



**Universidad de Las Américas**

**Facultad de Ingeniería y Ciencias Aplicadas**

**Ingeniería de Ciberseguridad**

***Evaluación de riesgos y gestión de activos críticos,  
implementando inteligencia artificial, en una institución de  
educación superior***

**Brandon Sebastián Villacis Salazar**

**Fernando Nicolas Alomoto Quintanilla**

**2026**

**Quito, Ecuador**



## Contenido

|  |                               |
|--|-------------------------------|
| Resumen.....   | 4                             |
| Abstract .....   | 5                             |
| 1. Introducción.....   | 6                             |
| 1.1. Identificación y descripción del problema o necesidad.....                  | 6                             |
| 1.2. Descripción de la organización .....  | 7                             |
| 1.3. Impacto del proyecto en la sociedad .....                                   | 8                             |
| 2. Análisis de posibles soluciones.....  | 10                            |
| 2.1. Descripción de estudios realizados .....                                    | 10                            |
| 2.2. Limitaciones y restricciones del proyecto.....                              | 12                            |
| 2.3. Identificación y selección de la mejor solución .....                       | 12                            |
| 3. Alcance .....   | 18                            |
| 3.1. Alcance de la solución seleccionada.....                                    | 18                            |
| 4. Objetivos.....  | 19                            |
| 4.1. Objetivo General .....  | 19                            |
| 4.2. Objetivos Específicos .....   | 19                            |
| 5. Planificación y costos del proyecto.....                                      | 20                            |
| 6. Desarrollo del proyecto .....   | 22                            |
| 6.1. Diseño de la solución .....   | 22                            |
| 6.2. Desarrollo de la solución.....  | 25                            |
| 6.2.1 Identificación de activos críticos .....                                   | 25                            |
| 6.2.2 Análisis de amenazas y vulnerabilidades .....                              | 28                            |
| 6.2.3 Recolección de información mediante cuestionario MAGERIT .....             | 31                            |
| 6.2.4 Evaluación automatizada de riesgos con inteligencia artificial local ..... | 35                            |
| 6.2.5 Construcción de la matriz de riesgos .....                                 | ¡Error! Marcador no definido. |
| 6.2.6 Visualización de resultados mediante dashboards interactivos .....         | 37                            |
| 6.2.7 Apoyo a la toma de decisiones y mejora continua.....                       | 37                            |
| 6.3. Pruebas y evaluación de la solución.....                                    | 38                            |
| 6.4. Resultados y Discusión.....   | 52                            |
| 6.5. Implicaciones éticas .....  | 54                            |
| 7. Conclusiones y Recomendaciones .....  | 55                            |
| Conclusiones .....   | 55                            |
| 8. Trabajo futuro.....   | 57                            |
| 9. Referencias bibliográficasFR.....   | 59                            |
| 10. Anexos .....   | 61                            |



## INDICE DE TABLAS

|   |    |
|---|----|
| Tabla 1: Mejor solución.....  | 16 |
| Tabla 2: Planificación de fechas del proyecto .....                 | 20 |
| Tabla 3: Costos del software .....                                  | 22 |
| Tabla 4: Relación activo-amenaza .....                              | 41 |
| Tabla 5: Comparación de resultados entre evaluaciones .....         | 53 |
| Tabla 6: Rol de la IA en el proceso de evaluación .....             | 54 |
| Tabla 7: Comparación de metodologías.....                           | 65 |
| Tabla 8: Comparación de herramientas.....                           | 68 |
| Tabla 9: Comparación de tecnologías de inteligencia artificial..... | 71 |
| Tabla 10: Comparación de empresas solución 2.....                   | 75 |
| Tabla 11: Comparación herramientas solución 3.....                  | 78 |
| Tabla 12: Comparación 3.....  | 79 |
| Tabla 13: Comparación de costos .....                               | 81 |



## INDICE DE IMAGENES

|  |    |
|--|----|
| Ilustración 1: Diagrama de implementación .....  | 23 |
| Ilustración 2: Formulario de registro de activos nuevos.....                           | 26 |
| Ilustración 3: Valoración de Disponibilidad, Integridad y Confidencialidad (DIC) ..... | 26 |
| Ilustración 4: fórmulas del modelo. ....   | 27 |
| Ilustración 5: Catálogo de amenazas.....   | 28 |
| Ilustración 6: Catálogo de CONTROLES ISO27002.....                                     | 29 |
| Ilustración 7: Catálogo de Salvaguardas. ....  | 29 |
| Ilustración 8: Catálogo de vulnerabilidades por tipo de activo.....                    | 30 |
| Ilustración 9: Matriz de vulnerabilidades por tipo de activo. ....                     | 30 |
| Ilustración 10: Selección del activo a evaluar. ....                                   | 31 |
| Ilustración 11: Preguntas RTO .....  | 32 |
| Ilustración 12: Preguntas RPO.....   | 32 |
| Ilustración 13: Preguntas BIA .....  | 33 |
| Ilustración 14: Vista previa del cálculo de la valoración .....                        | 33 |
| Ilustración 15: Valoraciones DIC .....   | 34 |
| Ilustración 16: Distribución de criticidad. ....                                       | 35 |
| Ilustración 17: Cálculo automatizado de riesgos según MAGERIT v3. ....                 | 36 |
| Ilustración 18: Resumen y distribución de riesgos de ciberseguridad.....               | 36 |
| Ilustración 19: Evaluaciones existentes y creación de Nueva evaluación.....            | 38 |
| Ilustración 20: Listado de activos .....   | 39 |
| Ilustración 21: Valorar con IA (72 activos listos) .....                               | 39 |
| Ilustración 22: Catálogo de amenazas.....  | 40 |
| Ilustración 23: Mapa de radar.....   | 41 |
| Ilustración 24: Gráfico comparativo.....   | 42 |
| Ilustración 25: Mapa de calor.....   | 43 |
| Ilustración 26: Lista de riesgos. ....   | 43 |
| Ilustración 27: Niveles de madurez.....  | 44 |
| Ilustración 28: Nivel de madurez .....   | 45 |
| Ilustración 29: Componentes de la puntuación de madurez .....                          | 45 |
| Ilustración 30: Distribución de riesgos por nivel de severidad. ....                   | 46 |
| Ilustración 31: Salvaguardas implementada .....  | 46 |
| Ilustración 32: Indicador de nivel de riesgo. ....                                     | 47 |
| Ilustración 33: Reevaluación comparativa .....   | 47 |
| Ilustración 34: Inicio de procesos de reevaluación de riesgos.....                     | 48 |
| Ilustración 35: Resultados generales de reevaluación.....                              | 48 |
| Ilustración 36: Comparativa de Riesgo y Madurez: Antes vs Despues .....                | 49 |
| Ilustración 37: Distribución de riesgos. ....  | 49 |
| Ilustración 38: Listado salvaguardas .....   | 50 |
| Ilustración 39: Impacto de las Salvaguardas en la Reducción del Riesgo. ....           | 50 |
| Ilustración 40: Conclusión del Proceso de Reevaluación .....                           | 51 |
| Ilustración 41: Almacenamiento de resultados.....                                      | 51 |



|   |    |
|---|----|
| Ilustración 42: Módulo de inventario e identificación de activos.....                       | 81 |
| Ilustración 43: Módulo de inventario y agregar activos .....                                | 82 |
| Ilustración 44: Cuestionario Magerit aplicado a los activos tecnológicos .....              | 82 |
| Ilustración 45: Preguntas del cuestionario de Magerit.....                                  | 83 |
| Ilustración 46: Flujo de evaluación de riesgos mediante inteligencia artificial local ..... | 83 |
| Ilustración 47: Inteligencia artificial local avanzada.....                                 | 84 |
| Ilustración 48: Interfaz StreamLit.....   | 84 |
| Ilustración 49: Comando StreamLit.....  | 85 |
| Ilustración 50: Distribución por nivel de riesgo inherente.....                             | 85 |
| Ilustración 51: Dashboard comparativo riesgo inherente y residual .....                     | 86 |
| Ilustración 52: mapa de calor Magerit .....   | 86 |
| Ilustración 53; Módulos principales del sistema implementado en entorno local.....          | 87 |
| Ilustración 54: Registro e inventario de elementos tecnológicos en el sistema .....         | 87 |
| Ilustración 55: Registro e inventario de especificaciones técnicas.....                     | 88 |
| Ilustración 56: Registro e inventario de mantenimiento y soporte .....                      | 88 |
| Ilustración 57: Listado de activos.....   | 89 |
| Ilustración 58: Carga masiva de activos JSON.....   | 89 |
| Ilustración 59: Plantillas de JSON .....  | 90 |
| Ilustración 60: Catalogo de referencia.....   | 90 |
| Ilustración 61: Preguntas Disponibilidad.....   | 91 |
| Ilustración 62: Preguntas Integridad .....  | 91 |
| Ilustración 63: Preguntas de Confidencialidad.....  | 92 |
| Ilustración 64: Respuestas del cuestionario.....  | 92 |
| Ilustración 65: Resumen de valoraciones .....   | 93 |
| Ilustración 66: Tabla de valoraciones.....  | 93 |
| Ilustración 67: Tabla de valoraciones 2 .....   | 94 |
| Ilustración 68: Formulas de las vulnerabilidades.....                                       | 94 |
| Ilustración 69: Amenazas identificadas.....   | 95 |
| Ilustración 70: Registro de amenazas y vulnerabilidades .....                               | 95 |
| Ilustración 71: Advertencia del recalculo.....  | 96 |
| Ilustración 72: Interfaz StreamLit.....   | 96 |
| Ilustración 73: Dashboard interactivo .....   | 97 |
| Ilustración 74: Interpretación. ....  | 97 |



## Resumen

El presente proyecto propone el desarrollo e implementación de un sistema para la evaluación y gestión de riesgos en ciberseguridad, orientado a una institución de educación superior. La solución se basa en la metodología de Magerit v3 y en los controles de la norma ISO/IEC 27002, permitiendo identificar, analizar y priorizar riesgos de seguridad de la información de manera estructurada.

El sistema desarrollado incorpora un inventario de infraestructura tecnológica, la aplicación de un cuestionario de Magerit y el uso de la inteligencia artificial ejecutada de forma local como apoyo al análisis. La inteligencia artificial permite generar valoraciones de disponibilidad, integridad y confidencialidad, identificar amenazas relevantes y calcular niveles de riesgo inherente y residual.

Como resultado, la solución consolida la información en dashboards interactivos que facilitan la visualización de indicadores claves y el nivel de madurez organizacional en la gestión de riesgos, el proyecto demuestra cómo la integración de metodologías formales, inteligencia artificial y visualización de datos contribuye a mejorar la toma de decisiones en ciberseguridad dentro de un entorno académico.

**Palabras clave:** Ciberseguridad, gestión de riesgos, Magerit, inteligencia artificial, evaluación de riesgos.



## Abstract

This project proposes the development and implementation of a system for cybersecurity risk assessment and management, oriented to a higher education institution. The solution is based on the MAGERIT v3 methodology and the controls of the ISO/IEC 27002 standard, enabling the structured identification, analysis, and prioritization of information security risks.

The developed system incorporates an inventory of technological infrastructure, the application of a MAGERIT-based questionnaire, and the use of locally executed artificial intelligence to support the analysis process. The artificial intelligence component generates assessments of availability, integrity, and confidentiality, identifies relevant threats, and calculates inherent and residual risk levels.

As a result, the solution consolidates the information into interactive dashboards that facilitate the visualization of key indicators and the organizational maturity level in risk management. The project demonstrates how the integration of formal methodologies, artificial intelligence, and data visualization contributes to improving cybersecurity decision-making within an academic environment.

**Keywords:** cybersecurity, risk management, MAGERIT, artificial intelligence, risk assessment.



## 1. Introducción

### 1.1. Identificación y descripción del problema o necesidad

El consorcio académico entre Costa Rica y Ecuador carece de un sistema integral de evaluación de riesgos en ciberseguridad, lo que impide identificar, priorizar y mitigar adecuadamente las amenazas que afectan sus activos críticos de información.

Actualmente la institución de alto nivel no cuenta con una matriz de riesgos formalizada ni con un diagnóstico actualizado a su nivel de madurez en ciberseguridad, ya que, dificulta la identificación por activa de amenazas y la toma decisiones informadas para mitigar riesgos.

Representa un desafío crítico que requiere una metodología estructurada y adaptada a las realidades de ambos países. Como primer punto dentro de la metodología de evaluación de riesgos que vamos a usar es revisar el inventario de activo críticos, identificación de amenazas y vulnerabilidades, analizar la probabilidad y el impacto y diseñar un plan de mitigación.

Numerosos estudios han destacado la importancia de la seguridad en los entornos virtuales de aprendizaje y han explorado diferentes técnicas y enfoques para evaluar y mejorar la seguridad de estas plataformas (Oquendo, 2022). Tenemos que brindar

En Ecuador no se ha desarrollado aún una estrategia nacional de ciberseguridad que permita establecer los lineamientos, objetivos y planes de acción necesario para proteger los servicios, la información, las infraestructuras críticas y a los usuarios frente a las amenazas en el ciberspacio (Nerina Victoria Avellán Zambrano, 2019)

En Costa Rica llevan un nivel de seguridad más alto que Ecuador. Presenta un panorama más avanzado con formación sólida, prácticas activas y mecanismos de respuestas colaborativos. Tiene un alta, de cooperación nacional y sectorial ayuda a impulsar tanto a niños como a jóvenes en introducirles al mundo de la



ciberseguridad. En el 2023 fortalecieron la seguridad digital mediante conformación de CSIRT.

A pesar de que los dos países se encuentren en un nivel diferente en la seguridad de la información, nos vamos a concentrar en dos instituciones de alto nivel en Costa Rica y una institución de alto nivel en Ecuador, con la metodología de MAGERIT, vamos a identificar, analizar y evaluar, los riesgos que puede corres las instituciones de alto nivel.

En el caso de la institución de nivel superior, la ausencia de una gestión de la seguridad informática para identificar, evaluar y mitigar los riesgos ciberneticos y físicos aumenta la probabilidad de producir incidentes de seguridad y puede tener un impacto negativo, mala reputación dentro y fuera de la institución.

### **1.2. Descripción de la organización**

El consorcio está integrado por tres Universidades de prestigio en América Latina, en Costa Rica con Ulatina y UAM, y por parte de Ecuador con UDLA, estas Universidades han unido recursos tanto a nivel de hardware, software e inclusive personal humano, esto con el fin de crecer en conjunto.

Ulatina es una universidad que cuenta con más de 7 sedes alrededor del país, con el propósito de generar un impacto en la sociedad y a través de la innovación ser relevantes y competitivos, con principios fundamentales como la excelencia, integridad, resiliencia y responsabilidad social.

UAM cuenta con más de 25 años en el área de la educación superior, con el propósito de formar profesionales que impacten al desarrollo del país, busca ser accesible y asegurar el crecimiento, desarrollo y competitividad de sus estudiantes, con la visión de ser tecnológica y flexible para potenciar la empleabilidad y desarrollo del país.

“UDLA se ha posicionado en el área de la educación superior del Ecuador por más de 30 años, con la misión de formar personas con visión internacional y global, con el propósito de generar cambios en la sociedad, busca ser una referencia en la educación ecuatoriana, donde busca la excelencia académica, con tecnología de vanguardia e innovación.” (Universidad de Las Americas, s.f.)



El consorcio se forma gracias a la búsqueda de crecimiento internacional, las universidades que conforman el consorcio tienen misiones, visiones y propósitos muy alineados, lo cual hace que los objetivos se fusionen y se puedan convertir en objetivos en conjunto, siempre poniendo como punto importante la tecnología e innovación.

Las Universidades que conforman el consorcio cuentan con una estructura muy parecida, incluso compartiendo áreas que trabajan en conjunto por las mismas, se cuenta con áreas de infraestructura, desarrollo, sistemas de la información y seguridad.

### **1.3. Impacto del proyecto en la sociedad**

Los beneficios esperados del desarrollo del presente proyecto se detallan a continuación:

#### **Impacto social**

- El proyecto contribuye a generar conciencia institucional sobre la importancia de proteger los entornos digitales e instituciones de educación superior, fortaleciendo la confianza de estudiantes, docentes, autoridades comunidad externa en el uso de plataformas tecnológicas.
- La implementación de procesos de inventario y evaluación de riesgos promueve una cultura de seguridad preventiva y compartida, incentivando buenas prácticas en el manejo de la información y el uso responsable de los sistemas tecnológicos.

#### **Impacto económico**

- La identificación temprana de riesgos en la infraestructura tecnológica nos permite anticiparnos a fallos que pueden ocasionar pérdidas económicas por interrupciones de servicio o procesos de recuperación no planificados.
- Al priorizar los riesgos detectados el proyecto apoya la toma de decisiones estratégicas relacionados con intervenciones tecnológicas, optimizando el uso de los recursos institucionales disponibles.



## **Impacto ambiental**

- El análisis de la infraestructura tecnológica permite identificar equipos con alto consumo energético o sin mantenimiento adecuado, generando recomendaciones orientadas a un uso más eficiente de los recursos tecnológicos.
- Estas acciones puedes contribuir indirectamente a la reducción del consumo energético y a una gestión más sostenible de los activos tecnológicos a largo plazo.

## **Impacto académico**

- La evaluación preventiva de riesgos contribuye a garantizar la continuidad de servicios académicos esenciales, como plataformas virtuales, sistemas de calificaciones y recursos digitales.
- El proyecto favorece la estabilidad de los entornos de aprendizaje, docencia e investigación, reduciendo el impacto de fallos tecnológicos sobre las actividades académicas.

## **Impacto ético**

- El proyecto refuerza la importancia del manejo responsable de la información, promoviendo los principios de confidencialidad, integridad y disponibilidad en todas las fases del análisis.
- Asimismo, fomenta una conducta ética en estudiantes y profesionales, alineada con las buenas prácticas de la ciberseguridad y el respeto por la información institucional.

El presente estudio tiene como objetivo principal la implementación de un sistema inteligente que permita gestionar activos críticos y evaluar riesgos de manera estructurada, con el fin de determinar el nivel de madurez en ciberseguridad de una institución de educación superior. Sin embargo, los beneficios esperados trascienden lo técnico y abarcan diversas dimensiones sociales, económicas, ambientales, laborales, éticas y académicas.



## 2. Análisis de posibles soluciones

### 2.1. Descripción de estudios realizados

El aumento de la digitalización en las instituciones educativas ha incrementado significativamente la exposición a amenazas informáticas, lo que ha impulsado a diversas universidades y organizaciones a desarrollar mecanismos para el análisis de riesgos y la evaluación del nivel de madurez en ciberseguridad. En la Universidad de Cuenca, se desarrolló un proyecto que utilizó como base los estándares ISO/IEC 27001, NIST 800 y el modelo C2M2. A partir de estas referencias, se formularon requisitos de ciberseguridad para cada nivel de madurez, los cuales fueron integrados en una aplicación que facilita evaluaciones periódicas y visualización del estado de seguridad mediante dashboards interactivos. (Jiménez Mendieta & Sumba Naula, 2023)

En la Universidad de Costa Rica, se realizó un diagnóstico de cumplimiento de los controles de la norma ISO/IEC 27001 junto con el componente DES5 de COBIT 5, el cual incluye la gestión de servicios de seguridad, la administración de riesgos (AP12) y la gestión de seguridad (AP13). El objetivo fue determinar el grado de alineación y el nivel de madurez del Sistema de Gestión de Seguridad de la Información (SGSI) en relación con los estándares internacionales. (Hidalgo Quirós, s.f.)

Por su parte, la Pontificia Universidad Javeriana, en la ciudad de Bogotá desarrolló una metodología para la evaluación de la madurez frente a incidentes de ciberseguridad, basada en estándares como ISO/IEC 27035, NIST SP 800-61 Rev. 2, ITIL v4 y COBIT v4, integrados con el modelo CMMI. El estudio incluyó encuestas a expertos y usuarios funcionales, y propuso una herramienta de autoevaluación para que las organizaciones puedan diagnosticar su nivel de preparación y establecer planes de mejora (Pontificia Universidad Javeriana, s.f.). Esta investigación destaca la importancia de un enfoque sistemático para fortalecer la resiliencia organizacional frente a amenazas cibernéticas.



Asimismo, el estudio titulado “Implementación de un Sistema de Gestión de Seguridad de la Información para mejorar la Seguridad de la Información en una empresa MYPE” abordó la necesidad urgente de proteger los activos de información en entornos empresariales de rápido crecimiento. La propuesta se basó en la norma NTP-ISO/IEC 27001:2014 e incluyó análisis de riesgos, valoración de activos y establecimiento de controles preventivos, correctivos y directivos. La implementación del SGSI también consideró la capacitación del personal, la documentación de procesos clave y la adopción de medidas de mitigación, demostrando así la eficacia de un marco normativo para el fortalecimiento de la seguridad en MYPES. (Silva Guerrero, 2022)

Como antecedente adicional, aunque más antiguo, el estudio “Diagnóstico del Plan de Seguridad de las Tecnologías de la Información y Comunicación en una Organización” (Maza Cerón & Cabrera Villanueva, s.f.) sigue siendo relevante por su análisis integral. Evaluó la implementación de estrategias de seguridad en organizaciones académicas, gubernamentales y comerciales, usando marcos como COBIT, COSO, ITIL, ISO/IEC 27002, FIPS PUB 200 y CMMI. A través de encuestas y auditorías, se identificaron debilidades en aspectos como energía, control de accesos, software y telecomunicaciones, y se recomendó fortalecer los planes de seguridad con controles preventivos y monitoreo continuo.

Por tanto, los antecedentes revisados evidencian que diversas instituciones han optado por integrar marcos de referencia reconocidos internacionalmente con herramientas tecnológicas que permiten la visualización y evaluación continua del nivel de madurez en ciberseguridad. Estos estudios demuestran la efectividad de implementar metodologías estructuradas como ISO, NIST, MAGERIT o COBIT para mejorar la postura de seguridad de las organizaciones.



## 2.2. Limitaciones y restricciones del proyecto

### Limitaciones del proyecto

- El análisis se limita a la evaluación de riesgos sobre la infraestructura tecnológica de la institución de educación superior, considerando únicamente información técnica previamente autorizada.
- El proyecto se desarrolla en un periodo académico definido y con recursos limitados, los que restringe la realización de pruebas extensivas o el análisis de componentes adicionales fuera del alcance establecido.
- La solución tiene un enfoque exclusivamente en el diagnóstico y en recomendaciones, por lo que no contempla la mitigación directa de los riesgos identificados ni la ejecución de cambios en los sistemas productivos.

### Restricciones del proyecto.

- Se utiliza únicamente la metodología de Magerit v3 como marco principal para la evaluación de riesgos, tomando normas y controles internacionales únicamente como referencia técnica.
- No se contempla la integración con sistemas externos como SIEM, ERP, plataformas GRC ni desarrollo de aplicaciones móviles.
- La ejecución del diagnóstico y la obtención de información dependen de la disponibilidad y autorización del personal del área de tecnologías de la información, seguridad de la información y la infraestructura de la institución de educación superior.

## 2.3. Identificación y selección de la mejor solución

La mejor solución planteada, es el desarrollo de un sistema institucional para la evaluación de riesgos y madurez en ciberseguridad, apoyado por inteligencia artificial ejecutada de forma local, esta alternativa se considera la más adecuada frente a otras opciones debido a su capacidad de adaptarse las limitaciones académicas, técnicas y presupuestarias del proyecto, al mismo tiempo que permite realizar un diagnóstico estructurado repetible sobre la postura de seguridad de la información en la institución de educación superior.



El problema central identificado se relaciona con la ausencia de una evaluación formal y sistemática del nivel de madurez en ciberseguridad, causada principalmente por la falta de información consolidada sobre la infraestructura tecnológica, su criticidad y los riesgos asociados, la solución propuesta permite centralizar el inventario, aplicar la metodología Magerit v3 y generar una línea base cuantificable del estado actual de la organización, facilitando el análisis, priorización de riesgos y el seguimiento de su evolución a lo largo del tiempo.

Se analizaron otras dos alternativas. La primera corresponde a la contratación de auditorías externas especializadas, las cuales ofrecen diagnósticos profesionales, pero presentan limitaciones relacionadas con altos costos, dependencia de terceros y resultados puntuales sin continuidad en el tiempo. La segunda alternativa considera el uso de una plataforma SaaS de gestión de riesgos y cumplimiento normativo en la nube, se proporcionan funcionalidades avanzadas, requieren licenciamiento, procesos de integración complejos y una curva adopción que no se ajusta al contexto institucional ni al carácter académico del proyecto.

La solución seleccionada destaca por su viabilidad técnica, su bajo costo de implementación, su ejecución en entornos controlados y su alineación con las restricciones definidas. El uso de inteligencia artificial como apoyo al análisis permite automatizar la evaluación de disponibilidad, integridad y confidencialidad, identificar amenazas relevantes, estimar niveles de riesgo inherente y residual, generar resultados consolidados presentados mediante dashboards interactivos, la propuesta no solo resuelve el problema identificado, también establece una base sólida para futuras evaluaciones y procesos de mejora en la gestión de ciberseguridad.



### **2.3.1. Solución 1: Evaluación y gestión de riesgos en ciberseguridad institucional, implementando inteligencia artificial**

La solución 1 propuesta consiste en implementar un sistema institucional para la evaluación y gestión de riesgos en ciberseguridad, que integra metodologías formales de análisis de riesgos con el uso de inteligencia artificial como apoyo al proceso de evaluación, esta solución busca optimizar la identificación, análisis y priorización de riesgos asociados a la seguridad de la información, considerando el contexto y las limitaciones de una institución de educación superior.

La solución se fundamenta en la metodología Magerit v3, la cual proporciona un marco estructurado para la identificación de elementos tecnológicos relevantes, el análisis de amenazas y vulnerabilidades, la evaluación del impacto sobre los principios de disponibilidad, integridad y confidencialidad. De manera complementaria, se toman como referencia los controles de la norma ISO/IEC 27002 para orientar la generación de recomendaciones técnicas.

Como componente central, se incorpora la inteligencia artificial analiza la información a partir de un cuestionario de Magerit de 21 preguntas, la IA analiza la información recopilada de forma individual y grupal, generando valoraciones de confidencialidad, integridad, disponibilidad, identificando amenazas relevantes, estimando niveles de riesgo inherente y residual, y sugiriendo controles alineados con estándares internacionales, reduciendo la subjetividad y mejorando la consistencia.

Adicionalmente, la solución contempla el cálculo de un nivel de madurez organizacional en la gestión de riesgos de seguridad de la información, expresado mediante un puntaje cuantitativo, ese indicador permite evaluar el estado general de la organización y realizar el seguimiento de la evolución del riesgo a lo largo del tiempo, apoyando procesos de análisis y mejor continua.

Los resultados generados por el sistema estructuran en datasets orientados a su visualización mediante dashboards interactivos los cuales presentan indicadores clave, matrices de riesgo, comparaciones y métricas de madurez, la solución



proporciona a una base objetiva y estructurada para apoyar la toma de decisiones a nivel técnico y directivo.

Para más detalles de la solución ir al anexo 1 solución 1.

### **2.3.2. Solución 2: Evaluación de riesgos y madurez mediante auditoría externa especializada.**

La solución consiste en la contratación de una auditoría externa especializada, con el objetivo de realizar un análisis independiente y riguroso sobre la gestión de riesgos y nivel de madurez en ciberseguridad de la institución de educación superior, la auditoria será realizada por una firma registrada en el registro nacional de auditores externos y aplicará normas internacionales de auditoría, garantizando la imparcialidad, cumplimiento normativo y confiabilidad del proceso.

La solución se va a implementar, con la selección de la firma auditora, se identifican y comparan firmas como grant Thorton, opportne, Hlb o Big Four. La firma auditora accede a los documento, procesos y sistemas internos. La ejecución de la auditoria se aplica la metodología para poder evaluar activos y controles de seguridad, analizar vulnerabilidades y medir el nivel de madurez institucional.

Las normativas y metodologías que podrían aplicar es las Normas Internacionales de Auditoria, ISO/IEC27001:2022, NIST Cibersecurity Framework, controles CIS v8 y las propias metodologías según la firma.

Para más detalles de la solución ir al anexo 2 solución 2.

### **2.3.3. Solución 3: Plataforma en la nube para la gestión integral de riesgos y ciberseguridad (GRC SaaS).**

La tercera solución propone la implementación de una plataforma de gobierno, riesgo y cumplimiento en la nube bajo el modelo SaaS, que permite centralizar y automatizar la gestión de riesgos, cumplimiento normativo y nivel de madurez en ciberseguridad dentro de la institución de alto nivel.



Estas plataformas ofrecen una arquitectura escalable, acceso remoto, flujos de trabajo personalizables y reportes dinámicos, lo que facilita la colaboración entre áreas, el monitoreo continuo y la adaptabilidad y normativas como ISO/IEC27001, NIST o ISO 31000.

La implementación empieza por la selección de una plataforma GRC SaaS (LogicGate, RSA, Archer, MetricStream), la configuración inicial incluye los departamentos involucrados, matrices de riesgo y controles y reglas de flujo de trabajo, tiene que haber personal capacitado y responsable en el uso de la plataforma, ya que se encarga del monitoreo de datos en tiempo real, y la generación de informes automáticos y seguimientos de madurez y cumplimiento.

La adopción de una plataforma GRC SaaS como LogicGate ofrece una solución moderna, escalable y automatizada para la gestión de riesgos y madurez institucional, es útil para instituciones con múltiples áreas funcionales como la institución de alto nivel, permitiendo una gestión colaborativa, centralizada y conforme a estándares internacionales.

Para más detalles de la solución ir al anexo 3 solución 3.

### Solución escogida

Para más detalles se presentan en la *Tabla 1*.

*Tabla 1: Mejor solución*

| Criterio                     | Solución 1:<br>Sistema<br>institucional con<br>IA             | Solución 2:<br>Auditoría externa<br>especializada                 | Solución 3:<br>Plataforma GRC en la<br>nube (SaaS)    |
|------------------------------|---|---|---|
| <b>Tipo de desarrollo</b>    | Interno y personalizado                                       | Externo y contratado  | SaaS (tercerizado en la nube)                         |
| <b>Metodología de riesgo</b> | MAGERIT v3 + ISO/IEC 27002                                    | NIA, ISO/IEC 27001, NIST  | NIST RMF, COBIT 2019, ISO 31000                       |
| <b>Evaluación de madurez</b> | Cálculo automatizado de madurez organizacional basado en DIC, | Evaluación profesional puntual realizada por consultores externos | Indicadores de madurez predefinidos por la plataforma |



|  |   |   |  |
|--|---|---|--|
|  | cobertura de elementos evaluados y referencia a ISO/IEC 27002   |   |  |
| <b>Uso de inteligencia artificial</b>    | Inteligencia artificial local aplicada a la evaluación de DIC, amenazas, niveles de riesgo y recomendaciones        | No aplica                               | Inteligencia artificial propietaria limitada a las capacidades del proveedor |
| <b>Visualización de datos</b>            | Dashboards interactivos con indicadores clave, matrices de riesgo y análisis comparativo                            | Informe técnico en formato PDF          | Dashboards integrados propios de la plataforma                               |
| <b>Automatización de reportes</b>        | Generación automática de datasets y reportes visuales   | No contempla automatización             | Automatización nativa incluida en la plataforma                              |
| <b>Control del proceso</b>               | Alto, gestionado y administrado por el equipo interno   | Bajo, dependencia total del proveedor   | Medio, configuración inicial interna y dependencia posterior del proveedor   |
| <b>Escalabilidad y adaptabilidad</b>     | Alta, adaptable a nuevas áreas, elementos evaluados o instituciones   | Limitada al alcance contractual         | Alta, bajo un modelo cerrado y dependiente del proveedor                     |
| <b>Integración con otras tecnologías</b> | Herramientas ofimáticas, dashboards interactivos e IA local, con posibilidad de integración futura mediante scripts | No contempla integraciones adicionales  | Integración mediante APIs según el proveedor                                 |
| <b>Dependencia tecnológica</b>           | Baja, sin licencias propietarias y ejecución local  | Alta, dependencia del proveedor externo | Alta, dependencia de licenciamiento y plataforma SaaS                        |



|                       |   |   |   |
|-----------------------|---|---|---|
| <b>Costo estimado</b> | Bajo a medio, asociado al tiempo de desarrollo y uso de herramientas abiertas | Alto, por costos de consultoría especializada | Medio a alto, por licencias recurrentes |
|-----------------------|---|---|---|

Se seleccionó la solución 1, ya que, fue la más equilibrada entre autonomía técnica, viabilidad institucional y valor académico, esta solución permite a la institución de educación superior diseñar y aplicar una evaluación de riesgos adaptada a su contexto real, basada en la metodología Magerit v3, apoyada por inteligencia artificial ejecutada de forma local y presentada mediante dashboard interactivos, la propuesta se alinea con estándares internacionales de seguridad de la información, fortalece capacidades internas, es replicable y escalable a futuro, no depende de proveedores externos ni de licencias propietarias, lo que la convierte en una opción sostenible y adecuada para el entorno institucional.

### **3. Alcance**

#### **3.1. Alcance de la solución seleccionada**

El alcance del proyecto es implementar un sistema para la evaluación y gestión de riesgos en ciberseguridad, se enfoca en los activos tecnológicos críticos de una institución de educación superior. La solución se fundamenta en la metodología de Magerit v3 y se apoya en los controles de las normas ISO/IEC 27002, así permite identificar, analizar y priorizar riesgos de seguridad de la información de manera estructurada y alineada a estándares internacionales.

Nuestro sistema contempla la gestión e inventario de activos, seguido de un cuestionario de Magerit de 21 preguntas y la incorporación de la inteligencia artificial esto permite generar valoraciones de disponibilidad, integridad y confidencialidad, se identifica las amenazas relevantes, estimar riesgos, proponer controles de seguridad, tanto a nivel grupal como individual de los activos evaluados, incluye el cálculo del nivel de madurez organizacional en la gestión de riesgos, expresado mediante un puntaje cuantitativo.



La solución implementada será evaluada para medir su efectividad mediante pruebas funcionales y escenarios de evaluación de riesgos, aplicados sobre la infraestructura tecnológica de la institución de educación superior, y también a futuro sobre los elementos que se vayan incorporando al sistema de forma manual. Este proceso permitirá validar la correcta ejecución del inventario, la aplicación del cuestionario Magerit, la evaluación automatizada con inteligencia artificial y la generación de resultados consolidados.

## **4. Objetivos**

### **4.1. Objetivo General**

Implementar un sistema institucional para la evaluación y gestión de riesgos de ciberseguridad, basado en la metodología de Magerit v3 y los controles de la norma ISO/IEC 27002, incorporando inteligencia artificial ejecutada de forma local para la evaluación automatizada, con el fin de apoyar la toma de decisiones en seguridad de la información.

### **4.2. Objetivos Específicos**

1. Analizar la infraestructura tecnológica crítica de la institución de educación superior, aplicando la metodología Magerit v3 para la evaluación de riesgos asociados a la seguridad de la información.
2. Implementar un sistema de evaluación de riesgos que integre inteligencia artificial ejecutada de forma local para la valoración de Disponibilidad, Integridad y Confidencialidad, la identificación de amenazas y la recomendación de controles alineados a ISO/IEC 27002.
3. Evaluar los resultados obtenidos mediante pruebas funcionales y escenarios controlados de evaluación de riesgos, generando resultados consolidados y métricas de madurez organizacional presentadas a través de dashboards interactivos que faciliten el análisis, seguimiento y priorización.



## 5. Planificación y costos del proyecto

### 5.1. Planificación del proyecto

La planificación del proyecto se estructuró en fases secuenciales, considerando el desarrollo de un sistema institucional para la evaluación y gestión de riesgos en ciberseguridad, en una primera etapa se realizó la identificación de la infraestructura tecnológica crítica y un análisis preliminar de impacto, lo que permitió comprender el entorno sobre el cual se aplicaría la metodología Magerit v3.

Se diseñó el modelo de evaluación de riesgos y se desarrolló el sistema de inventario y análisis, incorporando inteligencia artificial ejecutada de forma local para la valoración de disponibilidad, integridad y confidencialidad, la identificación de amenazas y la estimación de riesgos, una vez implementada la solución, se llevaron a cabo pruebas finales y escenarios de evaluación para verificar su correcto funcionamiento.

Finalmente, se realizó la carga y validación de información, la evaluación de resultados obtenidos y la presentación de estos mediante dashboards interactivos, la planificación permitió mantener un control adecuado del avance del proyecto, asignando responsabilidades claras y asegurando el cumplimiento de los objetivos establecidos dentro del periodo académico definido. Estos detalles se presentan en la *Tabla 2*.

*Tabla 2: Planificación de fechas del proyecto*

| Fase / Actividad   | Inicio    | Fin       | Responsables                         |
|--|-----------|-----------|--------------------------------------|
| <b>Identificación de infraestructura tecnológica y análisis preliminar (BIA)</b> | 1/8/2025  | 22/8/2025 | Sebastián Villacís y Nicolás Alomoto |
| <b>Diseño del modelo de evaluación de riesgos (MAGERIT v3 e ISO/IEC 27002)</b>   | 23/8/2025 | 20/9/2025 | Sebastián Villacís y Nicolás Alomoto |



|   |            |            |                                      |
|---|------------|------------|--------------------------------------|
| <b>Desarrollo del sistema e inventario de elementos tecnológicos</b>              | 21/9/2025  | 12/10/2025 | Sebastián Villacís y Nicolás Alomoto |
| <b>Implementación de inteligencia artificial local para evaluación de riesgos</b> | 13/10/2025 | 17/11/2025 | Sebastián Villacís y Nicolás Alomoto |
| <b>Generación de la matriz de riesgos y estructuración de datos</b>               | 18/11/2025 | 2/12/2025  | Sebastián Villacís y Nicolás Alomoto |
| <b>Recolección y validación de información técnica</b>                            | 3/12/2025  | 24/12/2025 | Sebastián Villacís y Nicolás Alomoto |
| <b>Pruebas funcionales y verificación de resultados</b>                           | 25/12/2025 | 8/1/2026   | Sebastián Villacís y Nicolás Alomoto |
| <b>Visualización de resultados mediante dashboards interactivos</b>               | 9/1/2026   | 16/1/2026  | Sebastián Villacís y Nicolás Alomoto |
| <b>Evaluación final y análisis post- implementación</b>                           | 17/1/2026  | 24/1/2026  | Sebastián Villacís y Nicolás Alomoto |

## 5.2. Planificación costos

Como parte de la planificación del proyecto, se consideró el uso de herramientas de apoyo al desarrollo que permitan optimizar el tiempo de implementación y mejorar la calidad del código, se utilizó GitHub Copilot como herramienta de asistencia para el desarrollo del sistema, principalmente para la generación de fragmentos de código, validación de estructuradas y apoyo en tareas repetitivas de programación.

El uso de GitHub Copilot se realizó bajo un esquema de suscripción individual, orientado exclusivamente a actividades académicas y de desarrollo, sin que ello represente dependencia tecnológica para la operación final del sistema. Esta herramienta fue empleada únicamente en la fase de desarrollo, por lo que no constituye un costo operativo recurrente para la institución, para más detalles se presentan en la *Tabla 3*



Tabla 3: Costos del software

| Python   | Desarrollo del sistema        | Gratis                             |
|--|-------------------------------|------------------------------------|
| Ollama + Llama 3                               | Inteligencia artificial local | Gratis                             |
| Github Copilot                                 | Para desarrollar el programa  | \$10                               |
| Microsoft Excel                                | Gestión de datos              | Incluido en licencia institucional |
| Herramientas de diagramación (draw.io / Canva) | Diagramas                     | Gratis                             |

Los costos del proyecto se mantienen controlados y acordes al entorno académico, priorizando herramientas accesibles y de apoyo al desarrollo, sin requerir licencias propietarias para la ejecución, uso o mantenimiento de la solución implementada.

El detalle de los costos asociados a herramientas de apoyo al desarrollo se incluye en el *anexo 4 – Planificación de costos*.

## 6. Desarrollo del proyecto

### 6.1. Diseño de la solución

El diseño de la solución está con un enfoque estructurado y secuencial para la evaluación y gestión de riesgos en ciberseguridad institucional, integrando metodologías formales de análisis de riesgos, inteligencia artificial ejecutada de forma local y herramientas de visualización de datos, este diseño permite asegurar trazabilidad, estandarización del análisis y apoyo efectivo a la toma de decisiones.

Como se observa en la *Ilustración 1*, la solución se organiza en fases claramente definidas, iniciando desde la identificación de los activos tecnológicos críticos hasta la visualización de resultados mediante dashboards interactivos, este flujo garantiza que la información sea procesada de forma coherente, alineada a la metodología de Magerit y a los controles de la norma ISO/IEC 27002.

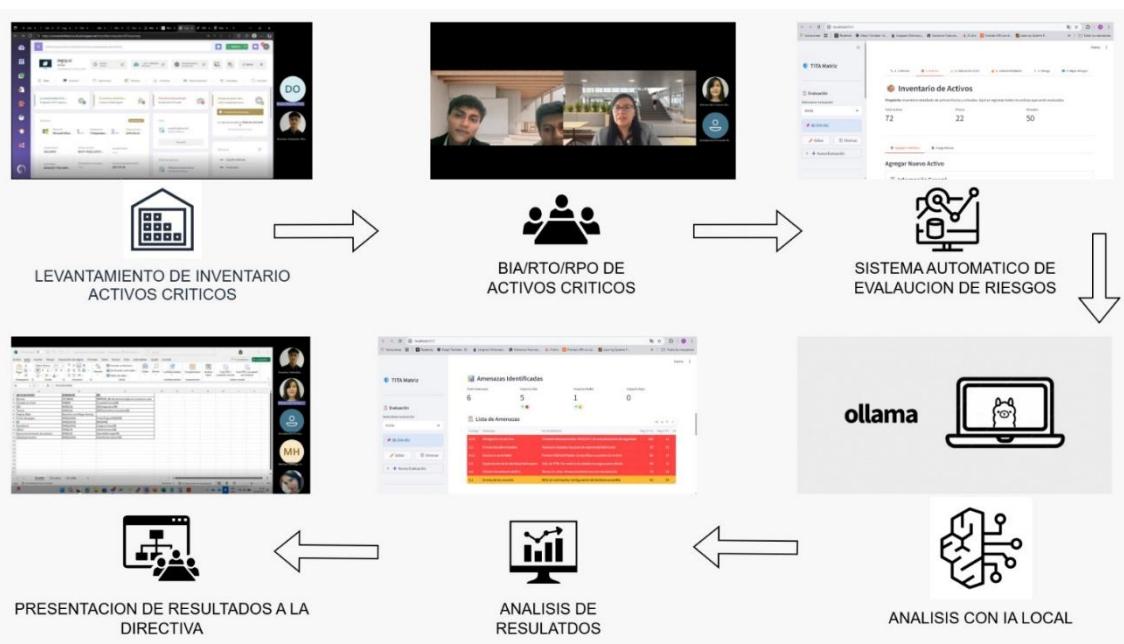


Ilustración 1: Diagrama de implementación

- **Identificación de activos críticos**

La primera fase del diseño corresponde a la identificación y clasificación de los activos tecnológicos que forman parte del entorno institucional. En esta etapa se consideran activos como servidores físicos y virtuales e infraestructura de red los cuales son esenciales para el funcionamiento de los procesos académicos y administrativos.

Para más detalle ir al *anexo 5 y 6*

- **Recolección de información mediante cuestionario MAGERIT**

Una vez identificados los activos, el diseño contempla la recolección de información a través de un cuestionario estructurado basado en la metodología de Magerit v3, este cuestionario este compuesto por 21 preguntas orientadas a evaluar aspectos relacionados con la disponibilidad, integridad y confidencialidad.

La información recopilada constituye la base objetiva para la evaluación automatizada, permitiendo reducir la subjetividad del análisis y mantener criterios homogéneos entre distintos activos evaluados.



Para más detalle ir al [anexo 7 y 8](#)

- **Evaluación automatizada de riesgos con inteligencia artificial**

En la siguiente fase, el diseño integra un componente de inteligencia artificial ejecutando de forma local mediante modelos de lenguaje de gran tamaño. La inteligencia artificial analiza el contexto de cada activo junto con las respuestas del cuestionario de Magerit, permitiendo generar valoraciones automáticas de disponibilidad, integridad y disponibilidad y así estima los niveles de riesgo.

Esto nos permite estandarizar el proceso de evaluación, optimizar los tiempos de análisis y mejorar la consistencia de los resultados, manteniendo la ejecución local de la IA para preservar la confidencialidad de la información institucional.

Para más detalle ir al [anexo 9 y 10](#)

- **Sistema automático de evaluación de riesgos.**

Con los resultados generados por la evaluación automatizada, el diseño contempla la construcción de un sistema automático de riesgos conforme a los lineamientos de la metodología Magerit. En este sistema se consolidan los valores de impacto, probabilidad y nivel de riesgo, permitiendo clasificar y priorizar los riesgos según su criticidad.

El sistema automático constituye el núcleo del análisis, ya que facilita la identificación de amenazas críticas, y la definición de tratamientos de riesgos adecuados.

Para más detalle ir al [anexo 11 y 12](#)

- **Visualización y análisis de resultados en Dashboards Interactivos**

El diseño de la solución incorpora dashboards interactivos como la capa de visualización y análisis de resultados, los datos obtenidos de la matriz de riesgos son estructurados en datasets que permiten la creación de dashboards interactivos con indicadores clave, matrices de riesgos, métricas de madurez organizacional y análisis comparativos.



Esta visualización facilita la comprensión de la información tanto a nivel técnico como directivo, apoyando la toma de decisiones en materia de ciberseguridad.

Para más detalle ir al [anexo 13, 14 y 15](#)

- **Apoyo a la toma de decisiones y mejora continua**

Finalmente, el diseño de la solución contempla el uso de los resultados obtenidos como insumo para la toma de decisiones estratégicas y la mejora continua en la gestión de riesgos, la información visualizada permite priorizar riesgos, definir acciones de mitigación y realizar evaluaciones periódicas que reflejen la evolución del nivel de riesgo y madurez institucional.

En conjunto, este diseño garantiza un proceso integral, trazable y alineado a estándares internacionales, integrando inteligencia artificial y visualización de datos.

## **6.2. Desarrollo de la solución**

El desarrollo de la solución se ejecutó siguiendo un flujo alineado a Magerit v3, iniciando con la consolidación del inventario, continuando con la recolección de información mediante un cuestionario estructurado y finalizado con la evaluación automatizada mediante inteligencia artificial local. Los resultados se consolidan en una matriz de riesgos y se presentan a través de dashboards interactivos, permitiendo interpretar el estado de riesgo y el nivel de madurez organizacional.

Para más detalle ir al [anexo 16](#)

### **6.2.1 Identificación de activos críticos**

En esta fase se realizó la identificación y clasificación de la infraestructura tecnológica crítica de la institución registrando información relevante como:

- tipo de elemento
- ubicación
- dependencia operacional
- rol dentro de los procesos institucionales.



El inventario establece el punto de partida del análisis, nos permite delimitar el alcance y asegurar que la evaluación se concentre en los componentes con mayor impacto sobre la operación académica y administrativa.

The screenshot shows a two-panel interface. On the left, a form titled 'Nuevo Evaluación' (New Evaluation) is displayed with fields for 'Nombre' (Name), 'Descripción' (Description), and 'Responsable' (Responsible). A dropdown menu labeled 'Filtro de Activo' (Active Filter) is open, showing a list of assets: 'Todos los activos' (All assets) selected, followed by 'BASTION\_PROD', 'OCADP01', 'OCBEP01', 'OCDBEIS01', 'OCEIS01', and 'OCEIS01\_02'. Below this is a table with columns 'Vulnerab.' (Vulnerable) and 'Urgentes' (Urgent). On the right, a 'Resumen' (Summary) panel displays statistics: 'Activos' (Assets) 72, 'Valorados' (Assessed) 21%, 'Vulnerab.' (Vulnerable) 0, 'Urgentes' (Urgent) 0. There are also 'Exportar' (Export) and 'Descargar Excel' (Download Excel) buttons.

Ilustración 2: Formulario de registro de activos nuevos.

Además, el inventario constituye la fuente de entrada para las fases posteriores, ya que cada registro se vincula con el cuestionario Magerit, la evaluación automatizada y la consolidación de resultados. Para más detalles del inventario ir al *anexo 17, 18, 19 y 20*. Adicionalmente, el sistema permite la importación masiva del inventario mediante archivos en formato JSON, facilitando la carga y actualización de la información para más detalle ir al *anexo 21, 22*

### Criterios de Valoración ea

Propósito: Define las escalas de medición para todo el modelo MAGERIT. Estas escalas son la referencia para valorar activos, degradación y frecuencia.

#### Disponibilidad (D)

| Nivel | Valor | Descripción   |
|-------|-------|---|
| Nula  | 0     | Inaccesibilidad no afecta actividad normal            |
| Baja  | 1     | Inaccesibilidad de 1 semana ocasiona perjuicio menor  |
| Media | 2     | Inaccesibilidad de 1 jornada impide actividades       |
| Alta  | 3     | Inaccesibilidad de 1 hora impide actividades críticas |

#### Confidencialidad (C)

| Nivel | Valor | Descripción  |
|-------|-------|--|
| Nula  | 0     | Cualquier persona dentro o fuera de la empresa         |
| Baja  | 1     | Todos los empleados de la empresa                      |
| Media | 2     | Solo quienes necesitan para su trabajo                 |
| Alta  | 3     | Solo grupo muy reducido, divulgación = perjuicio grave |

#### Integridad (I)

| Nivel | Valor | Descripción  |
|-------|-------|--|
| Nula  | 0     | Modificación reparable fácilmente, sin afectación        |
| Baja  | 1     | Modificación reparable, perjuicio menor                  |
| Media | 2     | Modificación difícil de reparar, perjuicio significativo |
| Alta  | 3     | Modificación no autorizada no puede repararse            |

#### Criticidad

| Nivel | Valor | Criterio               |
|-------|-------|------------------------|
| Nula  | 0     | Si todos D, I, C son 0 |
| Baja  | 1     | Si MAX(D,I,C) = 1      |
| Media | 2     | Si MAX(D,I,C) = 2      |
| Alta  | 3     | Si MAX(D,I,C) = 3      |

Ilustración 3: Valoración de Disponibilidad, Integridad y Confidencialidad (DIC)



La *ilustración 3* muestra el proceso de asignación de valores a las dimensiones de Disponibilidad, Integridad y Confidencialidad para cada activo, esta valoración nos permite cuantificar el impacto potencial ante la materialización de amenazas. Para más detalles

#### Fórmulas del Modelo

##### Fórmulas de Cálculo:

1. CRITICIDAD = MAX(D, I, C)
2. IMPACTO = CRITICIDAD × MAX(Deg\_D, Deg\_I, Deg\_C)
3. RIESGO = FRECUENCIA × IMPACTO
4. RIESGO\_ACTIVO = PROMEDIO(todos los riesgos)
5. OBJETIVO = RIESGO\_ACTUAL × 0.5

##### Constantes Organizacionales:

- Límite de Riesgo: 7.0
- Factor de Reducción: 50%

##### Regla de Decisión:

- Si RIESGO > LÍMITE → Tratamiento Urgente 
- Si RIESGO ≤ LÍMITE → Aceptable 

*Ilustración 4: fórmulas del modelo.*

La *ilustración 4* muestra el modelo de cálculo utilizado por el sistema para la evaluación de riesgos de Ciberseguridad, baso en los principios de la metodología de Magerit v3. En este modelo, la criticidad del activo se determina a partir del valor máximo entre la Disponibilidad, Integridad y Confidencialidad.

### **6.2.2 Evaluación automatizada de riesgos con inteligencia artificial local**

En esta fase se integra la inteligencia artificial ejecutada de forma local como apoyo a los procesos de evaluación. El modelo analiza las respuestas del cuestionario de Magerit junto con el contexto registrado en el inventario, generando valoraciones automáticas de disponibilidad, integridad y confidencialidad, identificando amenazas relevantes y estimados niveles de riesgo inherente y residual.

La inteligencia artificial funciona como un asistente para estandarizar resultados y acelerar el análisis, traduciendo criterios cualitativos en salidas cuantificables sin reemplazar el criterio del analista, esto permite mejorar la consistencia entre evaluaciones y mantener trazabilidad del proceso en entornos con múltiples elementos tecnológicos.



### 6.2.3 Análisis de amenazas y vulnerabilidades

Una vez consolidado el inventario, se realizó el análisis de amenazas y vulnerabilidades conforme a los lineamientos de Magerit. En esta etapa se consideraron amenazas controles ISO27002, salvaguardas y vulnerabilidades que podrían facilitar la materialización de eventos de seguridad. Para más detalles ir al *anexo 23*.

Dentro del análisis se contemplaron escenarios como fallos de hardware, interrupciones del servicio, accesos no autorizados, errores humanos. Nos permitió contextualizar los riesgos antes de su cuantificación, asegurando que la evaluación posterior se basa en condiciones reales del entorno institucional. Para conocer las fórmulas que utiliza la IA ir al *anexo 30*.

#### ⚠ Catálogo de Amenazas

52 amenazas clasificadas en 5 categorías:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Filtrar por tipo de amenaza:

| Total Amenazas | Naturales           | Errores                           | Ataques             |
|----------------|---------------------|-----------------------------------|---------------------|
| 52             | 3                   | 17                                | 21                  |
| <hr/>          |                     |                                   |                     |
| Código         | Amenaza             | Descripción                       | Tipo                |
| N.1            | Fuego               | Incendio natural o provocado      | Desastres Naturales |
| N.2            | Daños por agua      | Inundación, humedad, filtración   | Desastres Naturales |
| N.*            | Desastres naturales | Terremoto, tornado, huracán, etc. | Desastres Naturales |

*Ilustración 5: Catálogo de amenazas.*

El catálogo de amenazas se utiliza como base para asociar cada activo crítico con las amenazas que le resultan aplicables. La funcionalidad del filtrado facilita el análisis por tipo de amenaza y permite visualizar su distribución. Como se puede ver en la *ilustración 5*. Para conocer las amenazas identificadas ir al *anexo 32*.



## Catálogo de Controles ISO 27002:2022

93 controles organizados en 4 dominios:

- 5.x Controles Organizacionales (37 controles)
- 6.x Controles de Personas (8 controles)
- 7.x Controles Físicos (14 controles)
- 8.x Controles Tecnológicos (34 controles)

Filtrar por dominio:

| Total Controles | Organizacionales | Físicos | Tecnológicos |
|-----------------|------------------|---------|--------------|
| 93              | 37               | 14      | 34           |

| Código | Control                                  | Categoría      | Dominio          |
|--------|--|----------------|------------------|
| 5.1    | Políticas de seguridad de la información | Organizacional | Organizacionales |
| 5.2    | Roles y responsabilidades de seguridad   | Organizacional | Organizacionales |

Ilustración 6: Catálogo de CONTROLES ISO27002

Como se observa en la *ilustración 6* el catálogo de los controles se integra como apoyo al proceso de tratamiento del riesgo, esto permite asociar controles específicos a los activos evaluados. Esta integración facilita el análisis del estado de implementación de las salvaguardas.

## Catálogo de Salvaguardas

Las salvaguardas son medidas de protección para reducir el riesgo. Están organizadas por tipo de activo a proteger.

Total Salvaguardas

85

- > [H] Protecciones Generales (5 salvaguardas)
- > [D] Protección de los Datos/Información (6 salvaguardas)
- > [S] Protección de los Servicios (5 salvaguardas)
- > [SW] Protección de las Aplicaciones (Software) (7 salvaguardas)
- > [HW] Protección de los Equipos (Hardware) (6 salvaguardas)
- > [COM] Protección de las Comunicaciones (7 salvaguardas)

Ilustración 7: Catálogo de Salvaguardas.

En la *ilustración 7* se puede observar el catálogo de salvaguardas reúne las medidas de protección definidas para reducir los riesgos identificados durante la evaluación Magerit v3, se encuentran organizadas por tipo de activo a proteger, lo que permite seleccionar controles adecuados según la naturaleza del riesgo y del activo. Este catálogo se utilizó para el tratamiento del riesgo, permite asociar salvaguardas específicas a las amenazas.



## Catálogo de Vulnerabilidades por Tipo de Activo

Las vulnerabilidades son debilidades que pueden ser explotadas por las amenazas. Este catálogo muestra las vulnerabilidades más comunes para cada tipo de activo según MAGERIT.

| Total Vulnerabilidades | Altas | Medias |
|------------------------|-------|--------|
| 55                     | 36    | 17     |

Filtrar por nivel de riesgo:

Alto x Medio x Bajo x Nulo x

Filtrar por tipo de activo:

Software / A... x Hardware / E... x  
Comunicacio... x Datos / Infor... x  
Servicios x Personal x  
Instalaciones x Servicios Au... x

Buscar vulnerabilidad:

Buscar por código, nombre o descripción

Ilustración 8: Catálogo de vulnerabilidades por tipo de activo.

En la *ilustración 8* nos permite identificar de forma estructurada las vulnerabilidades aplicables a cada activo del inventario, sirviendo como insumo para el cálculo del riesgo inherente y para la posterior definición de salvaguardas y controles de mitigación.

### Matriz de Vulnerabilidades por Tipo de Activo

| Tipo                    | Altas | Medias | Bajas | Nulas | Total |
|-------------------------|-------|--------|-------|-------|-------|
| Software / Aplicaciones | 9     | 1      | 0     | 0     | 10    |
| Hardware / Equipos      | 3     | 3      | 1     | 0     | 7     |
| Comunicaciones / Red    | 6     | 2      | 0     | 0     | 8     |
| Datos / Información     | 4     | 3      | 0     | 0     | 7     |
| Servicios               | 3     | 3      | 0     | 0     | 6     |
| Personal                | 5     | 1      | 0     | 0     | 6     |
| Instalaciones           | 4     | 2      | 0     | 0     | 6     |
| Servicios Auxiliares    | 2     | 2      | 1     | 0     | 5     |

Ilustración 9: Matriz de vulnerabilidades por tipo de activo.

En la *ilustración 9*, la matriz permite identificar qué tipos de activos concentran un mayor número de vulnerabilidades críticas, priorizando las acciones de tratamiento y la toma de decisiones enfocadas en los componentes con mayor campo institucional.



#### 6.2.4 Recolección de información mediante cuestionario MAGERIT

Para obtener información homogénea y comparable, entre todos los activos evaluados, el sistema incorpora un cuestionario basado en la metodología de Magerit v3, compuesto por 21 preguntas orientadas a recolectar datos relaciones con la Disponibilidad, Integridad y Confidencialidad. El cuestionario considera:

- aspectos de respaldo
- redundancia
- control de accesos
- dependencias operativas.

Esta fase es clave dentro del proceso, ya que estandariza el levantamiento de información y garantiza que la evaluación automatizada procese entradas consistentes y comparables para todos los activos analizados.

#### Identificación y Valoración

Propósito: Valorar cada activo en las dimensiones D (Disponibilidad), I (Integridad), C (Confidencialidad) mediante cuestionario guiado por tipo de activo.

Metodología: Cada tipo de activo tiene preguntas específicas. Las respuestas determinan el nivel (N/B/M/A).

Fórmula:  $\text{CRITICIDAD} = \text{MAX}(\text{Valor\_D}, \text{Valor\_I}, \text{Valor\_C})$

⚠ Importante: Cada activo solo puede ser valorado una vez. La valoración D/I/C es la base de toda la evaluación de riesgos.

The screenshot shows a user interface for asset valuation. At the top, there are two tabs: 'Cuestionario D/I/C' (selected) and 'Resumen Valoraciones'. Below the tabs, a button labeled 'Seleccionar Activo para Valorar' is visible. A dropdown menu is open, showing the option 'SNAPI01 (Servidor Virtual)'. The background of the interface is white, and the text is in a standard black font.

Ilustración 10: Selección del activo a evaluar.

Como se puede observar en la *ilustración 10*, la interfaz permite seleccionar el activo sobre el cual se aplicará el cuestionario de Magerit. Sirve como punto de inicio del proceso de recolección de información, así se puede asegurar la trazabilidad entre el activo, sus respuestas y los resultados de riesgo generados posteriormente.

Para seguir con el cuestionario se presentan las preguntas relacionadas con la dimensión de Disponibilidad, Integridad y Confidencialidad, el sistema incorpora un conjunto estructurado de preguntas basado en la metodología Magerit v3. Estas preguntas permiten evaluar aspectos como la criticidad del servicio, la



tolerancia a interrupciones, los mecanismos de control y validación de la información, así como los controles de accesos asociados a cada activo. La información obtenida constituye la base para la valoración del impacto. Para mayor detalle ir al *anexo 24, 25 y 26*.



### ¿Cuál es el tiempo máximo aceptable de recuperación?

RTO define cuánto tiempo puede estar inoperativo el activo antes de causar impacto inaceptable.

1. ¿Cuál es el tiempo máximo aceptable para restaurar esta VM?

- (3) Menos de 1 hora
- (2) Entre 1 y 4 horas
- (1) Entre 4 y 24 horas
- (0) Más de 24 horas

2. ¿Existe una réplica de esta VM en otro sitio (DR)?

- (3) No hay réplica en DR
- (2) Réplica manual periódica
- (1) Réplica automatizada (Zerto, SRM, ASR)
- (0) Active-Active en múltiples sitios

*Ilustración 11: Preguntas RTO*

En la *ilustración 11* muestra el formulario utilizado para la recolección del RTO, se implementó como parte del cuestionario Magerit, permitiendo asignar valores ponderados según el tiempo de recuperación seleccionado, dichos valores se integran directamente en el cálculo del impacto del activo.



### ¿Cuánta pérdida de datos es aceptable?

RPO define cuántos datos (en tiempo) se pueden perder sin causar impacto inaceptable.

1. ¿Cuánta pérdida de datos es aceptable para esta VM?

- (3) Cero - Replicación síncrona requerida
- (2) Hasta 1 hora de datos
- (1) Hasta 4 horas de datos
- (0) Hasta 24 horas de datos

2. ¿Cuál es la frecuencia de respaldos/snapshots de esta VM?

- (3) Sin respaldos automáticos
- (2) Respaldo diario
- (1) Respaldo cada hora
- (0) Replicación continua (CDP)

*Ilustración 12: Preguntas RPO*



En la *ilustración 12* se presenta el módulo de evaluacion del RPO, para determinar la cantidad máxima de pérdida de datos aceptable ante un incidente, fue incorporado como criterio adicional de evaluación, cuyos valores determinan el análisis de integridad y disponibilidad.

Disponibilidad (D)    Integridad (I)    Confidencialidad (C)    RTO    RPO    BIA

¿Cuál es el impacto al negocio si este activo falla?

BIA analiza el impacto financiero, operacional y reputacional en caso de falla.

1. ¿Qué procesos de negocio dependen de esta VM?  
 (3) Procesos core del negocio  
 (2) Procesos importantes  
 (1) Procesos de soporte  
 (0) Procesos no críticos
2. ¿Cuál es el impacto financiero estimado por hora de inactividad?  
 (3) Más de \$10,000/hora  
 (2) Entre 1,000 y 10,000/hora  
 (1) Entre 100 y 1,000/hora  
 (0) Menos de \$100/hora

*Ilustración 13: Preguntas BIA*

En la *ilustración 13* está el módulo de BIA, en el cual se evalúa el impacto operativo, financiero y reputacional que tendría la falla del activo, se integró como un componente clave para observar el impacto real de los activos dentro de la organización. Además, dentro del sistema de evaluacion de riesgos se puede visualizar las respuestas de los cuestionarios, para más detalles ir al *anexo 27*.

Vista Previa del Cálculo

Valoración D/I/C:

|   |   |   |   |
|---|---|---|---|
| <input checked="" type="radio"/> Disponibilidad | <input checked="" type="radio"/> Integridad | <input checked="" type="radio"/> Confidencialidad | <input checked="" type="radio"/> CRITICIDAD |
| 3 (A)   | 3 (A)                                       | 3 (A)   | 3 (Alta)                                    |

Continuidad del Negocio (RTO/RPO/BIA):

|                                      |                                      |  |
|--------------------------------------|--------------------------------------|--|
| <input checked="" type="radio"/> RTO | <input checked="" type="radio"/> RPO | <input checked="" type="radio"/> Impacto BIA |
| < 1 hora                             | 0 (cero pérdida)                     | Alto   |
| ↑ Alto                               | ↑ Alto                               | ↑ Nivel 3                                    |

Guardar Valoración

*Ilustración 14: Vista previa del cálculo de la valoración*



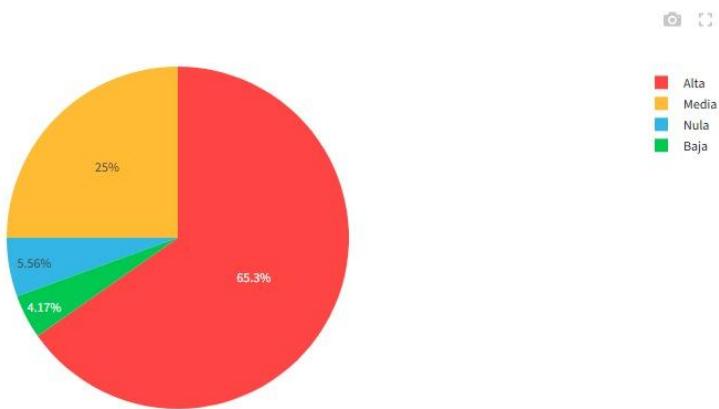
En la *ilustración 14* se muestra que el activo evaluado presenta valores altos en las tres dimensiones de seguridad. Esto indica que el activo es crítico para la institución, ya que una falla afectaría de forma directa la operación, la confiabilidad de la información y la protección de datos. Adicionalmente, los valores de RTO menor a 1 hora, RPO igual a cero y BIA alto, esto evidencia que el activo no tolera tiempos prolongados de indisponibilidad ni perdida de información y que su interrupción tendría un impacto significativo en los procesos institucionales.



*Ilustración 15: Valoraciones DIC*

En la *ilustración 15*, se confirma que la valoración DIC del activo ha sido registrada correctamente, los valores altos en la Disponibilidad, Integridad y Confidencialidad indican que cualquier amenaza que afecte a ese activo se incrementará significativamente el nivel de riesgo. Y se puede observar el resumen general del estado de valoración de los activos registrados en el sistema para más detalles ir al *anexo 28*.

Distribución de Criticidad



*Ilustración 16: Distribución de criticidad.*

Como se puede ver en el grafico de la *ilustración 16*, muestra la distribución porcentual de los activos según su nivel de criticidad (Alta, Media, Baja y Nula), partiendo de las valoraciones del DIC, la alta concentración de activos en niveles de criticidad alta evidencia una exposición relevante al riesgo dentro de la institución de educación superior, este resultado justifica la necesidad de aplicar controles de seguridad alineados con la ISO/IEC 27002. Para visualizar la tabla de valoraciones ir al *anexo 29 y 30*.

#### **6.2.5 Evaluación de riesgo automatizada con inteligencia artificial local**

En esta fase se integra evaluación automatizada de riesgos a partir de la relación activo amenaza previamente definida. El sistema procesa de forma estructurada las valoraciones de Disponibilidad, Integridad y Confidencialidad, junto con los niveles de frecuencia asociados a cada amenaza, generando de manera automática los valores de riesgo por cada par activo-amenaza identificado.

La inteligencia artificial ejecutada de forma local actúa como un mecanismo de apoyo al análisis, permitiendo estandarizar el cálculo, consolidar grandes volúmenes de información y reducir inconsistencias entre evaluaciones, sin sustituir el criterio del analista.



1. Criterios    2. Activos    3. Valoración D/I/C    4. Vulnerabilidades    5. Riesgo    6. Mapa Riesgos    7. Riesgo Activos    8. Salvaguardas    9. Madurez    10. Cor.

## ⚡ Cálculo de Riesgo

Propósito: Calcular el riesgo para cada par activo-amenaza identificado.

Fórmula MAGERIT: RIESGO = FRECUENCIA × IMPACTO

⚠ Importante: El cálculo de riesgos se ejecuta una vez. Los resultados alimentan el mapa de riesgos, agregaciones y salvaguardas.

> Ver Escalas de Referencia MAGERIT

## -Calcular Riesgos

Riesgos Calculados: Se identificaron 409 riesgos en la evaluación. Los resultados alimentan el mapa de riesgos (Tab 6), agregación (Tab 7) y salvaguardas (Tab 8).

| Total Riesgos | Riesgo Alto | Riesgo Medio | Riesgo Bajo |
|---------------|-------------|--------------|-------------|
| 409           | 211         | 126          | 72          |

Ilustración 17: Cálculo automatizado de riesgos según MAGERIT v3.

La ilustración 17, muestra el proceso de cálculo automatizado de riesgos realizado por el sistema, donde se aplica la fórmula de Magerit (Riesgo = Probabilidad x Impacto), para cada combinación de activo-amenaza identificada. Se obtienen valores consolidados de riesgos clasificados en niveles alto, medio y bajo, si se necesita recalcular el riesgo se detalla en el anexo 34.

## Resumen de Riesgos

Pasa el mouse sobre la Amenaza para ver la descripción completa

| Activo       | Amenaza | Frecuencia | Impacto | Riesgo |
|--------------|---------|------------|---------|--------|
| BASTION_PROD | A_24    | 3.00       | 3.00    | 9.00   |
| OCADP01      | A_24    | 3.00       | 3.00    | 9.00   |
| OCBEP01      | A_24    | 3.00       | 3.00    | 9.00   |
| OCDBEIS01    | A_24    | 3.00       | 3.00    | 9.00   |
| OCDBEIS01    | A_24    | 3.00       | 3.00    | 9.00   |
| OCEIS01      | A_24    | 3.00       | 3.00    | 9.00   |
| OCEIS01_02   | A_24    | 3.00       | 3.00    | 9.00   |
| OCICOG01     | A_24    | 3.00       | 3.00    | 9.00   |
| OCJEB01      | A_24    | 3.00       | 3.00    | 9.00   |
| OCREG01      | A_24    | 3.00       | 3.00    | 9.00   |
| OCREG01_02   | A_24    | 3.00       | 3.00    | 9.00   |
| OCREG02      | A_24    | 3.00       | 3.00    | 9.00   |

## Estadísticas de Riesgo

| Total Riesgos | Altos (≥6) | Medios (4-6) | Promedio |
|---------------|------------|--------------|----------|
| 409           | 211        | 126          | 5.81     |

Ilustración 18: Resumen y distribución de riesgos de ciberseguridad.

En la ilustración 18 se presenta un resumen detallado de los riesgos calculados, incluyendo el total de riesgos identificados y su distribución por niveles de criticidad. La tabla permite analizar cada riesgo a nivel de activo y amenaza, mostrando los valores de frecuencia e impacto y el riesgo resultante.



### **6.2.6 Sistema automático de evaluación de riesgos**

Tomando como referencia las matrices y escalas definidas por la metodología MAGERIT v3, se desarrolló un sistema automatizado de evaluación de riesgos que permite calcular de forma estructurada el nivel de riesgo asociado a cada activo crítico. El sistema integra las valoraciones de impacto, frecuencia y criticidad obtenidas en fases previas, aplicando las reglas de cálculo establecidas por la metodología.

Este enfoque automatizado permite consolidar los resultados individuales de cada activo en una visión global del estado de riesgo institucional, facilitando la identificación de concentraciones de riesgo y la priorización de acciones de tratamiento. De esta manera, la matriz de riesgos deja de ser un elemento estático y se convierte en un resultado dinámico generado directamente por el sistema.

Para más detalles ir al [anexo 35](#).

### **6.2.7 Visualización de resultados mediante dashboards interactivos**

Los resultados generados por el sistema se estructuran en datasets para su consumo en dashboards interactivos. Esta capa visualización permite representar de forma clara indicadores clave, niveles de riesgo, comparativas, matrices de madurez organizacional.

El objetivo de esta fase es convertir resultados técnicos en información comprensible para análisis y seguimiento, facilitando la interpretación por perfiles técnicos y directivos.

Para más detalle ir al [anexo 36](#).

### **6.2.8 Apoyo a la toma de decisiones y mejora continua**

Finalmente, los resultados consolidados sirven como insumo para la toma de decisiones estratégicas en ciberseguridad. La priorización de riesgos, la identificación de componentes críticos y el análisis del nivel de madurez permiten orientar acciones futuras y realizar evaluaciones periódicas.



Este enfoque impulsa la mejora continua, ya que el sistema puede ser utilizado confirme cambie la infraestructura, se incorporen nuevos elementos o se requiera actualizar evaluaciones, fortaleciendo progresivamente la gestión de los riesgos institucionales.

## 6.2. Pruebas y evaluación de la solución

Las pruebas se realizaron para verificar el funcionamiento integral del sistema de evaluación de riesgos: creación de evaluaciones, carga/gestión de activos, ejecución de evaluación Magerit con IA local, construcción automática de la matriz de riesgos, cálculo de madurez y visualización en dashboards de Streamlit.

### Entorno y datos de prueba

- **Aplicación:** Streamlit (dashboard y módulos del sistema)
- **IA:** LLM local vía Ollama (no se envía datos a servicios externos)
- **Dataset:** Inventario cargado en formato JSON

#### 6.2.2. Creación y gestión de una evaluación

En esta fase se comprobó que el sistema permite crear una evaluación desde cero, registrarla y luego seleccionarla para gestionarla, se ingresó al módulo evaluaciones existentes y se verificó la lista. Se creó una nueva evaluación ingresando el nombre, responsable y descripción.

Ilustración 19: Evaluaciones existentes y creación de Nueva evaluación



La evaluacion queda registrada y disponible para seleccionarse y administrarse.

### 6.2.3. Carga/listado de activos y los evalúa

En este apartado se validó que los activos cargados se visualicen correctamente y quedan listos para ejecución de la evaluación, se cargó el inventario de activos en un archivo JSON. Se verifico el listado de activos con tu tipo y estado.

| Lista de Activos |                 |           |                            |                |           |  |
|------------------|-----------------|-----------|----------------------------|----------------|-----------|--|
| Nombre_Activo    | Tipo_Activo     | Ubicacion | Area_Responsable           | Finalidad_Uso  | Estado    |  |
| BASTION_PROD     | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCADP01          | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCBEP01          | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCDBEIS01        | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCES01           | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCES01_02        | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCJC001          | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCJDB01          | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCREG01          | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |
| OCREG01_02       | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |  |

Ilustración 20: Listado de activos

Los activos se listan sin errores, mantienen su tipo y se marcan como “listos”

### 6.2.4. Evaluación con IA

Se confirma que la evaluación se ejecuta sobre todos los activos, mostrando el progreso y finalización, también se seleccionó la evaluación activa y se evalúo todos los activos con Magerit, y se comprobó la finalización sin errores.

| Resumen de Valoraciones             |           |         |   |         |   |         |            |                  |            |           |                  |           |           |
|-------------------------------------|-----------|---------|---|---------|---|---------|------------|------------------|------------|-----------|------------------|-----------|-----------|
| Total Activos                       | Valorados |         |   |         |   |         | Pendientes |                  |            |           |                  |           |           |
| 75                                  | 7         |         |   |         |   |         |            |                  |            |           |                  |           | 68        |
| Nombre_Activo                       | D         | Valor_D | I | Valor_I | C | Valor_C | Criticidad | Criticidad_Nivel | RTO_Tiempo | RTO_Nivel | RPO_Tiempo       | RPO_Nivel | BIA_Nivel |
| Servidor Físico Dell PowerEdge R750 | A         | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) | Alto      | Alto      |
| BASTION_PROD                        | A         | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) | Alto      | Alto      |
| OCDBEIS01                           | M         | 2       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) | Alto      | Alto      |
| OCBEP01                             | M         | 2       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) | Alto      | Alto      |
| OCADP01                             | A         | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) | Alto      | Alto      |
| VM-DB-ORACLE-PROD-01                | B         | 1       | B | 1       | B | 1       | 1          | Baja             | 4-24 horas | Bajo      | 1-4 horas        | Bajo      | Bajo      |
| VM-WEB-NGINX-PROD-02                | B         | 1       | B | 1       | B | 1       | 1          | Baja             | 4-24 horas | Bajo      | 1-4 horas        | Bajo      | Medio     |

Ilustración 21: Valorar con IA (72 activos listos)

El proceso termina, no hay fallos y se genera salida evaluada por activo.



### 6.2.5. Vulnerabilidades y amenazas

Se valido que el sistema construye con relaciones activo-amenaza, valores disponibilidad, integridad, confidencialidad, probabilidad y riesgo. En la *ilustración 22* se presenta el catálogo de amenazas.

#### ⚠ Catálogo de Amenazas

52 amenazas clasificadas en 5 categorías:

- [N] Desastres naturales
- [I] De origen industrial
- [E] Errores y fallos no intencionados
- [A] Ataques intencionados

Filtrar por tipo de amenaza:



*Ilustración 22: Catálogo de amenazas.*

| Columna         | Descripción   |
|-----------------|---|
| Evaluación      | Identificador de la evaluación en la que se genera la matriz (ej. <i>Evaluación Activos Críticos 01</i> ).                    |
| ID Activo       | Código único asignado al activo dentro del sistema (ej. ACT-EVA-001-020).   |
| Activo          | Nombre del activo evaluado (servidor, base de datos, aplicación, etc.).   |
| Tipo de Activo  | Clasificación del activo (Servidor Físico, Servidor Virtual, Base de Datos, etc.).  |
| Código Amenaza  | Identificador de la amenaza según el catálogo MAGERIT (ej. A.6, E.2, A.11).   |
| Amenaza         | Descripción de la amenaza asociada al activo (acceso no autorizado, errores del administrador, denegación de servicio, etc.). |
| Tipo de Amenaza | Clasificación de la amenaza (Ataques Intencionados, Errores no Intencionados, Origen Industrial, Desastres Naturales).        |
| Dimensión       | Dimensión principal afectada (Disponibilidad, Integridad o Confidencialidad).   |
| D               | Valor asignado a la Disponibilidad del activo frente a la amenaza (escala 1–5).   |
| I               | Valor asignado a la Integridad del activo frente a la amenaza (escala 1–5).   |
| C               | Valor asignado a la Confidencialidad del activo frente a la amenaza (escala 1–5).   |
| Impacto         | Valor de impacto calculado en función de los criterios DIC.   |

| Probabilidad | Probabilidad estimada de ocurrencia de la amenaza (escala 1–5). |
|--------------|---|
|--------------|---|

Tabla 4: Relación activo-amenaza

La presenta *tabla 4* muestra la matriz de relación activo-amenaza conforme con la metodología de Magerit v3, donde cada fila representa la evaluación de una amenaza específica sobre un activo identificado. Se consolidan los valores de Disponibilidad, Integridad y Confidencialidad, junto con la estimación de impacto, probabilidad esto permite a la matriz analizar, comparar y priorizar los riesgos de seguridad de la información.

#### 6.2.6. Dashboards de riesgo en Streamlit

En esta etapa se va a comprobar que el dashboard muestra indicadores ejecutivos para análisis rápido y priorización. Se revisaron los KPIs (activos regulados, riesgo máximo, críticos/altos, riesgos residuales, promedio) y se validó el ranking de los activos más críticos.

##### Mapa Radar de Riesgos

Visualización comparativa de riesgo actual vs objetivo vs límite por activo

##### Comparativo de Riesgos por Activo

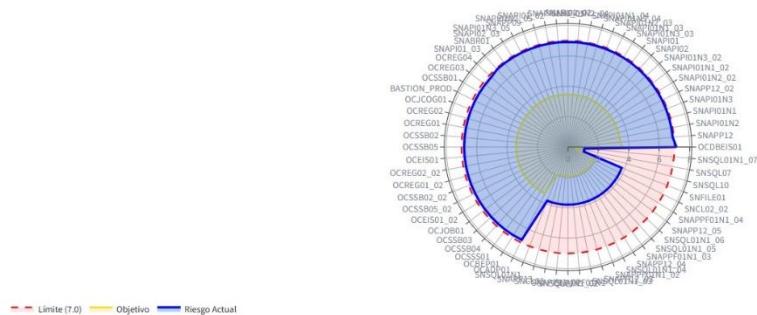


Ilustración 23: Mapa de radar.

Como se observa en la *ilustración 24*. EL mapa de radar muestra una visualización comparativa entre el riesgo actual, el riesgo objetivo y el límite organizacional para cada activo evaluado. Esta representación facilita identificar patrones y concentraciones de riesgo, evidenciando activos que se encuentran alejados del objetivo y requieren acciones prioritarias de mitigación. Para interpretar el mapa del radar ir al anexo

Gráfico Comparativo Riesgo Actual vs Objetivo vs Límite

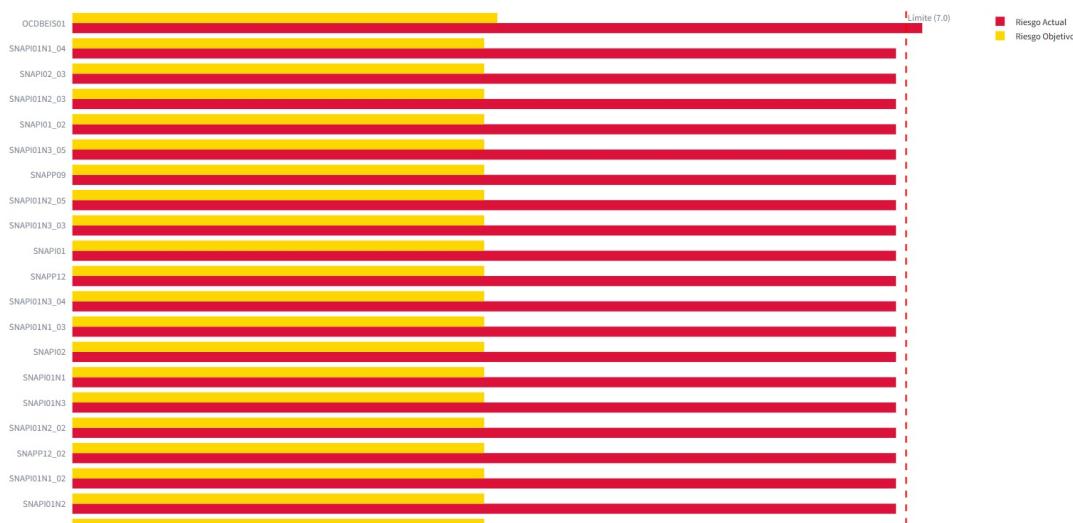


Ilustración 24: Gráfico comparativo.

Como se muestra en la ilustración 25, el grafico compara de manera individual el riesgo actual de cada activo frente al riesgo objetivo y el límite máximo permitido. La visualización permite priorizar acciones de tratamiento al identificar activos con mayores desviaciones respecto al objetivo de riesgo.

#### 6.2.7. Mapa de calor

Esta visualización permite identificar de forma inmediata las concentraciones de riesgo que requieren mayor atención, destacando los riesgos altos que demandan acciones inmediatas de tratamiento, facilita la priorización de controles y salvaguardas al mostrar qué combinaciones de impacto y probabilidad representan una mayor amenaza para la institución. La matriz funciona como un resumen visual del estado global del riesgo y como un

insumo fundamental para la toma de decisiones en la gestión de riesgos de ciberseguridad

#### Matriz de Riesgos (Probabilidad x Impacto)

Como en Excel: Las celdas muestran cuántos riesgos caen en cada zona.

Matriz de Riesgos - Impacto vs Frecuencia (Probabilidad)

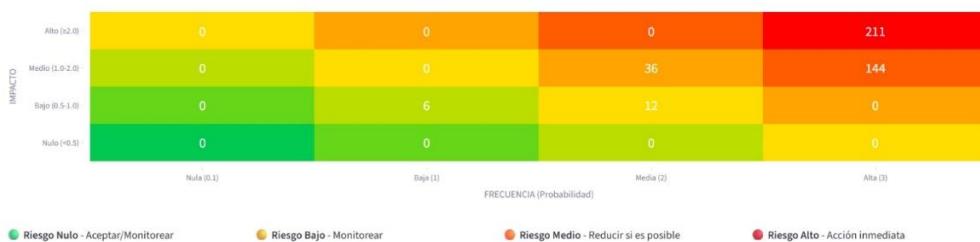


Ilustración 25: Mapa de calor

#### 6.2.8. Lista de riesgos

Esta vista permite analizar los riesgos de forma granular, facilitando la trazabilidad desde el activo afectado hasta la amenaza asociada. La información presentada constituye la base para las fases posteriores de agregación, priorización y definición de salvaguardas, además de permitir la exportación de los resultados para su análisis externo o documentación formal.

#### Lista de Riesgos

| ID  | Impacto | Frecuencia | Riesgo | Descripción   |
|-----|---------|------------|--------|---|
| R1  | 3.00    | 3.00       | 9.00   | Riesgo en 'BASTION_PROD' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado. |
| R2  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCADP01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.      |
| R3  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCBEF01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.      |
| R4  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCDBEIS01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.    |
| R5  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCDBEIS01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.    |
| R6  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCEIS01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.      |
| R7  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCEIS01_02' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.   |
| R8  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCJCOG01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.     |
| R9  | 3.00    | 3.00       | 9.00   | Riesgo en 'OCJOB01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.      |
| R10 | 3.00    | 3.00       | 9.00   | Riesgo en 'OCREG01' por amenaza A.24: Denegación de servicio. Vulnerabilidad: Firmware desactualizado.      |

Descargar Lista de Riesgos (CSV)

Guardar Mapa de Riesgos

Ilustración 26: Lista de riesgos.



### 6.2.9. Cálculo de nivel de madurez

En la *ilustración 27* presenta el módulo de evaluación del nivel de madurez de la gestión de riesgos de TI, basado en la completitud del análisis realizado y siguiendo un esquema progresivo de cinco niveles. El sistema define claramente los criterios de cada nivel, desde un estado inicial hasta uno optimizado, permitiendo contextualizar el grado de avance institucional en la gestión de riesgos.

Propósito: Evaluar el nivel de madurez de la gestión de riesgos de TI basado en la completitud de la evaluación.

Niveles de Madurez:

- Nivel 1 - Inicial (0-19%): Evaluación mínima, sin análisis completo
- Nivel 2 - Básico (20-39%): Evaluación parcial, análisis básico de riesgos
- Nivel 3 - Definido (40-59%): Evaluación completa, riesgos identificados y documentados
- Nivel 4 - Gestionado (60-79%): Evaluación detallada con salvaguardas definidas
- Nivel 5 - Optimizado (80-100%): Evaluación exhaustiva con análisis completo y controles recomendados

Este es el nivel de madurez ACTUAL (inherente) - SIN considerar salvaguardas implementadas.

La puntuación se basa en:

- 60% → Distribución de riesgos (% en zona BAJA vs ALTA)
- 40% → Severidad del riesgo máximo identificado

⚠️ Para ver el nivel de madurez CON los controles aplicados, ve al Tab 10 (Comparativa).

Calcular Nivel de Madurez Actual

*Ilustración 27: Niveles de madurez.*

La ilustración 28 muestra el resultado del cálculo automático del nivel de madurez actual, el cual se ubica en Nivel 1 – Inicial, con una puntuación de 6.6/100. Este resultado indica que, si bien los riesgos han sido identificados, la gestión aún se encuentra en una etapa temprana, caracterizada por una alta concentración de riesgos elevados y la ausencia de salvaguardas implementadas en esta fase del análisis.



Deploy



Ilustración 28: Nivel de madurez

En la ilustración 29 descompone la puntuación de madurez en sus componentes principales: la distribución de riesgos y la severidad del riesgo máximo identificado. Se observa que la severidad de los riesgos aporta el mayor peso a la puntuación final, mientras que la distribución muestra una baja proporción de riesgos en niveles aceptables

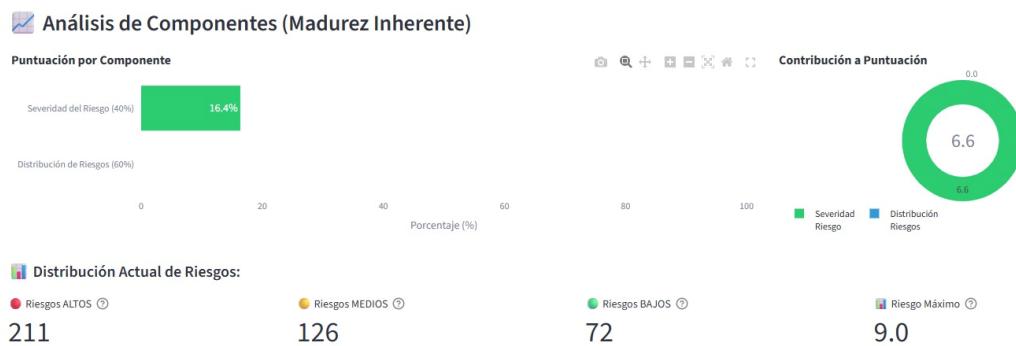


Ilustración 29: Componentes de la puntuación de madurez



La *ilustración 30* presenta la distribución total de los riesgos identificados durante la evaluación, destacando una alta cantidad de riesgos clasificados como altos y medios, frente a un número reducido de riesgos bajos.

#### Interpretación del Nivel de Madurez

##### Nivel 1 - Inicial

La gestión de riesgos de TI está en etapa inicial. Los riesgos identificados son mayormente ALTOS y no hay suficientes controles definidos.

##### Recomendaciones para Mejorar:

1. **Priorizar activos críticos:** Identificar los 10 activos más críticos para el negocio y enfocar la evaluación en ellos primero
2. **Reducir riesgos ALTOS:** Para cada riesgo  $\geq 6$ , definir al menos 2 salvaguardas específicas que reduzcan probabilidad o impacto
3. **Implementar controles básicos:** Aplicar controles de seguridad esenciales como backups, control de acceso y actualizaciones de software
4. **Documentar amenazas:** Usar el análisis con IA para identificar vulnerabilidades y amenazas específicas de cada activo
5. **Capacitar al personal:** Realizar capacitación básica de seguridad informática para todo el personal de TI

*Ilustración 30: Distribución de riesgos por nivel de severidad.*

Esta *ilustración 31* corresponde a la fase de implementación de salvaguardas, donde se registran las medidas aplicadas a cada activo crítico. El sistema permite marcar controles implementados según su nivel de prioridad, como protección contra DDoS, autenticación multifactor y control de accesos.

#### Fase 2: Salvaguardas Implementadas

Marca las salvaguardas que fueron implementadas desde la última evaluación:

| Actividad    | Descripción   | Nivel |
|--------------|---|-------|
| BASTION_PROD | Alta: Implementar protección DDoS, WAF y balanceo de carga con redundancia      | Alta  |
| BASTION_PROD | Alta: Implementar procedimientos documentados y capacitación del personal       | Alta  |
| BASTION_PROD | Alta: Establecer control de acceso basado en roles (RBAC) con principio de m... | Alta  |
| BASTION_PROD | Alta: Implementar autenticación multifactor (MFA) y políticas de contraseñas... | Alta  |
| BASTION_PROD | Alta: Establecer medidas de protección prioritarias según análisis de vulner... | Alta  |
| BASTION_PROD | Media: Implementar procedimientos documentados y capacitación del personal      | Media |
| OCADPO1      | Alta: Implementar protección DDoS, WAF y balanceo de carga con redundancia      | Alta  |
| OCADPO1      | Alta: Implementar procedimientos documentados y capacitación del personal       | Alta  |
| OCADPO1      | Alta: Establecer control de acceso basado en roles (RBAC) con principio de m... | Alta  |
| OCADPO1      | Alta: Implementar autenticación multifactor (MFA) y políticas de contraseñas... | Alta  |
| OCADPO1      | Alta: Establecer medidas de protección prioritarias según análisis de vulner... | Alta  |
| OCADPO1      | Media: Implementar procedimientos documentados y capacitación del personal      | Media |

*Ilustración 31: Salvaguardas implementada*



El indicador gráfico de la *ilustración 31* muestra de forma visual e intuitiva la puntuación obtenida en el nivel de madurez, reforzando el resultado numérico con una representación semaforizada.



*Ilustración 32: Indicador de nivel de riesgo.*

#### 6.2.10. Resultado de la reevaluación.

En la *ilustración 33* muestra el estado consolidado de la evaluación inicial de riesgos, confirmando que el inventario de activos, la identificación de riesgos, la definición de salvaguardas y el cálculo del nivel de madurez han sido completados correctamente.

A screenshot of a software interface for risk reevaluation. At the top, there's a navigation bar with icons and labels: 1. Iterios, 2. Activos, 3. Valoración D/I/C, 4. Vulnerabilidades, 5. Riesgo, 6. Mapa Riesgos, 7. Riesgo Activos, 8. Salvaguardas, 9. Madurez, and 10. Comparativa. The 10. Comparativa icon is highlighted with a red border. Below the navigation, there's a section titled "Reevaluación y Comparativa" with a sub-section "Propósito: Realizar una reevaluación periódica para comparar el estado actual vs anterior." A list titled "Este proceso incluye:" contains five items, each with an icon and a checkbox: 1. Verificar requisitos de la evaluación inicial (checked), 2. Revisar cambios en el inventario de activos (unchecked), 3. Evaluar implementación de salvaguardas (checked), 4. Recalcular riesgos y madurez (checked), and 5. Comparar resultados (checked). Below this is a section titled "Estado de la Evaluación Inicial" with four status boxes: "Activos: 72" (checked), "Riesgos: 409" (checked), "Madurez: Nivel 1" (checked), and "Salvaguardas: 409" (checked). At the bottom, a green bar displays the message "Evaluación inicial completa. Puedes iniciar la reevaluación." with a checked checkbox icon.

*Ilustración 33: Reevaluación comparativa*



En la *ilustración 34* el sistema habilita el proceso de reevaluación periódica de riesgos, permitiendo registrar cambios en el inventario de activos, verificar la implementación de salvaguardas y recalcular los niveles de riesgo y madurez.

Iniciar Proceso de Reevaluación

La reevaluación te permitirá:

- Registrar cambios en el inventario de activos (nuevos, eliminados, editados)
- Evaluar qué salvaguardas fueron implementadas
- Recalcular el nivel de riesgo y madurez
- Comparar el estado actual vs el anterior

Estado Actual (Evaluación Inicial)

| Riesgo Promedio | Madurez | Activos |
|-----------------|---------|---------|
| 5.81            | 7%      | 72      |

Iniciar Reevaluación

*Ilustración 34: Inicio de procesos de reevaluación de riesgos.*

La *ilustración 35* presenta un resumen cuantitativo de los resultados obtenidos tras la reevaluación, evidenciando una reducción del riesgo promedio y una variación en el nivel de madurez.



*Ilustración 35: Resultados generales de reevaluación.*



Este gráfico comparativo que se muestra de forma visual en la *ilustración 36* se puede observar la diferencia entre la evaluación inicial y la reevaluación, tanto en términos de riesgo promedio como de madurez.

| Resumen Comparativo Detallado |                    |              |        |            |
|-------------------------------|--------------------|--------------|--------|------------|
| Métrica                       | Evaluación Inicial | Reevaluación | Cambio | Estado     |
| Riesgo Promedio               | 5.81               | 5.28         | -0.53  | Mejora     |
| Puntuación Madurez            | 7%                 | 4%           | -2%    | Empeoró    |
| Nivel de Madurez              | Nivel 1            | Nivel 1      | 0      | Sin cambio |
| Total Activos                 | 72                 | 72           | 0      | Sin cambio |
| Salvaguardas Implementadas    | 0                  | 75           | +75    | Progreso   |

#### 🕒 Evolución del Riesgo por Activo



*Ilustración 36: Comparativa de Riesgo y Madurez: Antes vs Despues*

Los gráficos circulares que están en la *ilustración 37*, muestran la redistribución de los niveles de riesgo (alto, medio, bajo y nulo) tras la reevaluación. La disminución relativa de riesgos altos y el incremento de riesgos medios o bajos reflejan el efecto positivo de las salvaguardas implementadas



*Ilustración 37: Distribución de riesgos.*



En la ilustración 38, presenta el detalle de las salvaguardas aplicadas por activo, indicando su prioridad y estado de implementación. La información permite evidenciar la trazabilidad entre riesgos identificados y controles aplicados, reforzando la alineación con los controles de la norma ISO/IEC 27002.

#### 💡 Salvaguardas Implementadas

| Activo       | Salvaguarda   | Prioridad | Estado   |
|--------------|---|-----------|--|
| BASTION_PROD | Implementar procedimientos documentados y capacita... | Alta      | <input checked="" type="checkbox"/> Implementada |
| BASTION_PROD | Implementar autenticación multifactor (MFA) y polí... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCADP01      | Implementar protección DDoS, WAF y balanceo de car... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCADP01      | Implementar procedimientos documentados y capacita... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCBEP01      | Implementar protección DDoS, WAF y balanceo de car... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCBEP01      | Implementar procedimientos documentados y capacita... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCDBEIS01    | Implementar procedimientos documentados y capacita... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCEIS01      | Establecer medidas de protección prioritarias segú... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCEIS01_02   | Establecer control de acceso basado en roles (RBAC... | Alta      | <input checked="" type="checkbox"/> Implementada |
| OCJCOG01     | Implementar procedimientos documentados y capacita... | Alta      | <input checked="" type="checkbox"/> Implementada |

☒ La implementación de 75 salvaguardas redujo el riesgo en aproximadamente 9.2%

Ilustración 38: Listado salvaguardas

La *ilustración 39* la vista resume el impacto global de las salvaguardas implementadas, cuantificando la reducción porcentual del riesgo institucional.

#### 📄 Conclusión de la Reevaluación

☒ Mejora detectada: El riesgo promedio disminuyó de 5.81 a 5.28

💾 Guardar Resultados de Reevaluación

🆕 Nueva Reevaluación

Ilustración 39: Impacto de las Salvaguardas en la Reducción del Riesgo.

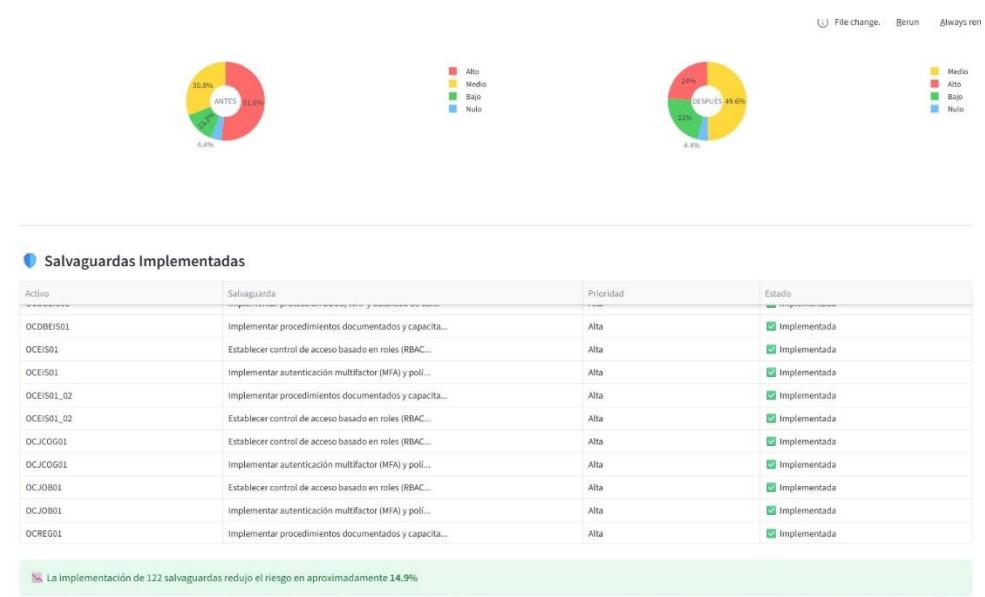


En la *ilustración 40* consolida los resultados finales del proceso de reevaluación, confirmando una mejora en el riesgo promedio institucional. La conclusión refuerza la importancia de realizar evaluaciones periódicas y demuestra que el sistema automatizado permite medir de forma objetiva la evolución del riesgo



*Ilustración 40: Conclusión del Proceso de Reevaluación*

En la *ilustración 41* evidencia el almacenamiento exitoso de los resultados de la reevaluación, asegurando la persistencia de la información para análisis históricos y futuras comparativas.



*Ilustración 41: Almacenamiento de resultados.*



### 6.3. Resultados y Discusión.

Como parte del análisis de resultados, se realizó una segunda evaluación de riesgos sobre los mismos activos previamente analizados, con el objetivo de simular la aplicación de controles y salvaguardas alineados a la norma ISO/IEC 27002. Esta reevaluación que se muestra en la *tabla 5* permitió observar el comportamiento del riesgo una vez considerados los mecanismos de tratamiento, manteniendo constante el inventario de activos y los criterios de evaluación definidos en la metodología MAGERIT v3

| Criterio                    | Evaluación Inicial | Reevaluación (Posterior)                  | Análisis  |
|-----------------------------|--------------------|---|---|
| Activos evaluados           | 72                 | 72  | Se mantiene el mismo inventario de activos, lo que garantiza la consistencia y comparabilidad de los resultados entre evaluaciones.                             |
| Riesgo máximo identificado  | 9.0 (Alto)         | 9.0 (Alto)                                | El riesgo máximo permanece sin cambios, evidenciando la existencia de activos altamente críticos que requieren tratamiento prioritario continuo.                |
| Riesgos altos identificados | 211                | Disminución progresiva                    | Se observa una reducción gradual de riesgos altos tras la implementación de salvaguardas, reflejando una mejora en el perfil de riesgo.                         |
| Riesgo promedio             | 5.81               | 4.94                                      | El riesgo promedio disminuye, evidenciando el impacto positivo de las salvaguardas aplicadas sobre los riesgos identificados.                                   |
| Nivel de madurez            | Nivel 1 – Inicial  | Nivel 1 – Inicial (con mejora porcentual) | Aunque el nivel se mantiene, se registra un incremento en la puntuación de madurez, lo que indica un avance progresivo en la gestión de riesgos.                |
| Puntuación de madurez       | 7%                 | 10%                                       | El aumento en la puntuación refleja una mejora en la cobertura de la evaluación y en la aplicación de controles, aunque aún insuficiente para cambiar de nivel. |

|                                      |           |          |  |
|--------------------------------------|-----------|----------|--|
| <b>Salvaguardas implementadas</b>    | 0         | 122      | La implementación de salvaguardas demuestra el inicio formal del tratamiento del riesgo y contribuye a la reducción del riesgo residual. |
| <b>Reducción estimada del riesgo</b> | No aplica | ≈ 14.9 % | La reducción porcentual confirma la efectividad del sistema automatizado para medir el impacto del tratamiento del riesgo.               |

Tabla 5: Comparación de resultados entre evaluaciones

Los resultados obtenidos en la segunda evaluación evidencian una reducción significativa en los niveles de riesgo y de madurez, así como una disminución en la cantidad de activos clasificados en niveles críticos. De forma paralela, se observó un incremento en el nivel de madurez en ciberseguridad de la institución, pasando de un estado inicial o básico a un nivel definido, lo cual refleja un mayor grado de formalización en la gestión de riesgos y en la implementación de controles de seguridad.

A partir de la aplicación de la solución desarrollada permite evidenciar el correcto funcionamiento del sistema de evaluación de riesgos propuesto, a través de la ejecución completa del proceso, desde la carga del inventario de activos hasta la generación de matrices, dashboard, se verificó que la solución es capaz de analizar de forma estructurada los riesgos asociados a los activos críticos de la organización, manteniendo coherencia con la metodología de Magerit v3.

La utilización de Magerit v3 facilitó la identificación sistemática de amenazas y la valoración de los riesgos inherentes y residuales considerando los criterios de disponibilidad, integridad y confidencialidad. Los resultados reflejaron una distribución clara de los niveles de riesgo, permitiendo identificar activos con requerimientos urgentes de tratamiento, así como aquellos que presentan niveles de riesgo aceptables dentro del contexto institucional. La matriz de riesgos 5x5 permitió visualizar de manera intuitiva la posición de los activos según su impacto y probabilidad, lo cual constituye un insumo clave para la priorización de acciones.



La incorporación de la inteligencia artificial local permitió apoyar el análisis de la información recolectada y generar valoraciones consistentes a partir de los criterios definidos en la metodología, las decisiones finales se mantienen alineadas a los parámetros establecidos Magerit, el uso de la IA permitió reducir la dependencia exclusiva del criterio manual del evaluador, así ayudo a una mayor uniformidad en los resultados obtenidos entre activos con características similares.

| Aspecto evaluado                 | Evaluación manual | Evaluación con IA |
|----------------------------------|-------------------|-------------------|
| <b>Consistencia de criterios</b> | Variable          | Homogénea         |
| <b>Dependencia del evaluador</b> | Alta              | Reducida          |
| <b>Alineación con MAGERIT</b>    | Manual            | Guiada por reglas |

Tabla 6: Rol de la IA en el proceso de evaluación

Los dashboards desarrolladas en Streamlit facilitaron la interpretación de los resultados al presentar de forma visual el estado general de los riesgos, la clasificación de activos críticos, la distribución de amenazas y el nivel de madurez de ciberseguridad, esta visualización permitió validar los resultados obtenidos y comunicar la información de manera clara a los diferentes actores del proyecto, sin requerir un conocimiento técnico profundo de la metodología subyacente.

En conjunto, los resultados obtenidos respaldan que la integración de una metodología formal de análisis de riesgos, el uso de inteligencia artificial local y la visualización interactiva de la información constituyen un enfoque adecuado para apoyar la gestión de riesgos de seguridad de la información en un entorno institucional de educación superior.

#### 6.4. Implicaciones éticas

Durante el desarrollo y ejecución del presente proyecto se consideran diversas implicaciones éticas, orientadas a garantizar el uso responsable de tecnología, la protección de la información y el respeto a los principios fundamentales de la seguridad de la información.



**Confidencialidad y protección de la información:** La información utilizada para la evaluación de riesgos corresponden a datos técnicos autorizados relacionados con activos tecnológicos de la institución de educación superior, estos datos fueron empleados exclusivamente para fines académicos y de análisis, evitando en todo momento la divulgación de información sensible.

**Uso responsable de la inteligencia artificial:** La IA integrada en la solución se ejecuta de forma local, lo que elimina la necesidad de enviar información a servicios externos o plataformas en la nube, esto reduce los riesgos de exposición de datos y garantiza que la información evaluada permanezca bajo el control de la institución de educación superior.

**Transparencia y trazabilidad del análisis:** El diseño de la solución permite mantener trazabilidad sobre los resultados generados durante el proceso de evaluación de riesgos, las valoraciones, matrices y dashboards producidos pueden ser revisados y verificados, lo que contribuye a la transparencia del análisis y facilita una explicación ante los responsables de seguridad de la información.

**Impacto ético y académico:** El proyecto promueve un uso ético de la tecnología al enfocarse en el fortalecimiento de la seguridad de la información y la mejora de la gestión de riesgos, sin afectar la operación normal de los sistemas productivos ni vulnerar derechos de privacidad, la solución contribuye a la información en buenas prácticas de ciberseguridad y al uso responsable de la inteligencia artificial en contexto reales.

## 7. Conclusiones y Recomendaciones

### Conclusiones

- Se logró implementar un sistema institucional para evaluacion y gestión de riesgos de ciberseguridad basado en la metodología Magerit v3 y los controles de la norma ISO/IEC 27002, cumpliendo con el objetivo general del proyecto y permitiendo analizar de manera estructurada los riesgos asociados a los activos críticos de una institución de educación superior.



- El análisis de la infraestructura tecnológica crítica, realizado mediante la aplicación de Magerit v3, permitió identificar activos relevantes, amenazas asociadas y niveles de riesgo inherente y residual, considerando los criterios de disponibilidad, integridad y confidencialidad, este enfoque facilitó una compresión clara del estado de los riesgos dentro del contexto institucional.
- La integración de inteligencia artificial ejecutada de forma local permitió apoyar el proceso de evaluación de riesgos mediante la generación de valoraciones consistentes y alineadas a los criterios definidos por la metodología, manteniendo siempre el control de la información y sin reemplazar el criterio del analista humano.
- Las pruebas funcionales y escenarios controlados realizados evidenciaron el correcto funcionamiento del sistema, validando la coherencia de los resultados obtenidos y permitiendo comparar diferentes evaluaciones sobre los mismos activos, lo cual facilitó el análisis del impacto de la aplicación de controles y salvaguardas de seguridad.
- La presentación de los resultados a través de dashboards interactivos desarrollados en Streamlit permitió visualizar de forma clara los niveles de riesgo, la clasificación de activos críticos y el nivel de madurez en ciberseguridad, apoyando el análisis, seguimiento y priorización de acciones sin requerir conocimientos técnicos avanzados por parte de los usuarios.
- Finalmente, se concluye que la solución propuesta es viable, replicable y adaptable a otros entornos institucionales, constituyéndose en una herramienta de apoyo para la toma de decisiones en seguridad de la información y sentando una base sólida para futuras mejoras en la gestión de riesgos de ciberseguridad.

## Recomendaciones

- Se recomienda realizar evaluaciones periódicas de riesgos utilizando la solución desarrollada con el fin de mantener actualizada la matriz de



riesgos y reflejar los cambios en la infraestructura tecnológica, los activos críticos y el entorno de amenazas.

- Es aconsejable ampliar progresivamente el alcance del sistema para incorporar análisis históricos y comparativos entre evaluaciones, lo que permitirá observar la evolución de los riesgos, el impacto de la aplicación de controles y el nivel de madurez organizacional
- Se recomienda fortalecer la capacitación del personal en gestión de riesgos y seguridad de la información, tanto en el uso de la metodología Magerit como en la interpretación de los dashboards interactivos, con el objetivo de mejorar la toma de decisiones y el aprovechamiento de los resultados generados por el sistema.
- Es importante mantener un enfoque de mejora continua en la gestión de riesgos, revisando periódicamente los criterios de evaluación, los controles de seguridad propuestos y las reglas utilizadas por la inteligencia artificial.

## 8. Trabajo futuro

Como trabajo futuro, se recomienda ampliar la solución para incorporar de forma más profunda las fases posteriores al análisis de riesgos definidas por la metodología MAGERIT, particularmente en lo relacionado con el seguimiento continuo de riesgos y la evaluación periódica de la efectividad de los controles implementados, fortaleciendo así el enfoque de mejora continua en la gestión de la seguridad de la información.

Se sugiere extender el sistema para permitir la comparación histórica entre múltiples evaluaciones de los mismos activos, lo que facilitaría el análisis de la evolución del riesgo, la medición del impacto de las salvaguardas aplicadas y el seguimiento del nivel de madurez organizacional a lo largo del tiempo.

Para futuras versiones, podría integrarse un módulo adicional que permita mapear de forma más detallada los controles propuestos con otros marcos de referencia complementarios, como ISO/IEC 27001 o NIST, sin reemplazar a



MAGERIT, con el objetivo de fortalecer la interoperabilidad del sistema y su aplicabilidad en distintos contextos institucionales.

En relación con la inteligencia artificial, se recomienda explorar modelos más avanzados o especializados que permitan enriquecer el análisis, por ejemplo, mediante la detección de patrones recurrentes en los riesgos evaluados o la generación de recomendaciones más contextualizadas, manteniendo siempre el enfoque de ejecución local para preservar la confidencialidad de la información.

Finalmente, se plantea como línea futura de trabajo la adaptación del sistema para su uso en otras áreas de la institución o en diferentes organizaciones, ajustando los catálogos de activos, amenazas y controles, lo que permitiría validar la escalabilidad y reutilización de la solución en distintos escenarios de gestión de riesgos en ciberseguridad.



## 9. Referencias bibliográficas

- Aldrin Jefferson Calle García, B. M. (05 de febrero de 2024). *Ciencia y Desarrollo. Universidad Alas Peruanas*. Obtenido de LA AUDITORÍA EXTERNA COMO ESTRATEGIA EMPRESARIAL PARA: file:///C:/Users/biblioteca/Downloads/Dialnet-LaAuditoriaExternaComoEstrategiaEmpresarialParaOpt-9604348.pdf
- AWS. (2024). *amazon.com*. Obtenido de ¿Qué es un LLM (modelo de lenguaje de gran tamaño)?: <https://aws.amazon.com/es/what-is/large-language-model/>
- Coelho, F. (2024). *significados.com*. Obtenido de Metodología: <https://www.significados.com/metodologia/>
- Global Solutions. (17 de octubre de 2023). *Globar Suite*. Obtenido de ¿Qué es la norma ISO 27002 y para qué sirve?: <https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27002-y-para-que-sirve/>
- Hidalgo Quirós, N. (s.f.). *Diagnóstico y evaluación de cumplimiento de la norma ISO/IEC 27001 y COBIT 5 para determinar el grado de alineación y nivel de madurez del SGSI*. Obtenido de Repositorio Institucional – Universidad de Costa Rica: <https://hdl.handle.net/10669/15659>
- Jiménez Mendieta, D. D., & Sumba Naula, J. A. (2023). *Construcción e implementación de un modelo para diagnosticar el nivel de la ciberseguridad en una micro-red*. Obtenido de DSpace – Universidad de Cuenca Repositorio: <https://dspace.ucuenca.edu.ec/handle/123456789/41963>
- Jímenez, M. M. (07 de octubre de 2024). *Opirani*. Obtenido de MAGERIT: gestión de riesgos de Seguridad de la Información: <https://www.piranirisk.com/es/blog/metodologia-magerit-gestion-riesgos-sistemas-de-informacion>
- Maza Cerón, Á., & Cabrera Villanueva, C. (s.f.). *Repositorio Digital UNAM*. Obtenido de Diagnóstico del plan de seguridad de las tecnologías de la información y comunicación en una organización: <https://hdl.handle.net/20.500.14330/TES01000705795>
- Nerina Victoria Avellán Zambrano, M. F. (2019). *CIBERSEGURIDAD Y SU APLICACIÓN EN LAS INSTITUCIONES DE EDUCACION SUPERIOR PUBLICAS DE MANABI*. Manaíb.



Oquendo, H. G. (2022). Análisis de riesgos y vulnerabilidades en la educación 4.0 del proceso de enseñanza – aprendizaje.

Pedro, S. d. (22 de enero de 2023). *Gaptain*. Obtenido de La ciberseguridad como responsabilidad social: <https://gaptain.com/blog/la-ciberseguridad-como-responsabilidad-social/>

Pontificia Universidad Javeriana. (s.f.). *Repositorio Académico Javeriana*. Obtenido de Metodología para la evaluación de madurez en gestión de incidentes de ciberseguridad:  
<https://apidspace.javeriana.edu.co/server/api/core/bitstreams/bef1f83e-05c8-4def-b3e0-176c8d0d09a3/content>

rightpeoplegroup. (s.f.). Obtenido de 5 consecuencias devastadoras de ignorar la gestión de riesgos informáticos con ejemplos reales: <https://rightpeoplegroup.com/es/blog/5-consecuencias-devastadoras-de-ignorar-la-gestion-de-riesgos-informaticos-con-ejemplos-reales>

Salzar Mata, C. N. (24 de septiembre de 2021). LA SEGURIDAD INFORMÁTICA EN LAS INSTITUCIONES DE . México, México.

Silva Guerrero, A. R. (2022). *Repositorio Institucional UTP*. Obtenido de Implementación de un sistema de gestión de seguridad de la información para mejorar la seguridad de la información en una empresa MyPE: <https://hdl.handle.net/20.500.12867/5705>

Universidad de Las Américas. (s.f.). *Historia, misión y visión*. Obtenido de Universidad de las Américas (UDLA): <https://www.udla.edu.ec/la-udla/sobre-nosotros/historia-mision-vision/>



## 10. Anexos

**Anexo 1 Solución 1: Evaluación y gestión de riesgos en ciberseguridad institucional, implementando inteligencia artificial.**

**Anexo 2 Solución 2: Evaluación de riesgos y madurez mediante auditoría externa especializada.**

**Anexo 3 Solución 3: Formación institucional obligatoria en gestión de riesgos para directivos.**



## **Anexo 1 Solución 1: Evaluación y gestión de riesgos en ciberseguridad institucional, implementando inteligencia artificial.**

Para el presente proyecto se debe tener un previo conocimiento sobre una matriz de riesgo. “La matriz de riesgo es una herramienta de gestión fundamental que permite identificar, evaluar y priorizar los riesgos a los que se enfrenta una organización, proyecto o proceso, facilitando la toma de decisiones para su mitigación o control”. (EALDE, 2023), es una herramienta flexible, que documenta procesos y evalúa el riesgo integral de una organización.

La matriz de riesgo se va a regir con la metodología de Magerit, “es una metodología de análisis y gestión de riesgos de los sistemas de información, desarrollada por el consejo superior de administración electrónica (CSAE) es un organismo del ministerio de hacienda y administraciones públicas del gobierno de España (Eduarda, 2024).

Tomando en cuenta como referencia la norma ISO3100, Magerit responde al proceso de gestión de riesgos del marco gestión de riesgos, es decir la metodología implementa la gestión de riesgos dentro de un marco de trabajo que va a permitir a la institución de alto nivel tomar decisiones considerando los riesgos derivados del uso de tecnologías de la información.

Magerit tiene objetivos directos como concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos, ofrece métodos sistemáticos para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones. Esto es importante ya que prepara a la organización para procesos de evaluación, auditoria, certificación o acreditación.

La matriz de riesgo se va a implementar con la metodología de Magerit, ya que, ambos analizan los riesgos sirve para establecer que tiene la institución de nivel superior, es decir con que activos cuenta, en el análisis se deben considerar los activos, amenazas y las salvaguardas, partiendo de esos elementos es posible estimar tanto el impacto como el riesgo. La ventaja al usar Magerit, facilita la alineación con normativas y estándares internacionales (ISO27001).



La matriz de riesgos en Magerit es un componente esencial del análisis de riesgos que cruza la probabilidad y el impacto de amenazas sobre activos, facilitando la priorización y el tratamiento adecuado para proteger los sistemas de información de la institución de alto nivel.

Otra metodología que se planeó implementar es la ISO/IEC 27005 ya que, es un estándar internacional que proporciona directrices para la gestión de riesgos de seguridad de la información, el objetivo principal es ofrecer un marco sistemático y estructurado para identificar, analizar, evaluar y tratar los riesgos que pueden afectar a la confidencialidad, integridad y disponibilidad de la información.

El ciclo de gestión según la ISO 27005, establece un proceso estructurado que sigue algunas fases, el establecimiento del contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento de riesgos y monitoreo y revisión. Se integra muy bien con la ISO 27001 ya que establece los requisitos para un SIGSI, incluyendo el análisis de riesgos.

La ISO 27005 podrá ser sólida y estar alineada a la ISO/IEC 27001, pero no define herramientas ni estructura específicas para crear una matriz de riesgos desde cero, el nivel de abstracción exige SGSI previo implementado, lo cual excede el tiempo y el alcance de este proyecto capstone.

La metodología de NIST SP 800-30, es una guía estadounidense del Instituto Nacional de Estándares y Tecnología, que describe un enfoque sistemático para la evaluación de riesgos informáticos se orienta más a las organizaciones gubernamentales o de alta regulación.

En términos más específicos, NIST SP 800-30 describe los pasos a seguir para realizar una evaluación de riesgos de seguridad de la información en una organización. Esto incluye la identificación de los activos de información críticos, la evaluación de las amenazas potenciales, la evaluación de las vulnerabilidades existentes y la estimación del impacto de un evento de seguridad (Areandina, s.f.)

El modelo NIST es complejo y está orientado a entornos con estructuras de ciberseguridad avanzadas, además de estar en el marco de la normativa



estadounidense, la adaptación al contexto universitario requiere ajustes significativos que piden limitar su aplicabilidad directa.

OCTAVE es una metodología de evaluación y gestión de riesgos, el objetivo principal es identificar y priorizar los riesgos operativos y de seguridad de la información en una organización, considerando no solo de aspectos técnicos también las prácticas y necesidades organizativas.

La perspectiva de OCTAVE se centra más en organizaciones técnicas, y su proceso de implementación es más cualitativo y menos automatizable, lo que le hace poco adecuado para ser visualizado en Power BI o automatizado con IA como busca este proyecto.

La evaluación cuantitativa de factores de riesgos de información, conocida como FAIR, es un instrumento utilizado para examinar y discernir los peligros en la relación a la seguridad informativa, creada por Jack Jones e implementada por el grupo abierto como un estándar para el manejo de riesgos de este tipo.

Entre todas las metodologías se eligió MAGERIT, ya que, es una metodología específica para sistemas de información nos permite construir una matriz de riesgos desde cero, adaptada con la realidad de la institución de educación superior, esta alineada con ISO/IEC 27001, facilitando futura certificaciones o auditorias. Es una metodología técnica, completa y gratuita, se alinea a los estándares internacionales y adaptable al desarrollo visual y automatizado.

La vimos que es diseñada para un plan de riesgos dentro del entorno universitario y para la gestión de riesgos en sistemas de información. Nos ofrece herramientas prácticas como el catálogo de activos, amenazas y salvaguardas, lo que facilita la adopción a la institución de alto nivel.

Es un estándar internacional que proporciona directrices para la implementación de controles de seguridad de información, lo que diferencia la ISO 27001, que se centra en los requisitos de un sistema de gestión de seguridad de la información. Un estándar que ofrece un conjunto detallado de directrices y mejores prácticas para implementar los controles de seguridad identificados en el anexo A de la ISO 27001. (Global Solutions, 2023)

| Metodología           | Enfoque principal                    | Nivel de detalle | Alineación con normas          | Aplicabilidad en universidades | Requiere software propio | Tipo de evaluación              |
|-----------------------|--------------------------------------|------------------|--------------------------------|--------------------------------|--------------------------|---------------------------------|
| <b>MAGERIT</b>        | Gestión de riesgos basada en activos | Alto             | Compatible con ISO 27001 y ENS | Alta                           | No obligatorio           | Cualitativa / Cuantitativa      |
| <b>ISO/IEC 27005</b>  | Gestión del riesgo en SGSI           | Medio-Alto       | ISO/IEC 27001                  | Alta                           | No                       | Cualitativa                     |
| <b>NIST SP 800-30</b> | Evaluación de riesgos TI             | Alto             | NIST CSF, FIPS                 | Media                          | No                       | Cualitativa / Semi-cuantitativa |
| <b>OCTAVE</b>         | Evaluación organizacional            | Medio            | Compatible con ISO/NIST        | Media                          | No                       | Cualitativa                     |
| <b>FAIR</b>           | Análisis financiero del riesgo       | Medio-Bajo       | Frameworks internacionales     | Baja                           | Sí                       | Cuantitativa                    |

Tabla 7: Comparación de metodologías

Finalmente, como complemento a MAGERIT, se emplean los controles de la norma ISO/IEC 27002, la cual proporciona directrices y buenas prácticas para la implementación de controles de seguridad de la información, apoyando la definición de recomendaciones técnicas derivadas del análisis de riesgos realizado en el proyecto.



Los dashboards interactivos constituyen la capa de visualización y análisis del sistema propuesto, permitiendo transformar los resultados técnicos de la evaluación de riesgos en información comprensible y útil para la toma de decisiones. Estas herramientas no ejecutan procesos de inteligencia artificial, sino que consumen y representan los resultados previamente generados por el sistema de evaluación de automatizada.

En el contexto del proyecto, los dashboards interactivos fueron desarrollados utilizando Streamlit, un framework de código abierto orientado a la creación rápida de aplicaciones web interactivas para análisis de datos. “Streamlit permite integrar directamente scripts en Python con componentes visuales, facilitando la construcción de interfaces dinámicas sin necesidad de tecnologías web complejas.” Streamlit. (2024).

“La visualización de datos permite transformar grandes volúmenes de información en representaciones gráficas que facilitan la compresión, el análisis y la toma de decisiones” Few, S. (2013). Los dashboards interactivos permiten convertir conjuntos de datos estructurados en visualizaciones dinámicas, facilitando el análisis de la información compleja mediante gráficos, matrices, indicadores clave y filtros interactivos.

“Tableau se utiliza ampliamente para análisis avanzados y paneles de control empresariales, pero los costos de licencia y la complejidad técnica pueden limitar su adopción en proyectos académicos o de pequeña escala.” Tableau Software. (2023). Su potencia y flexibilidad la convierten en una herramienta robusta para grandes organizaciones.

Entre los principales inconvenientes se encuentra su elevado costo de licenciamiento, la necesidad de configuraciones más técnicas para la integración con procesos externos y una curva de aprendizaje más pronunciada y la integración con inteligencia artificial requiere módulos adicionales o el uso de lenguaje como Python lo que incrementa la complejidad del entorno.

“Qlik Sense se centra en el modelado de datos asociativo para apoyar la analítica guiada, principalmente en escenarios de inteligencia empresarial” Qlik. (2023).



Es una herramienta de análisis visual orientada al modelado asociativo de datos y al descubrimiento guiado de información, permite analizar grandes volúmenes de datos y generar paneles interactivos enfocados principalmente en áreas como ventas, marketing y análisis financiero.

Su enfoque corporativo y financiero, junto con una integración limitada con procesos de evaluación automatizada y modelos de inteligencia artificial externos, reduce su adecuación al contexto del proyecto. Además, su uso resulta menos intuitivo para la presentación de modelos de riesgo basados en metodologías como Magerit.

"Looker Studio permite a los usuarios crear informes y paneles utilizando datos principalmente de los servicios de Google y de las plataformas de marketing." Google. (2024). Su principal ventaja es la accesibilidad y facilidad para compartir información. Sin embargo, esta herramienta carece de funcionalidades avanzadas para el modelado analítico, no ofrece soporte para lenguajes de expresión complejos y presenta limitaciones en términos de control.

| Herramienta                                | Enfoque principal                                       | Facilidad de uso | Integración con IA (contexto del proyecto)                | Integración con Excel | Costo                  | Soporte para automatización | Accesibilidad |
|--|---|------------------|---|-----------------------|------------------------|-----------------------------|---------------|
| <b>Dashboards interactivos (Streamlit)</b> | Visualización y análisis de riesgos en aplicaciones web | Alta             | Alta (consume resultados de IA local integrada en Python) | Excelente             | Gratis (Open Source)   | Alta (scripts Python)       | Alta          |
| <b>Tableau</b>                             | Visualización empresarial avanzada                      | Media            | Media (requiere integración externa con Python/R)         | Buena                 | Licencia de pago       | Alta                        | Alta          |
| <b>Qlik Sense</b>                          | Análisis asociativo de datos corporativos               | Media            | Baja (IA dependiente del proveedor)                       | Baja                  | Básico gratuito / pago | Media                       | Alta          |



|                             |                                    |      |  |           |                    |          |       |
|-----------------------------|------------------------------------|------|--|-----------|--------------------|----------|-------|
| <b>Google Looker Studio</b> | Reportes simples en la nube        | Alta | Baja (sin soporte para IA de evaluación) | Muy buena | Gratis             | Baja     | Alta  |
| <b>Excel</b>                | Análisis manual y tablas estáticas | Alta | Nula                                     | Nativa    | Licencia educativa | Muy baja | Media |

Tabla 8: Comparación de herramientas

Streamlit fue seleccionado debido a su capacidad para desarrollar dashboards interactivos directamente integrados con el sistema de evaluación de riesgos, permitiendo consumir los resultados generados por la inteligencia artificial local sin depender de licencias propietarias ni plataformas externas. Este enfoque garantiza flexibilidad, escalabilidad y coherencia con la arquitectura del proyecto.



La inteligencia artificial utilizada en el presente proyecto se basa en el uso de modelos de lenguaje de gran tamaño (LLM) ejecutados de forma local, los cuales permiten apoyar el proceso de evaluación de riesgos de seguridad de la información sin depender de servicios externos en la nube. Esta tecnología posibilita el análisis automatizado de información técnica y estructurada, facilitando la interpretación de criterios relacionados con la Disponibilidad, Integridad y Confidencialidad (DIC) de los activos evaluados. El uso de modelos locales contribuye además a mantener un mayor control sobre los datos analizados y a reducir riesgos asociados a la exposición de información sensible en entornos externos (Bommasani et al., 2021).

Una de las principales ventajas del uso de modelos de lenguaje ejecutados localmente es que estos han sido previamente entrenados con grandes volúmenes de información, lo que les permite comprender contextos complejos y generar evaluaciones coherentes sin necesidad de procesos adicionales de entrenamiento. Esta característica permite aprovechar la inteligencia artificial como un apoyo al análisis de riesgos, identificando patrones, amenazas y recomendaciones de control de manera eficiente. De acuerdo con Brown et al. (2020), los modelos de lenguaje de gran escala pueden realizar tareas de razonamiento y análisis contextual de forma efectiva mediante instrucciones adecuadas, sin requerir un reentrenamiento específico para cada caso de uso.

La integración de la inteligencia artificial con el sistema de evaluación de riesgos permite automatizar tareas clave del análisis, como la valoración de Disponibilidad, Integridad y Confidencialidad, la identificación de amenazas relevantes y el cálculo de riesgos inherentes y residuales. En este contexto, la inteligencia artificial actúa como un componente de apoyo al analista de seguridad, contribuyendo a reducir la subjetividad del proceso y a mejorar la consistencia de las evaluaciones. Este enfoque coincide con lo señalado por ISO/IEC 27005, donde se destaca la importancia de utilizar métodos sistemáticos y repetibles para el análisis de riesgos de seguridad de la información (ISO/IEC, 2018).



La integración de la inteligencia artificial con el sistema de evaluación de riesgos permite automatizar tareas clave del análisis, como la valoración de DIC, la identificación de amenazas relevantes y el cálculo de riesgos inherentes y residuales. De esta manera, la IA actúa como un componente de apoyo al analista de seguridad, optimizando el tiempo de evaluación y garantizando un tratamiento homogéneo de los activos evaluados, lo que contribuye a una gestión de riesgos más eficiente y estructurada.

Por otra parte, Power BI se integra en la solución como una herramienta de visualización y análisis, consumiendo los resultados generados previamente por la inteligencia artificial. A través de dashboards interactivos, Power BI permite presentar indicadores clave, matrices de riesgos y métricas de madurez organizacional, facilitando la interpretación de los resultados y apoyando la toma de decisiones estratégicas. En este contexto, Power BI no ejecuta procesos de inteligencia artificial, sino que cumple un rol fundamental en la comunicación visual de la información generada por el sistema.

Finalmente, la arquitectura propuesta separa claramente la fase de evaluación automatizada con inteligencia artificial de la fase de análisis y visualización, lo que permite mantener un mayor control sobre los datos, mejorar la trazabilidad de los resultados y garantizar la confidencialidad de la información evaluada. Este enfoque refuerza la viabilidad técnica de la solución y demuestra que es posible implementar inteligencia artificial aplicada a la gestión de riesgos de ciberseguridad de forma local, escalable y alineada a estándares internacionales.

| Herramienta  | ¿Qué permite hacer?   | Facilidad de uso | Personalización                       | Integración con Power BI            | Requiere programación | Nivel de IA (en el proyecto)                    |
|--|---|------------------|---------------------------------------|-------------------------------------|-----------------------|---|
| <b>IA local (LLM ejecutado con Ollama - Llama 3)</b> | Evaluar riesgos, generar DIC, identificar amenazas y recomendar controles ISO 27002 | Media            | Alta (prompts y lógica personalizada) | Indirecta (exportación de datasets) | Sí (Python)           | Avanzada (NLP aplicado a evaluación de riesgos) |



|                                 |   |       |       |                              |               |   |
|---------------------------------|---|-------|-------|------------------------------|---------------|---|
| <b>Power BI Smart Narrative</b> | Generar descripciones automáticas a partir de métricas visualizadas | Alta  | Baja  | Nativo                       | No            | Básica (explicativa)                    |
| <b>Power BI Q&amp;A</b>         | Consultar datos del dashboard en lenguaje natural                   | Alta  | Media | Nativo                       | No            | Media (consulta semántica)              |
| <b>Scikit-learn (Python)</b>    | Entrenamiento de modelos ML tradicionales                           | Media | Alta  | Indirecta (scripts externos) | Sí            | Alta (ML clásico)                       |
| <b>LangChain</b>                | Orquestación avanzada de flujos conversacionales                    | Baja  | Alta  | No directa                   | Sí (avanzada) | Avanzada (IA conversacional contextual) |

Tabla 9: Comparación de tecnologías de inteligencia artificial

La inteligencia artificial local fue seleccionada por su capacidad para analizar información estructurada y cualitativa, automatizar la evaluación de los criterios de Disponibilidad, Integridad y Confidencialidad (DIC) y garantizar la confidencialidad de los datos evaluados. Al ejecutarse de forma local, se evita el envío de información a servicios externos o APIs en la nube, reduciendo el riesgo de exposición o uso indebido de datos sensibles y asegurando que toda la información permanezca bajo control institucional. Este enfoque se integra de manera coherente con la arquitectura del proyecto, donde los resultados son posteriormente visualizados mediante dashboards interactivos desarrollados en Streamlit.



## **Anexo 2 Solución 2: Evaluación de riesgos y madurez mediante auditoría externa especializada.**

La contratación de una auditoría externa en Ecuador para el análisis de riesgos y evaluación de madurez es una práctica clave para garantizar la transparencia, confiabilidad y cumplimiento normativo de las organizaciones. Consiste en contratar una firma independiente y autorizada que, mediante metodologías reconocidas y herramientas tecnológicas avanzadas, evalúa los riesgos específicos del negocio, la efectividad de los controles internos y el nivel de madurez en la gestión de riesgos y ciberseguridad (Grant Thornton Ecuador, 2014; Auditool, 2025).

La auditoría debe anticipar la forma de evaluar los controles establecidos, los cuales pueden ser complejos desde el punto de vista técnico y se necesita la participación de expertos en ciberseguridad para su verificación. En algunos momentos, la dirección puede carecer de controles necesarios, en algunas situaciones, la auditoria debe determinar la mejor manera de colaborar con los trabajadores pertenecientes a la primera y segunda línea.

Los auditores externos deben ser independientes y estar registrados en el Registro Nacional de Auditores Externos (RENAE), garantizando un análisis imparcial (Globaudit, 2024; Datil, 2024).

**Metodologías y normas aplicadas:** Las auditorías se realizan conforme a las Normas Internacionales de Auditoría (NIA), asegurando calidad y cumplimiento de estándares globales (Datil, 2024).

**Evaluación integral:** Se revisan estados financieros, controles internos, cumplimiento normativo y la madurez en la gestión de riesgos, incluyendo aspectos de ciberseguridad y continuidad operativa (Grant Thornton Ecuador, 2014; Auditool, 2025).

Se entrega un reporte con hallazgos, opinión sobre la confiabilidad de la información financiera, nivel de madurez y recomendaciones para fortalecer la gestión de riesgos (Datil, 2024).



Cumplimiento legal y regulatorio: Asegura que las empresas cumplan con las normativas de la Superintendencia de Compañías, Valores y Seguros y otras entidades regulatorias (Russell Bedford, 2023; Datil, 2024).

Confianza y transparencia: Proporciona confianza a inversionistas, acreedores y partes interesadas mediante informes precisos y confiables (Grant Thornton Ecuador, 2014). Prevención de fraudes y errores: Identifica debilidades en controles internos que pueden facilitar fraudes o errores significativos (Datil, 2024).

Mejora continua: Facilita la identificación de brechas en la gestión de riesgos y madurez, orientando acciones estratégicas para fortalecer la organización (Auditool, 2025).

Para la contratación de auditoría externa en Ecuador, existen diversas opciones que varían en tamaño, alcance, especialización y experiencia. A continuación, se comparan algunas de las principales firmas internacionales y locales con presencia en Ecuador, destacando sus características, ventajas y desventajas para facilitar la elección adecuada.

Las Big Four (PwC, Deloitte, EY, KPMG) son ideales para grandes empresas multinacionales o aquellas que requieren auditorías complejas con alto nivel tecnológico y cumplimiento global. Sin embargo, sus costos y procesos pueden ser elevados para organizaciones medianas o pequeñas.

Grant Thornton Ecuador ofrece un balance entre experiencia global y atención local personalizada, con metodologías adaptadas al contexto ecuatoriano, siendo una opción sólida para empresas medianas y grandes que buscan calidad con costos más accesibles.

Opertune y otras firmas locales brindan servicios con profundo conocimiento del mercado ecuatoriano, flexibilidad y costos competitivos, recomendables para empresas pequeñas y medianas que requieren asesoría cercana y adaptada.



HLB Ecuador combina experiencia internacional con enfoque local, siendo una opción intermedia para empresas que buscan calidad reconocida sin los costos de las Big Four.

Para una universidad o institución pública/privada de tamaño mediano a grande en Ecuador, que requiere una auditoría externa rigurosa, objetiva y alineada con normativas nacionales e internacionales, Grant Thornton Ecuador representa la mejor opción. Su experiencia local de más de 28 años, metodología adaptada y enfoque en mitigación de riesgos personalizados garantizan un servicio de alta calidad con costos razonables y atención cercana (Grant Thornton Ecuador, 2014; Auditool, 2025).

| Empresa                 | Características principales   | Ventajas   | Desventajas  |
|-------------------------|---|--|--|
| <b>PwC Ecuador</b>      | Parte de las Big Four, ofrece auditoría, consultoría, asesoría fiscal y servicios especializados en tecnología. | Amplia experiencia global y local, innovación tecnológica, enfoque en sostenibilidad y responsabilidad social. | Costos elevados, más orientada a grandes empresas multinacionales. |
| <b>Deloitte Ecuador</b> | Big Four con fuerte enfoque en auditoría, consultoría, ciberseguridad y gestión de riesgos.                     | Centros de innovación, soluciones avanzadas, compromiso con diversidad e inclusión.                            | Procesos complejos para empresas pequeñas y medianas.              |
| <b>EY Ecuador</b>       | Firma global con servicios en auditoría, consultoría, impuestos y transformación digital.                       | Amplia red global, enfoque en transformación digital y sostenibilidad, soporte a grandes y medianas empresas.  | Costos y procesos elevados para PYMES.                             |
| <b>KPMG Ecuador</b>     | Big Four con servicios integrales en auditoría, impuestos, consultoría y gestión de riesgos.                    | Enfoque en calidad, integridad y servicio al cliente,  | Costos elevados, menor flexibilidad para empresas pequeñas.        |



|                       |  |   |  |
|-----------------------|--|---|--|
|                       |  | fuerte presencia local y global.  |  |
| <b>Grant Thornton</b> | Firma global con más de 28 años en Ecuador, especializada en auditoría externa, asesoría financiera y gestión de riesgos.                  | Metodología adaptada a la realidad local, atención personalizada, experiencia en diversos sectores. | Menor alcance global que Big Four.                                     |
| <b>Opportune</b>      | Firma local con más de 10 años de experiencia, calificada por la Superintendencia de Compañías, especializada en NIIF y auditoría externa. | Conocimiento profundo del mercado ecuatoriano, servicios personalizados, costos competitivos.       | Menor reconocimiento internacional, alcance limitado fuera de Ecuador. |
| <b>HLB Ecuador</b>    | Miembro de una red global, reconocida entre las mejores firmas globales según IAB 2025.  | Combinación de experiencia local e internacional, servicios de alta calidad y confiabilidad.        | Menor tamaño que Big Four, menos recursos tecnológicos.                |

Tabla 10: Comparación de empresas solución 2



### Anexo 3 Solución 3: Formación institucional obligatoria en gestión de riesgos para directivos.

Adopción de una plataforma de GRC en la nube (SaaS) permite centralizar y automatizar la gestión de riesgos, cumplimiento y madurez en ciberseguridad, facilitando la colaboración y el monitoreo en tiempo real. Estas soluciones ofrecen ventajas como reducción de costos, escalabilidad y acceso remoto, promoviendo la mejora continua y el cumplimiento normativo (EY, 2023; GlobalSuite Solutions, 2024).

“Este tipo de software se basa precisamente en la metodología de GRC, con este modelo de gestión integrado, es posible tomar decisiones más informadas, proteger los activos y garantizar que la operación de una empresa cumpla con los requisitos legales y políticas internas.” (Guilherme Not)

Las funcionalidades y beneficios de un sistema GRC se centraliza en la gestión de políticas de controles de riesgos y cumplimiento en un solo entorno eliminando silos organizativos y facilitando la colaboración entre departamentos. Automatiza flujos de trabajo, controles y auditorias, proporcionando alertas y reportes en tiempo real para la toma de decisiones informada.

Los componentes principales de un sistema de GRC, se divide en tres, es la gobernanza, gestión de riesgos y cumplimiento. Cada uno con una metodología diferente, como lo es la gobernanza, que se refiere al establecimiento de políticas, normas, roles y responsabilidades que guían la toma de decisiones y el control dentro de la organización, la gestión de riesgos identifica, analiza, evalúa y mitiga los riesgos que puedan afectar a la organización, ya sean financieros o de reputación.

En referente a la gestión de riesgos, toda empresa se enfrenta a diferentes tipos de riesgos, incluidos financieros, legales, estratégicos y de seguridad, una gestión de riesgos adecuada ayuda a las empresas a identificar estos riesgos a encontrar formas de corregirlos, ahora adaptado a una institución de alto nivel



utilizan un programa de gestión de riesgos empresariales para reducir posibles problemas y minimizar las perdidas.

Es importante un enfoque al GRC ya que mediante la implementación de programas de GRC, las empresas pueden tomar mejores decisiones en un entorno en el que se cuenta los riesgos, un programa eficaz de GRC ayuda a las principales partes interesadas establecer políticas desde una perspectiva compartida y a cumplir con los requisitos regulatorios.

El SaaS es un modelo de distribución de software en el que las aplicaciones se alojan en la nube y se ofrecen a los usuarios a través de internet, generalmente mediante un navegador web, este modelo, el proveedor se encarga de operar, mantener y actualizar tanto el software como la infraestructura necesaria, mientras que el cliente simplemente accede y utiliza el servicio.

LogicGate es una plataforma SaaS que permite gestionar riesgos, controles y cumplimiento mediante flujos de trabajo personalizables y reportes dinámicos, facilitando la colaboración y la visibilidad en tiempo real (LogicGate, 2024). Su flexibilidad y capacidad de integración la hacen adecuada para organizaciones con múltiples departamentos (EY, 2023).

RSA Archer es una solución integral de GRC que ofrece módulos especializados para riesgos operativos, tecnológicos y cumplimiento normativo, con una interfaz intuitiva y funcionalidades avanzadas de workflow (Dell Technologies, 2015). Es reconocida por su robustez y capacidad de personalización, aunque su configuración inicial puede ser compleja (Gartner, 2024).

MetricStream es una plataforma SaaS líder en GRC que automatiza la recopilación de datos, evaluaciones de riesgos y generación de informes, integrando capacidades analíticas avanzadas para la toma de decisiones informadas (CanvasBusinessModel.com, 2024). Destaca por su enfoque integral y adaptabilidad (Gartner, 2024).



| Herramienta         | Funcionalidades principales                                 | Ventajas   | Desventajas   |
|---------------------|---|--|---|
| <b>LogicGate</b>    | Flujos de trabajo personalizables, reportes en tiempo real. | Alta flexibilidad y fácil integración (LogicGate, 2024).                   | Costo variable según módulos.                       |
| <b>RSA Archer</b>   | Gestión integral de GRC con módulos especializados.         | Plataforma robusta y amplio soporte empresarial (Dell Technologies, 2015). | Alta complejidad en la configuración inicial.       |
| <b>MetricStream</b> | Automatización de procesos GRC y análisis avanzado.         | Ánálisis predictivo y reportes detallados (CanvasBusinessModel.com, 2024). | Curva de aprendizaje pronunciada y costos elevados. |

Tabla 11: Comparación herramientas solución 3

LogicGate destaca por su flexibilidad para personalizar flujos de trabajo y facilitar la colaboración entre áreas, lo que es ideal para una universidad con múltiples departamentos. Su capacidad de integración y reportes en tiempo real permite gestionar riesgos de manera eficiente y transparente (EY, 2023; LogicGate, 2024).

El NIST RMF es un marco que define un proceso de siete pasos para la gestión continua de riesgos en sistemas de información, desde la categorización hasta la monitorización continua (NIST, 2023). Es ampliamente utilizado por su enfoque estructurado y adaptable a diferentes tipos de organizaciones.

COBIT 2019 es un marco de gobierno y gestión de TI que incluye procesos, métricas y prácticas para el control y evaluación de riesgos, alineando la gestión



de TI con los objetivos empresariales (ISACA, 2023). Es ideal para integrar la gestión de riesgos TI en la estrategia organizacional.

ISO/IEC 31000:2018 es una norma internacional que proporciona principios y directrices para la gestión de riesgos en cualquier contexto organizacional (ISO, 2018). Su enfoque generalista permite su aplicación en diversos sectores y su integración en plataformas GRC.

| Metodología               | Enfoque principal                     | Ventajas   | Desventajas  |
|---------------------------|---------------------------------------|--|--|
| <b>NIST RMF</b>           | Gestión cíclica y continua de riesgos | Enfoque detallado para sistemas de información (NIST, 2023).       | Alta complejidad para entornos no gubernamentales. |
| <b>COBIT 2019</b>         | Gobierno y control de TI              | Alineación con objetivos empresariales y de negocio (ISACA, 2023). | Requiere adaptación en organizaciones pequeñas.    |
| <b>ISO/IEC 31000:2018</b> | Gestión general de riesgos            | Aplicable a cualquier sector y tipo de organización (ISO, 2018).   | Requiere interpretación para casos específicos.    |

Tabla 12: Comparación 3

Después de analizar las distintas metodologías, nos quedamos con NIST RMF es un marco reconocido internacionalmente que promueve la gestión continua del riesgo, adecuada para un entorno dinámico como la ciberseguridad universitaria. Su estructura por fases facilita la implementación gradual y el seguimiento constante (NIST, 2023).



#### Anexo 4: Planificación y costos

Para la implementación de la solución propuesta en el presente proyecto Capstone, se realizó una planificación de costos con el objetivo de identificar los recursos económicos necesarios durante el desarrollo del sistema de evaluación y gestión de riesgos en ciberseguridad. Dado que el proyecto se desarrolla en un entorno académico y utiliza principalmente herramientas de libre acceso o incluidas dentro de licencias institucionales, no se requiere una inversión económica significativa, lo cual representa una ventaja para la organización.

No obstante, se consideraron los costos asociados a los recursos computacionales necesarios para la ejecución local de la inteligencia artificial, así como a las herramientas utilizadas para el análisis y visualización de los resultados. La arquitectura propuesta prioriza el procesamiento local de la información, evitando el uso de servicios externos en la nube y reduciendo costos operativos y riesgos asociados a la exposición de datos sensibles.

Para el desarrollo de los dashboards interactivos y la visualización de resultados, se emplea la herramienta Streamlit, la cual permite integrar directamente los resultados generados por el sistema de evaluación y la inteligencia artificial local. Al tratarse de una herramienta de código abierto, no implica costos de licenciamiento y facilita una implementación flexible, escalable y alineada con los objetivos académicos del proyecto.

En conjunto, esta planificación de costos demuestra que la solución propuesta es viable desde el punto de vista económico, sostenible en el tiempo y replicable en otras instituciones con recursos limitados, manteniendo un equilibrio entre funcionalidad, seguridad de la información y control de los datos evaluados.

| Herramienta      | Uso dentro del proyecto       | Costo estimado |
|------------------|-------------------------------|----------------|
| Python           | Desarrollo del sistema        | Gratis         |
| Ollama + Llama 3 | Inteligencia artificial local | Gratis         |



|   |   |                                    |
|---|---|------------------------------------|
| <b>Streamlit</b>                                      | Dashboards interactivos y visualización | Gratis                             |
| <b>GitHub Copilot</b>                                 | Apoyo al desarrollo del sistema         | \$10 USD                           |
| <b>Microsoft Excel</b>                                | Gestión y estructuración de datos       | Incluido en licencia institucional |
| <b>Herramientas de diagramación (draw.io / Canva)</b> | Diagramas y esquemas arquitectónicos    | Gratis                             |

Tabla 13: Comparación de costos

## Anexo 5

**Gestión de Activos**

Evaluación: segunda (EVA-002)

**Inventario de Activos**

| Tipo              | Ubicación     | Estado           |           |          |                |
|-------------------|---------------|------------------|-----------|----------|----------------|
| Todos             | Todas         | Todos            |           |          |                |
| ID_Activo         | Nombre_Activo | Tipo_Activo      | Ubicacion | Estado   | Tipo_Servicio  |
| 0 ACT-EVA-002-001 | snvm21        | Servidor Físico  | Granados  | Completo | Virtualización |
| 1 ACT-EVA-002-002 | snvm22        | Servidor Físico  | Granados  | Completo | Virtualización |
| 2 ACT-EVA-002-003 | snvm23        | Servidor Físico  | Granados  | Completo | Virtualización |
| 3 ACT-EVA-002-004 | snvm24        | Servidor Físico  | Granados  | Completo | Virtualización |
| 4 ACT-EVA-002-005 | snvm25        | Servidor Físico  | Granados  | Completo | Virtualización |
| 5 ACT-EVA-002-006 | snvm26        | Servidor Físico  | Granados  | Completo | Virtualización |
| 6 ACT-EVA-002-007 | snvm28        | Servidor Físico  | Granados  | Completo | Virtualización |
| 7 ACT-EVA-002-008 | SNSQL10       | Servidor Virtual | Granados  | Completo | Base de Datos  |
| 8 ACT-EVA-002-009 | SNAPP12       | Servidor Virtual | Granados  | Completo | Servidor IIS   |

Mostrando 11 de 11 activos

Ilustración 42: Módulo de inventario e identificación de activos



## Anexo 6

**+ Crear Activo**

Nombre \*  
Ej: Servidor DB Principal

Tipo \*  
Servidor Físico

Ubicación \*  
UdlaPark

Propietario \*  
Infraestructura

Tipo Servicio \*  
Base de datos

Aplicación Crítica  
 Sí  No

Ilustración 43: Módulo de inventario y agregar activos

## Anexo 7

| Seleccionar Activo                              |                        |                 |           |
|---|------------------------|-----------------|-----------|
| ID  | Nombre                 | Tipo            | Estado    |
| ACT-EVA-004-001                                 | Servidor base de datos | Servidor Físico | Pendiente |
| Seleccionar activo para responder cuestionario: |                        |                 |           |
| ACT-EVA-004-001 - Servidor base de datos        |                        |                 |           |
| Total Preguntas<br>21                           | Respondidas<br>0       | Pendiente       |           |

Ilustración 44: Cuestionario Magerit aplicado a los activos tecnológicos



## Anexo 8

The screenshot shows a question from a questionnaire titled "Disponibilidad" (Availability). The question is: "PF-A01. ¿Cuál es el tiempo máximo tolerable de interrupción (RTO) del servidor?" (What is the maximum tolerable time of interruption (RTO) of the server?). Below the question is a list of four options under the heading "A-Impacto":

- Más de 72 horas
- 24-72 horas
- 4-24 horas
- Menos de 4 horas

Below the options, it says "Peso: 5 | Dimensión: D".

Ilustración 45: Preguntas del cuestionario de Magerit

## Anexo 9

The screenshot shows the "Validación y Preparación de IA Local" (Validation and Preparation of Local AI) module. It displays the following information:

- Estado Actual:** IA Validada y Lista (checked)
- Última validación:** 2026-01-25T13:27:14.211217
- Ollama Local:** Conectado: <http://localhost:11434> (checked)
- Knowledge Base:**
  - Amenazas MAGERIT: 52
  - Controles ISO 27002: 93
  - Catálogos cargados correctamente (checked)

At the bottom, there is a button labeled "Ejecutar Validación Completa" (Execute Full Validation).

Ilustración 46: Flujo de evaluación de riesgos mediante inteligencia artificial local



## Anexo 10

The screenshot shows a dark-themed user interface for an AI-powered risk evaluation system. At the top, a green header bar indicates "Ollama disponible con 3 modelos" and "Evaluación activa: EVA-004". A dropdown menu shows "Modelo IA: llama3.2:1b". Below the header, a navigation bar includes links for "Planes de Tratamiento", "Chatbot MAGERIT" (which is underlined in red), "Resumen Ejecutivo", "Predicción de Riesgo", and "Priorización de Controles". The main content area is titled "Chatbot Consultor MAGERIT" and contains the message: "Pregunta sobre tu evaluación de riesgos. El asistente conoce todos los datos de tus activos, amenazas y controles." Below this is a text input field labeled "Escribe tu pregunta sobre la evaluación...". A section titled "Preguntas sugeridas:" lists four questions: "¿Cuál es el activo más crítico?", "Dame un resumen general", "¿Qué controles faltan?", and "¿Cuáles son las amenazas más frecuentes?".

Ilustración 47: Inteligencia artificial local avanzada

## Anexo 11

The screenshot displays the StreamLit application interface for asset management. On the left, a sidebar titled "TITA Matriz" shows sections for "Evaluación" (with "Evaluación inicial" and "ID: EVA-001"), "Filtro de Activo" (with "Todos los activos" selected), and "Resumen" (showing 75 Active, 9% Vulnerable, 0 Urgent). The main content area is titled "Inventario de Activos" and includes a table with columns "Total Activos" (75), "Físicos" (23), and "Virtuales" (52). Below this is a "Agregar Nuevo Activo" form with tabs for "Información General" and "Especificaciones Técnicas". The "Información General" tab contains fields for "Nombre del Activo", "Área Responsable" (Infraestructura), "Rack/Ubicación Física", "Finalidad de Uso" (Administradores), "Tipo de Activo" (Servidor Físico), "Ubicación" (Granados), and "Aplicación Crítica" (No Aplica). The "Especificaciones Técnicas" tab contains fields for "Modulo", "Sistema Operativo", and "Dependencias (otros activos)".

Ilustración 48: Interfaz StreamLit.



## Anexo 12

```
Stopping...
(.venv) PS C:\Users\nico_\Downloads\capston_riesgos-main (2)\capston_riesgos-main> .\venv\Scripts\streamlit.exe run app
_matriz.py

You can now view your Streamlit app in your browser.

Local URL: http://localhost:8501
Network URL: http://192.168.1.50:8501
```

Ilustración 49: Comando StreamLit

## Anexo 13



Ilustración 50: Distribución por nivel de riesgo inherente



## Anexo 14

Gráfico Comparativo Riesgo Actual vs Objetivo vs Límite

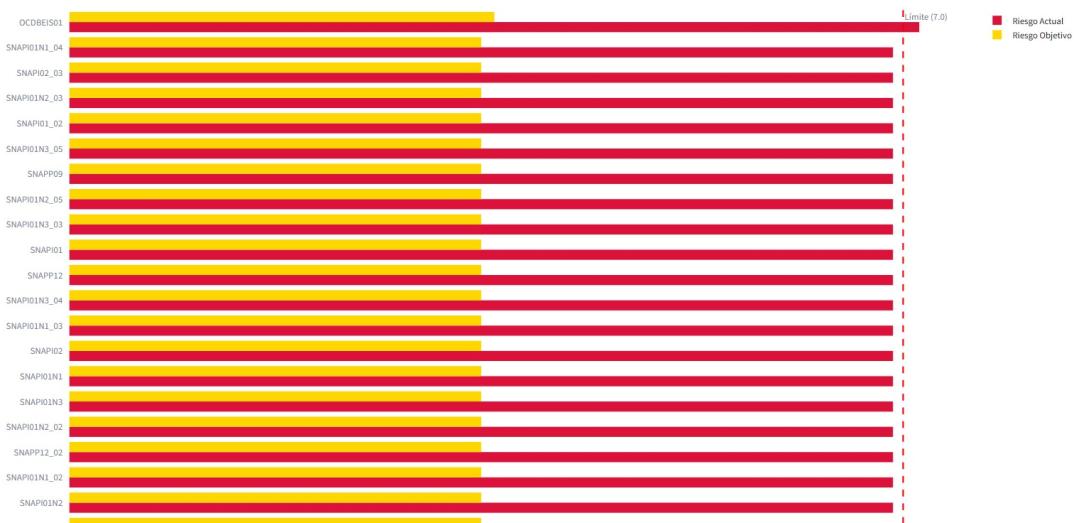


Ilustración 51: Dashboard comparativo riesgo inherente y residual

## Anexo 15

Matriz de Riesgos (Probabilidad x Impacto)

Como en Excel: Las celdas muestran cuántos riesgos caen en cada zona.

Matriz de Riesgos - Impacto vs Frecuencia (Probabilidad)



Ilustración 52: mapa de calor Magerit



## Anexo 16



Ilustración 53; Módulos principales del sistema implementado en entorno local

## Anexo 17

The screenshot shows a form titled 'Agregar Nuevo Activo' (Add New Asset). At the top, there are two buttons: '+ Agregar Individual' (Add Individual) and 'Carga Masiva' (Mass Import). The main section is titled 'Información General' (General Information) and contains the following fields:

|                     |                    |                       |
|---------------------|--------------------|-----------------------|
| Nombre del Activo * | Área Responsable * | Rack/Ubicación Física |
|                     | Infraestructura    |                       |
| Tipo de Activo *    | Finalidad de Uso * | Administradores       |
| Servidor Físico     |                    | 1 - +                 |
| Ubicación *         | Aplicación Crítica | (?)                   |
| Granados            | No Aplica          |                       |

Ilustración 54: Registro e inventario de elementos tecnológicos en el sistema



## Anexo 18

**Especificaciones Técnicas**

|                      |                           |                                  |
|----------------------|---------------------------|----------------------------------|
| Modelo               | Sistema Operativo         | Dependencias (otros activos)     |
| <input type="text"/> | <input type="text"/>      | <input type="text"/>             |
| Serial               | Plataforma Virtualización |                                  |
| <input type="text"/> | N/A                       | <input type="button" value="▼"/> |
| Fabricante           | Descripción Hardware      |                                  |
| <input type="text"/> | <input type="text"/>      |                                  |

Ilustración 55: Registro e inventario de especificaciones técnicas

## Anexo 19

**Mantenimiento y Soporte**

|                                 |                                 |                         |
|---------------------------------|---------------------------------|-------------------------|
| Fecha Instalación               | Vencimiento Garantía            | Contrato Mantenimiento  |
| <input type="text"/> YYYY/MM/DD | <input type="text"/> YYYY/MM/DD | <input type="text"/> Sí |
| Vigencia Tecnológica            | Proveedor Mantenimiento         |                         |
| <input type="text"/> Vigente    | <input type="text"/>            |                         |

Ilustración 56: Registro e inventario de mantenimiento y soporte



## Anexo 20

**Lista de Activos**

| Nombre_Activo | Tipo_Activo     | Ubicacion | Area_Responsable           | Finalidad_Uso  | Estado    |
|---------------|-----------------|-----------|----------------------------|----------------|-----------|
| BASTION_PROD  | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCADP01       | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCBEP01       | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCDBEIS01     | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCEIS01       | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCEIS01_02    | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCJCOG01      | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCJOB01       | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCREG01       | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |
| OCREG01_02    | Servidor Físico | UdlaPark  | Infraestructura servidores | Virtualización | Pendiente |

> Editar o Eliminar Activo

Ilustración 57: Listado de activos.

## Anexo 21

### Carga Masiva de Activos

Evaluación destino: inicio (EVA-001)

JSON (Recomendado) Excel Ayuda y Plantillas

#### Importar desde JSON

Formato JSON es el recomendado porque:

- Validación estricta de tipos
- Sin riesgo de macros o fórmulas
- Auditble (se genera hash del archivo)

Opción 1: Subir archivo JSON

Selecciona un archivo .json (?)

Drag and drop file here  
Limit 200MB per file • JSON Browse files

Ilustración 58: Carga masiva de activos JSON.



## Anexo 22

### Descargar Plantillas

Plantilla JSON:

 Descargar plantilla.json

> Ver contenido JSON

Plantilla Excel:

 Descargar plantilla.xlsx

*Ilustración 59: Plantillas de JSON*

## Anexo 23

### Catálogos de Referencia

Los siguientes catálogos son la base para identificar amenazas y recomendar controles. La IA utiliza estos catálogos para sus análisis.

 Amenazas

 Controles ISO 27002

 Salvaguardas

 Vulnerabilidades

*Ilustración 60: Catalogo de referencia.*



## Anexo 24

Disponibilidad (D)   Integridad (I)   Confidencialidad (C)   RTO   RPO   BIA

### ¿Qué tan crítico es que el activo esté disponible?

1. ¿Cuánto tiempo puede estar inoperativa esta VM sin afectar operaciones críticas?

- (3) Menos de 1 hora - Operaciones se detienen inmediatamente
- (2) Entre 1-4 horas - Afecta operaciones importantes
- (1) Entre 4 horas y 1 día - Afecta operaciones menores
- (0) Más de 1 día - No afecta operaciones críticas

2. ¿Cuántos usuarios/sistemas dependen directamente de esta VM?

- (3) Más de 100 usuarios o sistemas críticos
- (2) Entre 50-100 usuarios o sistemas importantes
- (1) Entre 10-50 usuarios o sistemas
- (0) Menos de 10 usuarios o sistemas no críticos

3. ¿La VM tiene configuración de alta disponibilidad (HA/vMotion)?

- (3) No - Sin HA, falla del host = caída de la VM
- (2) HA básico - Reinicio automático en otro host (minutos)
- (1) HA con DRS - Balanceo y migración automática
- (0) Fault Tolerance - Cero interrupción ante falla de host

*Ilustración 61: Preguntas Disponibilidad*

## Anexo 25

Disponibilidad (D)   Integridad (I)   Confidencialidad (C)   RTO   RPO   BIA

### ¿Qué tan crítico es mantener la integridad de los datos?

1. ¿Qué tan crítica es la integridad de los datos en esta VM?

- (3) Datos financieros/legales - Modificación causa pérdidas irreparables
- (2) Datos operacionales - Modificación causa problemas significativos
- (1) Datos de soporte - Modificación causa inconvenientes menores
- (0) Datos de prueba/desarrollo - Sin impacto

2. ¿La VM tiene snapshots y control de cambios implementado?

- (3) Sin snapshots ni control de cambios
- (2) Snapshots manuales ocasionales
- (1) Snapshots automáticos antes de cambios
- (0) Gestión completa con versionamiento y rollback

3. ¿Existen controles de acceso y auditoría en el hipervisor?

- (3) Acceso compartido sin auditoría
- (2) Acceso con roles básicos
- (1) RBAC completo con logs
- (0) RBAC + MFA + SIEM integrado

*Ilustración 62: Preguntas Integridad*



## Anexo 26

Disponibilidad (D)    Integridad (I)    Confidencialidad (C)    RTO    RPO    BIA

### ¿Qué nivel de confidencialidad requiere el activo?

#### 1. ¿Qué tipo de información maneja esta VM?

- (3) Información altamente confidencial (PII, financiera)
- (2) Información confidencial de uso interno restringido
- (1) Información interna de uso general
- (0) Información pública o sin restricciones

#### 2. ¿Los discos virtuales están encriptados?

- (3) No - Sin encriptación de discos
- (2) Parcial - Solo algunos discos críticos
- (1) Sí - Encriptación a nivel de storage
- (0) Sí - Encriptación a nivel de VM + gestión de llaves

#### 3. ¿La red virtual de esta VM está segmentada/aislada?

- (3) Red plana - Sin segmentación
- (2) VLANs básicas
- (1) Microsegmentación (NSX/similar)
- (0) Zero Trust con inspección de tráfico E-W

Ilustración 63: Preguntas de Confidencialidad

## Anexo 27

▼ Ver Respuestas del Cuestionario (Solo Lectura)

Disponibilidad    Integridad    Confidencialidad    RTO    RPO    BIA

1. ¿Cuánto tiempo puede estar inoperativa esta VM sin afectar operaciones críticas?  
→ Respuesta: (3) Menos de 1 hora - Operaciones se detienen inmediatamente

---

2. ¿Cuántos usuarios/sistemas dependen directamente de esta VM?  
→ Respuesta: (3) Más de 100 usuarios o sistemas críticos

---

3. ¿La VM tiene configuración de alta disponibilidad (HA/vMotion)?  
→ Respuesta: (3) No - Sin HA, falla del host = caída de la VM

---

4. ¿Cuál es el horario de operación crítica de esta VM?

Ilustración 64: Respuestas del cuestionario.



## Anexo 28

| Cuestionario D/I/C             | Resumen Valoraciones |
|--------------------------------|----------------------|
| <b>Resumen de Valoraciones</b> |                      |
| Total Activos                  | Valorados            |
| 72                             | 29                   |
| Pendientes                     | 43                   |

Ilustración 65: Resumen de valoraciones.

## Anexo 29

| Nombre_Activo | D | Valor_D | I | Valor_I | C | Valor_C | Criticidad | Criticidad_Nivel | RTO_Tiempo | RTO_Nivel | RPO_Tiempo       |
|---------------|---|---------|---|---------|---|---------|------------|------------------|------------|-----------|------------------|
| SNAPI01N2     | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| SNAPI01N1     | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCREG04       | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCREG03       | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCSSB01       | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| BASTION_PROD  | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCJCOG01      | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCDBEIS01     | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCREG02       | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |
| OCREG01       | A | 3       | A | 3       | A | 3       | 3          | Alta             | < 1 hora   | Alto      | 0 (cero pérdida) |

Ilustración 66: Tabla de valoraciones.



## Anexo 30

| Nombre_Activo | D | Valor_D | I | Valor_I | C | Valor_C | Criticidad | Criticidad_Nivel | RTO_Tiempo | RTO_Nivel | RPO_Tiempo |
|---------------|---|---------|---|---------|---|---------|------------|------------------|------------|-----------|------------|
| -             |   |         |   |         |   |         |            |                  |            |           |            |
| SNAPPF01N1_04 | M | 2       | M | 2       | M | 2       | 2          | Media            | 1-4 horas  | Medio     | < 1 hora   |
| SNCL02_02     | M | 2       | M | 2       | M | 2       | 2          | Media            | 1-4 horas  | Medio     | < 1 hora   |
| SNFILE01      | M | 2       | M | 2       | M | 2       | 2          | Media            | 1-4 horas  | Medio     | < 1 hora   |
| SNSQL10       | B | 1       | B | 1       | B | 1       | 1          | Baja             | 4-24 horas | Bajo      | 1-4 horas  |
| SNSQL07       | B | 1       | B | 1       | B | 1       | 1          | Baja             | 4-24 horas | Bajo      | 1-4 horas  |
| SNSQL01N1_07  | B | 1       | B | 1       | B | 1       | 1          | Baja             | 4-24 horas | Bajo      | 1-4 horas  |
| SNSQL10_02    | N | 0       | N | 0       | N | 0       | 0          | Nula             | > 24 horas | Nulo      | > 24 horas |
| SNSQL10_03    | N | 0       | N | 0       | N | 0       | 0          | Nula             | > 24 horas | Nulo      | > 24 horas |
| SNSQL10_04    | N | 0       | N | 0       | N | 0       | 0          | Nula             | > 24 horas | Nulo      | > 24 horas |
| SNSQL10_05    | N | 0       | N | 0       | N | 0       | 0          | Nula             | > 24 horas | Nulo      | > 24 horas |

Ilustración 67: Tabla de valoraciones 2

## Anexo 31

1. Criterios      2. Activos      3. Valoración D/I/C      4. Vulnerabilidades      5. Riesgo      6. Mapa Riesgos

### 🔒 Vulnerabilidades y Amenazas (Identificación con IA)

**Propósito:** La IA local identifica automáticamente vulnerabilidades y amenazas basándose en la CRITICIDAD del activo.

**Proceso MAGERIT con IA:**

1. La IA analiza el tipo de activo y su valoración D/I/C
2. Identifica amenazas relevantes del catálogo MAGERIT
3. Sugiere vulnerabilidades asociadas
4. Calcula la degradación según la criticidad

**Fórmulas:**

- $\text{Impacto}_D = \text{Valor}_D \times \text{Degradación}_D$
- $\text{Impacto}_I = \text{Valor}_I \times \text{Degradación}_I$
- $\text{Impacto}_C = \text{Valor}_C \times \text{Degradación}_C$
- $\text{IMPACTO\_TOTAL} = \text{MAX}(\text{Impacto}_D, \text{Impacto}_I, \text{Impacto}_C)$

**⚠ Importante:** El análisis IA se ejecuta una vez por activo. Los resultados alimentan el cálculo de riesgos y salvaguardas.

Ilustración 68: Formulas de las vulnerabilidades.



## Anexo 32

Análisis de Amenazas y Vulnerabilidades Realizado  
Se identificaron 6 amenazas/vulnerabilidades para este activo.  
Los resultados alimentan el cálculo de riesgos (Tab 5), salvaguardas (Tab 6) y mapa de riesgos (Tab 7).

**Amenazas Identificadas**

| Total Amenazas | Impacto Alto | Impacto Medio | Impacto Bajo |
|----------------|--------------|---------------|--------------|
| 6              | 5            | 1             | 0            |

**Lista de Amenazas**

| Código | Amenaza                                  | Vulnerabilidad  | Deg_D (%) | Deg_I (%) | Deg_C (%) | Impacto  |
|--------|--|---|-----------|-----------|-----------|----------|
| A.24   | Denegación de servicio                   | Firmware desactualizado: BIOS/UEFI sin actualizaciones de seguridad | 100       | 13        | 8         | 3.000000 |
| E.2    | Errores del administrador                | Hardware obsoleto: Equipos sin soporte del fabricante               | 76        | 63        | 24        | 2.280000 |
| A.11   | Acceso no autorizado                     | Puertos USB habilitados: Acceso físico a puertos sin control        | 65        | 72        | 72        | 2.160000 |
| A.5    | Suplantación de la identidad del usuario | Falta de TPM: Sin módulo de plataforma segura para cifrado          | 43        | 72        | 72        | 2.160000 |
| A.8    | Difusión de software dañino              | Discos sin cifrar; Almacenamiento local sin encriptación            | 70        | 59        | 32        | 2.100000 |
| E.1    | Errores de los usuarios                  | BIOS sin contraseña: Configuración de hardware accesible            | 65        | 59        | 32        | 1.950000 |

Ilustración 69: Amenazas identificadas.

## Anexo 33

**Registro de Vulnerabilidades y Amenazas**

💡 Pasa el mouse sobre Amenaza o Vulnerabilidad para ver la descripción completa

| Nombre_Activo | Criticidad | Cod_Amenaza | Cod_Vuln | Deg_D | Deg_I | Deg_C | Impacto |
|---------------|------------|-------------|----------|-------|-------|-------|---------|
| BASTION_PROD  | Alta       | A.24        | HW-V01   | 100%  | 13%   | 8%    | 3.00    |
| BASTION_PROD  | Alta       | E.2         | HW-V06   | 76%   | 63%   | 24%   | 2.28    |
| BASTION_PROD  | Alta       | A.11        | HW-V02   | 65%   | 72%   | 72%   | 2.16    |
| BASTION_PROD  | Alta       | A.5         | HW-V03   | 43%   | 72%   | 72%   | 2.16    |
| BASTION_PROD  | Alta       | A.8         | HW-V04   | 70%   | 59%   | 32%   | 2.10    |
| BASTION_PROD  | Alta       | E.1         | HW-V05   | 65%   | 59%   | 32%   | 1.95    |
| OCADP01       | Alta       | A.24        | HW-V01   | 100%  | 13%   | 8%    | 3.00    |
| OCADP01       | Alta       | E.2         | HW-V06   | 76%   | 63%   | 24%   | 2.28    |
| OCADP01       | Alta       | A.11        | HW-V02   | 65%   | 72%   | 72%   | 2.16    |
| OCADP01       | Alta       | A.5         | HW-V03   | 43%   | 72%   | 72%   | 2.16    |
| OCADP01       | Alta       | A.8         | HW-V04   | 70%   | 59%   | 32%   | 2.10    |

**Estadísticas**

| Total Registros | Alto Impacto (>1.5) | Activos Afectados |
|-----------------|---------------------|-------------------|
| 409             | 337                 | 68                |

Ilustración 70: Registro de amenazas y vulnerabilidades.



## Anexo 34

**⚠️ Advertencia sobre Recálculo**

Recalcular los riesgos afectará:

- El mapa de riesgos en el Tab 6
- La agregación de riesgos por activo en el Tab 7
- Las salvaguardas recomendadas en el Tab 8
- Todas las métricas derivadas de riesgos

Solo recalcule si cambió la frecuencia de amenazas o la valoración D/I/C.

Habilitar Recálculo 💡 Al habilitar el recálculo, podrá ejecutar el cálculo de riesgos nuevamente.

Ilustración 71: Advertencia del recálculo.

## Anexo 35

The screenshot displays the StreamLit interface for the TITA Matrix MAGERIT tool. On the left, there's a sidebar with navigation links: 'TITA Matriz', 'Evaluación' (with 'Evaluación inicial' selected), 'ID: EVA-001' (with 'Editar' and 'Eliminar' buttons), and 'Filtro de Activo' (with 'Aplica a todos los tabs', 'Todos los activos', and 'Todos los activos' selected). Below these are 'Resumen' sections showing 'Activos: 75' and 'Valoreados: 4%', and 'Vulnerab.: 18' and 'Urgentes: 0'. The main content area is titled 'Criterios de Valoración' and includes six tables corresponding to the MAGERIT dimensions: Disponibilidad (D), Confidencialidad (C), Integridad (I), Criticidad, Frecuencia, and Degradación. Each table maps levels (Nula, Baja, Media, Alta) to values and descriptions. At the top of the main content area, there's a navigation bar with tabs: 1. Índices, 2. Activos, 3. Valoración D/I/C, 4. Vulnerabilidades, 5. Riesgo, 6. Mapa Riesgos, 7. Riesgo Activos, 8. Salvaguardas, 9. Madurez, and 10. Comparativa.

Ilustración 72: Interfaz StreamLit.



## Anexo 36

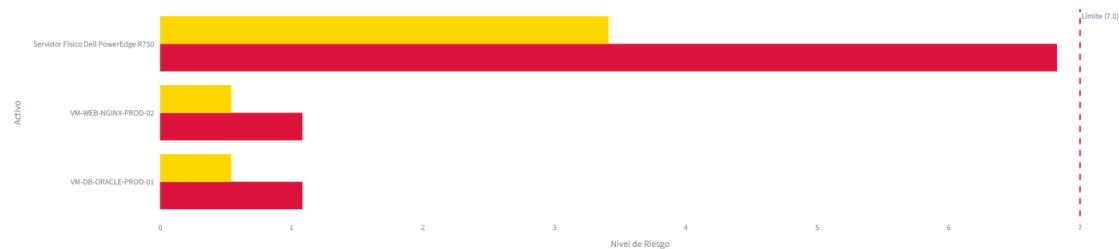


Ilustración 73: Dashboard interactivo.

## Anexo 37

### Leyenda de Interpretación

En el Radar:

- Área Azul: Riesgo actual de cada activo
- Línea Amarilla: Meta/Objetivo a alcanzar
- Línea Roja: Límite máximo aceptable

Estados:

- ✓ Cumple objetivo: Riesgo  $\leq$  Objetivo
- ⚠ Dentro de límite: Objetivo < Riesgo  $\leq$  Límite
- ✗ Excede límite: Riesgo > Límite (requiere acción urgente)

Ilustración 74: Interpretación.