2	3	7,69%
ESPEMATICO	0	0	2	2	5,13%
Directorio Activo AD	1	3	1	5	12,82%
QUIPUX	0	1	2	3	7,69%
InnovativaSalud	0	1	2	3	7,69%
TOTAL	2	13	24	**39**	100,00%
	15				
Porcentaje	38,46%		61,54%		100,00%

Salvaguardas

Los riesgos críticos se constituyen en el foco principal de atención a partir de este momento. Estos riesgos requieren la aplicación de un tratamiento específico para mitigar su probabilidad o impacto en los procesos críticos de la institución.

Todos los controles específicos por cada riesgo se adjuntan en **APÉNDICE A**, sin embargo, en **Tabla 14** se adjunta los controles y salvaguardas seleccionados para el activo Bases de Datos a manera de ejemplificar su desarrollo.

Tabla 14.

Controles y salvaguardas seleccionados

Vulnerabilidades	***Estrategia***	***Controles y salvaguardas***
Ausencia de procesos de auditoría	Reducción de riesgo	Implantar y ejecutar auditorías en forma permanente

Vulnerabilidades	*Estrategia*	*Controles y salvaguardas*
Capacidad para inhabilitar logs de auditoría	Reducción de riesgo	Establecer un proceso para revisar la aplicación de la capacidad del DBMS para activar los logs de auditoría de la BDD en forma permanente y revisar la autorización para los casos de excepción
Acceso a la información de la base de datos por parte del administrador	Reducción de riesgo	Determinar y controlar en forma específica los derechos del administrador de la BDD.
No existe concienciación al personal de TI acerca de la Ingeniería social	Reducción de riesgo	Capacitar y concienciar al personal técnico responsable acerca de las técnicas de ingeniería social
Mantenimiento no adecuado ni planificado de la BDD	Reducción de riesgo	Establecer una política para el mantenimiento preventivo y correctivo de la BDD.

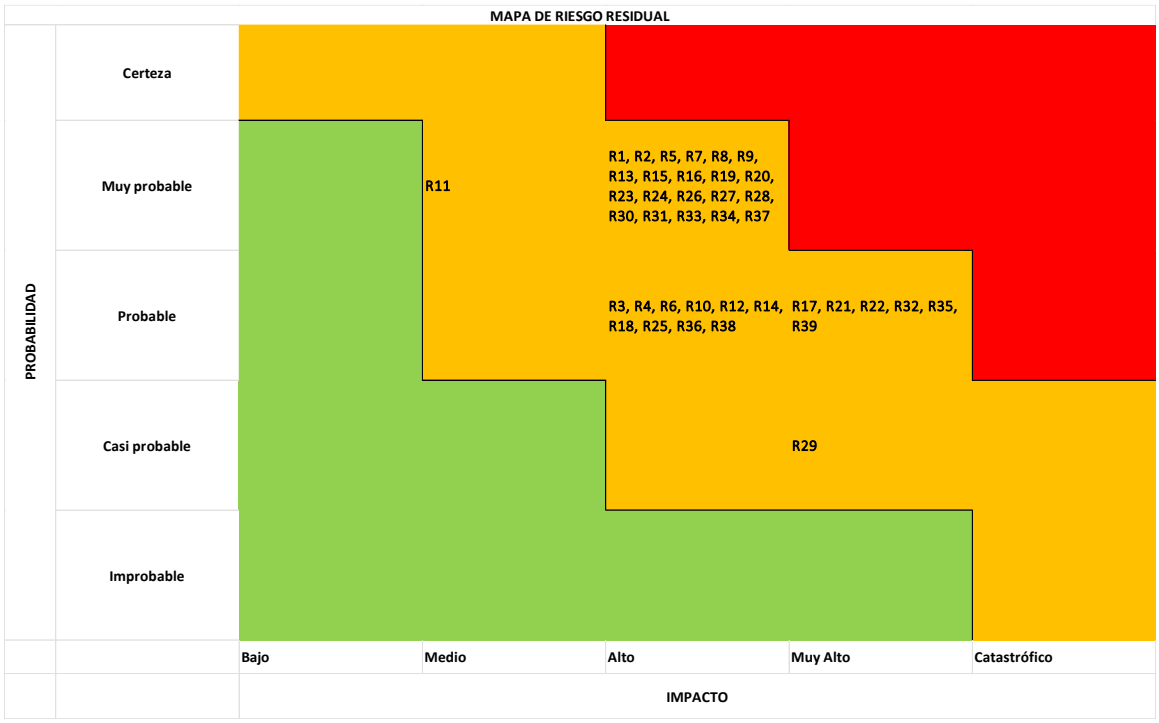
Resultados del Riesgo Residual

En esta sección se analizarán los resultados del riesgo residual, posterior a la implementación de los controles y salvaguardas correspondientes para cada riesgo identificado.

Pero primero podremos ver la nueva versión de mapa de riesgos una vez de aplicaran los controles y salvaguardas establecidos.

Figura 15.

Mapa de riesgos residual

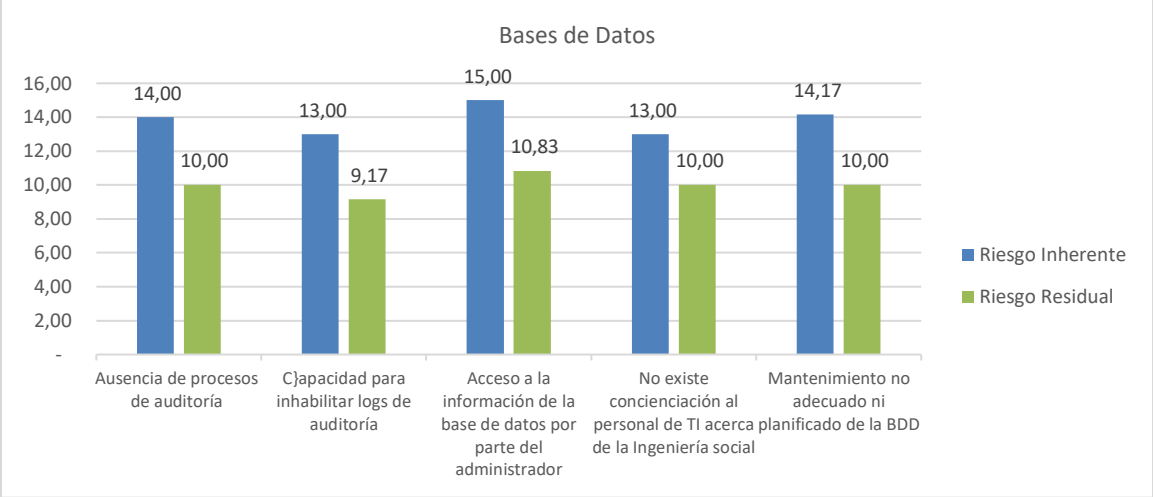


Podemos concluir que una vez se apliquen las salvaguardas indicadas, el nivel de los riesgos bajarán significativamente de nivel alto a nivel medio siendo el nivel de riesgo aceptable, en donde ya no existirá una brecha de seguridad de la información, garantizando que los procesos críticos que manejan y almacenan datos personales cumplen con principios de confidencialidad, integridad y disponibilidad de datos.

Ahora se elaborará un análisis comparativo que contraste el riesgo inherente con el riesgo residual, desglosando el análisis por cada activo.

Figura 16.

Riesgo residual activo: Bases de Datos



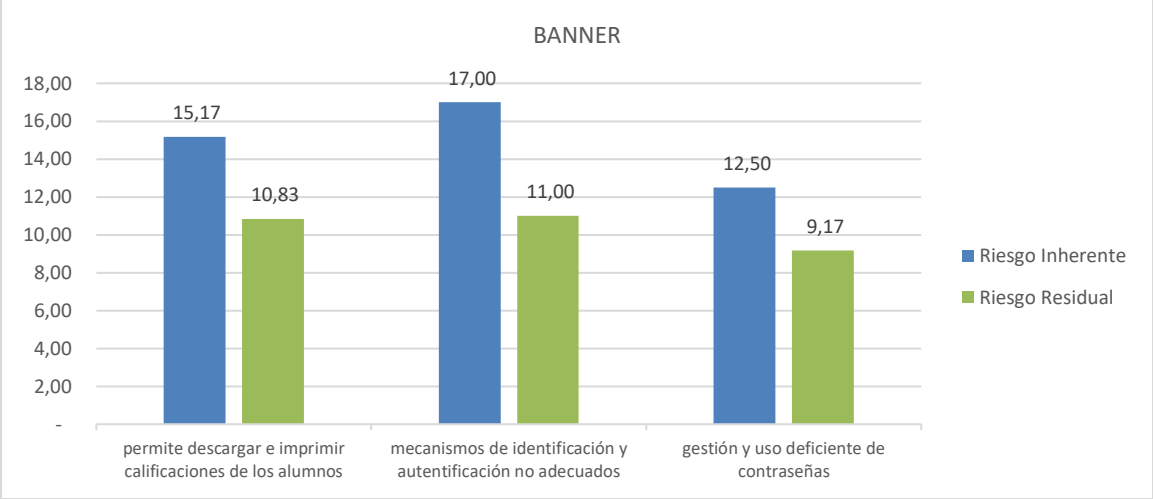
La **Figura 16** presenta la evaluación de riesgos de alto impacto asociados al activo Bases de Datos, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual

Principales riesgos

- “Acceso a la información de la base de datos por parte del administrador”: Este riesgo, inicialmente calificado como alto con un valor de 15,00, se reduce a un nivel aceptable (10,83) tras la aplicación de controles.
- “Mantenimiento no adecuado ni planificado de la BDD”: Inicialmente calificado como alto con un valor de 14,17, este riesgo se reduce a un nivel aceptable (10,00) con la implementación de medidas de control.

Figura 17.

Riesgo residual activo: Banner



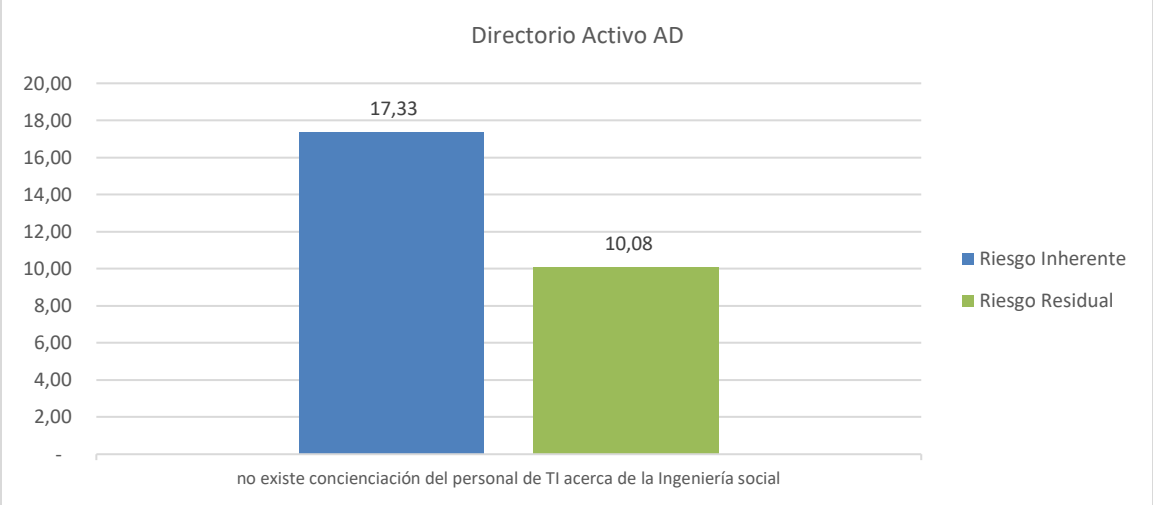
La **Figura 17** presenta la evaluación de riesgos de alto impacto asociados al activo Banner, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “Mecanismos de identificación y autentificación no adecuados”: Este riesgo, inicialmente calificado como alto con un valor de 17,00, se reduce a un nivel aceptable (11,00) tras la aplicación de controles.
- “Permite descargar e imprimir calificaciones de los alumnos”: Inicialmente calificado como alto con un valor de 15,17, este riesgo se reduce a un nivel aceptable (10,83) con la implementación de medidas de control.

Figura 18.

Riesgo residual activo: Directivo Activo



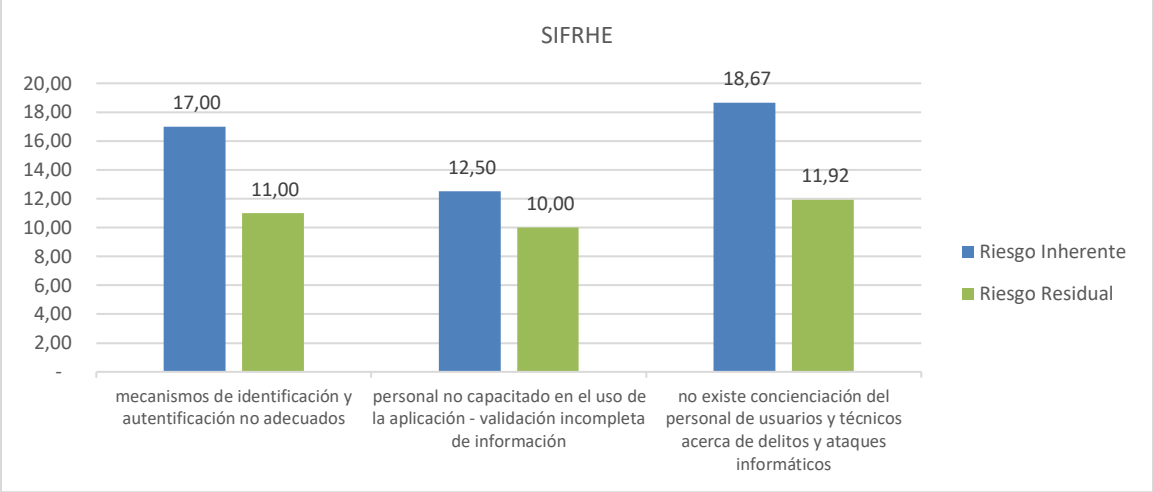
La **Figura 18** presenta la evaluación de riesgos de alto impacto asociados al activo Directorio Activo AD, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principal riesgo:

- “No existe concienciación del personal de TI acerca de la Ingeniería social”: Este riesgo, inicialmente calificado como alto con un valor de 17,33, se reduce a un nivel aceptable (10,08) tras la aplicación de controles.

Figura 19.

Riesgo residual activo: SIFRHE



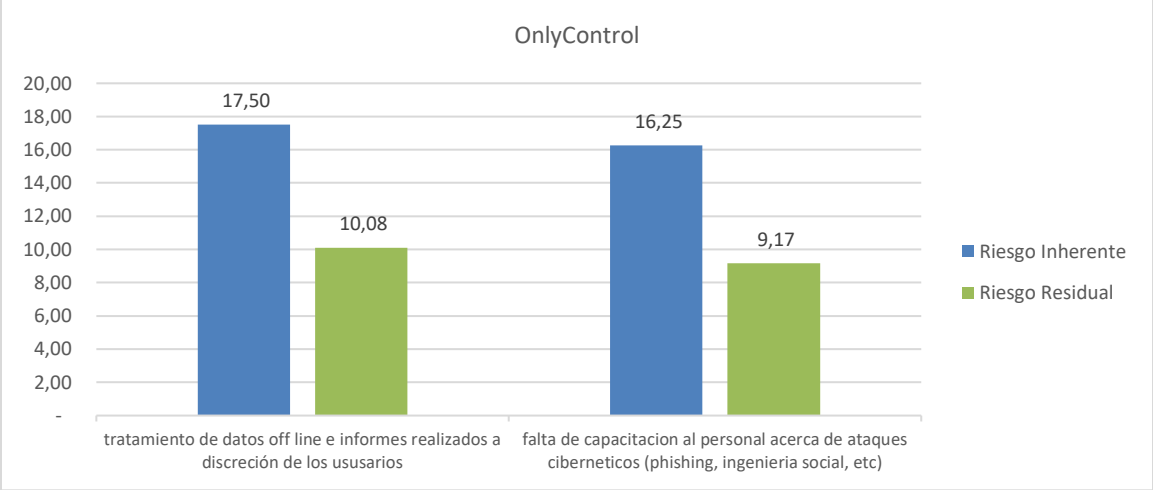
La **Figura 19** presenta la evaluación de riesgos de alto impacto asociados al activo SIFRHE, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “No existe concienciación del personal de usuarios y técnicos acerca de delitos y ataques informáticos”: Este riesgo, inicialmente calificado como alto con un valor de 18,67, se reduce a un nivel aceptable (11,92) tras la aplicación de controles.
- “Mecanismos de identificación y autentificación no adecuados”: Inicialmente calificado como alto con un valor de 17,00, este riesgo se reduce a un nivel aceptable (11,00) con la implementación de medidas de control.

Figura 20.

Riesgo residual activo: OnlyControl



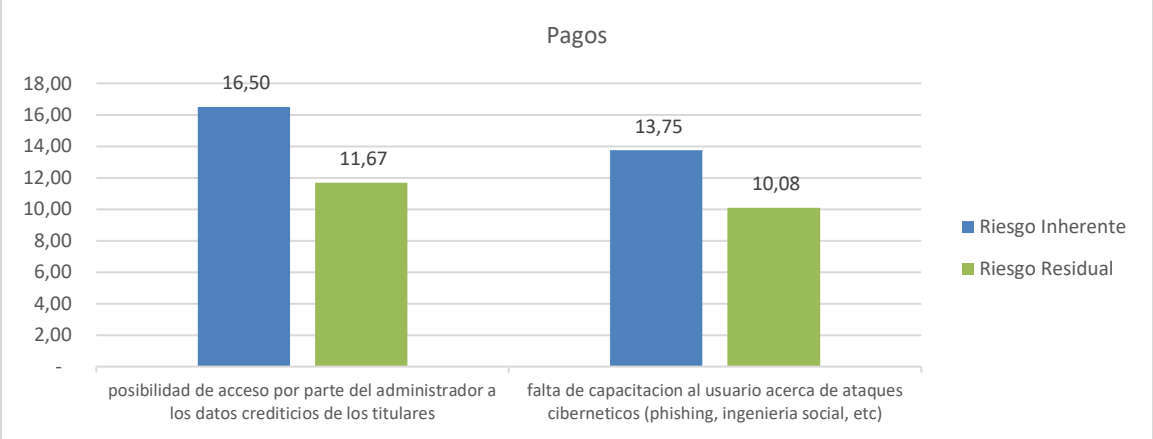
La **Figura 20** presenta la evaluación de riesgos de alto impacto asociados al activo OnlyControl, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “Tratamiento de datos off line e informes realizados a discreción de los usuarios”: Este riesgo, inicialmente calificado como alto con un valor de 17,50, se reduce a un nivel aceptable (10,08) tras la aplicación de controles.
- “Falta de capacitación al personal acerca de ataques cibernéticos (phishing, ingeniería social, etc.)”: Inicialmente calificado como alto con un valor de 16,25, este riesgo se reduce a un nivel aceptable (9,17) con la implementación de medidas de control.

Figura 21.

Riesgo residual activo: Pagos



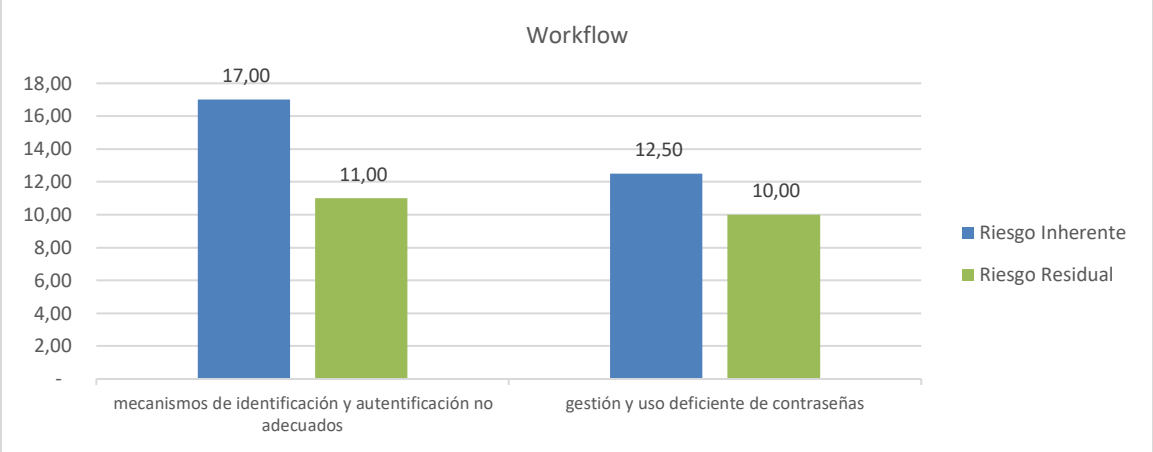
La **Figura 21** presenta la evaluación de riesgos de alto impacto asociados al activo Pagos, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados.

Principales riesgos

- “Posibilidad de acceso por parte del administrador a los datos crediticios de los titulares”: Este riesgo, inicialmente calificado como alto con un valor de 16,60, se reduce a un nivel aceptable (11,67) tras la aplicación de controles.
- “Falta de capacitación al usuario acerca de ataques cibernéticos (phishing, ingeniería social, etc.)”: Inicialmente calificado como alto con un valor de 13,75, este riesgo se reduce a un nivel aceptable (10,08) con la implementación de medidas de control.

Figura 22.

Riesgo residual activo: Workflow



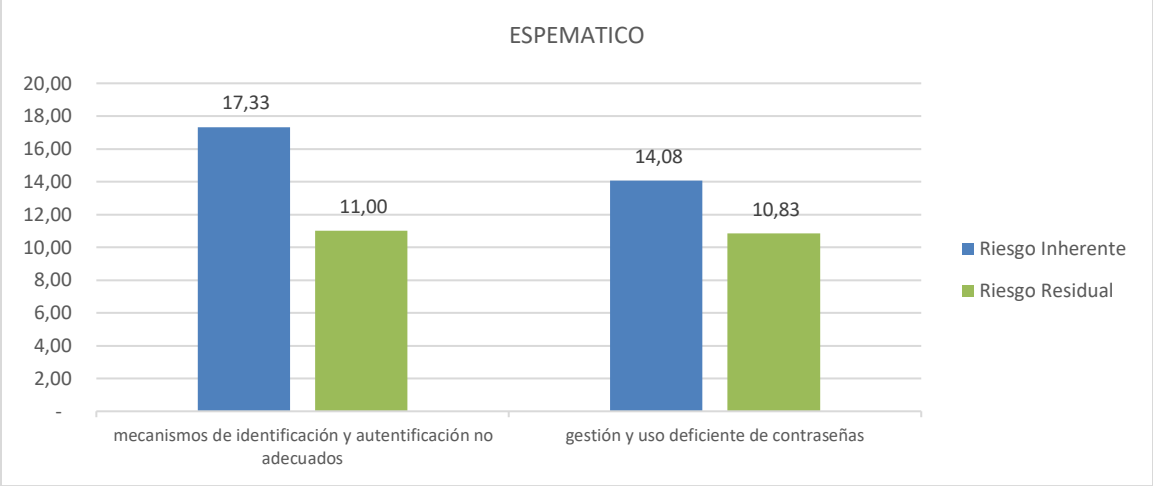
La **Figura 22** presenta la evaluación de riesgos de alto impacto asociados al activo Workflow, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “Mecanismos de identificación y autentificación no adecuados”: Este riesgo, inicialmente calificado como alto con un valor de 17,00, se reduce a un nivel aceptable (11,00) tras la aplicación de controles.
- “Gestión y uso deficiente de contraseñas”: Inicialmente calificado como alto con un valor de 12,50, este riesgo se reduce a un nivel aceptable (10,00) con la implementación de medidas de control.

Figura 23.

Riesgo residual activo: ESPEMATICO



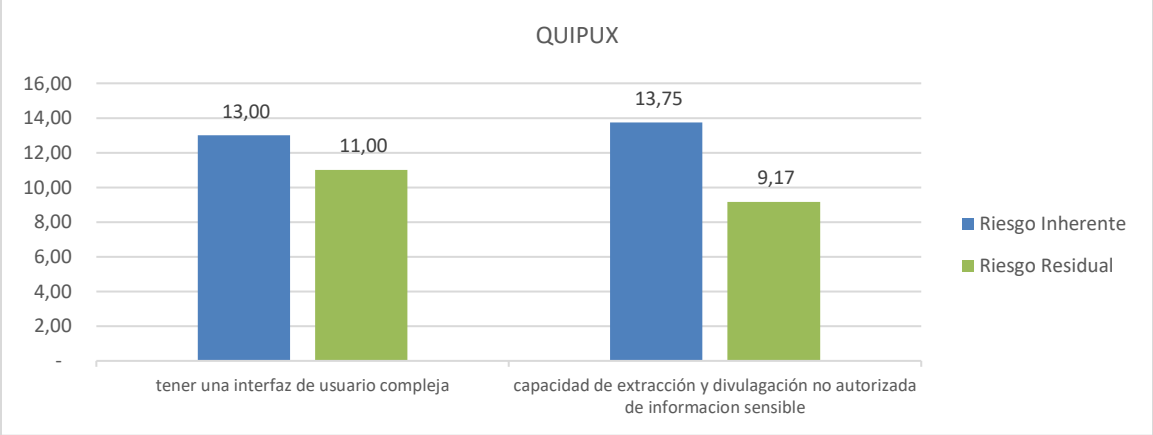
La **Figura 23** presenta la evaluación de riesgos de alto impacto asociados al activo ESPEMATICO, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “Mecanismos de identificación y autentificación no adecuados”: Este riesgo, inicialmente calificado como alto con un valor de 17,33, se reduce a un nivel aceptable (11,00) tras la aplicación de controles.
- “Gestión y uso deficiente de contraseñas”: Inicialmente calificado como alto con un valor de 14,08, este riesgo se reduce a un nivel aceptable (10,83) con la implementación de medidas de control.

Figura 24.

Riesgo residual activo: QUIPUX



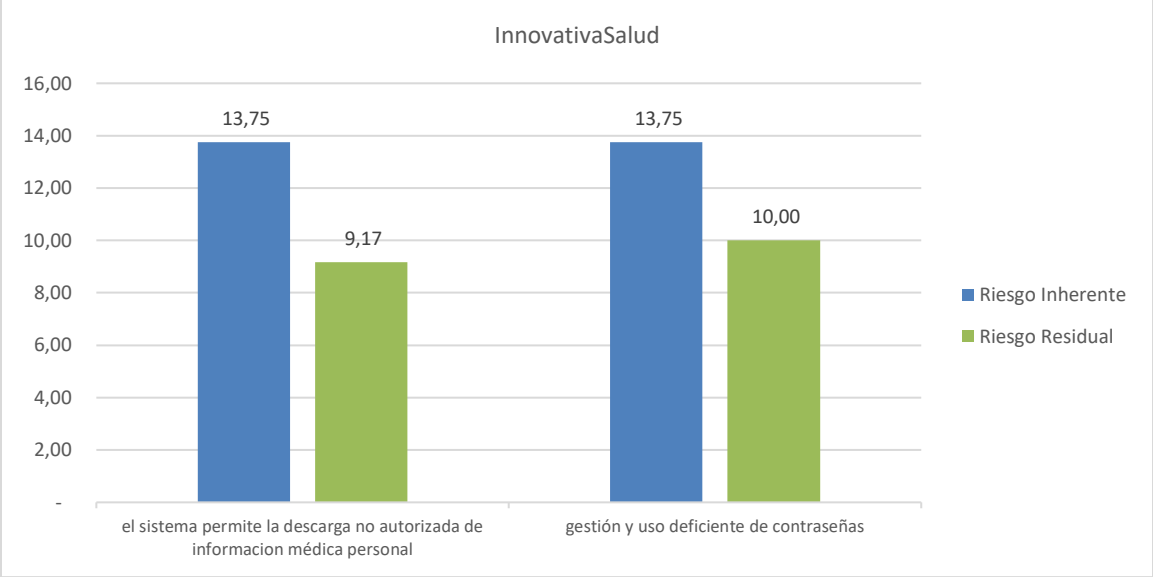
La **Figura 24** presenta la evaluación de riesgos de alto impacto asociados al activo QUIPUX, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “Capacidad de extracción y divulgación no autorizada de información sensible”: Este riesgo, inicialmente calificado como alto con un valor de 13,75, se reduce a un nivel aceptable 9.17 tras la aplicación de controles.
- “Tener un interfaz de usuario compleja”: Inicialmente calificado como alto con un valor de 13,00, este riesgo se reduce a un nivel aceptable (11,00) con la implementación de medidas de control.

Figura 25.

Riesgo residual activo: InnovativaSalud



La **Figura 25** presenta la evaluación de riesgos de alto impacto asociados al activo InnovativaSalud, considerando su estado inherente (Nivel de Riesgo) y el impacto de los controles y salvaguardas seleccionados dando como resultado el riesgo residual.

Principales riesgos

- “El sistema permite la descarga no autorizada de información médica personal”: Este riesgo, inicialmente calificado como alto con un valor de 13,75, se reduce a un nivel aceptable (9,17) tras la aplicación de controles.
- “Gestión y uso deficiente de contraseñas”: Inicialmente calificado como alto con un valor de 13,75, este riesgo se reduce a un nivel aceptable (10,00) con la implementación de medidas de control.

Capítulo VI

Plan de Implementación

Presupuesto

El presupuesto estimado total a gastar es de: **$14.200 USD** en **APÉNDICE A** podemos ver a detalle cual es el precio estimado para realizar cada control y salvaguarda.

Para calcular el tiempo y el presupuesto de la matriz de plan de implementación de salvaguardas, se consideró los siguientes factores:

Tiempo:

- La complejidad de la actividad.
- Los recursos disponibles.
- La experiencia del personal.

Presupuesto monetario:

- El costo de los recursos humanos (consultores, instructores, auditores, etc.).
- El costo de los recursos materiales (software, hardware, etc.).
- Los costos indirectos (viajes, alojamiento, etc.).

En total son 24 riesgos y cada uno de estos se le van a aplicar salvaguardas y controles necesarios, lo que da un total de **$30.200 USD,** pero basándonos en que varios activos, en parte, tienen los mismo controles y salvaguardas se realiza una resta de $**16.000 USD** por repetición de solución, dando la totalidad estimada de: **$14.200 USD.**

Responsabilidad

Se define que los controles y salvaguardas aplicados a cada uno de los riesgos presentes quedan en responsabilidad total de la persona responsable de cada uno de los activos, para ellos se toma en referencia al *ESGI – ESPE 4.1 Inventario de Activos*.

En **Tabla 15** se define los responsables de cada activo y por ende responsable de aplicar y evaluar las salvaguardas recomendadas.

Tabla 15.

Responsables de activos

ID	***Activo***	***Responsable***
ACT-1	Bases de Datos	Lorena Geselle Duque Cruz
ACT-2	Banner	Luis Gonzalo Rocha Hoyos
ACT-3	SIFRHE	Jaime Eduardo Mayla Tamayo
ACT-4	OnlyControl - biométrico	Jaime Eduardo Mayla Tamayo
ACT-5	Botón de Pagos	Luis Gonzalo Rocha Hoyos
ACT-6	Workflow	Luis Gonzalo Rocha Hoyos
ACT-7	ESPEMATICO	Luis Gonzalo Rocha Hoyos
ACT-8	Directorio Activo AD	Alexandra Bertha García León
ACT-9	QUIPUX	Nelly Oliva Cevallos Mejía
ACT-10	InnovativaSalud	Nelly Oliva Cevallos Mejía

Implantación de salvaguardas

El presente apartado define las actividades a realizar para cada salvaguarda seleccionada, incluyendo el tiempo de plazo aproximado para su ejecución. Cada actividad se asigna a un responsable específico, tal como se definió en la sección anterior.

El **Apéndice A** contiene un detalle de todas las actividades, responsables y tiempos de plazo estimados. Este plan de acción permitirá una implementación eficaz y eficiente de las salvaguardas, asegurando el cumplimiento de los objetivos establecidos.

Indicadores de eficacia y eficiencia

Los indicadores de eficacia y eficiencia son herramientas fundamentales para evaluar de manera cuantitativa el comportamiento del control y salvaguarda asignado a cada riesgo. Estos indicadores permiten determinar el grado en que los controles implementados están logrando los objetivos de seguridad de la información personal y sensible que maneja la universidad.

En el **Apéndice A** se presenta un detalle de los indicadores de eficacia y eficiencia, incluyendo la frecuencia de medición propuesta. Se espera que estos indicadores sirvan como base para la evaluación continua del programa de control y salvaguarda de riesgos, y para la toma de decisiones estratégicas en materia de seguridad de la información.

Conclusiones

En base al Esquema Gubernamental de Seguridad de la Información (ESGI) y en conformidad con lo dispuesto por el Acuerdo Ministerial 025-2021 en su forma más reciente, la Unidad de Seguridad Integrada de la Universidad ESPE propuso como objetivo la implementación de controles específicos dentro de los procesos internos de la universidad que manejen o almacenen datos personales para cumplir con la LOPDP.

Se realizo la selección de los datos personales mediante un análisis exhaustivo de la LOPDP y RGLOPDP donde se pudo definir que no todos los datos personales deben ser protegidos, si no únicamente los datos que sean categorizados como *Datos que puedan dar origen a la discriminación.*

Se ha realizado el análisis de riesgos en base a estos datos personales, utilizando los procesos internos que manejen o almacenen estos datos se obtuvo los principales activos que necesitan un tratamiento para así cumplir con la ley dispuesta, resaltando que los activos con mayor número de vulnerabilidades por corregir son las bases de datos ya que interfieren en todos los procesos internos.

Se ha definido un plan de implementación de salvaguardas en donde podemos destacar que los principales controles para mejorar la seguridad de la información a corto, mediano y largo plazo son la adopción y configuración de métodos de autenticación a las aplicaciones principales y la más importante es la concienciación del personal educativo en general hacia un cambio de cultura en donde la seguridad de la información sea lo primordial.

Recomendaciones

Para garantizar la seguridad de la información, se recomienda implementar la mayoría de los controles y salvaguardas del plan de implementación. Estos fueron seleccionados cuidadosamente mediante la evaluación de procesos internos, activos y riesgos. Se aconseja, además, utilizar los indicadores de efectividad y eficacia en los periodos recomendados para realizar una evaluación granular. La implementación de estas medidas permitirá reducir significativamente la brecha de seguridad de la información.

Para el análisis de riesgo, se recomienda tomar en consideración las normas ISO 27000 y sus derivados. Estas normas proporcionan un marco integral para la gestión de la seguridad de la información, incluyendo la identificación de vulnerabilidades y amenazas. La aplicación de estas normas permitirá realizar un análisis de riesgo más completo y efectivo, lo que a su vez ayudará a proteger mejor la información de la organización donde se desarrolle.

Se recomienda la creación e implementación de una campaña integral de concienciación sobre seguridad de la información y protección de datos personales dirigida a todo el personal educativo de la ESPE. Buscando fortalecer la cultura de seguridad informática dentro de la institución, brindando a los docentes, administrativos y personal de servicio las herramientas y conocimientos necesarios para proteger la información confidencial y los datos personales de la comunidad educativa, ya que el eslabón más débil y vulnerable de todo sistema o proceso siempre será el humano.

Lista de referencias

Código Orgánico Integral Penal. (s. f.). Recuperado 15 de enero de 2024, de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf

Constitución de la Republica del Ecuador.pdf. (s. f.). Recuperado 15 de enero de 2024, de https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Fuentes Serrate, R. C. (2020). *Sistema de Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27003 para la Universidad Nacional de Cajamarca*. http://repositorio.unprg.edu.pe/handle/20.500.12893/9097

Gobierno Electrónico de Ecuador. (2019). Esquema Gubernamental de Seguridad de la Información (EGSI). *Gobierno Electrónico de Ecuador*. https://www.gobiernoelectronico.gob.ec/normativa/

Instituto Ecuatoriano de Normalización. (2012). *Gestión del Riesgo en la Seguridad De La Información INEN-ISO/IEC 27005:2012*.

International Organization for Standardization. (2008, junio 19). *ISO/IEC 27005:2008*. ISO. https://www.iso.org/standard/42107.html

International Organization for Standardization. (2022a). *ISO/IEC 27002:2022*. ISO. https://www.iso.org/standard/75652.html

International Organization for Standardization. (2022b, febrero 4). *ISO 31000:2018*. ISO. https://www.iso.org/standard/65694.html

Jaramillo Burbano, J. L. (2022). *CONSIDERACIONES PARA LA IMPLEMENTACIÓN DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA LEY DE PROTECCIÓN DE DATOS PERSONALES CASO DE ESTUDIO: INSTITUTO NACIONAL DE PATRIMONIO CULTURAL* [masterThesis,

UISRAEL - QUITO]. http://repositorio.uisrael.edu.ec/handle/47000/3361

Ley Orgánica de Protección de Datos Personales, (2021). https://www.finanzaspopulares.gob.ec/wp-content/uploads/2021/07/ley_organica_de_proteccion_de_datos_personales.pdf

Ley Orgánica de Telecomunicaciones. (2015). https://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Org%C3%A1nica-de-Telecomunicaciones.pdf

Ley Orgánica del Sistema Nacional de Registro de Datos Públicos. (s. f.). Recuperado 15 de enero de 2024, de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/01/LEY-ORGANICA-DEL-SISTEMA-NACIONAL-DE-REGISTRO-DE-DATOS-PUBLICOS.pdf

López, J., Proaño, V., & Zabala, W. (2022, enero 31). *Políticas de Seguridad de la Información para la Universidad Politécnica Estatal del Carchi | SATHIRI*. https://revistasdigitales.upec.edu.ec/index.php/sathiri/article/view/1117

Mayorga Jácome, T. C., García Jiménez, M., Duret Gutiérrez, J. F., Carrión Jumbo, J., & Yarad Jeada, P. V. (2019). Historia de la normativa reguladora de la Protección de Datos de carácter personal en distintos países Latinoamericanos. *Dominio de las Ciencias*, *5*(1), 518-537.

Remache Arias, J. S. (2019). *Análisis de los aspectos técnicos del marco regulatorio para la protección de datos personales en Ecuador* [bachelorThesis, Quito: Universidad de las Américas, 2019]. http://dspace.udla.edu.ec/handle/33000/11581

Tenesaca Guamán, G. V., Mejía Quizhpe, L. D. C., Jara Obregón, L. S., & Tigre Sánchez, M. A. (2023). Sistema de información integrado en instituciones de educación

superior en Ecuador. *Revista Venezolana de Gerencia: RVG*, *28*(Extra 9), 777-795.

Vaca Escobar, P. N. (2020). *Modelo de gestión de seguridad lógica de la información en la protección de los datos sensibles de los distritos de educación del Ecuador* [masterThesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Maestría en Gerencia de Sistemas de Información]. https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/30565

Vivar Butiñá, J. J. (2022). *Alcance de la protección de datos personales en el marco legal ecuatoriano.* http://repositorio.ucsg.edu.ec/handle/3317/18649

Apéndice

- Apéndice_A_Evaluación de Riesgos de Datos Personales.xlsx