Aplicación web para la gestión de riesgos de seguridad de la información en empresas de software de Yopal - Casanare

Fabian David Guevara Bello

Iván Andrés Holguín Orduz

Universidad Internacional Del Trópico Americano - Unitrópico

Facultad De Ingenierías

Programa De Ingeniería De Sistemas

Yopal

2025

Aplicación web para la gestión de riesgos de seguridad de la información en empresas de software de Yopal - Casanare

Fabian David Guevara Bello

Iván Andrés Holguín Orduz

Proyecto presentado para optar por el título de

Ingeniero De Sistemas

Nombre

Fabián Alberto Ayala Lozano

Universidad Internacional Del Trópico Americano-Unitrópico

Facultad De Ingenierías

Programa De Ingeniería De Sistemas

Yopal

2025

Dedicatoria De Fabian

A Dios, por ser mi guía y darme la fortaleza en cada paso. A mi mamá, la mujer a quien le debo todo, mi razón más grande para esforzarme. Sin ella nada de esto sería posible. Por su amor, su sacrificio y su fe inquebrantable en mí. Por ella y para ella es este trabajo, como un pequeño tributo a todo lo que ha hecho y sigue haciendo por mí.

Dedicatoria De Iván

A mi familia, por su apoyo constante y paciencia durante todo este proceso. Gracias por estar ahí en los momentos clave y por brindarme el respaldo necesario para alcanzar esta meta. Este logro también es de ustedes.

Agradecimientos

Queremos expresar nuestro más sincero agradecimiento a la Universidad UNITRÓPICO por estos cinco años de formación, crecimiento y oportunidades. A todos los profesores que nos enseñaron y que, de una u otra forma, hicieron parte de este trabajo de grado, gracias por compartir su conocimiento y por su apoyo constante. A nuestros compañeros de la universidad, por los momentos compartidos, las ideas, las discusiones y la amistad que enriquecieron esta etapa.

Tabla de Contenido

Glosario 9
Resumen 11
Abstract 12
Introducción 13
Planteamiento Del Problema 14
Justificación 18
  Formulación 20
Delimitación 21
Estado del Arte 25
Objetivos 36
  Objetivo General 36
  Objetivos Específicos 36
Marco Teórico 37
Metodología 49
Resultados 56
  Analisis. 57
  Diseño. 117
  Desarrollo. 148
  Pruebas 149
  Manual de Usuario 150
Impactos 151
Recomendaciones 152
Cronograma de Actividades 153
Presupuesto 154
Conclusiones 155
Referencias Bibliográficas 157
Anexos 163

Lista de Cuadros

Cuadro 1 Comparacion de Metodologías de Gestión de Riesgos 45
Cuadro 2 Cronograma de actividades..... 153

Lista de Figuras

Figura 1 Elementos del análisis de riesgos 62
Figura 2 Contexto del análisis de riesgos 64
Figura 3 Zonas de riesgo 71
Figura 4 Método de Análisis de Riesgos 72
Figura 5 Lista de control de Método de Análisis de Riesgos 72
Figura 6 Criterios de valoración de un activo 75
Figura 7 Definición del proyecto general 96
Figura 8 Gestión y creación de usuarios 98
Figura 9 Creación de la gestión del riesgo de la empresa 99
Figura 10 Gestión de activos 100
Figura 11 Valoración de activos 101
Figura 12 Priorización de activos 102
Figura 13 Análisis del riesgo de manera general 104
Figura 14 Registro de amenazas asociadas a los activos 105
Figura 15 Registro de vulnerabilidades asociadas a las amenazas 106
Figura 16 Registro de consecuencias 107
Figura 17 Análisis de controles existentes 108
Figura 18 Evaluación de impacto y probabilidad de ocurrencia 109
Figura 19 Caracterización del riesgo 110
Figura 20 Tratamiento del riesgo de manera general 111
Figura 21 Mapeo de controles ISO 27002 112
Figura 22 Cálculo del riesgo residual 113
Figura 23 Plan de tratamiento del riesgo 114
Figura 24 Generación de reportes 116
Figura 25 Ciclo de desarrollo de la arquitectura del software 118
Figura 26 Modelo de comunicación Cliente-Servidor 121
Figura 27 Patrón Modelo Vista Controlador (MVC) 123
Figura 28 Empresas – Superusuario – Invitaciones 127
Figura 29 Empresas, Activos, ValoracionActivo y DependenciaActivo 128
Figura 30 Activos, Vulnerabilidades, Amenazas, Riesgos. 129
Figura 31 Entidades entre Riesgos, TratamientoRiesgo, DueñoRiesgo, EvaluacionRiesgo 130
Figura 32 Esquema de la base de datos 131
Figura 33 Diagrama de clases de la aplicación 132
Figura 34 Diagrama de Componentes de la Aplicación 135
Figura 35 Diagrama de Despliegue de la Aplicación 137
Figura 36 DFD Nivel 0 139
Figura 37 DFD Nivel 1 - Registro de Activos 141
Figura 38 DFD Nivel 2 Análisis del riesgo 143
Figura 39 DFD Nivel 3- Tratamiento del Riesgo 145

Lista de Tablas

Tabla 1 Historia de Usuario Creación Usuario Administrador 99
Tabla 2 Historia de usuario Creación de la Gestión de Riesgo General 100
Tabla 3 Historia de Usuario de Registro de activos de la empresa 101
Tabla 4 Historia de Usuario de Valoración de activos de información 102
Tabla 5 Historia de Usuario Priorización y Filtrado de Activos de Información 103
Tabla 6 Historia de Usuario de Análisis de Riesgo 104
Tabla 7 Historia de Usuario de Ingreso de amenazas 105
Tabla 8 Historia de Usuario de Ingreso de Vulnerabilidades 106
Tabla 9 Historia de Usuario de Registro de consecuencias 107
Tabla 10 Historia de Usuario de controles existentes 108
Tabla 11 Historia de Usuario de Evaluación de impacto y probabilidad de amenazas 109
Tabla 12 Historia de Usuario de Caracterización del Riesgo 110
Tabla 13 Historia de Usuario de Gestión del Tratamiento de Riesgos 111
Tabla 14 Historia de Usuario de Mapeo de Controles de Seguridad Basados en ISO 27002 112
Tabla 15 Historia de Usuario de Cálculo de Riesgo Residual 114
Tabla 16 Historia de Usuario de definición del Plan de Tratamiento de Riesgos 115
Tabla 17 Historia de Usuario de Generación de Reportes 116
Tabla 18 Relación entre las entidades Empresas – Superusuario – Invitaciones 127
Tabla 19 Relación entre las Empresas, Activos, ValoracionActivo y DependenciaActivo 128
Tabla 20 Relación entre Activos, Vulnerabilidades, Amenazas, Riesgos 129
Tabla 21 Relación Riesgos, TratamientoRiesgo, DueñoRiesgo, EvaluacionRiesgo 130
Tabla 22 Presupuesto de la Aplicación 154

Lista de Anexos

Anexo A Árbol del problema 163
Anexo B Árbol De Objetivos 164
Anexo C Los 5 Por qué 165
Anexo D Cadena de Valor 166
Anexo E Matriz de Expectativas y Necesidades de la Aplicación 167
Anexo F Solicitud de Información sobre empresas de Software 168
Anexo G Respuesta por parte de la Cámara de Comercio 169
Anexo H Video Entrevista Empresa Delta Solutions 170
Anexo I Información Recopilada Delta Solutions 171
Anexo J Video Entrevista Empresa Puntualtic 172
Anexo K Información Recopilada Puntualtic 173
Anexo L Matriz de Revisión de Literatura 174
Anexo M Acta de Reunión Delta Soluciones 175
Anexo N Acta de Reunión Inicial Puntualtic 176
Anexo O Socialización Final del Software 177
Anexo P Validación Final del Software Puntualtic 178
Anexo Q Validación Final del Software Puntualtic 179

Glosario

Activo: Es cualquier cosa tangible e intangible que tiene valor para la organización, por lo que debe ser protegida (Instituto Colombiano de Normas Técnicas y Certificación [ICONTEC], 2009).

Amenaza: Es una acción que se aprovecha de la vulnerabilidad de un sistema, capaz de comprometer un activo o activos de información (ISO/IEC 27000, 2018).

Análisis de gestión de riesgos: Es un estudio basado en procedimientos e investigaciones que permite a una organización identificar, evaluar y mitigar los riesgos a los que están expuestos los activos, valorando tanto las amenazas como las salvaguardas existentes para luego valorar su riesgo e impacto (Magerit, 2016).

Autenticidad: Es una característica de un dato o servicio en donde se garantiza que es auténtico y viene de donde dice ser. La autenticidad se logra mediante la verificación de la identidad a través de diferentes mecanismos de autenticación, como contraseñas, certificados digitales, biometría, etc. (Magerit, 2016).

Confidencialidad: Es una capacidad que se refiere a blindar un activo o servicio a personal autorizado (ISO/IEC 27000, 2018).

Control: Es una medida de protección diseñada para reducir el riesgo de que una amenaza se materialice sobre un activo (Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) & de Normas Técnicas y Certificación (ICONTEC), 2009).

Disponibilidad: Es una capacidad de un sistema para estar activo y disponible a los usuarios autorizados (ISO/IEC 27000, 2018).

Integridad: Es una protección contra la modificación y/o alteración de un dato por usuarios que no han sido autorizados para ello (ISO/IEC 27000, 2018).

MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información es una metodología que ayuda al análisis de los riesgos del sistema de información enfocado principalmente a TI, donde se busca conocer los riesgos para poder afrontarlos y conocer el riesgo al que están sometidos los elementos de trabajo (Magerit, 2016).

PYMES: Son definidas según las leyes colombianas como aquellas que poseen una planta de personal inferior a 200 empleados y activos totales de hasta 30.000 salarios mínimos mensuales legales vigentes, representan el 99,5% del parque empresarial nacional en Colombia (Del Do et al., 2023; Franco-Ángel & Urbano, 2019).

Riesgo: Es el efecto de la incertidumbre sobre los objetivos de la empresa (Organización Internacional de Normalización, 2018).

Seguridad de la información: Es la protección de la información en todas sus formas, tanto física como digital. su objetivo es priorizar la disponibilidad, integridad y confidencialidad de los datos, lo cual se logra aplicando un conjunto apropiado de controles, políticas y procesos dentro de una organización (Oscar, 2019).

SGSI (Sistema de Gestión de Seguridad de la Información): Un Sistema de Gestión de Seguridad de la Información (SGSI) es un marco de principios y procedimientos diseñados para identificar y gestionar riesgos, estableciendo los pasos necesarios para mitigar dichos riesgos. Este sistema asegura que las empresas adopten medidas sistemáticas para proteger sus datos e información, abarcando cualquier tipo de información que necesite ser resguardada.

Vulnerabilidad: Es una debilidad en un sistema de información producto de un fallo o bug que puede ser explotada por una amenaza (ISO/IEC 27000, 2018).

Empresas de software: Es una empresa de la industria del software cuya misión es el desarrollo de software para sus clientes de acuerdo a los requisitos específicos que aquel le solicita.

Resumen

Este trabajo de grado abordo el desarrollo de un software especializado para la gestión de riesgos de seguridad de la información enfocado a empresas de desarrollo de software en Yopal-Casanare. Estas empresas se ven afectadas por la falta de procesos, tecnologías y formación sólidas en materia de seguridad de la información, lo que aumenta su exposición a posibles ataques y pérdidas de datos. El objetivo de este proyecto fue desarrollar una aplicación web que ayudara a la gestión de riesgos de seguridad de la información en las empresas de software de Yopal. Se diseñó una arquitectura de software escalable y segura, junto con una interfaz de usuario intuitiva y accesible. Además, se documentó detalladamente el proceso de desarrollo. El trabajo de grado se centró en estudios y análisis de las amenazas actuales en seguridad de la información y las soluciones tecnológicas disponibles para la gestión de riesgos. La metodología utilizada integró diversas normativas y metodologías de análisis de riesgos, garantizando una evaluación precisa y continua de los riesgos, reduciendo costos asociados a incidentes de seguridad y aumentando la competitividad de estas empresas y promoviendo una mayor cultura de seguridad de la información en el entorno empresarial.

Palabras claves: Ciberseguridad, Riesgos de seguridad de la información, Gestión de los riesgos, Aplicación Web, Empresas de software.

Abstract

Currently, the increasing use of technology and digitization brings significant benefits in terms of efficiency and competitiveness, but also presents significant challenges in the management and protection of information. This thesis addresses the development of specialized software for information security risk management focused on software development companies in Yopal-Casanare. These companies are affected by the lack of sound information security processes, technologies and training, which increases their exposure to possible attacks and data loss. The objective of this project was to develop a web application to help manage information security risks in software companies in Yopal. A scalable and secure software architecture was designed, along with an intuitive and accessible user interface. In addition, the development process was documented in detail. The proposal focused on studies and analysis of current information security threats and the technological solutions available for risk management. The methodology used integrated various regulations and risk analysis methodologies, ensuring an accurate and continuous assessment of risks, reducing costs associated with security incidents and increasing the competitiveness of these companies and promoting a greater culture of information security in the business environment.

Keywords: Cybersecurity, Information security risks, Risk management, Web application, Software Companies.

Introducción

La rápida adopción de tecnologías digitales y la creciente dependencia de la información han convertido a la seguridad de la información en una prioridad crítica para las organizaciones (Álvarez et al., 2022). Este fenómeno es especialmente relevante para las empresas de desarrollo de software en Yopal, las cuales gestionan grandes volúmenes de datos y productos informáticos como activo de información. Aunque estas empresas son claves en el desarrollo tecnológico de la región, a menudo carecen de recursos y conocimientos especializados para implementar medidas robustas de seguridad.

Los antecedentes de esta investigación muestran que las PYMES colombianas enfrentan desafíos particulares en la gestión de la seguridad de la información. Estudios recientes indican que estas empresas tienden a subestimar la importancia de proteger sus datos y sistemas, lo que las deja expuestas a una variedad de ciberataques. Este problema se agrava por la falta de procesos, tecnologías y entrenamientos adecuados en seguridad de la información, lo cual incrementa su vulnerabilidad (Álvarez et al., 2022).

El presente trabajo de grado se fundamentó en la necesidad crítica de gestionar los riesgos de seguridad de la información producto de las amenazas cibernéticas, mediante el desarrollo de una aplicación web de gestión de riesgos de seguridad de la información. La aplicación es una herramienta accesible y efectiva, diseñada para permitir a las empresas de desarrollo de software identificar, evaluar y mitigar sus riesgos de seguridad de forma integral. La implementación de esta aplicación tuvo un impacto significativo, mejorando la gestión de riesgos. Además, ayudó a promover una mayor cultura de seguridad en la región, permitiendo que las empresas pudieran aspirar a certificaciones como la norma ISO 27001, elevando sus estándares de seguridad y confianza en el mercado.

Planteamiento Del Problema

En la actualidad, el uso de internet y tecnología es cada vez más constante, las personas acuden a internet como principal fuente de información, entretenimiento e interacción social (Martínez et al., 2020). Las organizaciones, por su parte, se acoplan cada vez más a los cambios tecnológicos actuales, realizando la transición de sistemas de información físicos o basados en papel a sistemas de información digitales (Álvarez et al., 2022). En este contexto, las Pequeñas y Medianas Empresas (PYMES) también están experimentando esta transición, especialmente aquellas cuyo principal activo primario es la información. Estas empresas reconocen la importancia de digitalizar sus procesos para mejorar la eficiencia y competitividad, aunque este cambio conlleva desafíos significativos en términos de gestión y protección de la información (Del Do et al., 2023).

La digitalización trae consigo numerosos beneficios, como la eficiencia en la gestión de la información, la reducción de costos y la facilidad de acceso a los datos (Calle Herencia, 2022). Sin embargo, también introduce nuevos desafíos y riesgos, especialmente en el ámbito de la seguridad de la información. A medida que las organizaciones digitalizan sus procesos, actividades de negocio principales y almacenan más datos en formato digital, se vuelven fácilmente blanco de amenazas cibernéticas tales como el malware, el phishing, el ransomware y los ataques de denegación de servicio (DoS).

Los ataques cibernéticos pueden traer consecuencias devastadoras para las organizaciones, incluyendo la perdida de información sensible, el robo de la propiedad intelectual, daños a la reputación y pérdidas financieras significativas (Banco Interamericano de Desarrollo, 2020). Según SonicWall Cyber Threat Report En 2023, los investigadores de amenazas de SonicWall Capture Labs registraron 6.060 millones de ataques de malware, un aumento interanual del 11%. Esto marca el volumen de ataque global más alto para cualquier año desde 2019, lo que indica que los niveles de malware han vuelto a subir a sus niveles

prepandémicos a medida que los actores de amenazas son más abundantes, ingeniosos y activos. En 2022, las organizaciones de todo el mundo detectaron 493,33 millones de ataques de ransomware. Mientras que el phishing sigue siendo el ciberataque más común con aproximadamente 3.400 millones de correos spam diarios. Además de que el coste medio de las brechas resultantes de credenciales robadas o comprometidas ascendió a 4,50 millones de dólares (Inc, 2024; Threat, 2023).

En Colombia, la cifra de ciberdelitos denunciados durante el 2022 ha crecido un 20.5% respecto al 2021 además de que Los sectores industriales, gobierno, educación y salud, fueron los más comprometidos en ataques durante el 2022 un 67% del total de denuncias se registran por parte de empresas y entidades del sector público y privado. Las PYMES continúan siendo el sector más vulnerable a los ciberataques en Colombia. Esto se debe principalmente a las débiles estrategias de ciberseguridad implementadas por los responsables de estas organizaciones. En muchos casos, esto ocurre porque no se reconoce la necesidad de incorporar la ciberseguridad como un factor estratégico dentro de los costos operativos del negocio, o por la falta de conocimiento sobre las amenazas cibernéticas por parte de quienes gestionan las operaciones diarias (Bautista García & Aguilar, 2023).

Debido a esta situación, es fundamental que las organizaciones fortalezcan sus sistemas de gestión de la información. Una gestión eficaz de la información contribuye a proteger los datos, disminuir la exposición a ciberataques, cumplir con las normativas y estándares de la industria, mejorar la confianza de clientes y socios, y garantizar la continuidad operativa en caso de incidentes de seguridad (Giraldo,2022). Para ello existen diferentes metodologías de análisis y tratamiento de los riesgos tales como Octave, Magerit, Mehari, NIST SP 800-30, Coras, Cramm y Ebios entre otros, que permiten una gestión eficiente y efectiva de los riesgos de seguridad de la información y ciberseguridad en las que se pueden ver envueltas las organizaciones (Novoa et al., 2022).

Sin embargo, al implementar estas normas para fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI), el proceso puede volverse obsoleto y lento, especialmente cuando se realiza mediante el uso de papel o formatos de Excel. Estos métodos tradicionales son difíciles de manejar, para las PYMES en Colombia y particularmente para las empresas de desarrollo de software en Yopal, ya que a medida que aumenta la cantidad de información digital que necesitan proteger, la gestión manual se vuelve más propensa a errores humanos y menos eficiente. Esto es especialmente perjudicial para estas empresas, donde la información es uno de los activos más valiosos. La incapacidad de gestionar eficazmente la seguridad de la información puede llevar a resultados adversos, como la pérdida de datos críticos, el incumplimiento de normativas, y una mayor exposición a ciberataques, comprometiendo así la competitividad y la continuidad de sus operaciones.

Aunque existen antecedentes de planes de tratamientos de riesgos y seguridad de la información, así como guías de implementación para un SGSI óptimo y escalable, como la "Guía de Gestión de Riesgos" proporcionada por el MinTIC, que establece un marco claro para la gestión de riesgos de seguridad de la información (Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, 2020) estos recursos, aunque valiosos, no son suficientes por sí solos. La guía facilita un orden en el proceso de gestión de riesgos, pero la criticidad y el volumen de información que manejan las organizaciones de software hoy en día requieren herramientas más avanzadas y eficientes.

Si bien el panorama global y nacional revelo la creciente importancia de la gestión de riesgos de seguridad de la información, se observó una carencia significativa de estudios y datos específicos centrados en el contexto de las empresas de desarrollo de software en Yopal-Casanare. Aunque existían investigaciones sobre las tendencias generales de ciberseguridad y las metodologías de gestión de riesgos, la información detallada sobre los desafíos particulares que enfrentaban estas empresas locales era muy limitada. Esta falta de

información representa un problema crucial, ya que impide una comprensión profunda de las vulnerabilidades y necesidades específicas de este sector en la región. Sin embargo, también presento una oportunidad significativa para este trabajo de grado. Al abordar esta brecha de conocimiento, este trabajo de grado no solo proporciona una solución práctica a través del desarrollo de la aplicación web, sino que también busca servir como una valiosa fuente de información y un catalizador para futuras investigaciones en el área.

Justificación

La digitalización ha transformado la gestión de la información en las organizaciones brindando numerosos beneficios, pero también exponiéndolas a un número creciente de ciberataques. Las PYMES en Colombia, entre ellas las empresas de desarrollo de software de Yopal, enfrentan una brecha significativa entre sus actuales prácticas de gestión de seguridad de la información y el estado deseado de una protección robusta y eficiente. La dependencia de métodos tradicionales, como el uso de papel y formatos de Excel, es insuficiente y propensa a errores humanos, resultando en una gestión ineficaz frente a la complejidad y volumen de datos digitales. Esta situación aumenta la vulnerabilidad a ataques cibernéticos y compromete la capacidad de estas organizaciones para responder adecuadamente a incidentes de seguridad.

El proyecto se propuso cerrar esta brecha mediante la creación de una aplicación web que optimizará el proceso de gestión de riesgos de seguridad de la información. Esta herramienta permitió a las empresas que hicieron partes de las pruebas, realizar evaluaciones de riesgos de manera más precisa y rápida, mejorando así su capacidad para monitorizar y proteger sus activos digitales de manera continua. La implementación exitosa trajo beneficios concretos como la mejora de la seguridad, reducción de errores humanos, eficiencia operativa, cumplimiento normativo, aumento de la confianza de clientes y socios.

La selección de empresas de desarrollo de software en Yopal como objeto de estudio para este proyecto se justificó por dos razones principales. Primero, uno de los activos más valiosos de estas empresas es la información y sus productos digitales, lo que las hace particularmente vulnerables a los riesgos de seguridad de la información. La protección de estos activos es crítica para la sostenibilidad de estas empresas. Segundo, las empresas de software, al estar en la vanguardia del desarrollo tecnológico, son un excelente punto de partida para innovaciones en la gestión de riesgos de seguridad. Implementar una solución de gestión

de riesgos en este entorno no solo ayuda a proteger los activos informáticos, sino que también promueve una cultura de seguridad cibernética que puede ser adaptada y extendida a otros sectores.

La aplicación se alineó con los objetivos estratégicos de estas empresas, fortaleciendo su competitividad y sostenibilidad en un entorno digital desafiante. La integración de metodologías reconocidas internacionalmente respalda la visión de ser organizaciones resilientes y adaptadas a las mejores prácticas de la industria. La relevancia y oportunidad del proyecto se acentúan en el contexto actual, donde el aumento de ciberataques y la acelerada adopción de tecnologías digitales, impulsada por la pandemia de COVID-19, hacen que la protección de la información sea más crucial que nunca.

Formulación

¿Cómo puede una aplicación web para la gestión de riesgos de seguridad de la información contribuir al análisis y tratamiento de riesgos en las empresas de desarrollo de software de Yopal-Casanare?

Delimitación

El proyecto se centró en el desarrollo de una aplicación web para la gestión de riesgos de seguridad de la información en las empresas de desarrollo de software de Yopal-Casanare. Geográficamente, el alcance del proyecto estuvo limitado al Municipio de Yopal, abarcando la industria del desarrollo de software. El proyecto se desarrolló y ejecutó en un periodo de 6 meses abarcando el ciclo de vida del desarrollo de software, desde la fase inicial de análisis, diseño, desarrollo, despliegue y pruebas finales. Funcionalmente, el proyecto se concentró en la identificación, valoración, evaluación y tratamiento de riesgos de seguridad de la información.

El proyecto incluyó la Integración de metodologías de análisis de riesgos como: MAGERIT, normas de seguridad de la información de carácter internacional como la ISO 27001:2022, 27002:20022 y ISO 27005:2018, a su vez como una evaluación continua y mejoras basadas en los comentarios de los usuarios. Para la ejecución del proyecto, se contó con un grupo de estudiantes (2) y el director de trabajo de grado. Los recursos tecnológicos abarcaron infraestructura de desarrollo y prueba en la nube, así como herramientas de desarrollo de software y bases de datos. Además, se dispuso de recursos materiales, como equipo y software necesarios para el desarrollo y prueba del proyecto.

El proyecto enfrentó ciertas limitaciones, tales como restricciones presupuestarias que limitaron la extensión de funcionalidades adicionales y un tiempo limitado para el desarrollo, lo que requirió una gestión eficiente del cronograma. Además, se contó con recursos humanos limitados, lo que implicó la necesidad de equilibrar la carga de trabajo y asegurar la calidad del producto final.

Dentro de las exclusiones y límites de la aplicación de gestión de riesgos de seguridad de la información se encuentran las siguientes:

Desarrollo de una Aplicación Móvil

La aplicación es exclusivamente una plataforma web. No se incluye el desarrollo de una versión móvil (iOS, Android) ni aplicaciones híbridas.

Implementación De Hardware Adicional

El proyecto no incluyo la compra, instalación o configuración de hardware adicional (servidores, firewalls, dispositivos de red, etc.). Todo se realizó a través de Digital Ocean que Proporciono herramientas y recursos para crear, desplegar y gestionar la aplicación incluyendo el servidor virtual.

Detección automática de vulnerabilidades

La aplicación no realiza escaneos automáticos para descubrir vulnerabilidades en sistemas, redes o aplicaciones. El usuario debe ingresar manualmente la información sobre vulnerabilidades identificadas.

Implementación automática de controles de seguridad

La aplicación no implementa controles de seguridad de manera automática (por ejemplo, no aplica parches, no configura firewalls, no habilita cifrado). Solo sugiere controles basados en los riesgos identificados y basados en diferentes normas tales como ISO 27002, pero su implementación depende del usuario.

Conexión a APIs externas para acceder a información de otros sistemas

La aplicación no se conecta automáticamente a APIs externas (por ejemplo, SIEMs, escáneres de vulnerabilidades, bases de datos de amenazas) para obtener información. El usuario debe ingresar manualmente los datos relevantes.

Automatización completa del proceso de gestión de riesgos

La aplicación no automatiza la totalidad del proceso de gestión de riesgos, manteniendo la necesidad crucial de la intervención de un profesional en diversas etapas clave. En primer lugar, se requiere la experticia de un profesional para ingresar y validar la información concerniente a los activos de información, las amenazas potenciales y las vulnerabilidades existentes dentro de la organización. En segundo lugar, la toma de decisiones estratégicas sobre el tratamiento de los riesgos identificados (ya sea optar por la mitigación, la transferencia, la evitación o la aceptación) siempre requerirá el juicio y el conocimiento de un experto. Finalmente, la implementación efectiva y el monitoreo continuo de los controles de seguridad definidos también son tareas que demandan la supervisión y la acción de un profesional especializado en la gestión de riesgos de seguridad de la información.

Gestión de incidentes en tiempo real

La aplicación no monitorea sistemas en tiempo real ni genera alertas automáticas sobre incidentes de seguridad. Su enfoque es la gestión proactiva de riesgos, no la respuesta reactiva a incidentes.

Auditorías automáticas de cumplimiento

La aplicación no realiza auditorías automáticas para verificar el cumplimiento de normativas (por ejemplo, ISO 27001, GDPR, PCI DSS). Solo proporciona herramientas para documentar y gestionar los controles necesarios.

Análisis predictivo de riesgos

La aplicación no utiliza Inteligencia Artificial o Machine Learning para predecir riesgos futuros. Su enfoque es la gestión de riesgos basada en datos históricos y actuales proporcionados por el usuario.

Soporte técnico 24/7

El proyecto no incluye soporte técnico continuo o atención 24/7 para resolver problemas de la aplicación. Se proporcionará soporte básico durante la fase de implementación inicial.

Monitoreo y validación de la eficacia de los controles

Aunque el monitoreo es parte de la gestión del riesgo, la aplicación no puede determinar por sí sola si la implementación de un control es eficaz. Esta validación debe ser realizada por un profesional, quien debe analizar los resultados y tomar decisiones basadas en el contexto y los datos proporcionados.

Integración

En su versión inicial, la aplicación no se integra con ningún otro software externo, como SIEMs, escáneres de vulnerabilidades, o herramientas de monitoreo. Esto significa que los usuarios deberán ingresar manualmente los datos relevantes en la plataforma. Las integraciones con herramientas externas podrían considerarse en futuras versiones, dependiendo de las necesidades y feedback de los usuarios.

Estado del Arte

En el presente apartado se realizó una revisión exhaustiva de los trabajos relacionados y de las aplicaciones existentes en el ámbito de la seguridad de la información y ciberseguridad, con un enfoque particular en la gestión de riesgos de seguridad de la información dentro de empresas de desarrollo de software. Esta revisión tuvo como objetivo identificar las herramientas y metodologías más efectivas utilizadas en ese momento para la protección de datos y la mitigación de amenazas en entornos digitales. Además, se exploraron las soluciones digitales que surgieron para abordar los desafíos específicos de la gestión de riesgos en el sector del desarrollo de software, considerando tanto las tendencias recientes como las mejores prácticas adoptadas por la industria. Para lograr este objetivo, se diseñó un Protocolo de Revisión Sistemática de Literatura. La Fase 1 de este protocolo, denominada Planificación de la Revisión, estableció como objetivo principal explorar y analizar las herramientas y metodologías actuales para la gestión de riesgos de seguridad de la información, haciendo énfasis en la aplicación de soluciones digitales en empresas cuyo activo de información principal recaía en la propia información, y no en activos secundarios. De esta planificación surgen las siguientes Preguntas de Investigación:

- ¿Cuáles son las herramientas más efectivas para la gestión de riesgos de seguridad de la información en PYMES según la literatura reciente?
- ¿Qué metodologías se han implementado exitosamente en la gestión de riesgos de seguridad de la información y cómo han evolucionado con el tiempo?

Para la selección de la literatura, se establecieron criterios de inclusión y exclusión. Se incluyeron estudios publicados en revistas científicas e información de fuentes locales oficiales entre los años 2020 y 2024. Adicionalmente, se consideraron artículos en inglés (clasificados de Q1 a Q3 según el portal ScimagoJR) y en español (clasificados como A1-B según el portal oficial de PubliIndex) que abordaran herramientas, metodologías o aplicaciones relacionadas

con la gestión de riesgos de seguridad de la información. La revisión también incorporó investigaciones empíricas, revisiones de literatura, estudios de casos y artículos teóricos que ofrecieran información relevante sobre la temática. Por otro lado, se definieron como criterios de exclusión los artículos no revisados por pares, así como documentos no académicos, tales como blogs, opiniones o informes no validados científicamente. Finalmente, las palabras clave utilizadas para la búsqueda y recuperación de información fueron: Gestión de riesgos de seguridad de la información, Ciberseguridad, Herramientas de gestión de riesgos, Metodologías de gestión de riesgos y Soluciones digitales para la seguridad de la información.

Con esta revisión, Además se busca poner en evidencia la escasa información existente sobre el desarrollo de aplicaciones de gestión de riesgos específicamente diseñadas para empresas de software, así como la limitada disponibilidad de estudios relacionados con la seguridad de la información en PYMES, particularmente en aquellas localizadas en Yopal, Casanare. Este análisis es fundamental para resaltar la necesidad de nuevas investigaciones y desarrollos tecnológicos que aborden las necesidades particulares de estas empresas, cuya principal vulnerabilidad recae en la protección de su información digital y sus productos.

Uno de los trabajos más relevantes en el ámbito de la seguridad de la información es el artículo titulado: Modelo de apoyo a la toma de decisiones en materia de ciberseguridad para diseñar un sistema de seguridad informática basado en el análisis de riesgos y la ciberseguridad (Razikin & Soewito, 2022).

El cual presenta un modelo de soporte para la toma de decisiones en ciberseguridad, basado en el análisis de riesgos y un marco de ciberseguridad. Este estudio propone un enfoque metodológico estructurado que permite a las organizaciones diseñar sistemas de seguridad en tecnologías de la información, optimizando los recursos y minimizando los riesgos de ciberataques. Este estudio señala la eficacia de la norma **ISO/IEC 27001** para mitigar los

ciberataques, particularmente en empresas que operan en sectores minoristas, lo cual subraya la capacidad de esta norma para adaptarse a diferentes contextos empresariales. Su implementación en el sector de desarrollo de software es igualmente beneficiosa, dado el aumento significativo de las ciber amenazas, lo que refuerza la necesidad de mejorar las medidas de seguridad. La relevancia de este enfoque radica en su capacidad para integrarse en entornos empresariales donde la información es el activo más importante, como es el caso de las empresas de desarrollo de software. La aplicación de este modelo es beneficiosa para el contexto de las empresas de software en Yopal, mejorando su capacidad de respuesta ante amenazas cibernéticas.

Otro aporte relevante en el campo de la seguridad de la información es el estudio titulado Marco y sistemas de seguridad de la información para pequeñas y medianas empresas (PYME): Un enfoque de meta análisis (AL-Dosari & Fetais, 2023) que presenta un enfoque exhaustivo para la evaluación de marcos de trabajo y sistemas de seguridad de la información aplicables a pequeñas y medianas empresas (PYMES). Este trabajo, basado en un meta-análisis de estudios previos, subraya la importancia de adaptar los sistemas de seguridad de la información a las necesidades particulares de las PYMES, resaltando los desafíos que enfrentan en términos de recursos limitados y menor capacidad de inversión en ciberseguridad.

El análisis del artículo muestra que los marcos de seguridad de la información deben ser escalables y flexibles, lo que resulta altamente relevante para empresas de desarrollo de software, como las que operan en Yopal. Al igual que las PYMES estudiadas, estas empresas enfrentan retos significativos en la protección de sus activos digitales debido a restricciones presupuestarias y la rápida evolución de las amenazas cibernéticas. El estudio también destaca la necesidad de implementar medidas personalizadas de seguridad en función del riesgo identificado y la capacidad organizativa, lo que coincide con el trabajo de grado de como una solución adaptable y centrada en las particularidades de cada empresa.

La adopción de estos marcos y sistemas sirvió como una estrategia eficaz para mitigar las vulnerabilidades en empresas de desarrollo de software a través de la aplicación, donde el principal activo es la información. Además, el enfoque presentado en el artículo refuerza la importancia de desarrollar herramientas tecnológicas que permitan una gestión de riesgos más eficiente y accesible para organizaciones con recursos limitados.

En el contexto de la gestión de riesgos de seguridad de la información en empresas de software, el artículo Estudio comparativo de las medidas de seguridad en las aplicaciones web para empresas de software (Shahid et al., 2022) realiza un análisis comparativo de diversas herramientas y metodologías utilizadas para gestionar la seguridad en aplicaciones web específicas para este tipo de organizaciones. Este estudio destaca cómo las empresas de desarrollo de software, cuyo principal activo es la información y el código fuente, deben implementar medidas robustas de seguridad en sus aplicaciones para protegerse de ciberamenazas crecientes. El estudio comparativo sostiene que, aunque existen múltiples herramientas para asegurar aplicaciones web, no todas son igualmente efectivas en función del contexto organizativo y los recursos disponibles. En particular, aquellas empresas que operan en entornos con recursos limitados, requieren soluciones que no solo sean efectivas, sino también accesibles y fáciles de implementar. Entre las metodologías más efectivas identificadas en el estudio se incluyen marcos basados en el análisis de riesgos y soluciones de monitoreo continuo, que permiten a las empresas de software identificar y mitigar vulnerabilidades de manera proactiva.

Un estudio clave en el ámbito de la gestión de riesgos de ciberseguridad en las pequeñas y medianas empresas es el artículo titulado Gestión de riesgos de ciberseguridad en pequeñas y medianas empresas (Alahmari & Duncan, 2020). Este artículo se enfoca en los desafíos específicos que enfrentan las PYMES para implementar sistemas efectivos de gestión de riesgos de ciberseguridad, debido a la limitada disponibilidad de recursos financieros,

tecnológicos y humanos. Estas limitaciones dificultan la adopción de medidas de ciberseguridad robustas, lo que hace a las PYMES más vulnerables frente a las crecientes amenazas cibernéticas.

El artículo analiza cómo, a pesar de estas restricciones, la implementación de marcos de trabajo adaptados, como ISO/IEC 27001 y el NIST Cybersecurity Framework, puede mejorar considerablemente la postura de seguridad de las PYMES. Estos marcos proporcionan guías claras para identificar, evaluar, y mitigar riesgos de seguridad de la información, y se pueden ajustar según las necesidades y capacidades de cada empresa. El estudio destaca la importancia de priorizar los riesgos más críticos y de aplicar soluciones que maximicen la protección dentro de los recursos limitados de las PYMES.

El artículo identifica cinco perspectivas de gestión que son esenciales para mitigar los riesgos de ciberseguridad en las PYMES. El estudio subraya la importancia de que las PYMES comprendan las diversas amenazas a las que están expuestas, incluidos los tipos de ciberataques y las vulnerabilidades específicas que enfrentan debido a su tamaño y recursos limitados. Se examina cómo los comportamientos de los empleados y la alta dirección afectan directamente las prácticas de ciberseguridad y la exposición al riesgo. Las PYMES deben fomentar una cultura de seguridad a nivel organizacional para reducir la probabilidad de incidentes.

El artículo identifica prácticas efectivas que las PYMES pueden adoptar para mejorar su postura de ciberseguridad, como la implementación de marcos de gestión de riesgos y la adopción de soluciones tecnológicas que optimicen la protección de sus activos digitales. Se resalta la importancia de la concienciación tanto entre la gestión como entre los empleados sobre los riesgos cibernéticos. Una mayor sensibilización es crucial para establecer una cultura proactiva de gestión de riesgos. El estudio analiza cómo los procesos de toma de decisiones en

las PYMES impactan en la forma en que estas organizaciones abordan la gestión de riesgos de ciberseguridad. Decisiones mal informadas o retrasadas pueden aumentar significativamente la vulnerabilidad.

El análisis de Alahmari & Duncan se basa en 15 estudios empíricos seleccionados de un total de 50, centrados en cómo las PYMES gestionan los riesgos de ciberseguridad. Estos estudios proporcionan una base sólida para comprender la realidad de las PYMES frente a las crecientes amenazas cibernéticas, revelando que la mayoría carece de recursos suficientes para adoptar medidas robustas. El artículo también destaca varias brechas en la investigación actual, incluyendo la falta de estudios empíricos, especialmente en países en desarrollo, lo que representa una oportunidad para futuras investigaciones. Además, sugiere que sería necesario investigar más a fondo las interrelaciones entre las diferentes perspectivas de gestión, así como extender el marco temporal de los estudios para obtener una visión más amplia de las tendencias y comportamientos en ciberseguridad.

El artículo también destaca varias brechas en la investigación actual, incluyendo la falta de estudios empíricos, especialmente en países en desarrollo, lo que representa una oportunidad para futuras investigaciones. Además, sugiere que sería necesario investigar más a fondo las interrelaciones entre las diferentes perspectivas de gestión, así como extender el marco temporal de los estudios para obtener una visión más amplia de las tendencias y comportamientos en ciberseguridad.

Estos hallazgos son de particular relevancia para las empresas de desarrollo de software en Yopal, ya que enfrentan muchos de los mismos desafíos que las PYMES analizadas en este artículo. La necesidad de una mayor concienciación, la implementación de mejores prácticas y la toma de decisiones informadas son elementos cruciales para mejorar su ciberseguridad. Además, desarrollar una aplicación web para la gestión de riesgos de

seguridad de la información se alinea perfectamente con la necesidad identificada de soluciones tecnológicas accesibles y eficaces que puedan ayudar a las empresas a gestionar sus riesgos de manera más eficiente.

El artículo Estudio comparativo entre las metodologías **CRAMM y MAGERIT** para la gestión de riesgo de TI en las MPYMES (Crespo-Martínez & Cordero-Torres, 2018) analiza y compara dos enfoques clave para la gestión de riesgos en la seguridad de la información: CRAMM y MAGERIT. Ambas metodologías son utilizadas para identificar, evaluar y tratar los riesgos en los sistemas de información, especialmente en pequeñas y medianas empresas, que enfrentan desafíos únicos debido a recursos limitados.

Las normas ISO juegan un papel crucial en la estandarización de la gestión de riesgos de seguridad de la información en las MPYMES, proporcionando un marco claro para identificar, evaluar y mitigar los riesgos. Entre las normas más relevantes se destacan: ISO 27001 que define los requisitos para un Sistema de Gestión de Seguridad de la Información (ISMS) ISO 27002 que proporciona directrices para la implementación de controles de seguridad basados en las mejores prácticas. ISO 27005 que se enfoca en la gestión de riesgos de seguridad de la información, ofreciendo una metodología estructurada para evaluar y tratar los riesgos.

El estudio resalta cómo MAGERIT, al igual que las normas ISO, enfatiza la identificación de activos críticos para las empresas, como hardware, software y personal, lo que resulta clave para una adecuada gestión de riesgos. CRAMM, por otro lado, se basa en una evaluación más sistemática, proporcionando directrices para evaluar tanto amenazas como vulnerabilidades.

Tanto MAGERIT como ISO 27005 ofrecen herramientas para identificar amenazas potenciales en los sistemas de información, lo que permite una evaluación más profunda de los riesgos y su impacto y además ofrece procedimientos detallados para evaluar los riesgos y

determinar el nivel de criticidad de los mismos, alineándose con las prácticas recomendadas por las normas ISO.

El artículo concluye que, si bien las normas ISO proporcionan un marco general para la gestión de riesgos de seguridad de la información MAGERIT añade valor al proporcionar herramientas específicas y detalladas para la identificación y tratamiento de riesgos. Esto convierte a MAGERIT en una opción práctica para las empresas que buscan fortalecer su postura de seguridad de la información de manera eficiente y efectiva.

Por último, el articulo La norma ISO/IEC 27001 de gestión de la seguridad de la información: Cómo extraer valor de los datos en el sector de TI (Kitsios et al., 2023) profundiza en cómo el estándar ISO/IEC 27001 puede ser implementado en empresas del sector de tecnología de la información (TI) para extraer valor de los datos y, al mismo tiempo, garantizar su protección. La norma establece los requisitos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), lo que permite a las empresas gestionar sus riesgos de manera efectiva y salvaguardar la confidencialidad, integridad y disponibilidad de la información. El artículo destaca que, en el sector del desarrollo de software, la aplicación de ISO/IEC 27001 no solo ayuda a las empresas a cumplir con normativas internacionales, sino que también facilita la obtención de un valor estratégico a partir de la gestión de datos seguros. Esto es especialmente relevante para las empresas de desarrollo de software en Yopal, que manejan grandes volúmenes de datos confidenciales y deben garantizar su seguridad para ser competitivas en un entorno regional y local.

Además, la ISO 27001 promueve la integración de estrategias de seguridad, lo que mejora la resiliencia frente a ataques cibernéticos. La capacidad de las empresas de desarrollo de software para manejar sus riesgos y cumplir con los requisitos legales es fundamental para mantener la confianza con sus socios y clientes. La implementación de este estándar puede

resultar compleja, ya que en muchos casos requiere la realización de evaluaciones exhaustivas de riesgos y documentación detallada de procesos, lo cual puede consumir tiempo y recursos significativos. Según el estudio, algunas organizaciones tardaron más de 11 meses en completar el proceso, destacando la importancia de un enfoque disciplinado y continuo para gestionar la seguridad.

El artículo también destaca que la implementación de ISO 27001 puede generar cambios importantes en las operaciones diarias de una organización. Esto incluye la promoción de la eficiencia mediante la reducción de redundancias y la formalización de procedimientos claros para la documentación y comunicación de calidad dentro de la empresa. Estos cambios operativos son cruciales en el contexto de las empresas de desarrollo de software en Yopal, donde la gestión de datos es un activo crítico. Además, el artículo enfatiza la importancia de fomentar una cultura de concienciación sobre la seguridad dentro de las organizaciones, garantizando que todos los empleados estén alineados con las mejores prácticas de ciberseguridad.

Con la información obtenida en los diferentes artículos está claro que existen brechas significativas en la aplicación práctica de estas metodologías. Los informes técnicos revelan que las PYMES son especialmente vulnerables debido a sus recursos limitados y a la falta de estrategias de ciberseguridad robustas (Bautista García & Aguilar, 2023). Las soluciones actuales no abordan suficientemente las necesidades específicas de estas empresas, particularmente en cuanto a la simplicidad y automatización de procesos. Además, la adopción tecnológica es desigual, y muchas de estas empresas carecen del conocimiento necesario para implementar soluciones de ciberseguridad complejas.

En los últimos años, se ha observado un aumento significativo en el desarrollo de software especializado para la gestión de riesgos de seguridad de la información. Herramientas

como Pirani, Resolver, LogicManager, MetricStream, y RSA Archer han ganado popularidad debido a su capacidad para automatizar y optimizar los procesos de gestión de riesgos. Estas soluciones no solo mejoran la eficiencia en la evaluación de riesgos, sino que también facilitan el cumplimiento de normativas y estándares internacionales como ISO 27001 y ISO 31000. Las soluciones actuales en el mercado ofrecen una variedad de funcionalidades que incluyen la identificación, medición, control y monitoreo de riesgos operacionales y de seguridad de la información. Por ejemplo, Pirani proporciona módulos para la gestión de riesgos operacionales, cumplimiento normativo, auditoría y riesgos activos, ofreciendo una plataforma integral para la gestión de riesgos empresariales.

Sin embargo, a pesar de la amplia gama de soluciones disponibles, muchas empresas de desarrollo de software en Yopal y en otras regiones aún enfrentan barreras significativas para adoptar estas tecnologías. La resistencia al cambio, la falta de conocimiento técnico y las limitaciones presupuestarias son algunos de los obstáculos que dificultan la implementación efectiva de sistemas de gestión de riesgos. Estas empresas, cuyo principal activo es la información, suelen carecer de personal especializado en ciberseguridad, lo que complica aún más la adopción de soluciones complejas.

Hasta el momento no existe información específica que aborde el estado actual de la seguridad de la información en las empresas de desarrollo de software en Yopal. Esto representa una brecha significativa en la literatura y evidencia la falta de estudios detallados sobre las prácticas de ciberseguridad y gestión de riesgos en esta región particular. A pesar de que existen múltiples investigaciones a nivel global sobre la implementación de marcos como ISO 27001 y MAGERIT en otros sectores y regiones, los estudios centrados en el contexto de empresas de desarrollo de software en ciudades intermedias como Yopal son escasos.

La ausencia de información local también se extiende a factores clave como la madurez de los sistemas de seguridad, la conciencia cibernética del personal, y el nivel de inversión en tecnologías de ciberseguridad por parte de estas empresas. Estas deficiencias destacan la necesidad de estudios empíricos y soluciones adaptadas a las características y necesidades de las empresas de software en ciudades con menor desarrollo tecnológico, donde la falta de personal especializado y la dependencia de métodos tradicionales incrementan los riesgos de seguridad. Por lo tanto, la creación de una herramienta de gestión de riesgos de seguridad de la información no solo busca resolver un problema práctico, sino que también contribuiría a la generación de conocimiento sobre el estado actual de la seguridad de la información en las empresas de desarrollo de software en Yopal. Esto refuerza la pertinencia del proyecto al tratar de llenar esta brecha en la literatura y ofrecer una solución accesible para la gestión de riesgos de ciberseguridad en un contexto donde dicha información es prácticamente inexistente.

Objetivos

Objetivo General

Desarrollar una aplicación web, que contribuya a la gestión de los riesgos de seguridad de la información en las empresas de software de Yopal según metodología MAGERIT.

Objetivos Específicos

Analizar la metodología de MAGERIT, la norma ISO 27001 y los controles de la norma ISO 27002 para, identificar y definir los requerimientos necesarios del software.

Diseñar una arquitectura de software escalable y segura para, que permita la integración de nuevas funcionalidades y actualizaciones en el futuro.

Crear una interfaz de usuario intuitiva y accesible, evaluada mediante pruebas de usabilidad, para facilitar la navegación y el uso de la aplicación por parte de los usuarios, independientemente de su nivel de experiencia técnica.

Realizar pruebas funcionales, de usabilidad y aceptación para validar el cumplimiento de los requerimientos definidos, garantizando la calidad del software y su adopción por parte de los usuarios.

Marco Teórico

El estudio de la seguridad de la información es crucial en la era digital, donde la información se ha convertido en uno de los activos más valiosos para las organizaciones. Este marco teórico se centra en tres aspectos principales: la seguridad de la información, los riesgos asociados a esta, especialmente en el contexto de las PYMES, y las soluciones tecnológicas disponibles para la gestión de estos riesgos. Primero, se definirán los conceptos fundamentales y los pilares de la seguridad de la información. A continuación, se analizarán las amenazas cibernéticas actuales y los riesgos específicos que enfrentan las PYMES. Finalmente, se explorarán las características y beneficios de diverso software de gestión de riesgos de seguridad de la información, proporcionando un panorama completo de las herramientas disponibles para proteger la información en el entorno empresarial moderno.

Seguridad de la Información

Definición

La seguridad de la información se refiere a los procesos, prácticas y metodologías destinadas a proteger la información y los sistemas de información contra accesos no autorizados, usos indebidos, divulgaciones, interrupciones, modificaciones o destrucciones. En esencia, esto implica salvaguardar nuestros datos y recursos tecnológicos de aquellos que puedan intentar utilizarlos de manera inapropiada (Vega, 2021).

Pilares de la seguridad de la información

La disponibilidad se refiere a que la información esté accesible cuando la necesitemos. Un fallo de disponibilidad ocurre cuando no podemos acceder a la información, ya sea por un error de configuración o por un ataque de Ransomware que cifra los archivos y nos impide el acceso. La integridad es la característica que asegura que la información esté libre de modificaciones y errores. Un fallo de integridad se da cuando la información es alterada, como en un informe de ventas modificado intencionadamente, o cuando se borran datos parcial o

accidentalmente. La confidencialidad significa que la información no debe ser accesible o revelada a individuos, entidades o procesos no autorizados. Para proteger la confidencialidad, se utilizan contratos de confidencialidad que evitan la difusión intencionada o accidental de la información. La divulgación no autorizada puede erosionar la confianza de clientes y proveedores (National,2019).

Garantizar los pilares de disponibilidad, integridad y confidencialidad de la información es crucial porque asegura que la información esté accesible cuando se necesite, sea precisa y libre de alteraciones no autorizadas, y esté protegida contra accesos no autorizados. Esto es fundamental para mantener la operatividad, tomar decisiones informadas y preservar la confianza y privacidad de clientes y socios, lo que en conjunto sostiene la eficiencia y seguridad de cualquier organización (Vega, 2021).

Riesgos de Seguridad de la Información

Definición

Potencialidad de que una amenaza puede explotar una vulnerabilidad de un activo o grupo de activos y en consecuencia cause daño a la entidad (ISO/IEC 27000, 2018).

Tipos de riesgos

Existen varios tipos de riesgos: estratégicos, que se relacionan con la administración y cumplimiento de objetivos; operativos, que abarcan deficiencias en sistemas, procesos y procedimientos; financieros, relacionados con la gestión de recursos y transparencia; de cumplimiento, que involucran la capacidad de la entidad para cumplir con requisitos legales y éticos; de conocimiento, asociados a la pérdida de información vital; normativos, que implican la violación de obligaciones legales y políticas internas; y de tecnología, que se refieren a la capacidad de la entidad para satisfacer sus necesidades tecnológicas y apoyar su misión (Tecnológicos, 2018).

Es crucial contar con un software, que permita identificar y gestionar estos riesgos que pueden impactar en la seguridad de la información. La aplicación facilita la identificación temprana de amenazas, proporciona herramientas para evaluar y mitigar riesgos, y ayuda a asegurar la conformidad con normativas y políticas internas.

Malware

Definición

Es un software malicioso que tiene por objetivo comprometer un ordenador, una red con el fin de obtener beneficios o utilizar de manera indebida el sistema u ordenador infectado (Guias de seguridad UJA, 2018).

Ataques informáticos a nivel mundial

De acuerdo al informe de Sonic Wall En 2022, la tecnología patentada Real-Time Deep Memory Inspection™(RTDMI) de SonicWall estableció un total de 465.501 variantes de malware nunca vistas hasta la fecha, con la cifra de detecciones totales por encima de 1 millón. En los últimos años, las tendencias globales de ciberataques han mostrado un aumento significativo en diversas áreas. Por ejemplo, los ataques de malware han alcanzado los 5,500 millones de incidentes. Por otro lado, los ataques de ransomware representan una amenaza considerable con 493,3 millones de incidentes. Los intentos de intrusión han llegado a 6,3 billones, lo que subraya la necesidad de fortalecer las barreras de seguridad (Sonicwall, 2023).

Estos datos resaltan la importancia de implementar soluciones robustas de gestión de riesgos de seguridad de la información, especialmente en las PYMES, que suelen estar menos preparadas para enfrentar estos desafíos. La adopción de tecnologías avanzadas y la capacitación continua en ciberseguridad son cruciales para mitigar estos riesgos y proteger la integridad de los datos y sistemas en un entorno cada vez más digitalizado.

Ataques Informáticos en Colombia

En el año 2023 se reportaron 59.033 denuncias por delitos informáticos, representando un decremento del –10% respecto del año 2022 con 65.794 denuncias. El hurto por medios informáticos y semejantes alcanzó 28,512 denuncias, reflejando un incremento del 8% respecto al año anterior. Los accesos abusivos a sistemas informáticos sumaron 10,883 denuncias. La violación de datos personales tuvo un total de 9,639 denuncias, mientras que la suplantación de sitios web registró 4,393 denuncias (Fredy et al., 2022).

Pymes

Definición

Son definidas según las leyes colombianas como aquellas que poseen una planta de personal inferior a 200 empleados y activos totales de hasta 30.000 salarios mínimos mensuales legales vigentes, representan el 99,5% del parque empresarial nacional en Colombia (Del Do et al., 2023; Franco-Ángel & Urbano, 2019).

Generalidades

Las pequeñas y medianas empresas (Pymes) deben estar preparadas para enfrentar los desafíos de un mundo cada vez más digitalizado, donde la información se ha convertido en un activo crucial. Es esencial adoptar medidas y controles que garanticen la confidencialidad, disponibilidad e integridad de la información tanto de la organización como de sus miembros. Para enfrentar estos desafíos, las Pymes deben dar prioridad a la seguridad de la información, estableciendo políticas y procedimientos formales para su implementación, y asignando los recursos necesarios para mantener controles efectivos que aseguren la protección y gestión adecuada de los datos de clientes, proveedores y empleados (Mayor, 2022.).

Muchas Pymes cometen el error de pensar que su tamaño las hace menos atractivas para los ciber atacantes, lo cual es un grave error. Los ciber atacantes no discriminan por el tamaño de la empresa; cualquier organización puede ser un objetivo o incluso pudo haber sido víctima de un ataque cibernético sin haberse percatado (ElevenPaths, 2019).

Metodologías de Gestión de Riesgos de Seguridad de la Información

Definición

Una metodología de gestión de riesgos de seguridad de la información es un conjunto estructurado de procesos, técnicas y herramientas que una organización utiliza para identificar, analizar, evaluar, tratar y monitorear los riesgos relacionados con la confidencialidad, integridad y disponibilidad de su información. Su objetivo principal es proteger los activos de información de la organización, minimizando la probabilidad de que las amenazas se materialicen y el impacto que estas podrían generar (Corporación Autónoma Regional del Valle del Cauca [CVC], 2020).

OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation)

La metodología OCTAVE (Operationally Critical Threats, Assets, and Vulnerability Evaluation), desarrollada por el Equipo de Respuesta ante Emergencias Informáticas (CERT), es un enfoque clave para la evaluación y mitigación de riesgos de seguridad de la información en empresas. Esta metodología se adapta a las necesidades específicas de cada organización, buscando reducir los riesgos y mejorar la protección de sus activos de información. OCTAVE integra aspectos operativos, prácticas de seguridad y tecnología, permitiendo a las empresas tomar decisiones informadas sobre la protección de datos, alineadas con los principios de seguridad de la información (Alberts et al., 1999).

Existen tres versiones principales: OCTAVE para grandes organizaciones (más de 300 empleados), OCTAVE-S para pequeñas y medianas empresas (20 a 80 empleados), y OCTAVE Allegro, que se enfoca más en el análisis de riesgos de activos de información. OCTAVE busca asegurar la continuidad del negocio, identificar y medir riesgos, implementar controles de mitigación, proteger la información como activo vital e involucrar a todas las áreas

de la organización para aprovechar su conocimiento colectivo (Vista de Análisis de Riesgos En Seguridad de la Información, 2013)

MEHARI

MEHARI (Método para el Análisis Armonizado de Riesgos) es una metodología de código abierto para la evaluación y gestión de riesgos de seguridad de la información. Fue desarrollada por el Club de la Securité De L'information Français (CLUSIF) en 1998 y se caracteriza por su enfoque sistemático y flexible, adaptable a diferentes niveles de madurez y situaciones. Permite una valoración tanto cualitativa como cuantitativa de los riesgos, considerando factores estructurales de la organización y la efectividad de las medidas de seguridad implementadas. A través de cuestionarios detallados, MEHARI evalúa la calidad de los controles de seguridad y las vulnerabilidades, no solo en el ámbito de TI, sino en toda la organización, incluyendo aspectos físicos y regulatorios, para generar planes de mejora. Asimismo, facilita la comprensión de las amenazas al negocio, clasificando la información y los activos según su sensibilidad a posibles malfuncionamientos, lo que permite a las organizaciones tomar decisiones informadas sobre las inversiones en seguridad y proteger sus activos más críticos (Alonso, 2023).

CRAMM (CCTA Risk Analysis and Management Method)

Desarrollada por la Central Computer and Telecommunications Agency (CCTA) del gobierno británico, es un enfoque estructurado y disciplinado para identificar, medir y minimizar los riesgos de seguridad de la información. Se destaca por ser una metodología mixta, ya que combina análisis de riesgo cualitativos y cuantitativos. CRAMM se apoya en una herramienta de gestión para proporcionar a las organizaciones una visión clara y priorizada de las amenazas que pueden afectar sus recursos y la continuidad del negocio. Opera mediante una matriz que relaciona los activos con los riesgos que podrían comprometer su integridad,

disponibilidad y confidencialidad, además de ofrecer información detallada sobre el funcionamiento del sistema y la identificación de los activos más expuestos. Para un análisis de riesgos efectivo con CRAMM, se consideran elementos clave como activos, vulnerabilidades, riesgos, amenazas, contramedidas, implementación y auditoría, lo que contribuye a asegurar la continuidad operativa de la organización (Tejena-Macías, 2018).

EBIOS

La metodología EBIOS (Expresión de las Necesidades e Identificación de los Objetos de Seguridad) es un enfoque francés para la gestión de riesgos de seguridad, desarrollada por la Dirección Central de Seguridad de los Sistemas de Información (DCSSI) de Francia. Su propósito es facilitar la comunicación entre los actores internos y externos de una organización en el proceso de gestión de riesgos, a la vez que contribuye al reconocimiento de sus actividades de seguridad, dada su compatibilidad con normas internacionales como la ISO. Esta metodología permite a las organizaciones comprender mejor sus activos y necesidades de seguridad, identificando las amenazas y vulnerabilidades a las que están expuestos para su posterior mitigación (Secrétariat général de la défense nationale, Direction centrale de la sécurité des systèmes d'information [SGDN/DCSSI], 2003).

NIST SP 800-30

NIST SP 800-30 es una guía desarrollada por el Instituto Nacional de Estándares y Tecnología (NIST), se enfoca en la gestión de riesgos de seguridad, particularmente en sistemas de Tecnología de la Información (TI), ofreciendo una perspectiva técnica para la seguridad de infraestructuras. Esta guía sienta las bases para la administración, evaluación y mitigación de riesgos identificados en los sistemas de TI, brindando soporte a las organizaciones en todo lo relacionado con la tecnología.

La metodología NIST SP 800-30 se compone de nueve fases clave. Inicia con la caracterización del sistema, estableciendo el alcance y los límites operacionales de la evaluación de riesgos. Seguidamente, se procede a la identificación de amenazas, definiendo sus fuentes y motivaciones, y a la identificación de vulnerabilidades, listando los defectos o debilidades del sistema que podrían ser explotados. Las fases siguientes incluyen el análisis de controles, la determinación de la probabilidad y el análisis de impacto. Posteriormente, se lleva a cabo la determinación del riesgo, evaluando el riesgo inherente al sistema de información. La fase de recomendaciones de control propone medidas para mitigar los riesgos identificados hasta un nivel aceptable. Finalmente, la documentación de resultados genera un informe detallado con la descripción de amenazas y vulnerabilidades, la medición del riesgo y las recomendaciones para la implementación de controles (National Institute of Standards and Technology [NIST], 2012).

MAGERIT

MAGERIT ofrece una guía estructurada en tres libros: el primero describe el modelo de gestión de riesgos, el segundo enfoca el inventario para el análisis, y el tercero compila técnicas de trabajo. Entre sus objetivos principales se encuentran conocer el estado de seguridad de los sistemas de información, asegurar la exhaustividad del análisis, mitigar vulnerabilidades y garantizar la seguridad en todas las fases de desarrollo del sistema. Estos objetivos han consolidado a MAGERIT como una de las metodologías preferidas en el ámbito empresarial, facilitando la preparación para auditorías, certificaciones y acreditaciones (Consejo Superior de Administración Electrónica, 2019).

Cuadro Comparativo de las Metodologías de Gestión del Riesgo

Cuadro 1

Cuadro Comparativo de Metodologías de Gestión de Riesgos de Seguridad de la Información

Fases	Metodologías					
	OCTAVE	**MEHARI**	**MAGERIT**	**CRAMM**	**EBIOS**	**NIST SP 800-30**
Caracterización del sistema	**x**	**x**	**x**	**x**	**x**	**x**
Identificación de Amenazas	**x**		**x**	**x**	**x**	**x**
Identificación de Vulnerabilidades	**x**		**x**	**x**		**x**
Análisis de controles	**x**	**x**	**x**		**x**	**x**
Determinación del nivel del riesgo		**x**	**x**	**x**		**x**
Análisis del Impacto	**x**		**x**	**x**		**x**
Recomendaciones de control		**x**	**x**			**x**
Medidas de Control	**x**		**x**		**x**	**x**
Identificación de activos			**x**			
Identificación de Dependencias			**x**			

Selección de Metodología de Gestión del Riesgo para el trabajo

MAGERIT fue seleccionada como la metodología base para este proyecto debido a que ofrece una cobertura exhaustiva de todo el ciclo de vida del análisis y gestión de riesgos de seguridad de la información. A diferencia de otras metodologías como OCTAVE, MEHARI o NIST SP 800-30 que pueden enfocarse en aspectos organizacionales o en la evaluación conceptual, MAGERIT proporciona una estructura técnica detallada y una secuencia clara de acciones. Su enfoque parte desde identificar qué proteger (activos), para luego definir de qué protegerlo (amenazas y vulnerabilidades), y finalmente determinar cómo protegerlo(mediante salvaguardas), lo cual da lugar a un proceso lógico, estructurado y replicable que se sigue dentro de la aplicación.

Uno de los aspectos más valiosos de MAGERIT es que está completamente disponible en español, lo que elimina barreras de lenguaje y facilita su adopción en organizaciones hispanohablantes. Además, se complementa de manera excelente con la norma ISO 27005, ya

que mientras esta proporciona las directrices generales para la gestión del riesgo, MAGERIT actúa como una guía práctica que operacionaliza esas directrices en actividades concretas.

La metodología también incorpora elementos clave que otras metodologías no siempre abordan, como la gestión del riesgo residual, la trazabilidad del análisis, y la evaluación de la eficacia de los controles. Además, va más allá de solo identificar y mitigar riesgos, proponiendo como uno de sus principios fundamentales la concienciación organizacional sobre la seguridad de la información. Esto se alinea directamente con el propósito de la aplicación desarrollada, que no busca únicamente automatizar la gestión de riesgos, sino transformar la manera en que las organizaciones entienden, valoran y responden ante dichos riesgos, facilitando así decisiones más asertivas y alineadas con los objetivos del negocio. Por ello, MAGERIT representa no solo una metodología técnica, sino también una herramienta de cambio cultural, ideal para los objetivos del presente proyecto**.**

Software de Gestión de Riesgos

La aplicación web es una solución de gestión de riesgos de uso libre que incorpora las mejores metodologías y prácticas del sector. Esta plataforma se desarrolla para proporcionar a las Pymes una herramienta accesible y efectiva para gestionar sus riesgos de seguridad de la información de manera integral. Ofrece funcionalidades que permiten la identificación, evaluación y mitigación de riesgos, adaptándose a las características y requerimientos específicos de cada empresa.

Generalidades

En el contexto actual, donde las amenazas cibernéticas están en constante evolución. Las aplicaciones de gestión de riesgos se han convertido en herramientas que buscan proteger la integridad, confidencialidad y disponibilidad de la información. Estas aplicaciones permiten a las empresas identificar, evaluar y mitigar riesgos de manera más eficiente y eficaz.

Pirani

Se especializa en proporcionar soluciones que permiten a las Pymes gestionar de manera efectiva sus riesgos de seguridad de la información. Esta plataforma ofrece una variedad de funcionalidades que incluyen la identificación de amenazas, la evaluación de vulnerabilidades y la implementación de controles adecuados para mitigar riesgos. Con Pirani, las empresas pueden automatizar el proceso de gestión de riesgos, obteniendo reportes detallados y personalizados que ayudan en la toma de decisiones informadas (Guía Para Usar Un Software de Gestión de Riesgos Pirani,2022.).

Risk Watch

Proporciona un marco para evaluar amenazas potenciales y vulnerabilidades en los sistemas de información. RiskWatch permite a las organizaciones automatizar el proceso de evaluación y obtener reportes detallados sobre posibles áreas de mejora. (Best Risk and Compliance Assessment Software- RiskWatch,2022).

Logic Manager

Ofrece soluciones integrales para la gestión de riesgos, incluyendo módulos específicos para la seguridad de la información. LogicManager ayuda a las empresas a identificar y priorizar riesgos, implementar controles y monitorear la efectividad de las estrategias de mitigación a través de un enfoque basado en datos (LogicManager | Enterprise Risk Management Software, 2022.).

Protecht

Es un software integral de gestión de riesgos que permite a las organizaciones monitorear, gestionar y mitigar riesgos en tiempo real. Ofrece una plataforma flexible y escalable que integra módulos para la gestión de riesgos operacionales, cibernéticos y de cumplimiento normativo. Protecht es conocido por su capacidad para ofrecer una visión unificada de riesgos, lo que permite a las empresas tomar decisiones informadas y gestionar sus controles de manera

proactiva. Sin embargo, La amplitud de sus funcionalidades puede ser abrumadora para usuarios nuevos y para solicitar los costos del software hay que comunicarse de manera directa con un asesor.

Strike Graph

Es una plataforma de gestión de riesgos centrada específicamente en la seguridad de la información y el cumplimiento normativo. Es ampliamente utilizada para ayudar a las organizaciones a automatizar la creación y gestión de controles relacionados con auditorías de seguridad, como SOC 2, ISO 27001, HIPAA y otros marcos normativos. Strike Graph facilita a las empresas el desarrollo, implementación y seguimiento de controles de seguridad sin tener que gestionar manualmente cada proceso. Esto reduce significativamente la carga administrativa, especialmente en auditorías de cumplimiento además de proporcionar herramientas que ayudan a las empresas a evaluar y mitigar continuamente los riesgos de seguridad, alineando las prácticas con estándares como ISO 27001 y SOC 2. Esta evaluación constante es crucial en un entorno donde las amenazas cibernéticas evolucionan rápidamente.

Ncontracts

Ncontracts es una plataforma de software diseñada para gestionar los riesgos empresariales, con un enfoque en la gestión de contratos, cumplimiento normativo, y riesgos de seguridad de la información. Es utilizada ampliamente por empresas que buscan integrar la gestión de riesgos con la administración de proveedores, contratos y cumplimiento regulatorio en un solo sistema. Ncontracts permite a las organizaciones gestionar de manera eficiente sus relaciones con proveedores y los riesgos asociados, asegurando que todos los contratos y acuerdos cumplan con las normativas y estándares de seguridad aplicables. Esto es fundamental para garantizar que las empresas de software puedan mantener su seguridad a través de proveedores externos confiables.

Metodología

El ciclo en cascada fue la metodología de desarrollo de software seleccionada para este proyecto, debido a su enfoque estructurado y secuencial, el cual sigue una serie de fases bien definidas (Lledó & Rivarola, 2021). Esta metodología fue especialmente adecuada para el desarrollo de una aplicación orientada a la seguridad de la información, ya que garantizó que cada etapa desde el análisis de requisitos hasta la implementación y las pruebas fuera cuidadosamente documentada y verificada para cumplir con los estándares de seguridad y funcionalidad establecidos.

Para asegurar una gestión efectiva de los riesgos de seguridad de la información, el análisis de riesgos se basó en una combinación de la norma ISO 27005 y la metodología MAGERIT. ISO 27005 proporcionó un marco detallado y alineado con las mejores prácticas de la ISO 27001, mientras que MAGERIT permitió un análisis exhaustivo, proporcionando una estructura clara para la identificación de activos, evaluación de amenazas y definición de tratamientos de riesgos. Esta combinación fortaleció la solidez del proceso de análisis, asegurando una cobertura integral en términos de gestión del riesgo. A continuación, se relacionan los métodos, procedimientos y resultados basados en los objetivos propuestos.

Analizar la metodología MAGERIT, la norma ISO 27001 y los controles de la norma ISO 27002 para identificar y definir los requerimientos necesarios del software.

Método - Revisión documental y análisis comparativo.

Procedimiento

Se realizó una revisión exhaustiva de la literatura y documentos técnicos sobre las metodologías seleccionadas, específicamente MAGERIT, ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005. El objetivo fue identificar los controles de seguridad y las prácticas recomendadas más relevantes que debían ser tenidas en cuenta en el diseño de la aplicación

de gestión de riesgos de seguridad de la información. Para ello, se emplearon matrices de evaluación que permitieron identificar similitudes, diferencias y enfoques complementarios entre dichas metodologías.

Además de la revisión documental, se llevó a cabo un proceso de análisis de requerimientos basado en entrevistas realizadas a gerentes y dueños de empresas de desarrollo de software localizadas en Yopal. Estas entrevistas permitieron obtener información contextual, operativa y normativa sobre cómo las organizaciones gestionan actualmente sus riesgos de seguridad de la información. La combinación de estas dos fuentes sirvió como insumo para establecer los requisitos funcionales y no funcionales de la aplicación, alineando su diseño con necesidades reales del entorno empresarial y con las mejores prácticas internacionales en gestión de riesgos.

Técnica

Se realizaron análisis exhaustivos a las normativas de seguridad de la información para obtener una visión más práctica sobre los requerimientos, así como entrevistas a empresas del sector.

Resultados

Los resultados alcanzados incluyen: un análisis detallado de la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), abarcando el Libro I (Método), el Libro II (Catálogo de Elementos MAGERIT) y el Libro III (Libro de Técnicas); un estudio de la norma ISO/IEC 27001:2022 relativa a la seguridad de la información, la ciberseguridad y la protección de la privacidad en los sistemas de gestión de seguridad de la información; un análisis de la norma ISO/IEC 27002:2022 sobre los controles de seguridad de la información, la ciberseguridad y la protección de la privacidad; la definición del alcance específico de la aplicación de gestión de riesgos de seguridad de la información; una matriz

para la identificación de las partes interesadas del proyecto; un análisis de los requerimientos recopilados a través de entrevistas con empresas de software de Yopal, específicamente Puntualtic y DeltaSolutions; la formulación de los requisitos funcionales y no funcionales de la aplicación; la identificación de los casos de uso dentro de la aplicación; y la elaboración de las historias de usuario correspondientes.

Diseñar una arquitectura de software escalable y segura para la aplicación, que permita la integración de nuevas funcionalidades y actualizaciones en el futuro.

Método – Diseño arquitectónico basado en patrones de software.

Procedimiento

A partir del capítulo 1 definido previamente, se diseñó una arquitectura escalable y segura que respondiera a las necesidades del sistema. Se optó por un modelo de comunicación cliente-servidor, el cual separa claramente el frontend y el backend, favoreciendo la escalabilidad, el mantenimiento y la seguridad. Este modelo facilita la interacción desde el navegador del usuario con la lógica del servidor a través de API REST.

Para la estructura del software se eligió un patrón de arquitectura MVC monolítico, en donde el framework Laravel 12 (PHP 8.3) implementa los roles de Modelo, Vista (API JSON) y Controlador en el backend, mientras que el frontend está construido con React 18 y TypeScript, consumiendo las APIs como una vista remota. La base de datos seleccionada fue MySQL 8, una base de datos relacional confiable, robusta y ampliamente utilizada que permite modelar con claridad las relaciones entre activos, amenazas, vulnerabilidades, riesgos y controles. Adicionalmente, se integró Redis como sistema de cacheo y manejo de sesiones para mejorar el rendimiento y escalabilidad de la aplicación.

Herramienta

Se utilizo UML (Lenguaje Unificado de Modelado) para la creación de diagramas de arquitectura.

Resultados

Los resultados obtenidos en cuanto a la arquitectura del sistema comprenden la elaboración de un modelo cliente-servidor, donde se detalló y se representó gráficamente la relación entre los componentes frontend y backend, así como su comunicación a través de los protocolos HTTP/s y las interfaces de programación de aplicaciones (API) REST. Se diseñó un diagrama de arquitectura lógica basado en el patrón Modelo-Vista-Controlador (MVC) con una estructura monolítica, ilustrando la interacción de sus componentes tanto en el lado del cliente como en el del servidor.

Adicionalmente, se generó un diagrama de clases que representa las entidades principales del sistema, tales como activos, riesgos, controles y usuarios, especificando sus atributos, métodos y las relaciones existentes entre ellas, incluyendo agregación, composición y herencia. Se creó un diagrama de componentes que muestra la estructura del sistema en módulos funcionales y la manera en que estos interactúan mediante interfaces definidas. Asimismo, se elaboró un diagrama de despliegue que ilustra la distribución de la aplicación en un entorno real, utilizando DigitalOcean como proveedor de servidor privado virtual (VPS), detallando los servidores, la base de datos, el sistema de caché Redis, el almacenamiento en la nube y la implementación de comunicación segura a través de HTTPS. Se diseñaron diagramas de flujo de datos (DFD) en niveles 0,1,2,3 para visualizar el movimiento de la información entre los procesos clave de la aplicación, como el registro de activos, el análisis de riesgos y su respectivo tratamiento. Finalmente, se produjo un diseño de arquitectura completo

y debidamente documentado, que busca garantizar la escalabilidad y la seguridad integral del sistema.

Crear una interfaz de usuario intuitiva y accesible que facilite la navegación y el uso de la aplicación por parte de los usuarios de las empresas de desarrollo de software, independientemente de su nivel de experiencia técnica.

Método - Diseño centrado en el usuario y pruebas de usabilidad.

Procedimiento

Se desarrolló una versión funcional del software, abarcando la gestión de activos, análisis y tratamiento de riesgos de seguridad de la información. La interfaz fue diseñada teniendo en cuenta principios de simplicidad, jerarquía visual clara y accesibilidad para profesionales con una formación en seguridad de la información o ciberseguridad.

Una vez que el software fue desarrollado se llevaron a cabo pruebas de validación con usuarios reales provenientes de empresas dedicadas al desarrollo de software. Estos usuarios exploraron las diversas funcionalidades de la aplicación y proporcionaron retroalimentación directa sobre su experiencia. Adicionalmente, el equipo de desarrollo interno realizó exhaustivas pruebas funcionales con el objetivo de asegurar que todos los flujos de navegación dentro de la aplicación fueran coherentes, fluidos y fácilmente comprensibles para el usuario.

Es importante destacar que estudiantes de décimo semestre del programa de Ingeniería de Sistemas de la materia de seguridad informática también probaron el software en diferentes entornos empresariales. lo que permitió obtener una evaluación sobre su correcto funcionamiento y la identificación de posibles áreas de mejora.

Resultados

Se obtuvo una interfaz de usuario funcional e intuitiva, la cual fue validada de manera satisfactoria tanto por los usuarios finales pertenecientes a empresas de desarrollo de software como por el equipo de desarrollo interno. Es importante señalar que, si bien la interfaz se considera intuitiva, está principalmente orientada a profesionales de seguridad de la información o personas con conocimientos en el área. Aunque su diseño facilita la navegación y el uso de las funcionalidades, un usuario sin familiaridad con las normas y los conceptos fundamentales de seguridad de la información podría encontrarla menos comprensible. La estructura modular y clara de la interfaz permite al usuario con experiencia en el campo gestionar activos de información, realizar análisis de riesgos y aplicar los tratamientos definidos de una manera sencilla y guiada.

Adicionalmente a la interfaz validada, se generó el código fuente completo de la aplicación, el cual representa la implementación técnica de todas las funcionalidades diseñadas. Finalmente, se elaboró un manual de usuario detallado, que proporciona una guía paso a paso sobre cómo utilizar cada una de las características y funcionalidades de la aplicación, buscando facilitar su adopción y uso efectivo por parte del público objetivo.

Realizar pruebas funcionales, de usabilidad y aceptación para validar el cumplimiento de los requerimientos definidos, garantizando la calidad del software y su adopción por parte de los usuarios.

Método

Se empleó una combinación de pruebas funcionales, pruebas de usabilidad y pruebas de aceptación de usuarios, con el fin de evaluar el correcto funcionamiento del software, su facilidad de uso y su alineación con las necesidades reales de las empresas de desarrollo de software.

Procedimiento

1. **Pruebas funcionales:** Se verificó que cada requisito funcional se cumpliera adecuadamente, mediante el uso de casos de prueba diseñados para evaluar funcionalidades clave como el registro de activos, análisis de riesgos y asignación de controles.
2. **Pruebas de usabilidad:** Se permitió que usuarios de diferentes niveles técnicos interactuaran con la aplicación, evaluando la facilidad de navegación, claridad en la interfaz y comprensión de los procesos dentro del sistema.
3. **Pruebas de aceptación:** Se realizó una entrega preliminar del software a empresas seleccionadas (como Puntualtic y DeltaSolutions), quienes probaron la herramienta en contextos reales y brindaron retroalimentación sobre su utilidad, pertinencia y mejoras sugeridas.
4. **Registro de incidencias:** Se documentaron los hallazgos, errores detectados y sugerencias, permitiendo realizar ajustes antes de la liberación final.

Resultados

Se llevó a cabo una validación completa de los requisitos funcionales y no funcionales que se establecieron durante la fase de análisis. Se buscó una alta aceptación del software por parte de las empresas participantes en el estudio. Además, se identificaron oportunidades de mejora que serían consideradas para futuras versiones del sistema. Finalmente, se garantizó el aseguramiento de la calidad y estabilidad del sistema antes de su implementación definitiva.

Resultados

Para presentar de manera clara y estructurada los avances y logros obtenidos en el desarrollo del proyecto, los resultados se organizaron en función de los cuatro objetivos específicos planteados desde el inicio del trabajo, permitiendo así una mejor comprensión del proceso, la metodología aplicada y los entregables alcanzados.

El primer objetivo se centró en el análisis de la metodología de MAGERIT, la norma ISO 27001 y los controles de la norma ISO 27002, con el fin de identificar y definir los requerimientos funcionales y no funcionales del software, así como establecer el alcance del sistema de gestión de riesgos propuesto. Adicionalmente, se incluyó el análisis de la norma ISO 27005, guía internacional que establece directrices para gestionar los riesgos de seguridad de la información.

El segundo objetivo consistió en el diseño de una arquitectura de software escalable y segura, que asegurara la posibilidad de integración de nuevas funcionalidades y actualizaciones futuras, garantizando la sostenibilidad técnica del sistema.

El tercer objetivo se enfocó en la creación de una interfaz de usuario intuitiva y accesible, la cual fue validada mediante pruebas realizadas tanto por usuarios de empresas de desarrollo de software como por el equipo de desarrollo interno, con el fin de facilitar el uso del sistema independientemente del nivel técnico del usuario.

Finalmente, el cuarto objetivo se enfocó en la validación del software desarrollado mediante la ejecución de pruebas funcionales, de usabilidad y de aceptación. Estas pruebas permitieron comprobar que los requerimientos definidos en las fases anteriores fueron correctamente implementados, y que la aplicación cumple con los estándares de calidad esperados. A través de la participación de usuarios reales y representantes de empresas del sector, se obtuvieron resultados que reflejan tanto el grado de adopción de la herramienta

como oportunidades de mejora identificadas para futuras versiones. Esta etapa consolidó el trabajo realizado en los objetivos 1, 2 y 3, validando el análisis normativo, la arquitectura diseñada y la experiencia de usuario implementada.

Analizar la Metodología de MAGERIT, la Norma ISO 27001 Y los Controles de la Norma ISO 27002 para Identificar y Definir los Requerimientos Necesarios del Software.

Para el desarrollo de la aplicación de gestión de riesgos de seguridad de la información, fue fundamental aplicar un proceso de ingeniería de requerimientos. Este proceso se encarga de identificar, documentar y gestionar las necesidades de los usuarios y Stakeholders(partes interesadas) con el fin de garantizar que el producto final cumpla con sus expectativas y requerimientos específicos (Ralph R. Young, 2014). La ingeniería de requerimientos en este proyecto se dividió en dos etapas principales : primero, a través del desarrollo de un MVP (Producto Mínimo Viable) basado en normativas de seguridad de la información reconocidas como MAGERIT e ISO 27001, el cual sirvió como base para la validación y mejora del sistema con las empresas; y segundo, mediante el análisis directo con empresas de software en Yopal, donde se exploraron sus procesos y necesidades específicas; además de una demostración del MVP que buscaba entender que era indispensables para ellos y cuáles eran las expectativas generales en la explicación tomando como punto de partida el MVP.

Desarrollo de un MVP basado en estándares internacionales

Previo a la recolección de requerimientos en las empresas, se había desarrollado un MVP (Producto Mínimo Viable) que servía como guía de referencia para los entrevistados. Este MVP incorporaba principios y metodologías reconocidas a nivel internacional en la gestión de riesgos de seguridad de la información, tales como:

MAGERIT

Este marco metodológico, desarrollado por el Gobierno de España, proporciona un enfoque estructurado para la gestión de riesgos en los sistemas de información (CSAE, 2012). Su aplicación en el proyecto permitió estructurar la identificación de activos, dependencias y amenazas de manera sistemática, estableciendo relaciones entre estos elementos y generando matrices de riesgos. Además, MAGERIT se destaca por su enfoque en la evaluación de riesgos con base en impactos y probabilidades, lo que permitió definir criterios objetivos dentro del software.

ISO 27001

Estándar internacional para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), la ISO 27001 establece un marco sólido para proteger la confidencialidad, integridad y disponibilidad de la información (ISO, 2022a).En el contexto del software, esta norma sirvió de referencia para diseñar una estructura de gestión alineada con las mejores prácticas y permitir que las empresas puedan seguir un modelo que facilite una futura certificación en seguridad de la información.

ISO 27005

Esta norma, derivada de la ISO 31000 (gestión de riesgos en un contexto general), se centra en la gestión del riesgo de seguridad de la información y complementa la ISO 27001 proporcionando una guía detallada sobre amenazas, vulnerabilidades, contexto del riesgo y escenarios posibles. (ISO, 2009). Su inclusión permitió definir mecanismos sólidos para la identificación y evaluación de riesgos y tratamiento del riesgo, asegurando que la aplicación cumpliera con estándares reconocidos en el sector.

ISO 27002

Esta norma proporciona un conjunto de controles de seguridad recomendados para mitigar los riesgos identificados en la gestión de seguridad de la información. Sirve como referencia clave en la fase de tratamiento del riesgo, permitiendo la asignación de controles adecuados según la criticidad del riesgo y su contexto. La categorización de los controles en preventivos, detectivos y correctivos dentro de la aplicación facilita la implementación de medidas efectivas, asegurando que cada riesgo identificado tuviera una estrategia de mitigación alineada con estándares internacionales(ISO, 2022b).

Análisis de requerimientos en empresas de software de Yopal

Previo a la realización de las entrevistas, se llevó a cabo una consulta a la Cámara de Comercio de Casanare para determinar la cantidad de empresas registradas en Yopal que se dedican al desarrollo de software. Como respuesta, se indicó que, si bien los empresarios inscriben su actividad ante la Cámara de Comercio, no existe un CIIU específico para "desarrollo de software" como se detalla en el Anexo G, por lo que la categoría más cercana utilizada es J6201 - Actividades de desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas). Esta clasificación, aunque relevante, no permite esclarecer con precisión qué porcentaje de las empresas registradas se dedican exclusivamente al desarrollo de software.

A partir de esta información, se seleccionó una muestra de 2 empresas, Con base en esta muestra, se realizaron entrevistas a 2 gerentes y dueños de empresas de desarrollo de software, con el propósito de obtener información sobre su contexto, necesidades y expectativas en materia de gestión de riesgos de seguridad de la información. Las entrevistas se estructuraron en dos dimensiones clave: contextualización inicial, para comprender el entorno en el que operan las empresas en materia de seguridad de la información; y proceso y

flujo de trabajo, para analizar cómo gestionan actualmente sus riesgos. Este proceso permitió identificar oportunidades de mejora y validar si el MVP desarrollado respondía a las necesidades reales de las empresas de desarrollo de software en Yopal.

A continuación, se presenta un análisis detallado de las normas que sirvieron como referencia clave para el desarrollo de la aplicación de gestión de riesgos de seguridad de la información.

Análisis de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

La metodología MAGERIT se compone de tres libros fundamentales. El primero explica los métodos y estructura del análisis de riesgos libro fundamental, proporcionando un enfoque detallado para la identificación y evaluación de amenazas(CSAE, 2012a). El segundo es un catálogo de elementos, que sirve como inventario para enfatizar el análisis de riesgos a partir de activos, amenazas y salvaguardas(CSAE, 2012b). Finalmente, el tercer libro se centra en las técnicas utilizadas para el análisis, proporcionando herramientas específicas para su aplicación en distintos contextos organizacionales(CSAE, 2012c).

La gestión de riesgos es un aspecto clave dentro del gobierno corporativo, especialmente cuando se trata de riesgos derivados del uso de tecnologías de la información. De acuerdo con la metodología ISO 31000, MAGERIT se enmarca dentro del proceso de gestión del riesgo, lo que permite que las decisiones estratégicas de la organización consideren los riesgos asociados a sus activos digitales Esta metodología garantiza una toma de decisiones informada y estructurada, asegurando la continuidad del negocio y la protección de la información (CSAE, 2012a, p.7).

Según la metodología MAGERIT Libro I, la gestión del riesgo se divide en dos procesos fundamentales:

Análisis de Riesgos

El proceso de Análisis de Riesgos tiene como objetivo principal evaluar el estado actual de los activos de información dentro de una organización y se articula en torno a tres aspectos fundamentales (CSAE, 2012a, p.19). En primer lugar, se busca comprender cómo es cada activo, lo que implica su identificación y caracterización detallada, así como la determinación de sus dependencias, las amenazas potenciales que lo acechan y las vulnerabilidades que podrían ser explotadas. En segundo lugar, se evalúa cuánto vale cada activo, realizando una valoración en función de su importancia estratégica para la organización y el impacto que se derivaría de una eventual pérdida de confidencialidad, integridad o disponibilidad. Finalmente, se analiza cómo de protegido se encuentra cada activo en el momento actual, evaluando el nivel de protección existente a través de las salvaguardas y los controles de seguridad que ya han sido implementados.

Tratamiento de Riesgos

Una vez realizado el análisis, se procede a la definición de estrategias para gestionar los riesgos identificados (CSAE, 2012a, p.19) a través de planes de acción que consisten en la implementación de controles y medidas de seguridad adecuadas para mitigar, transferir, aceptar o eliminar los riesgos, asegurando una protección efectiva de los activos de información.

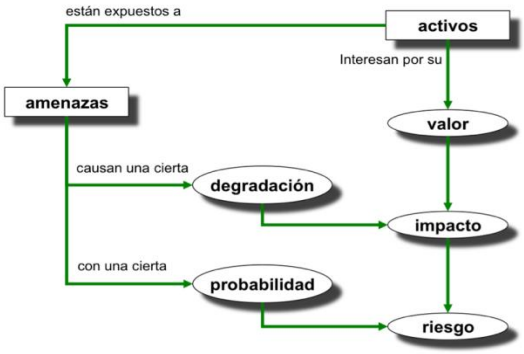
El análisis de riesgos es un proceso organizado para entender y evaluar las posibles amenazas. Primero, se identifica lo más valioso para la empresa, cómo se relaciona y cuánto daño causaría si fallaran. Luego, se ponderan qué amenazas están expuestos a esos activos. Después, se revisan las medidas de seguridad que se tienen y qué tan efectivas son. Se calcula el daño potencial que causaría cada amenaza y, finalmente, se estima el riesgo

combinando el daño con la probabilidad de que la amenaza ocurra. El resultado es una imagen clara de los riesgos más importantes para poder enfocarse en ellos (CSAE, 2012a, p.22).

Este análisis permite priorizar las acciones de mitigación de manera eficiente, destinando los recursos a las áreas más críticas. Además, es un proceso dinámico que debe actualizarse periódicamente para reflejar los cambios en el entorno y en los activos de la organización.

Figura 1

Elementos del análisis de riesgos



Nota. Este diagrama muestra los elementos que hacen parte del análisis de riesgos tomando como punto central los activos de información (p.22). Tomado de MAGERIT I. por Centro Superior de Administración Electrónica (CSAE), 2012.

MAGERIT detalla de manera estructurada el proceso de análisis de riesgos de seguridad de la información, apoyándose también de normas y metodologías ampliamente aceptadas como ISO 27001, ISO 27005 e IS0 31000 Este proceso sigue una serie de fases clave que han sido tomadas como referencia para la implementación de la aplicación de gestión de riesgos, asegurando una cobertura integral en la identificación y mitigación de amenazas. El proceso de gestión del riesgo en MAGERIT está detallado de la siguiente manera (CSAE, 2012a, p.20,21):

1. **Contexto del Riesgo:** Se establece el alcance del análisis, considerando el entorno organizacional, activos de información, amenazas y vulnerabilidades. En la aplicación, este paso se refleja en la configuración inicial del mapa de gestión de riesgos y de activos.

2. **Identificación del Riesgo:** Se determinan los activos críticos de la empresa y se identifican amenazas y vulnerabilidades asociadas. La aplicación permite registrar estos elementos de manera estructurada, asegurando una documentación detallada del riesgo en función de los activos protegidos.

3. **Análisis del Riesgo:** En esta fase, se evalúan la probabilidad e impacto de cada riesgo identificado, clasificándolas en diferentes niveles de criticidad. La plataforma implementa una matriz de evaluación que facilita este proceso y permite priorizar los riesgos según su nivel de amenaza.

4. **Evaluación del Riesgo:** Se realiza una valoración del nivel de riesgo inherente y residual, considerando la existencia de controles previos. La aplicación integra este proceso en su flujo de trabajo, proporcionando herramientas que permiten caracterizar el riesgo como aceptable, moderado o inaceptable, según su impacto en la organización.

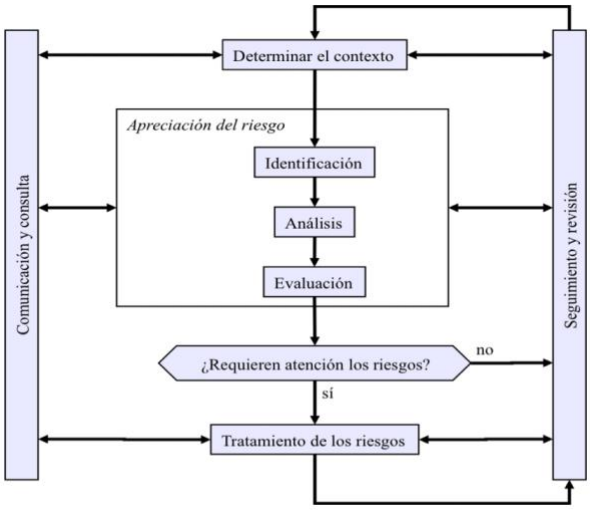
5. **Tratamiento del Riesgo:** Se definen estrategias para abordar los riesgos identificados, como su eliminación, mitigación, transferencia o aceptación. La aplicación proporciona un módulo específico para asignar controles de seguridad basados en ISO 27002 y documentar planes de acción para la reducción del riesgo.

6. **Comunicación y Consulta:** La gestión de riesgos debe ser un proceso colaborativo dentro de la organización. La aplicación permite la trazabilidad de los riesgos y la generación de reportes detallados que pueden ser utilizados en auditorías, reuniones de seguridad y procesos de toma de decisiones.

7. **Seguimiento y Revisión:** Dado que la gestión de riesgos es un proceso continuo, es fundamental monitorear los riesgos identificados, evaluar la efectividad de los controles implementados y realizar ajustes cuando sea necesario. La aplicación facilita este seguimiento a través de un historial de cambios y métricas que permiten evaluar la evolución del riesgo en el tiempo.

Figura 2

Contexto del análisis de riesgos



Nota. Etapas detalladas del proceso de gestión de riesgos (p.54). Tomado de MAGERIT I. por Centro Superior de Administración Electrónica (CSAE), 2012.

A continuación, se hace un análisis detallado de MAGERIT, esto con la finalidad de comprender qué aspectos son fundamentales en materia de requerimientos a la hora de desarrollar una aplicación de gestión de riesgos de seguridad de la información.

MAGERIT: Activos de seguridad de la información

En un sistema de información, lo esencial es la información que se gestiona y los servicios que se ofrecen. Todo lo demás, desde los datos concretos hasta las personas que lo operan, se considera un activo que, según MAGERIT (CSAE, 2012a, p.23), puede ser

susceptible de amenazas que comprometan su integridad, disponibilidad o confidencialidad. Estos activos comprenden, entre otros, los datos que contienen la información, los servicios de apoyo como la autenticación o las copias de seguridad, los programas informáticos (software) que permiten operar con dichos datos, y los equipos físicos (hardware) que los almacenan. También se consideran activos los soportes de información donde se guardan los datos, los periféricos que complementan al hardware principal, las redes que permiten la comunicación e intercambio de datos, los espacios físicos como edificios o salas que albergan los sistemas, y finalmente, las personas que interactúan directamente con el sistema de información. Todos estos elementos deben ser protegidos, ya que cualquier falla, ataque o negligencia sobre ellos puede comprometer gravemente el funcionamiento y los objetivos de la organización.

MAGERIT resalta la importancia del concepto de "dependencias entre activos" dentro del análisis de riesgos. Subraya que comprender cómo la seguridad de un activo de nivel superior se ve comprometida por incidentes en activos de nivel inferior es crucial para una gestión de riesgos efectiva. Propone una estructuración jerárquica de los activos en capas, donde las capas superiores dependen de la correcta funcionalidad y seguridad de las inferiores. Define esta dependencia estableciendo que las necesidades de seguridad de un activo superior se ven reflejadas en las del activo inferior. En términos prácticos, la materialización de una amenaza en un activo inferior tiene un impacto negativo en el activo superior. MAGERIT utiliza la analogía de los activos inferiores como "pilares" que sostienen la seguridad de los superiores, enfatizando su rol fundamental en la arquitectura de seguridad. Esto es primordial a la hora de desarrollar la aplicación y será tomado en cuenta como un requisito funcional MAGERIT subraya la importancia de valorar los activos superiores en un árbol de dependencias, ya que son intrínsecamente valiosos. Este valor se propaga automáticamente a los activos inferiores de los que dependen, aunque estos últimos también pueden tener su propio valor adicional (CSAE, 2012a, p.23).

Posteriormente, MAGERIT aborda la cuestión del valor de los activos. Clarifica que este valor no se refiere al costo monetario, sino a la importancia y necesidad del activo para la organización. La premisa fundamental es que solo se deben proteger aquellos activos que tienen un valor significativo, es decir, aquellos cuya pérdida o daño tendría consecuencias negativas para la organización. Se relaciona directamente este valor con la "necesidad de proteger", indicando que, a mayor valor de un activo, mayores serán los requerimientos de seguridad para salvaguardarlo. Finalmente, identifica como activos primordiales la información que el sistema gestiona y los servicios que proporciona, denominándolos "esenciales". Los demás activos se consideran subordinados, ya que su importancia deriva de su contribución a la operación y protección de estos activos esenciales. (CSAE, 2012a, p.24).

MAGERIT: Dimensiones de Valoración de Activos

El documento MAGERIT subraya que, para llevar a cabo un análisis de riesgos exhaustivo, resulta crucial calibrar diversas dimensiones del valor de un activo (CSAE, 2012a, p.24). Una de estas dimensiones es la confidencialidad, que se refiere al impacto negativo que se generaría si el activo fuera divulgado a personas no autorizadas. Esta dimensión adquiere una relevancia particular cuando se trata de datos sensibles. Otra dimensión importante es la integridad, que evalúa el perjuicio que podría ocasionar la alteración, la corrupción o la pérdida de datos. Esta dimensión es clave para los datos, ya que su validez y fiabilidad podrían verse comprometidas. Finalmente, se considera la disponibilidad, que mide el impacto que tendría la inaccesibilidad del activo o la imposibilidad de utilizarlo cuando sea necesario. Esta dimensión es especialmente importante para los servicios que la organización ofrece o de los que depende para su operación.

Dentro de la metodología MAGERIT, la valoración de los activos se basa en múltiples criterios, incluyendo integridad, disponibilidad, confidencialidad, trazabilidad y autenticidad. Estos dos últimos aspectos son fundamentales en ciertos contextos donde se requiere

garantizar la capacidad de rastrear todas las interacciones con un activo (trazabilidad) y verificar su origen y validez (autenticidad).

Sin embargo, debido al alcance del proyecto, no se considera necesario incluir la trazabilidad y autenticidad en la valoración de los activos. La razón principal es que la aplicación está enfocada en la gestión de riesgos de seguridad de la información en empresas de desarrollo de software, donde los principales objetivos son identificar, evaluar y mitigar los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información.

Además, el proyecto no aborda auditorías forenses ni escenarios donde la trazabilidad sea crítica, como en entornos regulados con estrictos requerimientos de auditoría (banca, salud, administración pública).

La autenticidad de los activos suele estar más ligada a la gestión de identidades y accesos, un aspecto que, si bien es clave en seguridad, se encuentra fuera del alcance del sistema propuesto, cuyo propósito es facilitar la identificación y tratamiento de riesgos (gestión del riesgo). La inclusión de estos criterios podría añadir complejidad innecesaria al análisis, sin aportar un beneficio significativo dentro del marco de gestión de riesgos planteado.

Por estas razones, la aplicación se centrará en confidencialidad, integridad y disponibilidad (CID), los cuales son los pilares esenciales en la evaluación de riesgos de seguridad de la información dentro del contexto del proyecto.

El documento también trata la valoración de los activos, indicando que esta puede realizarse de manera cuantitativa, mediante la asignación de valores numéricos, o cualitativa, utilizando una escala de niveles predefinidos. Se hace hincapié en dos criterios fundamentales que deben guiar este proceso de valoración (CSAE, 2012a, p.25). El primero es la homogeneidad, que subraya la necesidad de que los valores asignados a los activos, incluso si

corresponden a diferentes dimensiones como la confidencialidad, la integridad y la disponibilidad, sean comparables entre sí.

Esta comparabilidad facilita la combinación de valores propios y heredados, así como la determinación de la gravedad relativa del daño que podría ocurrir en diferentes dimensiones. El segundo criterio es la relatividad, que resalta la importancia de poder establecer comparaciones entre el valor de un activo específico y el valor de otros activos que forman parte del mismo sistema de información.

MAGERIT: Amenazas y su Valoración

El documento MAGERIT aborda el segundo paso fundamental en el análisis de riesgos: la identificación de las amenazas que pueden afectar a los activos previamente definidos. Define las amenazas como "cosas que ocurren" y, específicamente, aquellas que pueden causar daño a los activos de la organización.

MAGERIT clasifica las amenazas en las siguientes categorías (CSAE, 2012a, p.27):

- **De origen natural:** Eventos como terremotos o inundaciones, ante los cuales el sistema de información es una víctima pasiva. No obstante, el documento enfatiza la necesidad de considerar sus posibles consecuencias.
- **Del entorno (de origen industrial):** Desastres como contaminación o fallos eléctricos, donde el sistema también es una víctima pasiva. MAGERIT señala que la pasividad no implica indefensión.
- **Defectos de las aplicaciones:** Problemas inherentes al diseño o implementación del propio sistema, a menudo denominados vulnerabilidades técnicas.
- **Causadas por las personas de forma accidental:** Errores u omisiones no intencionados por parte de personas con acceso al sistema.

- **Causadas por las personas de forma deliberada:** Acciones intencionadas para obtener un beneficio indebido o causar daño al sistema por parte de personas con acceso.

MAGERIT subraya que no todas las amenazas afectan a todos los activos, existiendo una relación específica entre el tipo de activo y las amenazas potenciales (CSAE, 2012a). Una vez identificada una amenaza que puede impactar un activo, el documento establece la necesidad de valorar su influencia en el valor del activo en dos dimensiones (CSAE, 2012a, p.28): Degradación, la magnitud del perjuicio que la materialización de la amenaza causaría al valor del activo. Probabilidad, la posibilidad de que la amenaza realmente ocurra.

MAGERIT: Salvaguardas

Se introduce el concepto de salvaguardas como procedimientos o mecanismos tecnológicos diseñados para disminuir el riesgo. Se destaca que, en los pasos previos del análisis, no se consideraron las salvaguardas existentes, por lo que los impactos y riesgos evaluados representan la exposición de los activos en ausencia total de protección (CSAE, 2012a, p.31).

Según MAGERIT, las salvaguardas influyen en el cálculo del riesgo de dos maneras principales (CSAE, 2012a, p.32). Primero, reducen la probabilidad de que una amenaza se materialice a través de salvaguardas preventivas, cuyo objetivo ideal es impedir que el evento ocurra. Segundo, actúan limitando el daño causado en caso de que la amenaza se concrete, mitigando así sus consecuencias mediante medidas de contención y respuesta. Salvaguardas que directamente limitan la posible degradación del activo.

MAGERIT: Impacto y Determinación del Riesgo Potencial

El documento MAGERIT detalla cómo se determina el impacto de las amenazas sobre los activos y cómo este, junto con la probabilidad, permite calcular el riesgo potencial (CSAE, 2012a).

Impacto Potencial.

MAGERIT establece que el impacto potencial se puede determinar al combinar el valor de los activos con la degradación que las amenazas pueden causarles (CSAE, 2012a, p.28).

Impacto Acumulado.

Este concepto se refiere al impacto calculado sobre un activo, considerando (CSAE, 2012a, p.29) su valor acumulado, que incluye su valor propio más el valor acumulado de los activos de los que depende. Las amenazas a las que está expuesto.

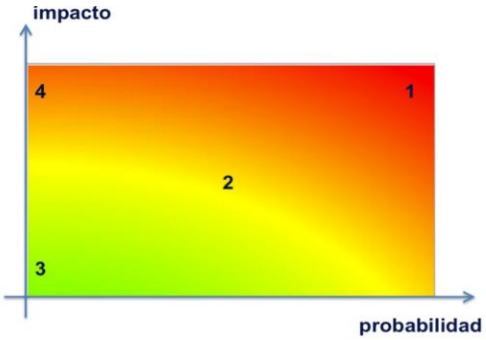
El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, y es una función del valor acumulado y la degradación causada.

MAGERIT explica que el riesgo aumenta tanto con el impacto como con la probabilidad de la amenaza. Se distinguen cuatro zonas para el tratamiento del riesgo (CSAE, 2012a, p.30):

1. **Zona 1:** Riesgos muy probables y de muy alto impacto.
2. **Zona 2** (Franja Amarilla): Un rango amplio que va desde situaciones improbables con impacto medio hasta situaciones muy probables con impacto bajo o muy bajo.
3. **Zona 3:** Riesgos improbables y de bajo impacto.
4. **Zona 4**: Riesgos improbables, pero de muy alto impacto.

Figura 3

Zonas de riesgo



Nota. Este cuadro muestra las zonas de riesgo en los que se puede ubicar una organización (p.49). Tomado de MAGERIT I. por Centro Superior de Administración Electrónica (CSAE), 2012.

Riesgo Acumulado.

Se calcula sobre un activo considerando el impacto acumulado sobre el activo debido a una amenaza y la probabilidad de la amenaza.

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, y es una función del valor acumulado, la degradación causada y la probabilidad de la amenaza. MAGERIT señala que el riesgo acumulado es útil para determinar las salvaguardas necesarias para los medios de trabajo, como la protección de equipos y las copias de respaldo. (CSAE, 2012a, p.30).Según MAGERIT el análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

Figura 4

Método de Análisis de Riesgos

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Nota. Tareas a realizar en un análisis de riesgos (p.36). Tomado de MAGERIT I. por Centro Superior de Administración Electrónica (CSAE), 2012.

Estas tareas serán tomadas como requisitos funcionales dentro de la aplicación de gestión de riesgos de seguridad de la información, Además MAGERIT proporciona una lista de tareas específicas para el análisis del riesgo, actividades que también estarán presentes en la aplicación.

Figura 5

Lista de control de Método de Análisis de Riesgos

3.4. Lista de control

√	actividad	tarea
	Se han identificado los activos esenciales: información que se trata y servicios que se prestan	MAR.11
	Se han valorado las necesidades o niveles de seguridad requeridos por cada activo esencial en cada dimensión de seguridad	MAR.13
	Se han identificado los demás activos del sistema	MAR.11
	Se han establecido el valor (o nivel requerido de seguridad) de los demás activos en función de su relación con los activos esenciales (por ejemplo, mediante identificación de las dependencias)	MAR.12
	Se han identificado las amenazas posibles sobre los activos	MAR.21
	Se han estimado las consecuencias que se derivarían de la materialización de dichas amenazas	MAR.22
	Se ha estimado la probabilidad de que dichas amenazas se materialicen	MAR.23
	Se han estimado los impactos y riesgos potenciales, inherentes al sistema	MAR.4
	Se han identificado las salvaguardas apropiadas para atajar los impactos y riesgos potenciales	MAR.31
	Se ha valorado el despliegue de las salvaguardas identificadas	MAR.32
	Se han estimado los valores de impacto y riesgo residuales, que es el nivel de impacto y riesgo que aún soporta el sistema tras el despliegue de las salvaguardas	MAR.4

Nota. Lista de control de tareas a realizar en un análisis de riesgos (p.46). Tomado de MAGERIT I. por Centro Superior de Administración Electrónica (CSAE), 2012.

Análisis Libro II. Catálogo De Elementos MAGERIT

Sirve como una referencia estructurada que facilita la identificación y clasificación de los componentes clave involucrados en la gestión de riesgos de seguridad de la información. Su propósito principal es proporcionar un inventario detallado de elementos que permitan un análisis de riesgos más preciso y sistemático(CSAE, 2012b).

Clasificación de Activos

En un sistema de información, MAGERIT identifica dos elementos esenciales: la información que se procesa y los servicios que se ofrecen (CSAE, 2012b, pp. 8, 14). En este sentido, la metodología ayuda a identificar y categorizar los diversos activos de información que podrían estar expuestos a riesgos. Estos activos incluyen datos, elementos criptográficos, servicios ofrecidos, software utilizado, hardware de los sistemas, comunicaciones, documentación de soporte, elementos auxiliares, instalaciones físicas y el personal que interactúa con el sistema. Además de la identificación, MAGERIT facilita la priorización de estos activos en función de su valor estratégico para la organización y la criticidad de su función dentro del sistema de información.

Identificación de Amenazas

Proporciona una lista estructurada de amenazas potenciales que pueden afectar los activos. Según MAGERIT, las amenazas se dividen en cinco categorías principales (CSAE, 2012b, p. 25,52):

- Naturales (desastres naturales como incendios, inundaciones).
- Industriales (fallos en infraestructuras o equipos).

- Defectos de aplicaciones (errores en el desarrollo de software o configuraciones incorrectas).
- Ataques accidentales (errores humanos o negligencia).
- Ataques intencionados (ciberataques, fraude, sabotaje).

Salvaguardas

Las salvaguardas permiten mitigar las amenazas (CSAE, 2012b, p. 53,58) presentan medidas de protección aplicables a cada tipo de amenaza y activo además de que permite seleccionar controles adecuados para mitigar los riesgos identificados.

Criterios de valoración

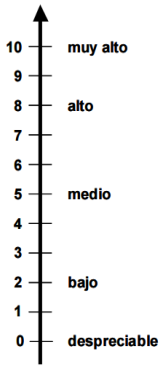
El documento MAGERIT presenta dos escalas para la valoración de activos (CSAE, 2012b, p. 19):

Una detallada de diez valores y una simplificada de cinco niveles. La escala detallada de diez valores incluye el valor 0, que se define como un valor despreciable a efectos de riesgo. Esto implica que los activos con valor 0 no se consideran significativos en el análisis de riesgos.

Para análisis de riesgos menos exhaustivos, MAGERIT propone una escala simplificada de cinco niveles. El documento indica que existe una correlación entre ambas escalas, lo que sugiere que los niveles de la escala simplificada se corresponden con rangos de valores de la escala detallada. La existencia de estas dos escalas permite adaptar la profundidad del análisis de riesgos a las necesidades específicas de la organización y al nivel de detalle requerido. La escala detallada proporciona una mayor granularidad en la valoración, mientras que la escala simplificada ofrece una visión más general pero igualmente útil para ciertos contextos.

Figura 6

Criterios de valoración de un activo



valor		*criterio*
10	muy alto	daño muy grave a la organización
7-9	alto	daño grave a la organización
4-6	medio	daño importante a la organización
1-3	bajo	daño menor a la organización
0	despreciable	irrelevante a efectos prácticos

Nota. Lista de control de tareas a realizar en un análisis de riesgos (p.19). Tomado de MAGERIT II. por Centro Superior de Administración Electrónica (CSAE), 2012.

MAGERIT Libro III. Libro de Técnicas

Proporciona un conjunto de herramientas y metodologías que facilitan la aplicación práctica del análisis y gestión de riesgos. Este documento actúa como una guía complementaria a los otros libros de MAGERIT, ofreciendo procedimientos específicos para evaluar amenazas, calcular impactos y establecer controles de seguridad de manera sistemáticas(CSAE, 2012c).

Definir los métodos de análisis de riesgos

Se emplean técnicas cualitativas y cuantitativas descritas en el libro para evaluar amenazas, vulnerabilidades y su impacto en los activos de información (CSAE, 2012c, p.8,16).

Clasificación y evaluación de riesgos

Se aplican técnicas de cálculo para determinar el nivel de riesgo inherente (antes de aplicar controles) y el riesgo residual (después de la implementación de medidas de seguridad) (CSAE, 2012c, p.22,23). Se utiliza la metodología propuesta en MAGERIT para relacionar la probabilidad de ocurrencia con el impacto en la organización, reflejándose en una matriz de riesgos dentro del sistema.

Identificación y selección de controles de seguridad

La aplicación implementa los lineamientos de MAGERIT para seleccionar controles adecuados basados en el tipo de riesgo identificado (CSAE, 2012c, p.20). Se complementa con los controles definidos en la **ISO 27002**, garantizando una alineación con buenas prácticas internacionales.

Los tres libros de MAGERIT proporcionan un enfoque estructurado y detallado para el análisis de riesgos en sistemas de información, lo que los convierte en una referencia clave para la gestión de seguridad en organizaciones. El Libro I establece el marco metodológico, definiendo los principios, procesos y objetivos de la gestión del riesgo, asegurando que la toma de decisiones se base en un análisis detallado de amenazas y vulnerabilidades (CSAE, 2012a). El Libro II actúa como un catálogo de referencia que permite estandarizar los elementos del análisis, facilitando la identificación de activos, amenazas y salvaguardas, lo que mejora la coherencia y comparabilidad de los resultados(CSAE, 2012b). Finalmente, el Libro III proporciona técnicas y herramientas específicas para la valoración y modelado del riesgo, permitiendo que los análisis sean replicables y cuantificables (CSAE, 2012c).

Dentro de la aplicación de gestión de riesgos de seguridad de la información, estos tres libros sirven de base para estructurar el proceso de identificación, evaluación y documentación del riesgo antes de proceder al tratamiento. La combinación de estos enfoques permite que el sistema garantice un análisis preciso y alineado con estándares internacionales, facilitando la toma de decisiones basada en la criticidad de los riesgos detectados. Para la fase de tratamiento del riesgo, la aplicación se complementará con las normas **ISO 27001 e ISO 27002**, asegurando un enfoque integral que no solo identifica riesgos, sino que también proporciona mecanismos efectivos para su mitigación y control.

Análisis de la ISO/IEC 27001:2022 Seguridad de la información, Ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información.

La ISO 27001:2022 es una norma internacional enfocada en la gestión de riesgos de seguridad de la información dentro de una organización. Su propósito es proporcionar un marco sistemático para establecer, operar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la confidencialidad, integridad y disponibilidad de los datos. A diferencia de otros enfoques de seguridad, la ISO 27001 está centrada en el riesgo del negocio, alineando la seguridad de la información con los objetivos estratégicos de la empresa(Culot et al., 2021).

Un SGSI se compone de políticas, procedimientos, guías, recursos y actividades, que trabajan en conjunto para mitigar riesgos y asegurar la protección de la información en todas sus formas, ya sea digital, física o en tránsito. Dentro de este enfoque, es importante diferenciar entre seguridad de la información y ciberseguridad: mientras que la seguridad de la información abarca la protección de los datos en general, la ciberseguridad se enfoca en la protección de los sistemas tecnológicos frente a amenazas cibernéticas, como ataques informáticos, malware o robo de datos(ISO, 2022a).

La versión 2022 de la norma introduce una actualización significativa en la estructura de sus controles. En comparación con la versión anterior de 2013, el número de controles pasó de 114 a 93, organizados en 4 grupos en lugar de 14 cláusulas. Además, se incorporaron 11 nuevos controles, enfocados en áreas clave como seguridad en la nube, inteligencia de amenazas, monitoreo y continuidad del negocio. Se fusionaron 24 controles para reducir redundancias, y se eliminaron aquellos que no aportaban valor a la gestión del SGSI(NQA, 2022).

Según la guía de implementación de sistemas de gestión de seguridad de la información desarrollada por el organismo de certificación global NQA, la implementación de la norma ISO 27001 aporta múltiples beneficios. Entre ellos se destaca el fortalecimiento de la gobernanza del riesgo corporativo, la promoción de buenas prácticas de seguridad reconocidas

a nivel mundial y la creación de un lenguaje común para la seguridad de la información dentro de la organización. Además, contribuye al aumento de la confianza de los clientes y demás partes interesadas, facilita la obtención de una certificación internacional que mejora la competitividad en el mercado y optimiza las inversiones en seguridad, asegurando un retorno eficiente a través de la implementación de medidas de protección adecuadas.

Los principios y beneficios de la ISO 27001:2022 están directamente acoplados a la aplicación de gestión de riesgos de seguridad de la información, ya que esta herramienta está diseñada para automatizar y optimizar la identificación, evaluación y tratamiento de riesgos dentro de las empresas de desarrollo de software. Asimismo, la aplicación actúa como un soporte para la certificación en ISO 27001, ya que proporciona una metodología clara para documentar y evidenciar la gestión de riesgos. Con esto, las empresas pueden fortalecer su postura de seguridad, aumentar la confianza de sus clientes y socios comerciales, y mejorar su competitividad en el mercado.

La ISO 27001:2022 establece una estructura basada en cláusulas que van desde la 4 hasta la 10, las cuales forman la base para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) y siguen el ciclo de mejora continua PHVA (Planificar-Hacer-Verificar-Actuar)(ISO, 2022a).

Cláusulas 4 A 10 y su Relación con PHVA según ISO: IEC 27001:2022

Contexto de la organización (Cláusula 4 - Planificar).

La organización debe identificar los factores internos y externos que afectan la seguridad de la información, determinar sus partes interesadas y definir el alcance del SGSI.

Liderazgo (Cláusula 5 - Planificar).

La alta dirección debe demostrar compromiso con la seguridad de la información, estableciendo políticas, roles y responsabilidades.

Planificación (Cláusula 6 - Planificar).

Se enfoca en la identificación y tratamiento de riesgos, estableciendo objetivos de seguridad alineados con la organización. La aplicación facilita este proceso permitiendo priorizar y analizar riesgos inherentes y residuales para planificar su tratamiento de manera estructurada.

Soporte (Cláusula 7 - Hacer).

Incluye la gestión de recursos, competencias, comunicación y documentación del SGSI.

Operación (Cláusula 8 - Hacer).

Requiere implementar y gestionar los controles de seguridad de la información. La aplicación automatiza este proceso al permitir mapear los controles de la ISO 27002, asegurando que las empresas implementen medidas efectivas para mitigar riesgos.

Evaluación del desempeño (Cláusula 9 - Verificar).

Se deben monitorear, medir y analizar los procesos de seguridad para garantizar su efectividad. La aplicación proporciona métricas y reportes que permiten evaluar la efectividad de los controles implementados y ajustar estrategias si es necesario.

Mejora continua (Cláusula 10 - Actuar).

Se enfoca en la corrección y mejora del SGSI basándose en hallazgos y no conformidades. La aplicación apoya este proceso permitiendo realizar seguimientos, auditorías y ajustes en la gestión del riesgo, asegurando un ciclo de mejora constante.

Es importante señalar que, aunque la aplicación se encuentra alineada con la norma ISO 27001:2022, esta no posee la facultad de certificar a una organización bajo dicha normativa. En cambio, la aplicación ofrece herramientas fundamentales que simplifican la

implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), concentrándose en las fases más complejas y que suelen generar mayores costos dentro del proceso de certificación.

En primer lugar, se encuentra la Planificación del Riesgo (correspondiente a la Cláusula 6 - Planificar de la ISO 27001:2022). La aplicación capacita a la organización para identificar y evaluar los riesgos inherentes a la seguridad de la información, permitiendo el establecimiento de estrategias de tratamiento que se ajusten a las necesidades específicas de la empresa. Esta etapa reviste una gran exigencia en el proceso de certificación, dado que demanda un análisis minucioso de los activos de información, las posibles amenazas y las vulnerabilidades existentes.

En segundo lugar, la aplicación aborda la Operación del Riesgo (vinculada a la Cláusula 8 - Hacer de la ISO 27001:2022). La herramienta facilita la gestión operativa de los riesgos a través de la implementación de controles de seguridad que se basan en la norma ISO 27002. Esto permite a la organización documentar y llevar a cabo el seguimiento del tratamiento de los riesgos identificados. Esta etapa se considera crucial, ya que implica la ejecución concreta de las medidas de seguridad dentro del entorno operativo de la organización. La norma ISO 27001 enfatiza la gestión del riesgo como pilar central del SGSI. Esto se relaciona directamente con la aplicación, ya que su funcionalidad principal es permitir la identificación, análisis, evaluación y tratamiento de riesgos de seguridad de la información dentro de las empresas de desarrollo de software. Además, La ISO 27002 complementa la ISO 27001 proporcionando un catálogo detallado de controles de seguridad, lo que facilita la implementación de medidas de protección dentro de la aplicación (NQA, 2022).

La app permite a los usuarios asignar controles específicos a los riesgos identificados, asegurando que la gestión del riesgo esté alineada con los estándares internacionales. Aunque la aplicación no cubre completamente la fase de "Verificar y Actuar" del PHVA, proporciona una

base estructurada para futuras mejoras en la seguridad de la información, asegurando que las empresas puedan adaptar y actualizar su gestión del riesgo con el tiempo. La aplicación no reemplaza un SGSI completo ni garantiza la certificación ISO 27001, pero representa un soporte valioso para estructurar y agilizar el proceso de gestión de riesgos, especialmente en sus fases más críticas, ayudando a las empresas a acercarse a los requisitos exigidos.

Análisis ISO/IEC 27002:2022 Seguridad de la información, Ciberseguridad y protección de la privacidad - Controles de seguridad de la información

Mientras que la ISO 27001 establece los requisitos para implementar un SGSI, la ISO 27002 proporciona un catálogo detallado de controles de seguridad que pueden aplicarse para mitigar los riesgos identificados (NQA, 2022). En la aplicación, estos controles se utilizan en la fase de tratamiento del riesgo, permitiendo que los usuarios asocien controles específicos a cada riesgo identificado.

Estructura de la ISO/IEC 27002:2022

La norma ISO/IEC 27002:2022 presenta una reestructuración significativa de sus controles, agrupándolos en cuatro dominios principales en lugar de las catorce cláusulas de la versión anterior (ISO/IEC 27002:2013).

El primer dominio corresponde a los controles organizacionales. Estos se centran en la definición de las políticas, los procedimientos y las medidas de gestión que son esenciales para asegurar una gobernanza efectiva de la seguridad de la información dentro de la organización.

En segundo lugar, los controles de personas. Este dominio pone el foco en la concienciación, la formación y el control del comportamiento humano. Su objetivo principal es la reducción de los riesgos que se originan por errores humanos o por amenazas internas a la seguridad de la información.

El tercer dominio abarca los controles físicos. Estos controles están dedicados a la protección de los activos físicos y de la infraestructura de tecnología de la información. Su propósito es prevenir accesos no autorizados, daños o cualquier tipo de sabotaje que pueda afectar a estos elementos.

Finalmente, el cuarto dominio se refiere a los controles tecnológicos. Estos controles se relacionan directamente con la ciberseguridad y la protección de los sistemas de información. Su implementación busca establecer mecanismos técnicos robustos para evitar intrusiones y, de esta manera, garantizar la confidencialidad, la integridad y la disponibilidad de los datos manejados por la organización.

Además, Se han reducido los controles de 114 a 93, con fusiones y la adición de 11 nuevos controles, incluyendo inteligencia de amenazas, seguridad en la nube, monitoreo de seguridad, eliminación de la información, encriptación de datos y codificación segura (ISO, 2022b).

En el contexto de la aplicación de gestión de riesgos de seguridad de la información, la ISO 27002 es clave para definir el tratamiento del riesgo, ya que proporciona un marco de referencia para:

- Asignar controles adecuados a cada riesgo identificado.
- Clasificar los controles en preventivos, detectivos y correctivos según su función en la mitigación de riesgos.
- Proporcionar un catálogo de controles para que las empresas elijan los más adecuados según sus necesidades y presupuesto.
- Facilitar la generación de reportes que permitan evidenciar qué controles han sido implementados y su impacto en la reducción del riesgo.

Es importante aclarar que no todos los controles de la ISO 27002 son aplicables a todas las organizaciones o contextos. En la ISO 27001, la selección de controles se realiza mediante una Declaración de Aplicabilidad (SoA, Statement of Applicability), la cual justifica qué controles son relevantes y cuáles pueden ser excluidos en función del análisis de riesgos y las necesidades específicas de la empresa.

Sin embargo, este proceso de selección queda fuera del alcance del proyecto, ya que la aplicación no impone el uso obligatorio de controles específicos, sino que ofrece los controles de la ISO 27002 como una guía para ayudar a las empresas a fortalecer su postura de seguridad de la información.

Dentro de la aplicación, los administradores tienen la capacidad de asignar los controles de seguridad más apropiados para cada riesgo que haya sido identificado. Estos controles se pueden clasificar en tres categorías principales. Los controles preventivos son aquellos que se implementan con el objetivo de evitar que un incidente de seguridad llegue a ocurrir. Los controles detectivos son mecanismos diseñados para identificar y registrar cualquier evento o actividad que pueda comprometer la seguridad del sistema o de la información. Finalmente, los controles correctivos son las acciones que se toman una vez que un incidente de seguridad ha ocurrido, con el fin de minimizar su impacto y restaurar la normalidad de las operaciones.

La selección de controles se alinea con el nivel de riesgo identificado, ayudando a priorizar qué medidas deben implementarse según la criticidad de los activos y la exposición a amenazas.

Análisis ISO/IEC 27005: Gestión del Riesgo en la Seguridad de la Información

La NTC ISO/IEC 27005 es una norma internacional que proporciona directrices específicas para la gestión de riesgos de seguridad de la información, complementando el marco general definido por la ISO/IEC 27001. A diferencia de esta última, que se enfoca en los

requisitos para establecer un Sistema de Gestión de Seguridad de la Información (SGSI), la 27005 profundiza en el proceso de análisis y tratamiento del riesgo, describiendo con mayor detalle cada fase e incluyendo métodos prácticos de evaluación (ISO, 2009b).

En este proyecto, la norma NTC ISO/IEC 27005 fue utilizada como referencia clave, particularmente en la fase de tratamiento del riesgo. La aplicación desarrollada integra sus lineamientos al permitir que los usuarios identifiquen opciones de tratamiento como aceptar, transferir, evitar o mitigar el riesgo, justifiquen la decisión tomada con base en requerimientos legales, contractuales o de negocio, asignen de forma clara un responsable del riesgo, e implementen controles de seguridad específicos. Además, permite evaluar la efectividad de dichos controles a través del cálculo automatizado del riesgo residual, lo cual contribuye a una gestión más estructurada y fundamentada en estándares internacionales.

Alcance de la Aplicación de Gestión de Riesgos de Seguridad de la Información Previo a las Reuniones con Diferentes Empresas de Software de Yopal

Habiendo identificado y analizado las 3 normas principales que se van a usar, el alcance del proyecto quedaría reducido de la siguiente manera:

Aplicación dirigida a empresas de desarrollo de software en Yopal especialmente a aquellas que busquen fortalecer su gestión de los riesgos de seguridad de la información, y alinearse a estándares internacionales como ISO 27001. También podría ser útil para consultores en ciberseguridad, auditores de seguridad de la información e implementadores de normativas de seguridad, quienes requieren herramientas eficientes para evaluar, mitigar riesgos en entornos digitales. Además, puede ser utilizada por gerentes de TI y responsables de seguridad informática, permitiéndoles mejorar la protección de los activos de información y optimizar la toma de decisiones en materia de ciberseguridad.

La Gestión del Riesgo de la aplicación constara de las siguientes partes:

1. Análisis del riesgo
2. Tratamiento del riesgo

Módulos de la Aplicación para la gestión de riesgos de seguridad de la información:

I. Módulo de gestión del riesgo

A. Análisis del riesgo asociado a empresas

1. Nombre de la empresa
2. Número de empleados
3. Responsable de la seguridad de la información

II. Módulo de activos

A. Añadir activo

1. ID único
2. Tipo/Categoría de activo
3. Ubicación (Física/Lógica)
4. Dependencia del activo
5. Propietario /Responsable del activo
    a) Es el que determina el valor que tiene el activo
6. Control existente

B. Valoración del activo - Valoración Cuantitativa y Cualitativa

1. Integridad
    a) Medir las consecuencias de que el activo sea modificado sin autorización
2. Disponibilidad
    a) Medir las consecuencias operativas y financieras
3. Confidencialidad

a) Medir las consecuencias legales, reputacionales y financieras

C. Priorización de activos

1. Matriz de priorización
    a) Impacto
    b) Probabilidad

III. Módulo de Riesgos asociado a los Activos

A. Identificar Amenazas

1. Fuente de la amenaza
    a) Natural
    b) Humano
        (1) Accidentales
        (2) Deliberadas

B. Identificar Vulnerabilidades

C. Estimación del riesgo/Consecuencias -

1. Identificar la probabilidad - Valoración Mixta
2. Identificar el impacto Valoración Cualitativa
3. Cálculo del riesgo
4. Valoración y Priorización del riesgo

IV. Módulo del Tratamiento del Riesgo - Plan de tratamiento de Riesgos

A. Definir controles de seguridad

1. Mitigar/ Reducir
    a) Reducir la probabilidad o el impacto del riesgo mediante controles de seguridad
2. Transferir

a) Transferir el riesgo a un tercero (mediante seguros o outsourcing).

3. Evitar

a) Eliminar el riesgo al eliminar la actividad o el activo que lo genera.

4. Aceptar

a) Aceptar el riesgo cuando el costo de mitigarlo es mayor que el impacto potencial

B. Asignación de responsables

C. Riesgo Residual

D. ISO 27002 controles

E. Descripción del plan tratamiento de riesgos

Análisis de Requerimientos Basado en las Entrevistas a Empresas de Software de Yopal.

A partir de las entrevistas realizadas a empresas de desarrollo de software en Yopal, se han identificado diversos aspectos clave sobre la gestión de riesgos de seguridad de la información. Se ha categorizado la información en función de los requisitos funcionales, no funcionales, cumplimiento normativo y expectativas generales respecto a la aplicación en desarrollo.

Empresa Puntualtic

La empresa PuntualTIC implementa algunas prácticas de seguridad en su proceso de desarrollo de software, aunque no cuenta con una política de seguridad de la información formalmente establecida. Sus medidas de seguridad incluyen el acceso restringido y otros controles básicos. Destaca la aplicación de la metodología OWASP en sus desarrollos, lo cual sugiere un enfoque en la seguridad del software desde una perspectiva técnica, aunque sin un marco organizacional de gestión de riesgos consolidado.

Sin embargo, la seguridad no es una prioridad para la empresa, ya que su enfoque está orientado en la rapidez de entrega de los productos. No utilizan herramientas para la gestión de riesgos, lo que indica una falta de sistematización en la identificación y mitigación de amenazas. Actualmente, la empresa gestiona los riesgos asociados a dependencias y librerías de software de manera manual, lo que representa un posible punto de debilidad. Un miembro del equipo verifica manualmente la seguridad y actualización de las librerías utilizadas.

Si bien cuentan con un documento de recuperación de desastres y algunas políticas de respaldo, no tienen un plan formal de tratamiento de riesgos. Además, aunque realizan seguimiento a los controles de seguridad, este solo aplica a los productos que desarrollan y no a su proceso de desarrollo interno.

Según la información proporcionada por la empresa a través de la entrevista, la aplicación debe cumplir con una serie de aspectos fundamentales en cuanto a su funcionalidad y características clave.

En primer lugar, la aplicación debe facilitar la gestión de activos de información. Esto implica que debe permitir a la organización la identificación y la clasificación de aquellos activos que son considerados críticos para su operación.

En segundo lugar, se requiere la evaluación de riesgos. La aplicación debe ofrecer herramientas específicas para llevar a cabo el análisis de las posibles amenazas y vulnerabilidades que puedan afectar a la seguridad de la información. Asimismo, debe posibilitar el establecimiento de planes de mitigación para abordar estos riesgos de manera efectiva.

En tercer lugar, la herramienta debe contar con la capacidad de generar reportes automatizados. Estos reportes deben proporcionar información relevante sobre el estado actual del tratamiento de los riesgos identificados, facilitando el seguimiento y la toma de decisiones.

Un cuarto aspecto crucial es que la aplicación debe poseer una interfaz intuitiva. Esto significa que su diseño debe ser fácil de comprender y utilizar, de manera que los usuarios no requieran una capacitación especializada para poder interactuar con ella de forma eficiente.

En quinto lugar, se destaca la compatibilidad con estándares de seguridad. Es importante que la aplicación se encuentre alineada con metodologías reconocidas en el ámbito de la seguridad de la información, como OWASP, especialmente en lo referente al desarrollo seguro de software.

Finalmente, un sexto aspecto a considerar es el almacenamiento seguro. Dentro de la aplicación, se deben implementar medidas de protección robustas para garantizar la confidencialidad, la integridad y la disponibilidad de toda la información sensible que se gestione a través de ella.

Oportunidades y Desafíos Según Puntualtic

Entre las oportunidades, se destaca en primer lugar la existencia de una necesidad cada vez mayor de soluciones de seguridad de la información en sectores específicos como las Entidades Promotoras de Salud (EPS) y las Instituciones Prestadoras de Servicios de Salud (IPS). Esta creciente demanda amplía significativamente el mercado potencial al que la aplicación podría dirigirse.

En segundo lugar, se menciona el interés expresado por Puntualtic en participar en una fase piloto para probar el software. Esta disposición representa una oportunidad valiosa para obtener retroalimentación directa y validar la efectividad de la aplicación en un entorno real.

Además, se sugiere que el software podría lograr una diferenciación importante si se posiciona no solo como una herramienta de gestión de riesgos, sino también como un recurso educativo en el ámbito de la seguridad de la información.

En cuanto a los desafíos, se señala en primer lugar que la seguridad de la información podría no ser percibida como una prioridad dentro de la cultura organizacional de la empresa. Esta situación podría generar dificultades en el proceso de adopción de la aplicación.

En segundo lugar, se indica que Puntualtic actualmente no cuenta con políticas de seguridad de la información claramente definidas. Esta falta de un marco normativo interno podría generar resistencia al cambio y dificultar la implementación de la aplicación.

Finalmente, en tercer lugar, se observa que la mayoría de los controles de seguridad existentes en la empresa son de naturaleza manual y no están sistematizados. Esto implica la necesidad de abordar una automatización progresiva de estos controles, lo cual podría requerir tiempo y recursos adicionales.

Nota: La entrevista completa se puede ver en el anexo J , así como el documento donde se encuentran diligenciadas las respuestas y la constancia de la reunión.

Empresa Delta Solutions

Delta Solutions ha adoptado ciertas medidas de seguridad en su desarrollo de software, como el uso de las últimas versiones de los frameworks en los que trabaja y la implementación de una arquitectura serverless. Sin embargo, la empresa no cuenta con una estrategia integral para la gestión de riesgos de seguridad de la información.

Actualmente, Delta Solutions no utiliza ninguna herramienta para la gestión de riesgos de seguridad de la información. La razón principal es que no han sido atacados directamente, lo que ha generado una percepción de baja prioridad en la implementación de controles formales.

Sin embargo, la empresa reconoce que enfrenta dificultades en la identificación, evaluación y tratamiento de riesgos debido a la falta de experiencia en este ámbito. Además,

aunque no han sido atacados de manera directa, su software desarrollado para terceros ha sido víctima de ataques, especialmente de phishing.

El monitoreo de seguridad en Delta Solutions es llevado a cabo de manera informal y sin herramientas automatizadas. No cuentan con documentación formal para la gestión de riesgos ni con un plan de tratamiento de riesgos, lo que puede afectar la capacidad de respuesta ante incidentes de seguridad. La empresa no gestiona de manera sistemática los riesgos asociados a las librerías y dependencias de software, realizando revisiones manuales cada tres meses. Asimismo, no realizan seguimiento formal a los controles de seguridad implementados.

Necesidades Funcionales Identificadas.

A. Plan de tratamiento del riesgo

Requisitos No Funcionales.

Delta Solutions considera la necesaria la incorporación de un módulo de ayuda o capacitación dentro de la aplicación al igual que Puntualtic.

Cumplimiento Normativo.

En sus procesos internos, la empresa no sigue normativas o metodologías de seguridad de la información como ISO 27001, NIST, MAGERIT u OWASP. Esto representa una oportunidad para mejorar su gestión de riesgos alineándose con estándares reconocidos. La empresa está dispuesta a participar en una fase piloto y probar el software una vez finalizado su desarrollo. Además, considera que una herramienta de este tipo es relevante para fortalecer la gestión de riesgos de seguridad de la información en empresas de desarrollo de software en Yopal.

Nota: La entrevista completa se puede ver en anexo H así como el documento donde se encuentran diligenciadas las respuestas

Una vez finalizada la recolección y análisis de los requerimientos obtenidos a través de entrevistas con empresas de desarrollo de software en Yopal, se procede a consolidar esta información con los lineamientos establecidos en normativas y metodologías reconocidas en seguridad de la información. Entre estas, se consideran la norma ISO 27001, que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI); la metodología MAGERIT, en sus tres libros, que proporciona un marco para el análisis y gestión de riesgos tecnológicos; y la norma ISO 27002, que detalla los controles de seguridad recomendados para la protección de la información.

El cruce de estas normativas con las necesidades y prácticas identificadas en las entrevistas permitirá definir los requisitos funcionales del software. Este proceso garantizará que la solución propuesta no solo se alinee con estándares internacionales de seguridad, sino que también responda a los desafíos y expectativas reales de las empresas consultadas, asegurando una herramienta eficaz para la gestión de riesgos de seguridad de la información.

Requisitos Funcionales y No Funcionales de la aplicación una vez completado el análisis de las normas y las entrevistas a las empresas de desarrollo de software de Yopal.

Requisitos Funcionales

1. **Creación de la gestión del riesgo**

- RF1: Permitir la creación de un análisis de riesgo asociado a empresas,
    - RF1.1: Registrar el nombre de la empresa.
    - RF1.2: Registrar el número de empleados de la empresa.
    - RF 1.3: Identificar al responsable de la seguridad de la información dentro de la empresa.

2. **Gestión de Activos**

- RF2: Permitir el registro y clasificación de activos
- RF3: Identificar las dependencias entre activos
- RF4: Identificar control existente al activo
- RF5: Asignar un valor a cada activo basado en su criticidad
- RF6: Permitir la asignación de responsables y dueños de cada activo.

3. **Identificación de Riesgos**

- RF7: Permitir la identificación de amenazas asociadas a los activos.
- RF8: Permitir la identificación de vulnerabilidades asociadas a los activos.
- RF9: Facilitar la relación entre activos, amenazas y vulnerabilidades para identificar riesgos.

4. **Evaluación y Priorización de Riesgos**

- RF10: Identificar la probabilidad.
- RF11: Identificar el impacto.
- RF12: Calculo del riesgo.
- RF13: Priorizar los riesgos según su criticidad.
- RF14: Permitir la visualización de riesgos en un Dashboard
- RF15: Visualizar el riesgo Inherente en una matriz de riesgos
- RF16: Identificar el nivel de aceptación del riesgo.

5. **Tratamiento de Riesgos**

- RF17: Ofrecer opciones de tratamiento de riesgos (mitigar, transferir, evitar, aceptar).
- RF18: Permitir la selección de controles de seguridad basados en la norma ISO 27002.

- RF19: Medir la probabilidad e impacto una vez identificados los controles que se van a usar para reducir el riesgo inherente.
- RF20: Medir el riesgo residual
- RF21: Permitir la creación de planes de acción para la implementación de controles.
- RF22: Asignar responsables y plazos para la implementación de controles.
- RF23: Identificar si el tratamiento al riesgo se hace producto de un requerimiento legal, obligación contractual, o requerimiento de negocio.

6. Reportes y Documentación

- RF24: Generar reportes personalizados sobre el estado de los riesgos y controles.
- RF25: Exportar reportes en formatos estándar (PDF, Excel).

7. Autenticación y Gestión de Usuarios

- RF26 Permitir el inicio de sesión mediante autenticación de usuarios (nombre de usuario y contraseña)
- RF27: Implementar roles de usuario diferenciados
    - RF27.1 **Superusuario:** Accede a las estadísticas de las empresas registradas en el software.
    - RF27.2 **Administrador:** Gestiona los usuarios y configuraciones de su empresa.
    - RF27.3 **Usuario normal:** Registra activos y gestiona riesgos dentro de su empresa.
- RF28: Permitir que el Administrador genere un enlace de registro para que un usuario normal pueda ingresar y registrar activos en el sistema.

- RF29: Restringir el acceso a la información de cada empresa, asegurando que solo el **Superusuario** pueda visualizar los análisis de todas las empresas.

8. Usabilidad y Acceso

- RF30: Proporcionar una interfaz de usuario intuitiva y fácil de usar.

Requisitos No Funcionales

1. Seguridad

- RNF1: La aplicación debe cumplir con los principios de seguridad de la información (confidencialidad, integridad, disponibilidad).
- RNF2: Implementar autenticación de usuarios con contraseñas seguras y políticas de caducidad.
- RNF3: Almacenar datos sensibles de manera cifrada.

2. Escalabilidad

- RNF4: La aplicación debe ser escalable para soportar un crecimiento futuro en el número de usuarios y activos.

3. Rendimiento

- RNF5: La aplicación debe responder en menos de 5 segundos para la mayoría de las operaciones.

4. Mantenibilidad

- RNF6: El código fuente debe estar bien documentado para facilitar futuras actualizaciones.

5. Cumplimiento Normativo

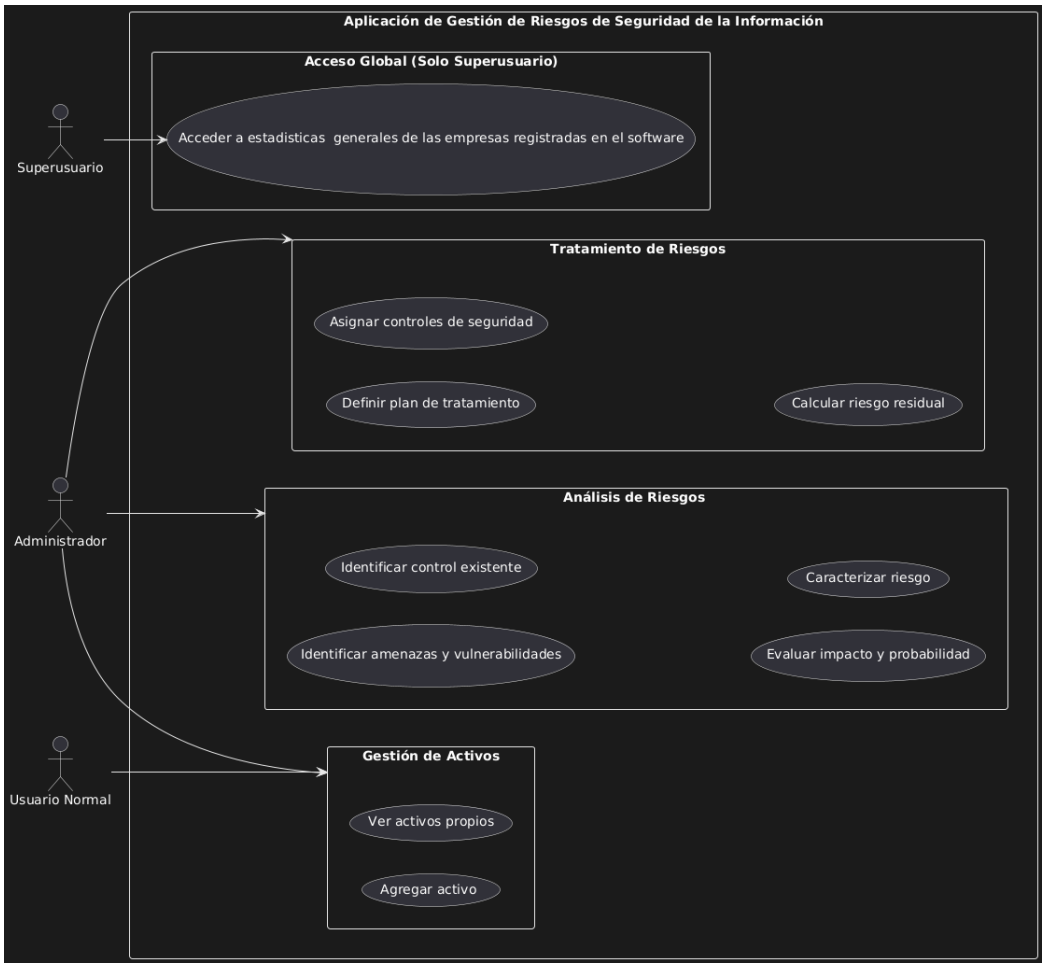
- **RNF12:** La aplicación debe facilitar el cumplimiento de normativas como ISO 27001.

Identificación de Casos de Uso Dentro de la Aplicación

Tomando como referencia los requisitos funcionales y no funcionales definidos, se procederá a la elaboración de los casos de uso del sistema. Estos casos de uso permitirán modelar las interacciones entre los diferentes tipos de usuarios y el software, asegurando que cada funcionalidad esté correctamente representada y alineada con las necesidades identificadas. Además, servirán como base para el diseño, desarrollo y pruebas del sistema, garantizando que cumpla con los objetivos establecidos en la gestión de riesgos de seguridad de la información.

Figura 7

Definición del proyecto general



Nota. Elaboración Propia

Este caso de uso representa la funcionalidad de la aplicación de gestión de Riesgos de Seguridad de la Información de manera general, en donde los usuarios interactúan con el sistema según sus roles: Superusuario, Administrador y Usuario Normal.

Gestión de Activos

1. Agregar activo: Permite registrar nuevos activos en el sistema, especificando detalles relevantes.
2. Ver activos propios: Los usuarios pueden consultar los activos que han registrado.

Análisis de Riesgos

1. Identificar amenazas y vulnerabilidades: Permite analizar posibles amenazas y vulnerabilidades asociadas a los activos registrados.
2. Identificar control existente: Verifica si ya existen controles implementados para mitigar los riesgos.
3. Evaluar impacto y probabilidad: Determina la criticidad de los riesgos en función de su impacto y probabilidad de ocurrencia.
4. Caracterizar riesgo: Define el nivel de riesgo en función del análisis realizado.

Tratamiento de Riesgos

1. Definir plan de tratamiento: Establece estrategias para abordar los riesgos identificados.
2. Asignar controles de seguridad: Relaciona los riesgos con controles específicos de seguridad según normativas.
3. Calcular riesgo residual: Evalúa el riesgo que persiste tras aplicar los controles.

Acceso Global (Solo Superusuario)

Acceder a estadísticas generales de las empresas registradas en el software El Superusuario puede visualizar métricas y tendencias sobre los riesgos en todas las empresas registradas, lo que le permite supervisar y tomar decisiones estratégicas.

Roles y Accesos

1. Superusuario: Tiene acceso global a las estadísticas de todas las empresas.
2. Administrador: Gestiona los activos, realiza análisis y tratamiento de riesgos.
3. Usuario Normal: Solo puede gestionar sus propios activos.

Este caso de uso refleja una estructura clara de permisos y acciones dentro del sistema, garantizando que cada usuario tenga acceso solo a la información y funcionalidades correspondientes a su rol.

De ahora en adelante, la justificación de cada caso de uso irá referenciada en la historia de usuario, ya que estas proporcionan el contexto y la necesidad real detrás de cada funcionalidad del sistema. Al basar los casos de uso en las historias de usuario, se garantiza que el software satisfaga los requerimientos específicos de los usuarios y refleje fielmente los procesos y necesidades identificados durante el análisis de requisitos.

Figura 8

Gestión y creación de usuarios



Nota. Elaboración Propia

Tabla 1

Creación Usuario Administrador

Código: EP001- HU01	**Nombre de la historia**: Creación Usuario Administrador
Descripción: **COMO** Administrador **QUIERO** poder registrarme en la plataforma web **PARA** posteriormente poder loguearme y crear el análisis de riesgo	
Criterios de aceptación: 1. El sistema debe permitir al usuario de la aplicación ingresar su nombre completo, dirección de correo electrónico y contraseña para registrarse en la plataforma. 2. El sistema debe validar que la dirección de correo electrónico ingresada sea única y no esté asociada a otra cuenta de usuario existente en la plataforma. 3. El sistema debe proporcionar mensajes de error claros y específicos en caso de que ocurra algún problema durante el proceso de registro, como una dirección de correo electrónico duplicada o una contraseña no válida. 4. Después de la confirmación exitosa, el Administrador de la aplicación debe poder iniciar sesión en la plataforma utilizando su dirección de correo electrónico y contraseña registrados. 5. Una vez autenticado, el Administrador de la aplicación debe poder acceder a la funcionalidad para crear un análisis de riesgo para su empresa, como la creación de un nuevo proyecto o la importación de datos existentes. 6. El administrador envía un código de invitación al usuario normal para que acceda al análisis de riesgos.	

Nota. Esta tabla muestra la historia de usuario para la creación del usuario. *Fuente.*

Elaboración propia.

Figura 9

Creación de la gestión del riesgo de la empresa



Nota. Elaboración propia.

Tabla 2

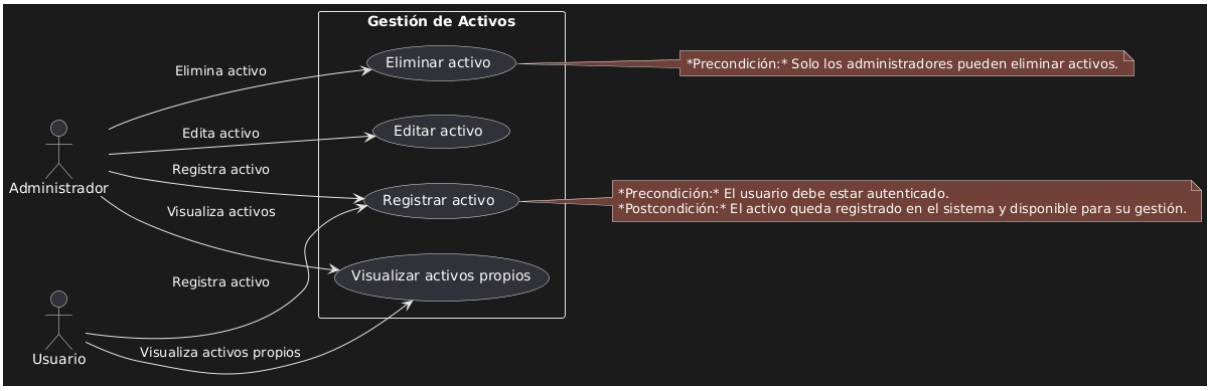
Historia de usuario Creación de la Gestión de Riesgo General

Código: EP002- HU01	**Nombre de la historia**: Creación de la Gestión de Riesgo General
Descripción: **COMO** Administrador **QUIERO** crear un mapa de gestión de riesgo general, **PARA** establecer una base estructurada antes de realizar un análisis detallado de los riesgos de seguridad de la información.	
Criterios de aceptación: 1El sistema debe permitir al usuario registrar los datos generales de su empresa, como: 1. Nombre de la empresa 2. Sector al que pertenece 3. Número de empleados 4. Responsable de la seguridad de la información 4. Se debe proporcionar una opción para guardar y editar posteriormente la información registrada.	

Nota. Esta tabla muestra la historia de usuario para la Creación de la Gestión de Riesgo General. *Fuente.* Elaboración propia.

Figura 10

Gestión de activos



Nota. Elaboración Propia.

Tabla 3

Historia de Usuario de Registro de activos de la empresa

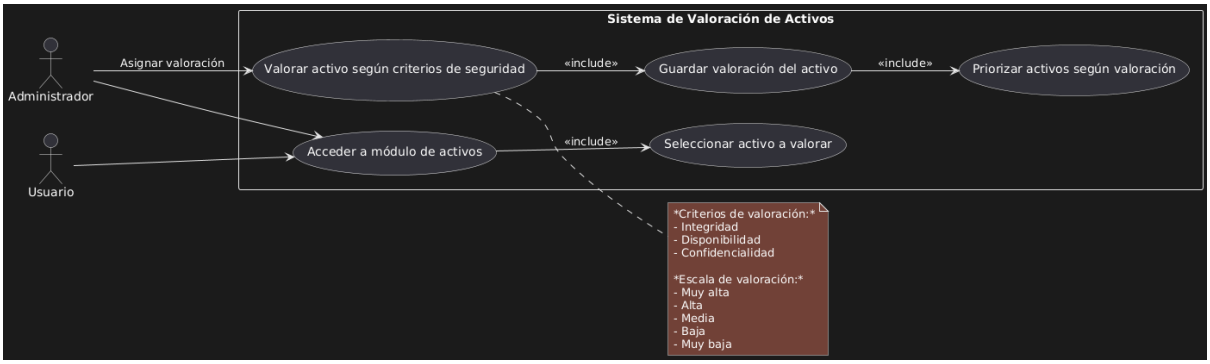
Código: EP003- HU001	**Nombre de la historia**: Registro de activos de la empresa
Descripción: **COMO** usuario/administrador de la aplicación, **QUIERO** poder iniciar sesión y acceder a la funcionalidad de registro de activos de la empresa, **PARA** mantener un inventario actualizado de los activos de información y recursos críticos de la empresa.	
Criterios de aceptación: 1. El usuario debe iniciar sesión utilizando sus credenciales. 2. Se proporciona la opción de acceder a la funcionalidad de registro de activos de la empresa. 3. Se permite al usuario agregar nuevos activos de información, proporcionando detalles como: código, nombre, descripción, unidad responsable, persona responsable, ubicación, cantidad, otras características específicas del activo 4. Se permite al administrador editar y eliminar activos existentes según sea necesario.	

Nota. Esta tabla muestra la historia de usuario para el registro de activos de la empresa.

Fuente. Elaboración propia.

Figura 11

Valoración de activos



Nota. Elaboración Propia.

Tabla 4

Historia de Usuario de Valoración de activos de información

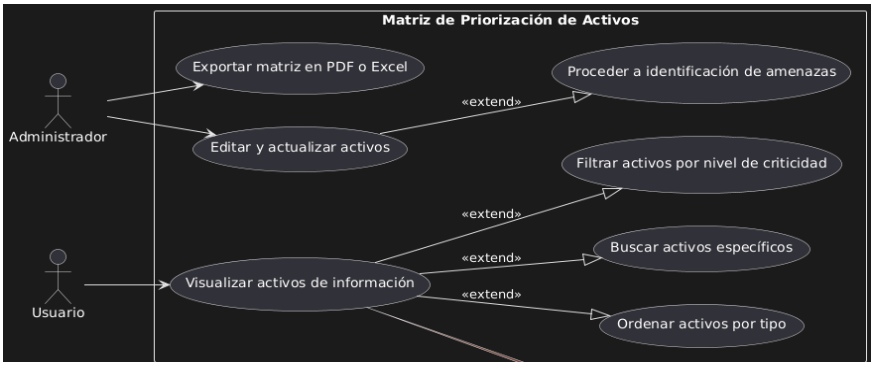
Código: EP003- HU002	**Nombre de la historia**: Valoración de activos de información
Descripción: **COMO** administrador de la aplicación **QUIERO** poder valorar los activos de información en términos de integridad, disponibilidad y confidencialidad **PARA** priorizar adecuadamente los recursos de seguridad y proteger los activos más críticos para la empresa.	
Criterios de aceptación: 1. Se proporciona la funcionalidad para valorar cada activo de información en términos de integridad, disponibilidad y confidencialidad 2. Se utiliza una escala de valoración (muy alta, alta, media, baja, muy baja) para cada aspecto (integridad, disponibilidad, confidencialidad, 3. La aplicación registra y almacena la valoración realizada para cada activo de información. 4. La valoración de los activos de información se utiliza para priorizar los recursos de seguridad y proteger adecuadamente los activos más críticos para la empresa.	

Nota. Esta tabla muestra la historia de usuario para la Valoración de activos de información.

Fuente. Elaboración propia.

Figura 12

Priorización de activos



Nota. Elaboración Propia.

Tabla 5

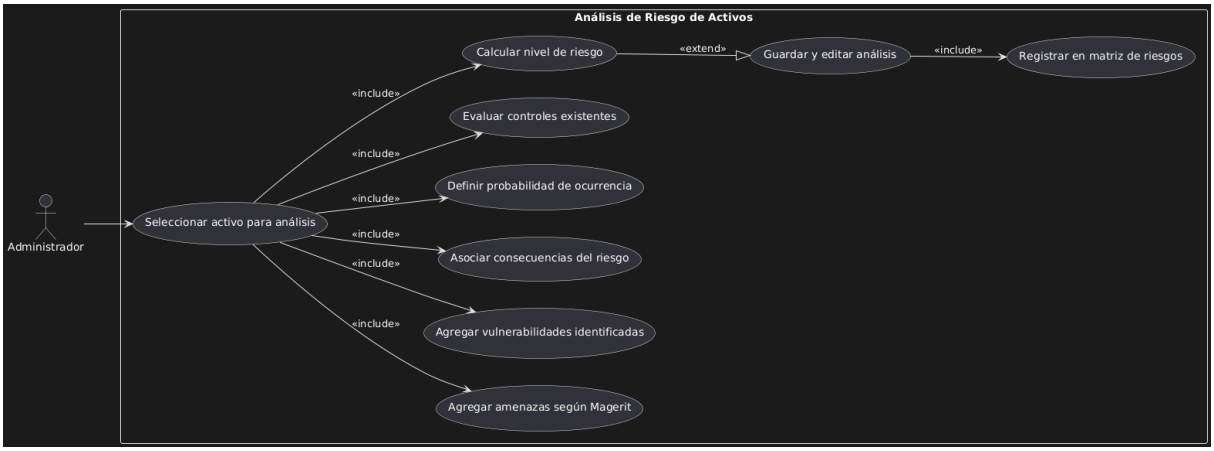
Historia de Usuario Priorización y Filtrado de Activos de Información

Código: EP003- HU003	**Nombre de la historia**: Priorización y Filtrado de Activos de Información
Descripción: **COMO** administrador de la aplicación, **QUIERO** visualizar y filtrar los activos de información según su nivel de importancia y criticidad, **PARA** priorizar aquellos que requieren mayor atención en la gestión de riesgos de seguridad de la información.	
Criterios de aceptación: 1. El sistema debe mostrar una matriz de activos de información con los siguientes criterios: A. Nombre del activo B. Tipo de activo (hardware, software, datos, recursos humanos, etc.) C. Nivel de criticidad (Alto, Medio, Bajo) D. Valor del activo en función de su impacto en la organización E. Responsable asignado 2. Debe permitir el filtrado y ordenamiento de los activos según: A. Nivel de criticidad (de mayor a menor y viceversa). B. Tipo de activo. 3. La matriz debe incluir una función de búsqueda para localizar activos específicos. 4. Se debe permitir exportar la matriz en formatos PDF y Excel para su consulta externa. 5. Desde la matriz, el administrador debe poder acceder a la edición y actualización de cada activo. 6. Una vez priorizados los activos, el usuario podrá proceder a la identificación y evaluación de amenazas asociadas a cada uno.	

Nota. Esta tabla muestra la historia de usuario para la Priorización y Filtrado de Activos de Información. *Fuente.* Elaboración propia.

Figura 13

Análisis del riesgo de manera general



Nota. Elaboración Propia.

Tabla 6

Historia de Usuario de Análisis de Riesgo

Código: EP005- HU001	**Nombre de la historia**: Análisis de Riesgo
Descripción: **COMO** administrador de la aplicación, **QUIERO realizar** un análisis de riesgo detallado para cada activo registrado, **PARA** evaluar amenazas, vulnerabilidades y posibles impactos, y así determinar su nivel de criticidad	
Criterios de aceptación: 1. El sistema debe permitir al usuario seleccionar un activo registrado para su análisis. 2. Se debe proporcionar una funcionalidad en donde el usuario pueda agregar: 1. Amenazas asociadas según Magerit 2. Vulnerabilidades identificadas que podrían ser explotadas. 3. Consecuencias asociadas en caso de materializarse el riesgo. 4. Probabilidad de ocurrencia, basada en categorías predefinidas (Alta, Media, Baja) 5. Controles existentes y su nivel de efectividad (si los hay).	

3. El sistema debe calcular automáticamente el nivel de riesgo combinando la probabilidad y el impacto. 4. Se debe permitir guardar el análisis y editarlo posteriormente. 5. Una vez analizado el riesgo del activo, este debe quedar registrado en una matriz de riesgos para su priorización.

Nota. Esta tabla muestra la historia de usuario de análisis de riesgos de manera general.

Fuente. Elaboración propia.

Figura 14

Registro de amenazas asociadas a los activos



Nota. Elaboración Propia.

Tabla 7

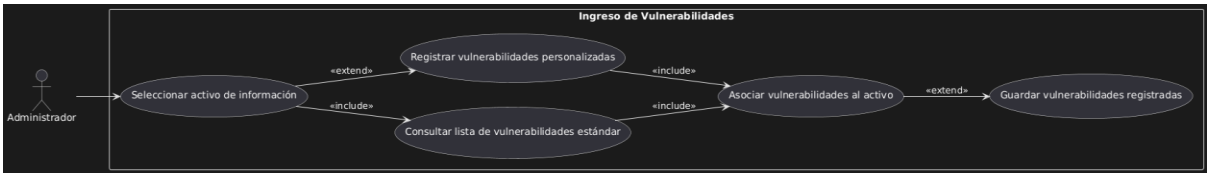
Historia de Usuario de Ingreso de amenazas

Código: EP005- HU002	**Nombre de la historia**: Ingreso de Amenazas
Descripción: **COMO** administrador de la aplicación**,** **QUIERO** poder identificar las amenazas asociadas a cada activo de información**,** **PARA** comprender los riesgos potenciales que enfrenta la empresa y tomar medidas de seguridad adecuada.	
Criterios de aceptación: 1. Se proporciona la funcionalidad para que el usuario seleccione un activo de información específico. 2. Se muestra una lista de amenazas comunes asociadas a ese tipo de activo.	

Nota. Esta tabla muestra la historia de usuario de Ingreso de Amenazas. *Fuente.* Elaboración propia.

Figura 15

Registro de vulnerabilidades asociadas a las amenazas



Nota. Elaboración propia

Tabla 8

Historia de Usuario de Ingreso de Vulnerabilidades

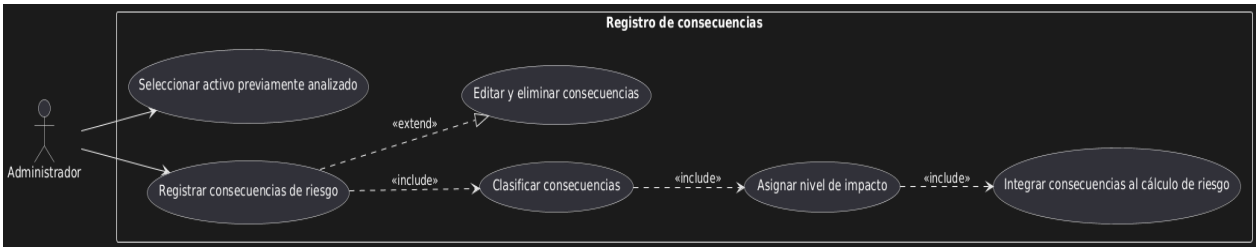
Código: EP005- HU003	**Nombre de la historia**: Ingreso de Vulnerabilidades
Descripción: **COMO** administrador de la aplicación, **QUIERO** poder identificar y registrar las vulnerabilidades asociadas a cada activo de información, **PARA** comprender los puntos débiles que pueden ser explotados y definir estrategias de mitigación adecuadas.	
Criterios de aceptación: 1. El sistema debe permitir al usuario seleccionar un activo de información específico para asociarlo a vulnerabilidades. 2. Se debe mostrar una lista de vulnerabilidades comunes asociadas a ese tipo de activo, basadas en estándares como **MAGERIT, ISO 27005**. 3. Se debe permitir la opción de ingresar vulnerabilidades personalizadas, en caso de que el usuario detecte riesgos específicos para su empresa.	

Nota. Esta tabla muestra la historia de usuario de Ingreso de Vulnerabilidades. *Fuente.*

Elaboración propia.

Figura 16

Registro de consecuencias



Nota. Elaboración propia.

Tabla 9

Historia de Usuario de Registro de consecuencias

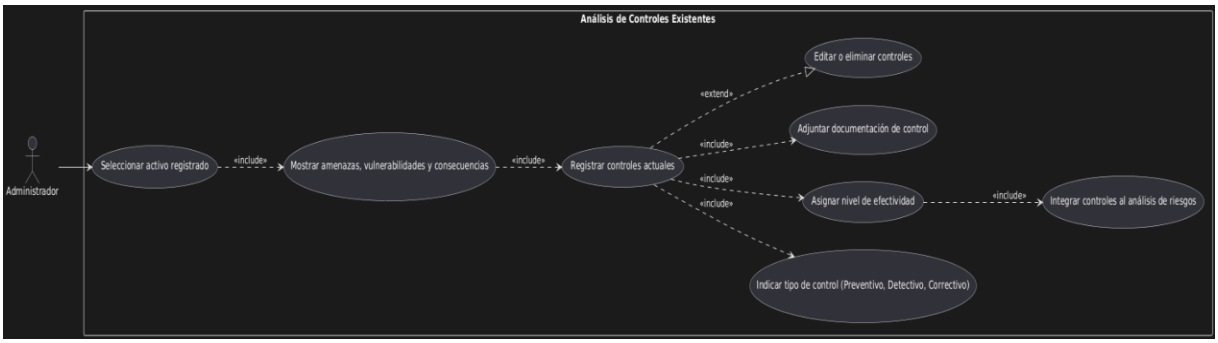
Código: EP005- HU004	**Nombre de la historia**: Registro de Consecuencias de Riesgo
Descripción: **COMO** administrador de la aplicación, **QUIERO** registrar las consecuencias asociadas a una amenaza y vulnerabilidad identificada en un activo, **PARA** comprender el impacto potencial y tomar decisiones informadas sobre su gestión.	
Criterios de aceptación: 1. El sistema debe permitir al usuario seleccionar un activo previamente analizado. 2. El usuario debe poder ingresar una o más **consecuencias** derivadas de la materialización del riesgo, clasificadas en: 1. **Operacionales:** Impacto en la continuidad del negocio. 2. **Económicas:** Pérdidas financieras asociadas. 3. **Legales:** Sanciones o incumplimientos normativos. 4. **Reputacionales:** Daño a la imagen de la empresa. 5. **Técnicas:** Fallos en infraestructura o sistemas. 3. El sistema debe permitir asignar un nivel de impacto (Alto, Medio, Bajo) para cada consecuencia. 4. Se debe permitir la edición y eliminación de consecuencias antes de guardar el análisis. 5. Una vez registradas las consecuencias, estas deben integrarse al cálculo de riesgo del activo.	

Nota. Esta tabla muestra la historia de usuario de Ingreso de consecuencias del riesgo. *Fuente.*

Elaboración propia.

Figura 17

Análisis de controles existentes



Nota. Elaboración propia.

Tabla 10

Historia de Usuario de controles existentes

Código: EP00- HU005	**Nombre de la historia**: Análisis de controles existentes
Descripción: **COMO** administrador de la aplicación, **QUIERO** identificar los controles de seguridad existentes en la organización, **PARA** determinar su efectividad en la mitigación de riesgos y definir si es necesario reforzarlos o implementar nuevos controles.	
Criterios de aceptación: 1. El sistema debe permitir al usuario seleccionar un activo registrado para revisar los controles asociados. 2. Se debe mostrar la amenaza, vulnerabilidad y consecuencias previamente identificadas para dicho activo. 3. El usuario debe poder: 1. Registrar los controles actuales en la organización relacionados con el activo y la amenaza identificada. 2. Indicar el tipo de control (Preventivo, Detectivo, Correctivo). 3. Asignar un nivel de efectividad al control (Alto, Medio, Bajo). 4. Adjuntar documentación o evidencia de la existencia del control.	

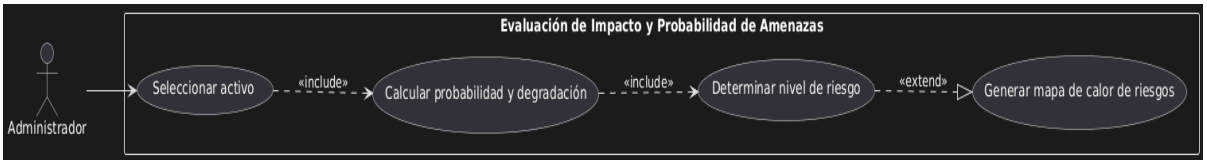
4. Se debe permitir la edición o eliminación de los controles antes de finalizar el análisis. 5. Una vez registrados los controles existentes, estos deben integrarse al análisis de riesgos para evaluar la necesidad de medidas adicionales.

Nota. Esta tabla muestra la historia de usuario de Ingreso de consecuencias del riesgo. *Fuente.*

Elaboración propia.

Figura 18

Evaluación de impacto y probabilidad de ocurrencia



Nota. Elaboración propia.

Tabla 11

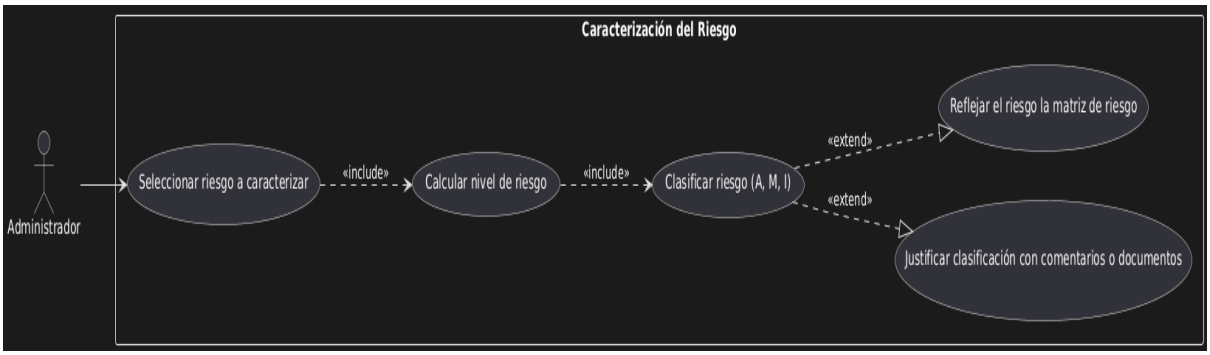
Historia de Usuario de Evaluación de impacto y probabilidad de amenazas

Código: EP005-HU006	**Nombre de la historia**: Evaluación de impacto y probabilidad de amenazas
Descripción: **COMO** administrador de la aplicación **QUIERO** poder ver el impacto y la probabilidad de que una amenaza sea efectiva sobre un activo de información sin haber aplicado controles previos **PARA** comprender mejor los riesgos y priorizar las medidas de seguridad adecuadas.	
Criterios de aceptación: 1. Se muestra la probabilidad y degradación de que la amenaza sea efectiva sobre el activo, especificada en una escala predefinida (muy alta, alta, media, baja, muy baja). 2. La aplicación calcula y muestra el nivel de riesgo resultante de la combinación del impacto y la probabilidad. 3. La evaluación de impacto y probabilidad se utiliza para comprender mejor los riesgos y priorizar las medidas de seguridad adecuadas para proteger los activos de información de la empresa. 4. Se genera un mapa de calor de los activos de la empresa con relación a las amenazas existentes en la empresa	

Nota. Esta tabla muestra la historia de usuario de Evaluación de impacto y probabilidad de amenazas. *Fuente.* Elaboración propia.

Figura 19

Caracterización del riesgo



Nota. Elaboración propia

Tabla 12

Historia de Usuario de Caracterización del Riesgo

Código: EP005- HU007	**Nombre de la historia**: Caracterización del Riesgo
Descripción: **COMO** administrador de la aplicación, **QUIERO** clasificar los riesgos identificados según su nivel de aceptación, **PARA** determinar si deben ser mitigados, monitoreados o asumidos dentro de la organización.	
Criterios de aceptación: 1. Se debe calcular el nivel de riesgo según la matriz de probabilidad e impacto. 2. El usuario debe poder clasificar el riesgo en una de las siguientes categorías: 1. Aceptable (A) → Nivel de riesgo entre 1 y 5. No requiere medidas adicionales. 2. Moderado (M) → Nivel de riesgo entre 6 y 15. Puede requerir mitigación o monitoreo.	

3. Inaceptable (I) → Nivel de riesgo entre 16 y 26. Debe ser tratado de inmediato. 3. El sistema debe registrar la clasificación del riesgo y permitir justificar la decisión con comentarios o documentación adicional. 4. Una vez caracterizado, el riesgo debe reflejarse en el tablero de gestión, facilitando su monitoreo y tratamiento.

Nota. Esta tabla muestra la historia de usuario de Caracterización del Riesgo *Fuente.*

Elaboración propia.

Figura 20

Tratamiento del riesgo de manera general



Nota. Elaboración propia

Tabla 13

Historia de Usuario de Gestión del Tratamiento de Riesgos

Código: EP006- HU001	**Nombre de la historia**: Gestión del Tratamiento de Riesgos
Descripción: **COMO** administrador de la aplicación, **QUIERO** gestionar el tratamiento de los riesgos de seguridad de la información, **PARA** definir y aplicar medidas adecuadas que minimicen su impacto en la organización.	
Criterios de aceptación: 1. El sistema debe permitir al usuario visualizar un listado de riesgos identificados, incluyendo: 1. Código del riesgo 2. Nombre del activo de información afectado 3. Descripción del riesgo	

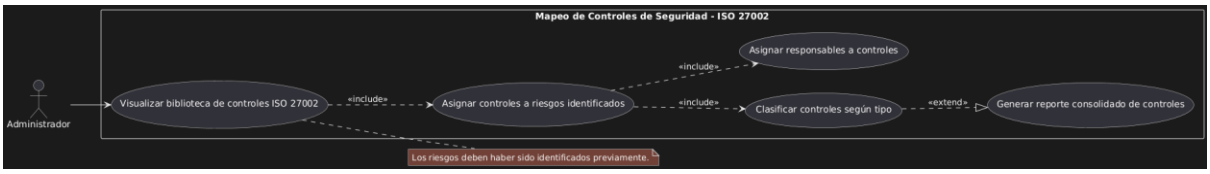
4. Nivel de riesgo inherente (sin controles aplicados) 5. Medidas de control actuales 2. Se debe proporcionar un módulo para ver las opciones de tratamiento del riesgo, permitiendo que el usuario seleccione una de las siguientes estrategias: 1. Aceptar (riesgo asumido sin medidas adicionales) 2. Eliminar (erradicar la causa del riesgo/eliminar proceso) 3. Mitigar (implementar controles adicionales para reducir impacto o probabilidad) 4. Transferir (trasladar la responsabilidad a un tercero, aseguradora) 3. Se debe incluir la justificación del tratamiento con los siguientes elementos: 1. Requerimiento legal: Indica si el riesgo debe ser tratado por normativas gubernamentales. 2. Obligación contractual: Aplica si existen contratos que exijan la mitigación del riesgo. 3. Requerimiento de negocio: Si el riesgo afecta la operatividad o continuidad del negocio. 4. Se debe asignar un responsable o dueño del riesgo, quien será el encargado de supervisar su tratamiento. 5. El sistema debe permitir la edición y actualización de la estrategia de tratamiento según cambios en la organización o nuevos controles implementados.

Nota. Esta tabla muestra la historia de usuario de Gestión del Tratamiento de Riesgos *Fuente.*

Elaboración propia.

Figura 21

Mapeo de controles ISO 27002



Nota. Elaboración propia

Tabla 14

Historia de Usuario de Mapeo de Controles de Seguridad Basados en ISO 27002

Código: EP006-HU002	**Nombre de la historia**: Mapeo de Controles de Seguridad Basados en ISO 27002

Descripción:

COMO administrador de la aplicación,

QUIERO visualizar y asignar controles de seguridad de acuerdo con la norma ISO 27002,

PARA mitigar los riesgos de seguridad de la información y fortalecer la postura de ciberseguridad de la empresa.

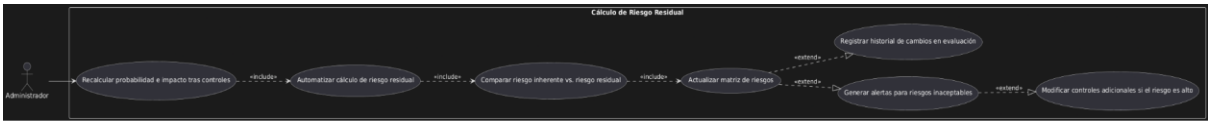
Criterios de aceptación:

1. El sistema debe permitir al usuario mapear los controles de seguridad basados en la ISO 27002, clasificándolos en:
    1. Preventivos: Controles diseñados para evitar que ocurra un incidente de seguridad.
    2. Detectivos: Controles que permiten identificar y registrar eventos de seguridad.
    3. Correctivos: Controles aplicados para minimizar el impacto de un incidente una vez ha ocurrido.
2. La aplicación debe permitir asociar controles específicos a los riesgos identificados, seleccionando el tipo de control adecuado.
3. Se debe proporcionar una biblioteca de controles de seguridad basada en la norma ISO 27002, que incluya tipo de control:
    1. Controles Organizacionales
    2. Controles Físicos.
    3. Controles al personal.
    4. Controles Tecnologicos
4. El usuario debe poder visualizar un reporte consolidado donde se muestren los controles aplicados, su tipo (preventivo, detectivo, correctivo) y su relación con los riesgos tratados.
5. Se debe permitir la asignación de responsables para cada control implementado dentro de la organización.

Nota. Esta tabla muestra la historia de usuario de Mapeo de Controles de Seguridad Basados en ISO 27002 *Fuente.* Elaboración propia.

Figura 22

Cálculo del riesgo residual



Nota. Elaboración propia

Tabla 15

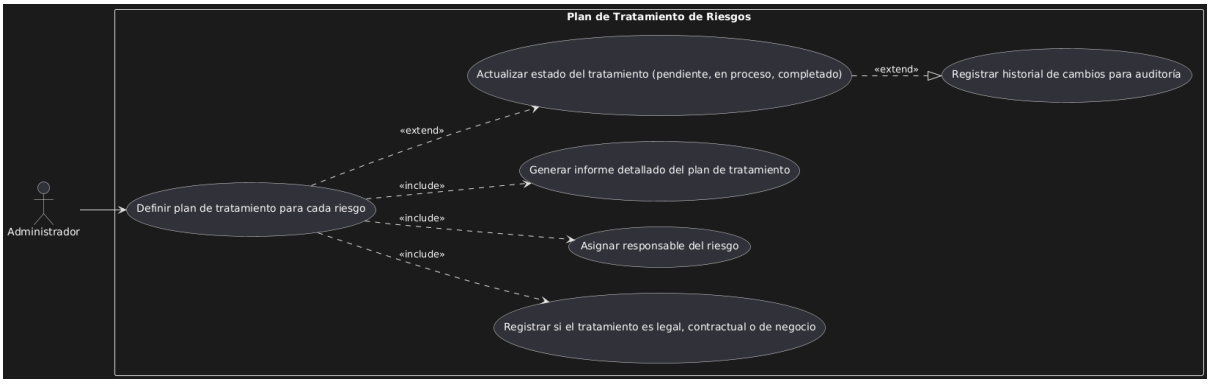
Historia de Usuario de Cálculo de Riesgo Residual

Código: EP006-HU03	**Nombre de la historia**: Cálculo de Riesgo Residual tras la Planificación de Controles
Descripción: **COMO** usuario de la aplicación, **QUIERO** calcular la probabilidad, impacto y nivel de riesgo residual después de la aplicación de controles, **PARA** determinar la efectividad de las medidas implementadas y ajustar el plan de tratamiento de riesgos si es necesario.	
Criterios de aceptación: 1. El sistema debe permitir recalcular la probabilidad e impacto de cada riesgo tras la implementación de controles de seguridad. 2. Se debe automatizar el cálculo del riesgo residual, considerando los controles aplicados y su efectividad en la reducción del riesgo. 3. La aplicación debe permitir la comparación entre el riesgo inherente (antes de los controles) y el riesgo residual (después de los controles). 4. Se debe generar una matriz de riesgos actualizada, mostrando la variación del nivel de riesgo después del tratamiento. 5. La interfaz debe proporcionar alertas visuales cuando un riesgo residual sigue siendo inaceptable, sugiriendo acciones adicionales. 6. El usuario debe poder modificar o agregar controles adicionales si el riesgo residual sigue siendo alto.	

Nota. Esta tabla muestra la historia de usuario de Mapeo de Cálculo de Riesgo Residual tras la Planificación de Controles *Fuente.* Elaboración propia.

Figura 23

Plan de tratamiento del riesgo



Nota. Elaboración propia

Tabla 16

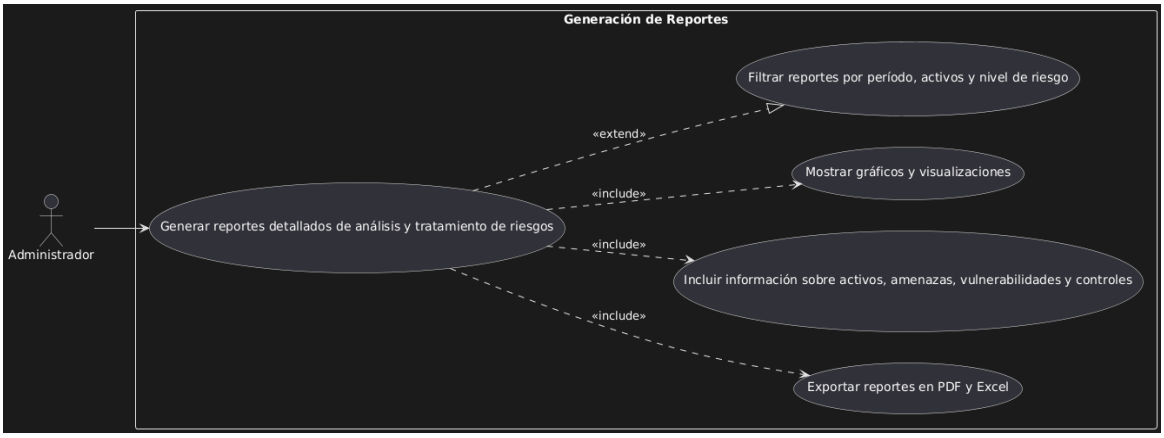
Historia de Usuario de definición del Plan de Tratamiento de Riesgos

Código: EP006-HU04	**Nombre de la historia**: Definición del Plan de Tratamiento de Riesgos
Descripción: **COMO** usuario de la aplicación, **QUIERO** definir un plan de tratamiento para cada riesgo identificado, **PARA** asegurar que se tomen las medidas necesarias según los requerimientos legales, contractuales y de negocio.	
Criterios de aceptación: 1. Debe registrarse si el tratamiento está basado en un requerimiento legal, una obligación contractual o una necesidad de negocio. 2. El usuario debe poder asignar un responsable o dueño del riesgo, quien será el encargado de la implementación y seguimiento del tratamiento. 3. La aplicación debe generar un informe detallado del plan de tratamiento de riesgos, con todos los elementos definidos. 4. Debe existir una sección de seguimiento, donde el usuario pueda actualizar el estado del tratamiento y marcarlo como "pendiente", "en proceso" o "completado". 5. Se debe registrar un historial de cambios, asegurando trazabilidad y auditoría del tratamiento del riesgo.	

Nota. Esta tabla muestra la historia de usuario de Mapeo de Definición del Plan de Tratamiento de Riesgos *Fuente.* Elaboración propia.

Figura 24

Generación de reportes



Nota. Elaboración propia

Tabla 17

Historia de Usuario de Generación de Reportes de Análisis y Tratamiento de Riesgos

Código: EP006-HU04	**Nombre de la historia**: Generación de Reportes de Análisis y Tratamiento de Riesgos
Descripción: **COMO** usuario de la aplicación, **QUIERO** generar reportes detallados del análisis y tratamiento de riesgos, **PARA** documentar el estado de seguridad de la empresa y cumplir con auditorías y normativas.	
Criterios de aceptación: 1. El sistema debe permitir la generación de reportes automatizados en formatos como PDF y Excel. ALTA DIRECCION 2. Se debe incluir información detallada sobre activos, amenazas, vulnerabilidades, riesgos inherentes, controles aplicados y riesgos residuales. 3. Los reportes deben mostrar gráficos y visualizaciones para facilitar la interpretación de los datos. 4. Debe existir la opción de filtrar los reportes según período de tiempo, activos específicos o nivel de riesgo.	

Nota. Esta tabla muestra la historia de Generación de Reportes de Análisis y Tratamiento de Riesgos. Elaboración propia

Diseñar Una Arquitectura de Software Escalable y Segura para, que Permita la Integración de Nuevas Funcionalidades y Actualizaciones en el Futuro.

Tal como señalan Bass, Clements y Kazman (2012), la arquitectura de software de un sistema es "el conjunto de estructuras necesarias para razonar sobre el sistema. Comprende elementos de software, relaciones entre ellos, y propiedades de ambos." Esta estructura es crucial dentro de la aplicación, ya que determina directamente la capacidad del sistema para satisfacer requerimientos no funcionales clave como el rendimiento (tiempo de respuesta, debe responder en menos de 5 segundos), la usabilidad (facilidad de uso para los usuarios que estén familiarizados con el tema de seguridad de la información) la escalabilidad (la aplicación debe ser escalable para soportar un crecimiento futuro en el número de usuarios y activos).

Definición de Requerimientos de La Arquitectura

Según Perla Velasco Elizondo y colaboradores (2015) el ciclo de desarrollo de la arquitectura comprende las siguientes etapas:

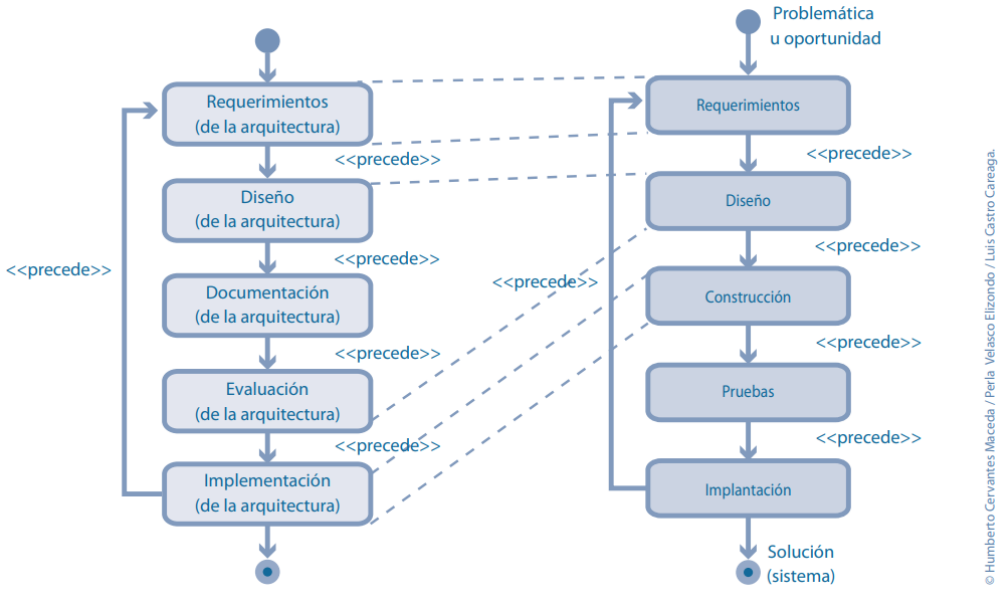
- Etapa de Requerimientos: se centra en la captura, documentación y priorización de los requerimientos que influyen en la arquitectura, conocidos como drivers arquitectónicos.
- Diseño de la arquitectura: considerada la etapa más compleja, define las estructuras del sistema mediante la toma de decisiones de diseño. Para esta creación estructural, se utilizan soluciones abstractas probadas (patrones de diseño y tácticas) y soluciones concretas (elecciones tecnológicas como frameworks).
- Documentación de la arquitectura: tiene como objetivo comunicar el diseño a los diversos interesados en el sistema (desarrolladores, líderes de proyecto, clientes, etc.). Si bien durante el diseño se realiza una documentación inicial, la documentación formal implica la representación de las estructuras a través de vistas (diagramas acompañados de información para su comprensión).

- Evaluación de la arquitectura: es una actividad crucial para identificar posibles riesgos o problemas en el diseño una vez documentado. Realizar esta evaluación de forma temprana, incluso antes de la codificación, permite corregir defectos a un costo significativamente menor que hacerlo después de la construcción del sistema.
- Implementación de la arquitectura: consiste en la construcción del sistema siguiendo estrictamente el diseño arquitectónico definido, evitando desviaciones.

En línea con esta importancia de la arquitectura de software, el siguiente paso se centra en el diseño de la arquitectura de software específica para la aplicación de gestión de riesgos de seguridad de la información. El objetivo principal de este diseño es crear una arquitectura que sea tanto escalable como segura, permitiendo la futura integración de nuevas funcionalidades y actualizaciones de manera eficiente.

Figura 25

Ciclo de desarrollo de la arquitectura del software



Nota. Actividades asociadas al ciclo de desarrollo de la arquitectura (a la izquierda) y su mapeo dentro de las actividades técnicas del desarrollo de sistemas (a la derecha). De Perla Velasco Elizondo, Humberto Cervantes Maceda y Luis Castro Careaga, 2015. Copyright por los autores.

Descripción General de la Arquitectura de Software

La arquitectura del sistema se basa en el modelo de comunicación cliente-servidor, donde el cliente representa la interfaz gráfica que interactúa con el usuario, mientras que el servidor procesa las solicitudes, gestiona la lógica del negocio y accede a la base de datos. Este modelo se implementa siguiendo un patrón de arquitectura MVC (Modelo-Vista-Controlador) en un diseño monolítico, lo cual permite mantener la estructura organizada, facilitando el desarrollo, mantenimiento y escalabilidad inicial del proyecto. En el frontend, se utiliza React 18 junto con TypeScript, una combinación que ofrece componentes reutilizables, desarrollo tipado y una experiencia de usuario dinámica e interactiva. En el backend, se optó por PHP 8.3 y el framework Laravel, gracias a su robustez, facilidad para estructurar proyectos bajo el patrón MVC, y su ecosistema que ofrece soluciones integradas para autenticación, manejo de rutas, controladores y seguridad. Para el almacenamiento de datos se utiliza MySQL 8, una base de datos relacional que permite mantener la integridad de los datos, realizar consultas complejas y escalar conforme crece el sistema. Adicionalmente, se incorpora Redis como mecanismo de caching y gestión de sesiones, lo que mejora significativamente el rendimiento de la aplicación al reducir la carga sobre la base de datos y acelerar el acceso a información frecuentemente consultada.

Modelo de Comunicación Cliente – Servidor

La elección del modelo cliente-servidor se basa en su capacidad para establecer una clara separación de responsabilidades entre la lógica del negocio (Servidor - Backend) y la interfaz de usuario (Cliente - Frontend).

- Servidor (Backend - Laravel + PHP 8.3): Centraliza la lógica de negocio, incluyendo los cálculos de riesgo (siguiendo metodologías como MAGERIT e ISO 27005), la gestión de la autenticación y el control del acceso a los datos.

- Cliente (Frontend - React 18 + TypeScript): Se encarga exclusivamente de la presentación de la información, la gestión de las interacciones básicas del usuario y la visualización de los datos.

Esta distinción inherente facilita la escalabilidad, el mantenimiento y la seguridad del sistema. Al residir la lógica crítica y el almacenamiento de datos de forma centralizada en el servidor, se permite un control más efectivo sobre los accesos y las actualizaciones (Oluwatosin, 2014).

La amplia adopción del modelo cliente-servidor en el desarrollo de aplicaciones web modernas asegura una gran disponibilidad de recursos, conocimientos y patrones de diseño probados. Su estructura se alinea de manera óptima con el flujo de trabajo requerido para la gestión eficiente de riesgos de seguridad de la información (Noman Shahid, 2019).

La arquitectura cliente-servidor, incluso implementada con un backend monolítico, mantiene las ventajas de la separación de responsabilidades. La relación de muchos a uno, donde un único servidor puede atender a múltiples clientes gestionando su acceso a recursos compartidos, optimiza la utilización de los recursos del sistema. La escalabilidad, tanto horizontal (añadir más clientes sin afectar el rendimiento) como vertical (mejorar las capacidades del servidor o añadir servidores), es una característica fundamental de este modelo, permitiendo un crecimiento flexible del sistema (Ruiz, 2018).

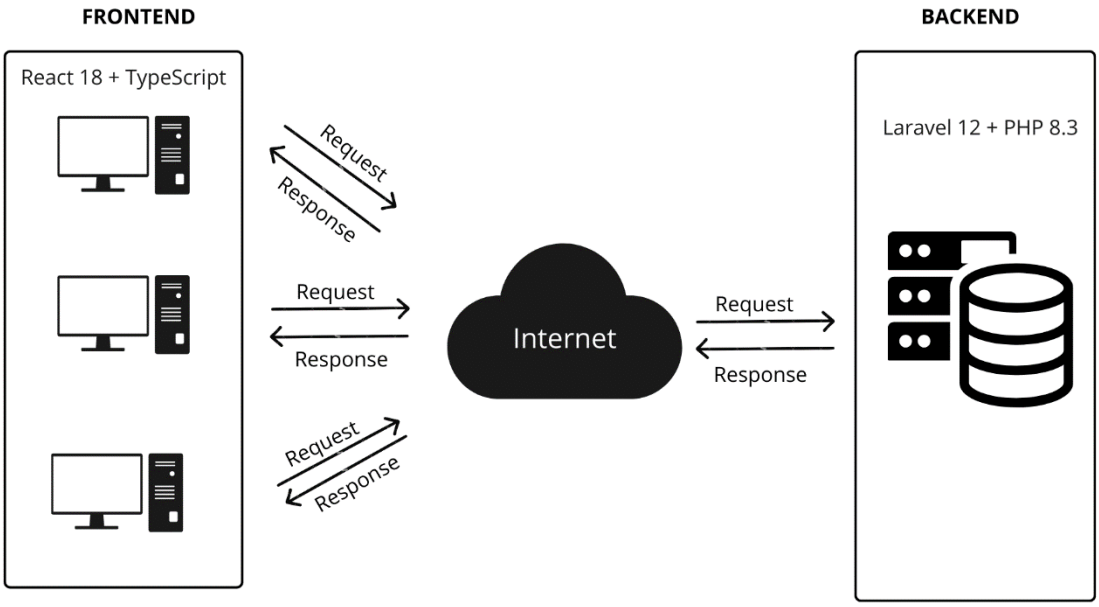
Si bien el mantenimiento en arquitecturas cliente-servidor podría presentar desafíos, la decisión de centralizar el hosting de la aplicación y el servidor en DigitalOcean mitiga significativamente este aspecto, simplificando la gestión y el diagnóstico de posibles problemas.

La seguridad es una prioridad inherente al modelo cliente-servidor. Aunque se implementan validaciones en el lado del cliente para una primera capa de protección, la gestión robusta de la seguridad crítica se realizará en el servidor, aprovechando las funcionalidades

integradas del framework Laravel. Esto proporciona una capa de protección sólida y centralizada para la aplicación de gestión de riesgos de seguridad de la información.

Figura 26

Modelo de comunicación Cliente-Servidor



Nota. Elaboración Propia.

Patrón Y Estructura De Despliegue - MVC Monolito

La aplicación está diseñada bajo una arquitectura monolítica, lo cual permite desplegar el frontend, backend y base de datos como una única unidad de software, facilitando su implementación y mantenimiento en etapas iniciales del proyecto (Monolítico Frente A Microservicios: Diferencia Entre Arquitecturas de Desarrollo de Software - AWS, 2020).

En este enfoque, el backend (Laravel), el frontend (React) y la base de datos (MySQL) se despliegan de manera unificada como una sola aplicación, esto le permite a la aplicación:

- Simplificar el despliegue y configuración del entorno, lo que reduce los costos.

- Facilitar el desarrollo en equipos pequeños como en este caso, que es un proyecto que consta de 2 personas.

Este tipo de arquitectura permite avanzar rápidamente en el desarrollo, concentrando los esfuerzos en la funcionalidad sin tener que gestionar múltiples servicios independientes como en una arquitectura de microservicios.

Patrón Modelo Vista Controlador (MVC)

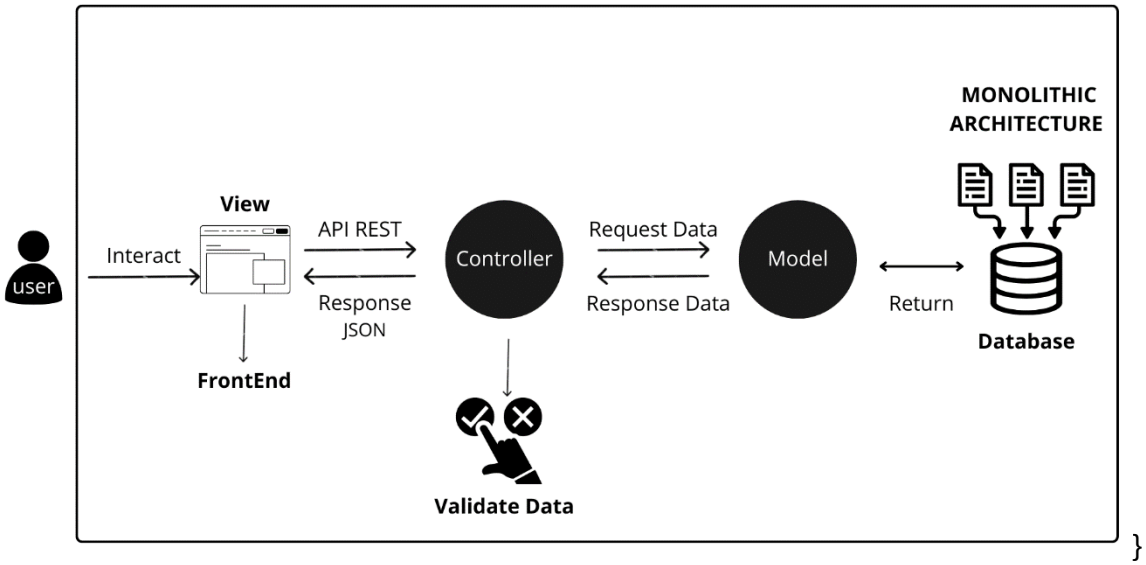
El patrón de diseño arquitectónico Modelo-Vista-Controlador (MVC) organiza la lógica de una aplicación en tres capas interconectadas: el Modelo gestiona los datos y la lógica de negocio, la Vista se encarga de la presentación e interacción con el usuario, y el Controlador actúa como intermediario, gestionando las peticiones y actualizando el Modelo y la Vista (Sheldon, 2023). En un contexto cliente-servidor, como con React en el frontend y Laravel en el backend, MVC se aplica principalmente en el servidor. El cliente envía una petición, que el servidor enruta al Controlador. Este interactúa con el Modelo para procesar los datos y luego prepara una respuesta que actúa como la "Vista" para el frontend. El frontend recibe esta respuesta y actualiza su propia Vista para reflejar los resultados, facilitando así una separación de responsabilidades que mejora la modularidad, mantenibilidad y escalabilidad de la aplicación.

- Modelo: Encapsula la lógica de negocio y el acceso a datos. En esta aplicación, los modelos representan entidades como riesgos, activos, amenazas, entre otros, y se encargan de interactuar con la base de datos.
- Vista: En lugar de renderizar vistas en el backend, Laravel expone la información a través de APIs REST, y React 18 se encarga del renderizado dinámico en el navegador del usuario, convirtiéndose en una "vista remota".

- Controlador: Gestiona las peticiones del cliente, ejecuta la lógica correspondiente y responde con los datos necesarios, usualmente en formato JSON.

Figura 27

Patrón Modelo Vista Controlador (MVC)



}

Nota. Elaboración Propia.

Base de Datos

Se optó por MySQL 8 como sistema de gestión de bases de datos relacional debido a varias razones estratégicas y técnicas que se alinean con las necesidades del proyecto:

Modelo relacional

La aplicación gestiona un conjunto de entidades claramente definidas, entre las que se encuentran los usuarios, los activos de información, los riesgos identificados, los controles de seguridad implementados y los planes de tratamiento diseñados para mitigar los riesgos. Estas entidades no operan de forma aislada, sino que mantienen relaciones significativas entre sí.

Debido a estas interconexiones, la aplicación requiere la implementación de integridad referencial y consistencia de datos. Este mecanismo asegura que cualquier valor de clave foránea, ya sea un dato en una sola columna o la combinación de datos en varias columnas, tenga la capacidad de referenciar y acceder de manera precisa a la clave primaria de una tabla relacionada dentro del sistema. Esto es fundamental para mantener la coherencia y la validez de la información gestionada por la aplicación, tal como se destaca en la documentación de IBM InfoSphere Information Server (2021).

Escalabilidad y rendimiento con MySQL 8:

Según Risso y Risso (2022), MySQL 8 incorpora una serie de mejoras sustanciales en comparación con sus versiones previas. Entre estas mejoras, se encuentra una optimización más eficiente del motor encargado de procesar las consultas a la base de datos, lo que puede traducirse en un rendimiento general superior.

Adicionalmente, MySQL 8 ofrece un soporte avanzado para funcionalidades como los índices invisibles (que permiten probar el impacto de eliminar un índice sin hacerlo realmente), el manejo de datos en formato JSON (facilitando el almacenamiento y la consulta de información no estructurada) y la utilización de expresiones regulares (para realizar búsquedas de patrones complejos dentro de los datos).

Otra característica relevante es la inclusión de un historial de transacciones, que puede ser útil para tareas de auditoría y recuperación, así como el soporte para Common Table Expressions (CTEs) recursivas. Estas últimas resultan especialmente valiosas para llevar a cabo análisis complejos de riesgos, donde a menudo se requiere la manipulación de datos jerárquicos o la realización de cálculos iterativos.

Integración nativa con Laravel

MySQL ofrece una integración nativa y completa con el framework Laravel, lo cual aporta diversas ventajas significativas para el desarrollo de la aplicación (Admin, 2023). En

primer lugar, permite la realización de migraciones automáticas de bases de datos, simplificando la gestión de los cambios en el esquema a lo largo del ciclo de vida del desarrollo. En segundo lugar, facilita la manipulación de los datos a través de Eloquent ORM (Object-Relational Mapping), que permite interactuar con las tablas de la base de datos utilizando objetos y sus métodos, lo que a menudo resulta en un código más legible y mantenible. Finalmente, la compatibilidad nativa se traduce en una gran facilidad tanto para la configuración como para el establecimiento de la conexión entre la aplicación desarrollada en Laravel y el servidor de bases de datos MySQL.

Seguridad de la aplicación

En el ámbito de la seguridad, MySQL proporciona funcionalidades esenciales para la protección de la información (Arsys, 2024). En primer lugar, ofrece un sistema de autenticación robusto basado en roles y usuarios, lo que permite una gestión precisa de los permisos de acceso. En segundo lugar, MySQL facilita la encriptación de los datos tanto cuando están en tránsito (es decir, durante la transferencia entre el cliente y el servidor) como cuando se encuentran almacenados en reposo en la base de datos. Finalmente, proporciona un control de accesos granular, que permite definir permisos específicos a nivel de tabla o incluso de columna, ofreciendo así una administración detallada de la seguridad. La aplicación protege la información sensible mediante la implementación de buenas prácticas de seguridad recomendadas por OWASP y el uso de herramientas propias del entorno Laravel y React. Para el manejo de contraseñas, se utiliza el algoritmo de hashing Bcrypt (o alternativamente Argon2), lo que garantiza que estas nunca se almacenen en texto plano y estén protegidas contra ataques por fuerza bruta. Los datos en tránsito se aseguran mediante el uso de HTTPS, y Laravel proporciona mecanismos de cifrado simétrico (AES-256-CBC) para la protección de datos en reposo cuando es necesario. Las sesiones se gestionan a través de Redis, lo cual fortalece la seguridad y rendimiento en el control de autenticación. Además, el sistema cuenta

con controles de acceso por roles (superusuario, administrador y usuario), políticas y middlewares que restringen adecuadamente las funcionalidades según el tipo de usuario. El cumplimiento de estas medidas, junto con pruebas funcionales realizadas con empresas reales y validaciones de seguridad durante el desarrollo, proporciono constancia de que se trata de un software desarrollado bajo principios seguros, alineado con estándares modernos de ciberseguridad.

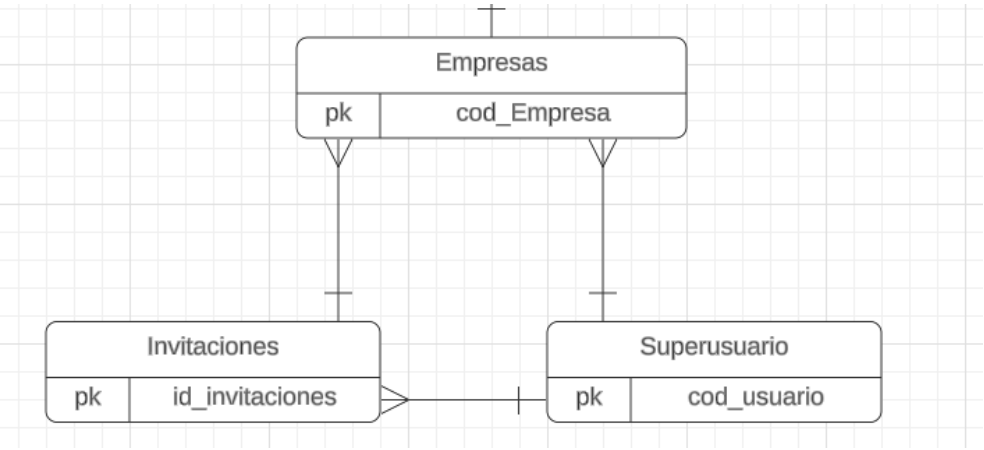
Gratuito y de código abierto

MySQL se presenta como una solución de base de datos de código abierto, lo que implica una ventaja significativa al evitar los costos asociados a licencias de software propietario. Esta característica también otorga un mayor grado de control sobre el proceso de instalación y la capacidad de personalizar el sistema para adaptarlo a las necesidades específicas del proyecto. Dada la situación actual del proyecto, que no cuenta con financiamiento externo de entidades ni de la universidad, la priorización de herramientas de código abierto como MySQL se convierte en la opción más viable y sostenible desde el punto de vista económico. La naturaleza de código abierto también fomenta una amplia comunidad de desarrolladores y usuarios, lo que puede traducirse en abundante documentación, foros de soporte y una constante evolución y mejora del software.

Esquema Base de datos

Figura 28

Relación de Entidades entre Empresas – Superusuario – Invitaciones



Nota. Elaboración Propia

Tabla 18

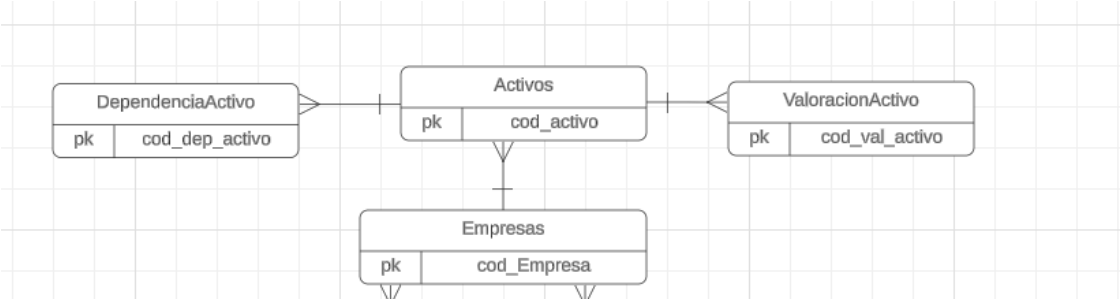
Relación entre las entidades Empresas – Superusuario – Invitaciones

ENTIDAD	DESCRIPCIÓN	RELACIÓN
SuperUsuarios	Representa al superusuario que pueda enviar invitaciones para que usuarios normales se intregren, además de gestionar la información de los activos y riesgos de la empresa.	1 superusuario puede enviar una o varias invitaciones. 1 Superusuario puede registrar información de una o varias empresas. 1 usuario - superusuario puede registrar uno o varios activos
Invitaciones	Representa a aquellos usuarios que se loguean producto de la invitación de un superusuario.	1 usuario puede crear varias invitaciones
Empresas	Representa a la empresa a la que se le está aplicando el análisis de riesgos.	1 empresa puede tener uno o varios activos de información.

Nota. Esta tabla muestra la explicación de la relación Empresas – Superusuario – Invitaciones entre *Fuente.* Elaboración Propia

Figura 29

Relación de Entidades entre Empresas, Activos, ValoracionActivo y DependenciaActivo



Nota. Elaboración Propia

Tabla 19

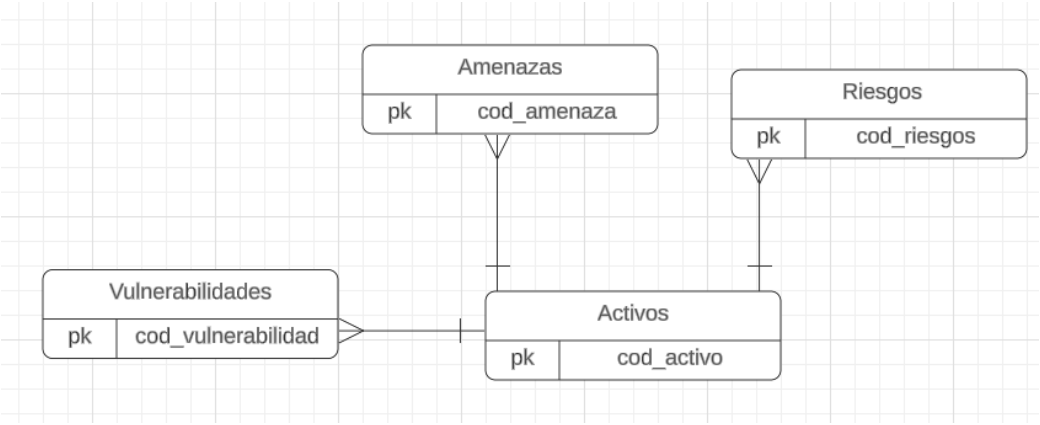
Relación entre las Empresas, Activos, ValoracionActivo y DependenciaActivo

ENTIDAD	DESCRIPCION	RELACION
Empresas	Representa a la empresa a la que se le está aplicando el análisis de riesgos.	1 empresa puede tener uno o varios activos de información.
Activos	Representa a los activos de información que tiene la empresa.	1 activo puede depender de uno o varios activos. 1 activo puede tener una o varias valoraciones.
Dependencia Activo	Representa a un activo que depende de otro activo, aspecto necesario en Magerit.	1 activo puede depender de uno o varios activos.
Valoración Activo	Representa la valoración que tiene cada activo a nivel de integridad disponibilidad y confidencialidad	1 activo puede tener una o varias valoraciones.

Nota. Esta tabla muestra la explicación de la relación Activos, ValoracionActivo y DependenciaActivo. *Fuente.* Elaboración Propia

Figura 30

Relación de Entidades entre Activos, Vulnerabilidades, Amenazas, Riesgos.



Nota. Elaboración Propia

Tabla 20

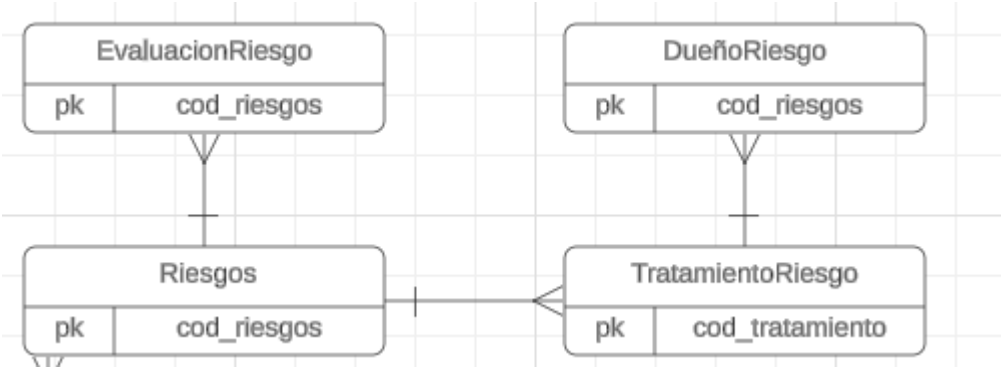
Explicación de la Relación entre Activos, Vulnerabilidades, Amenazas, Riesgos

ENTIDAD	DESCRIPCION	RELACION
Activos	Representa a los activos de información que tiene la empresa.	los activos pueden tener una o más vulnerabilidades. los activos pueden tener una o más amenazas. los activos pueden verse envueltos en uno o más riesgos
Vulnerabilidades	Representa una debilidad o brecha asociada a una activo de información	1 activo de activo de información puede presentar una o varias vulnerabilidades.
Amenazas	Representa un actor que pueda aprovecharse de la vulnerabilidad	1 activo puede tener una o varias amenazas.
Riesgos	Representa la consecuencia ocasionada por una amenaza que se aprovecha de una vulnerabilidad.	1 activo puede tener uno o varios riesgos asociados.

Nota. Esta tabla muestra la explicación de la relación Activos, Vulnerabilidades, Amenazas, Riesgos. *Fuente.* Elaboración Propia

Figura 31

Relación de Entidades entre Riesgos, TratamientoRiesgo, DueñoRiesgo, EvaluacionRiesgo



Nota. Elaboración Propia.

Tabla 21

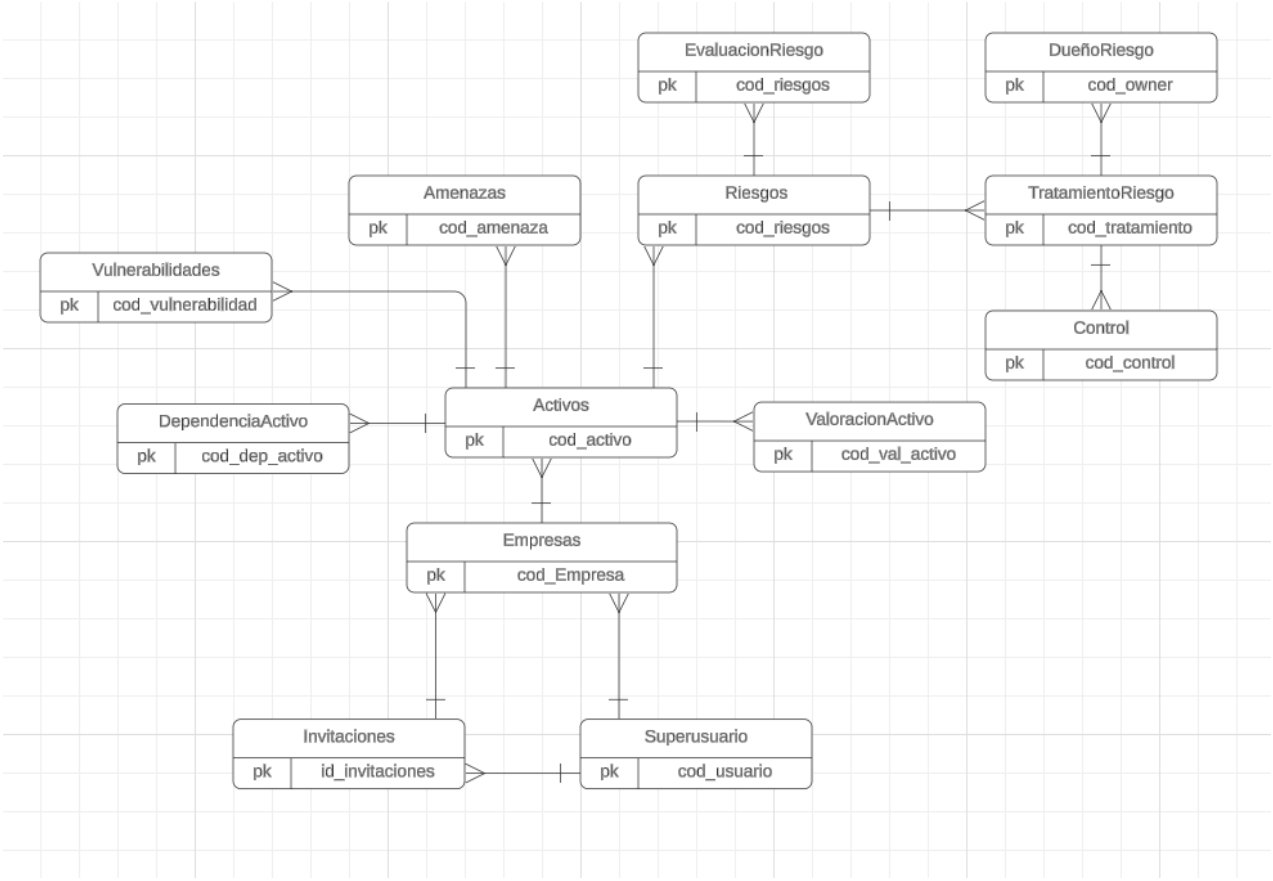
Riesgos, TratamientoRiesgo, DueñoRiesgo, EvaluacionRiesgo

ENTIDAD	DESCRIPCION	RELACION
Riesgos	Representa la consecuencia ocasionada por una amenaza que se aprovecha de una vulnerabilidad.	1 activo puede tener uno o varios riesgos asociados. 1 riesgo puede tener una o varias valoraciones. 1 riesgo puede tener una o varias formas de tratarse.
Evaluación del riesgo	Representa la probabilidad y el impacto de que un riesgo se materialice.	1 riesgo puede tener una o varias valoraciones.
Tratamiento del riesgo	Representa el plan de tratamiento que se va a llevar a cabo para disminuir el riesgo	1 activo puede tener una o varias amenazas.
Dueño del riesgo	Representa a la persona que es responsable del plan del tratamiento del riesgo en específico.	1 tratamiento del riesgo puede tener uno o varios dueños del riesgo.

Nota. Esta tabla muestra la explicación de la relación Riesgos, TratamientoRiesgo, DueñoRiesgo, EvaluacionRiesgo. *Fuente.* Elaboración Propia

Figura 32

Esquema de la base de datos



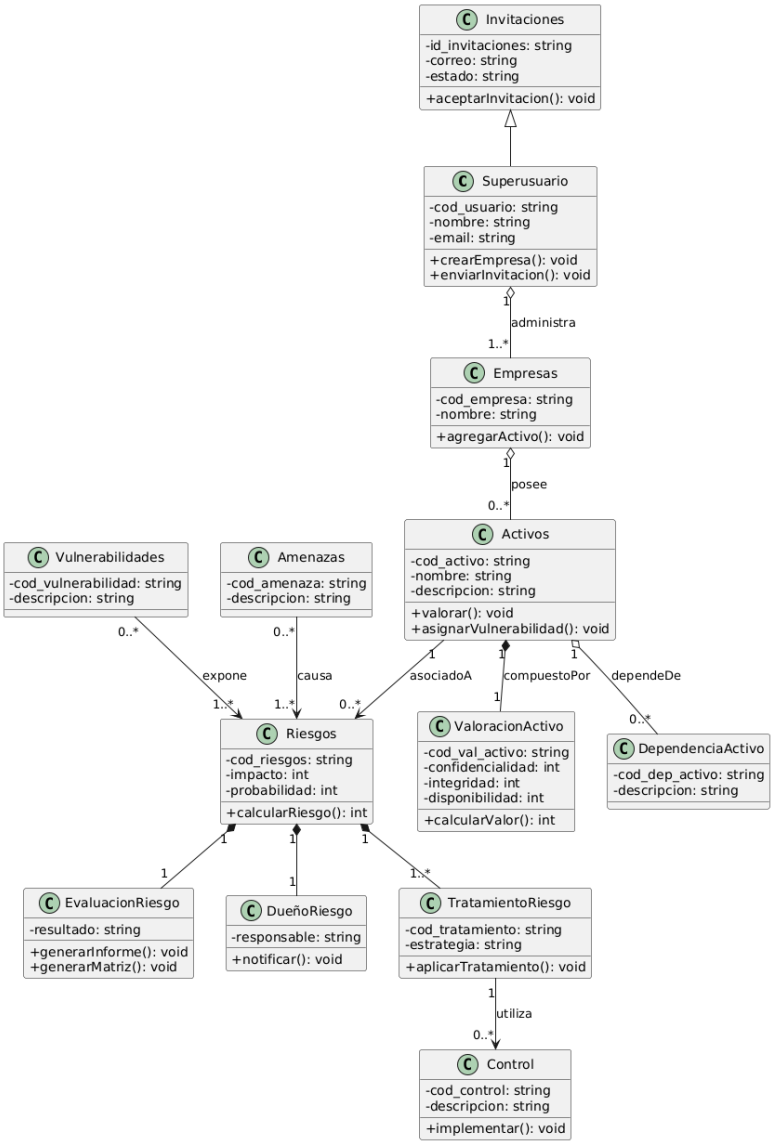
Nota. Elaboración Propia

Diagrama de Clases

Un diagrama de clases es la representación visual de la estructura estática de un sistema, mostrando sus clases, atributos, métodos y relaciones (Tutorial de Diagrama de Clases UML, 2025).

Figura 33

Diagrama de clases de la aplicación



Nota. Elaboración Propia

El diagrama de clases presentado refleja de forma estructurada y lógica los elementos principales del dominio de la aplicación de gestión de riesgos de seguridad de la información. Este diseño permite representar la forma en que los diferentes actores y entidades interactúan dentro del sistema y cómo se relacionan entre sí para cumplir los requisitos funcionales definidos previamente.

Modularidad y organización del sistema

La arquitectura del sistema se caracteriza por su modularidad y una organización lógica de las clases, diseñada para reflejar el flujo natural del proceso de gestión de riesgos. Este flujo se inicia con la gestión de las entidades fundamentales de la aplicación, como las empresas que utilizarán el sistema y los diferentes tipos de usuarios, incluyendo superusuarios, usuarios de empresas e invitaciones para nuevos usuarios. A continuación, el sistema guía al usuario a través de la etapa de identificación y valoración de los activos de información, donde se definen los activos, se evalúa su valor y se establecen sus dependencias. Posteriormente, se aborda el análisis de amenazas y riesgos, permitiendo la identificación de vulnerabilidades y amenazas, la definición de los riesgos asociados y su correspondiente evaluación. Finalmente, el sistema facilita la gestión del tratamiento de estos riesgos, incluyendo la planificación de las acciones de tratamiento, la selección de controles de seguridad y la asignación de responsables para la gestión de cada riesgo.

Relaciones expresivas y bien definidas

En el diseño del sistema, se han definido relaciones expresivas y claras entre las diferentes entidades para ilustrar su composición e interacción. Se utiliza la asociación para representar relaciones lógicas, como el hecho de que una empresa puede poseer múltiples activos. La agregación se emplea para mostrar relaciones donde una clase forma parte de otra, pero sin una dependencia existencial fuerte; por ejemplo, un activo puede depender de otro,

pero la existencia del activo principal no está intrínsecamente ligada a la del activo dependiente. La composición, por otro lado, se utiliza para establecer relaciones de dependencia fuerte; en este caso, si una instancia de una clase se elimina, las instancias relacionadas también se eliminan (como cuando se elimina un riesgo, su evaluación o tratamiento asociado también desaparecen). Finalmente, se especifica la multiplicidad de las relaciones para aclarar cuántas instancias de una clase pueden estar relacionadas con otra, utilizando notaciones como 1:1 (uno a uno), 1:N (uno a muchos) o N:M (muchos a muchos).

Separación de responsabilidades

Cada clase tiene atributos específicos que representan las características más relevantes del objeto por ejemplo, confidencialidad, integridad, disponibilidad en ValoracionActivo, así como métodos que ilustran las acciones principales asociadas (como calcularRiesgo(), aplicarTratamiento()). Debido a la complejidad del proyecto se colocan solo algunos atributos en el diagrama de clases, en el esquema general de la base de datos y en la base de datos como tal, se encuentran la información precisa y detallada de cada atributo y metodo correspondiente. Esto sigue el principio de responsabilidad única (SRP), lo cual facilita la extensibilidad futura del sistema.

Cohesión con los requisitos funcionales

El diagrama ha sido diseñado tomando como referencia los requisitos funcionales definidos durante la etapa de análisis. Cada clase y relación corresponde a una funcionalidad central del sistema, asegurando trazabilidad entre lo que el sistema debe hacer y cómo está estructurado internamente.

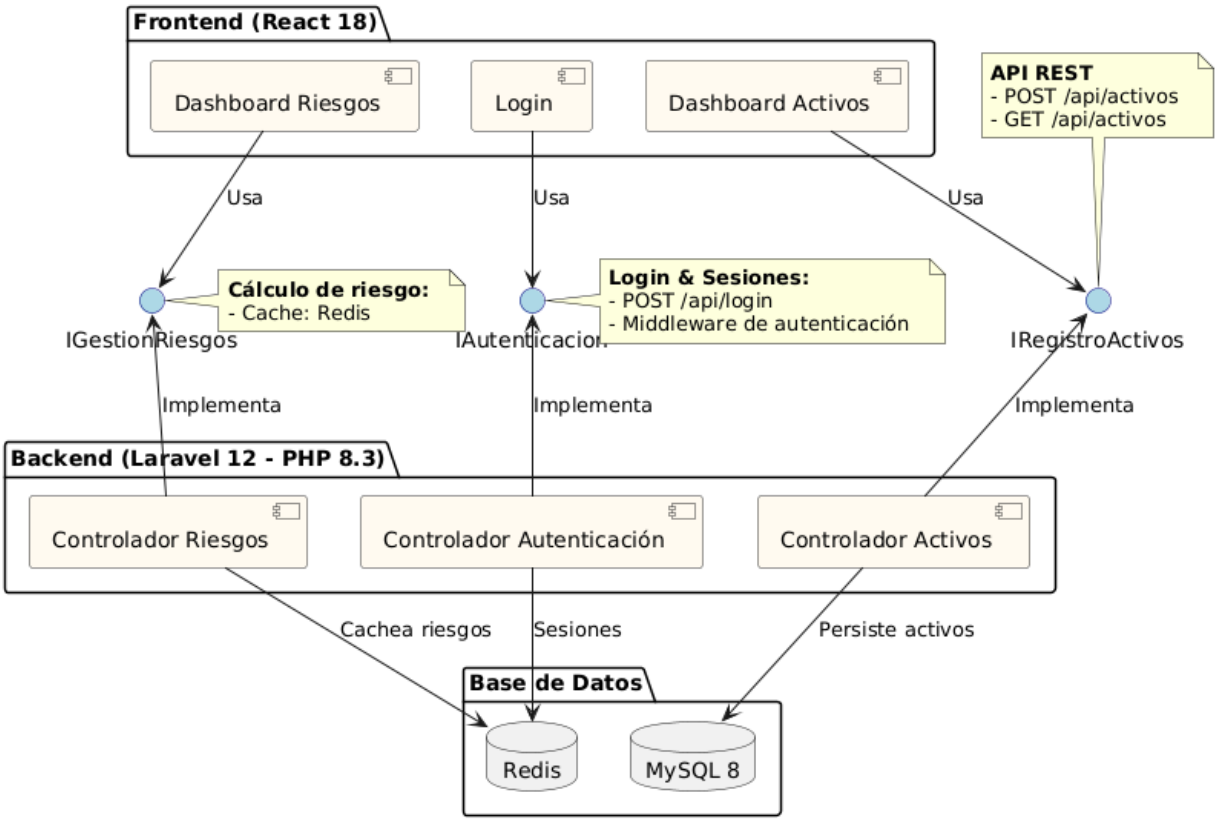
Diagrama de Componentes

Los diagramas de componentes se utilizan para visualizar la organización de los componentes de un sistema y las relaciones de dependencia entre ellos. Proporcionan una

visión de alto nivel de los componentes de un sistema. Los componentes pueden ser un componente de software como; una base de datos o una interfaz de usuario o un componente de hardware; como un circuito, un microchip o un dispositivo; o una unidad de negocio, como un proveedor, una nómina o un envío (Siriwardhana, 2022).

Figura 34

Diagrama de Componentes de la Aplicación



Nota. Elaboración Propia.

Frontend (React 18 con TypeScript)

La capa del Frontend de la aplicación se desarrolló utilizando React 18 y TypeScript, y alberga los componentes visuales a través de los cuales el usuario interactúa directamente con el sistema. Dentro de esta capa, se encuentra el Formulario de Activos, que permite a los usuarios ingresar la información relevante sobre los activos de información de la organización.

También se incluye el Dashboard de Riesgos, que ofrece una visualización del estado actual de los riesgos evaluados, presentando esta información a través de gráficas y reportes generados por el sistema. Finalmente, el Login es el módulo encargado de gestionar el ingreso autenticado de los usuarios al sistema, garantizando el acceso seguro a las funcionalidades de la aplicación. Es importante destacar que el Frontend se diseñó de manera desacoplada y con una estructura orientada al consumo de datos a través de APIs REST, adhiriéndose al patrón de arquitectura cliente-servidor para la comunicación con la capa del Backend.

Backend (Laravel 12, PHP 8.3)

La capa del Backend de la aplicación se construyó utilizando Laravel 12 y PHP 8.3, y alberga los controladores y servicios que implementan la lógica del negocio. Dentro de esta capa, se encuentra el Controlador de Activos, encargado de administrar los procesos de registro y consulta de los activos de información. El Controlador de Riesgos implementa la lógica para realizar el cálculo y el análisis de los riesgos identificados, considerando factores como la probabilidad y el impacto. Por último, el Controlador de Autenticación gestiona los procesos de inicio de sesión (login), el mantenimiento de las sesiones de usuario y la seguridad del acceso a la aplicación. Estos controladores implementan interfaces lógicas bien definidas que son consumidas por la capa del Frontend para la interacción con el usuario, y a su vez, se encargan de la persistencia de la información en la base de datos correspondiente.

Bases de Datos

En cuanto al almacenamiento de datos, la aplicación utiliza dos sistemas de bases de datos complementarios. MySQL 8 se emplea como la base de datos relacional principal. En ella se almacena la información estructurada fundamental para el funcionamiento del sistema.

Por otro lado, se utiliza Redis, una base de datos en memoria, con el propósito de optimizar el rendimiento de la aplicación. Redis se emplea para dos funciones principales: para

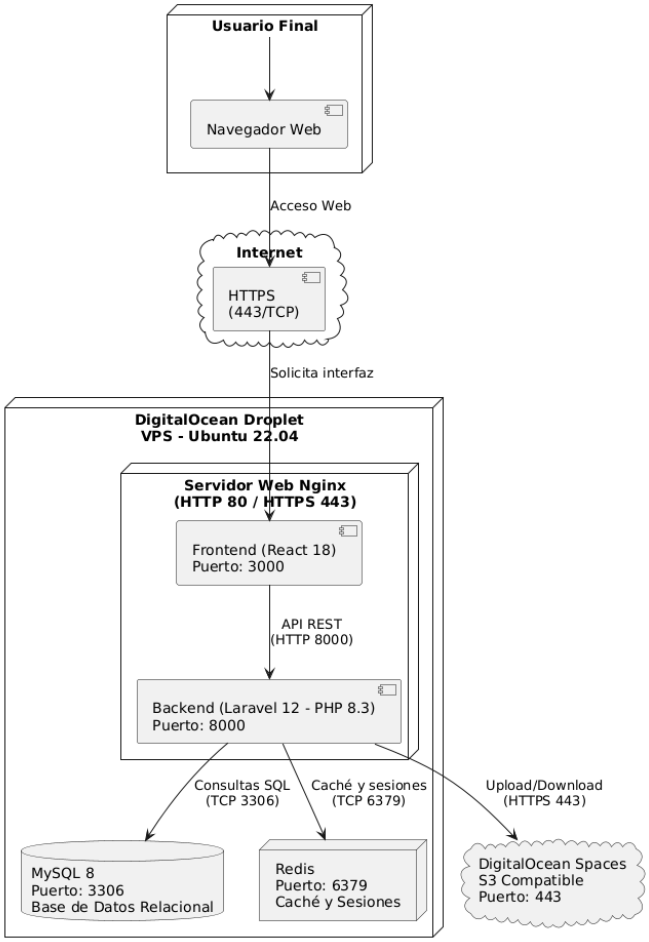
almacenar los resultados de los cálculos de riesgos y de la gestión de las sesiones de los usuarios que se han autenticado en el sistema.

Diagrama de Despliegue

El diagrama de despliegue es un modelo UML que muestra cómo los componentes del sistema (frontend, backend, bases de datos) se instalan y ejecutan en hardware real o entornos Cloud (como la VPS usada en DigitalOcean).

Figura 35

Diagrama de Despliegue de la Aplicación



Nota. Elaboración Propia

El diagrama de despliegue representa la arquitectura física de la aplicación web para la gestión de riesgos de seguridad de la información, la cual está implementada sobre un servidor

VPS proporcionado por DigitalOcean, específicamente en un droplet con Ubuntu 22.04. En esta infraestructura se encuentra desplegado un servidor web Nginx que gestiona tanto el frontend desarrollado en React 18 como el backend construido en Laravel 12 sobre PHP 8.3. La base de datos MySQL 8 actúa como almacenamiento principal de la información, mientras que Redis se emplea para el manejo eficiente de sesiones y caché, optimizando el rendimiento de la aplicación. Adicionalmente, se utiliza el servicio DigitalOcean Spaces para almacenar archivos como reportes generados por el sistema. El acceso de los usuarios se realiza a través de un navegador web mediante el protocolo HTTPS, asegurando la transmisión de datos. Las conexiones están claramente definidas con sus respectivos protocolos y puertos, lo que permite garantizar una comunicación segura, modular y escalable entre todos los componentes del sistema.

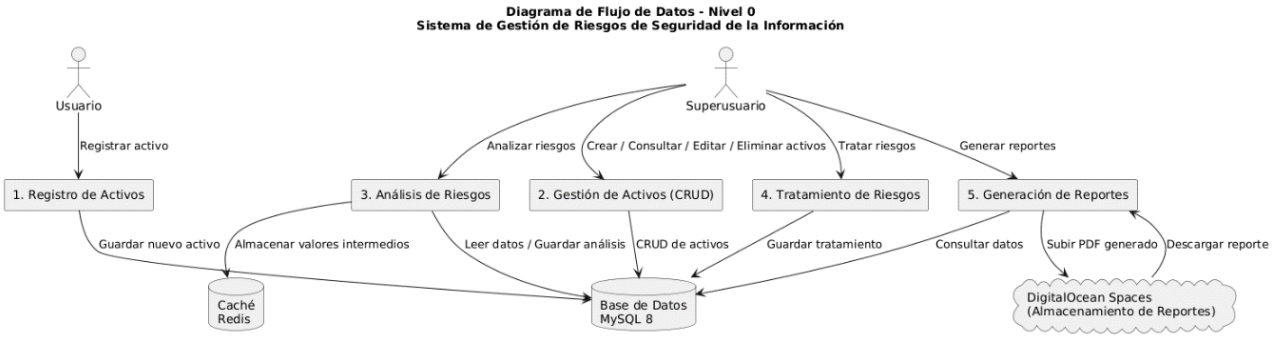
Diagrama de Flujo de Datos

El DFD es un modelo gráfico que muestra cómo los datos se mueven a través del sistema de gestión de riesgos, desde su entrada hasta su almacenamiento (MySQL/Redis) y salida. No muestra código ni componentes técnicos, sino el flujo lógico de la información (Qué Es un Diagrama de Flujo de Datos, 2025).

Estos DFD por lo general presentan niveles, en el nivel 0 se detalla una vista global. El nivel 1,2,3 se detalla por proceso por ejemplo de gestión de activos, análisis del riesgo y tratamiento del riesgo.

Figura 36

DFD Nivel 0



Nota. Elaboración Propia.

El Diagrama de Flujo de Datos de Nivel 0 presenta una visión de alto nivel del Sistema de Gestión de Riesgos de Seguridad de la Información, delineando las interacciones entre las entidades externas y los procesos centrales del sistema, así como los almacenes de datos fundamentales para su funcionamiento. La distinción entre el Usuario y el Superusuario como actores externos se basa en la necesidad de implementar un modelo de control de acceso granular, donde el Usuario interactúa principalmente para el registro y consulta de activos, además de participar en el análisis de riesgos. En contraste, el Superusuario ostenta privilegios elevados, permitiéndole la gestión integral del ciclo de vida de los riesgos, abarcando su creación, lectura, edición, eliminación y la definición de sus respectivos tratamientos. Esta segregación de roles es esencial para mantener la integridad y la seguridad de la información gestionada dentro del sistema.

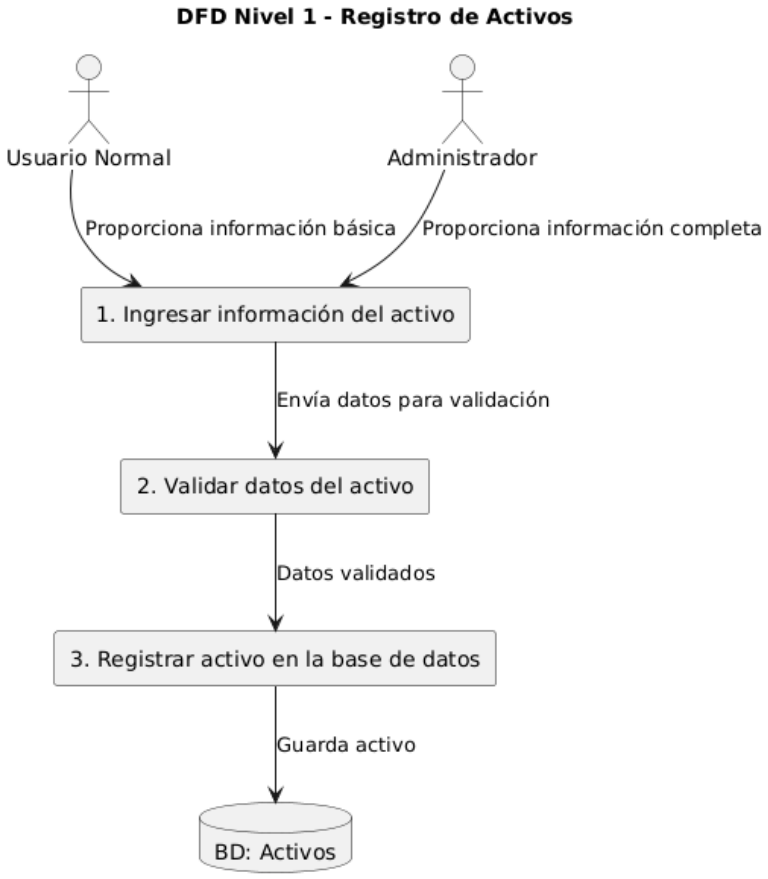
Los cinco procesos principales identificados en el diagrama representan las etapas críticas dentro del sistema de gestión de riesgos. El proceso 1. Registro de Activos constituye el punto de entrada para la identificación y documentación de los activos de información que son objeto de protección. El proceso 2. Gestión de Riesgos engloba las operaciones fundamentales para la administración de los riesgos identificados, permitiendo al Superusuario llevar a cabo

las acciones de Crear, Leer, Actualizar y Eliminar registros de riesgo como amenazas y vulnerabilidades. El proceso 3. Análisis de Riesgos se centra en la evaluación sistemática de las amenazas y vulnerabilidades que podrían impactar los activos previamente registrados. El proceso 4. Tratamiento de Riesgos aborda la planificación e implementación de las estrategias y controles destinados a mitigar, evitar, transferir o aceptar los riesgos analizados. Finalmente, el proceso 5. Generación de Reportes proporciona la funcionalidad para extraer información relevante del sistema, facilitando la toma de decisiones informadas y el cumplimiento de requisitos normativos.

Los almacenes de datos representados son componentes esenciales para la persistencia y la eficiencia del sistema. La Base de Datos sirve como el repositorio central y persistente para toda la información crítica del sistema, incluyendo el inventario de activos, el registro de riesgos, los resultados de los análisis, los planes de tratamiento y los datos necesarios para la generación de informes. La incorporación de Caché Redis se justifica por la necesidad de optimizar el rendimiento de la aplicación. Almacenando temporalmente datos de acceso frecuente y resultados intermedios de los procesos, se reduce la latencia y la carga sobre la base de datos principal, mejorando la experiencia tanto del Usuario como del Superusuario. Por último, DigitalOcean Spaces Almacenamiento de Reportes se utiliza como un sistema de almacenamiento externo y escalable para los informes generados. Esta decisión permite una gestión eficiente de los reportes sin sobrecargar la base de datos operativa y facilita su acceso y distribución.

Figura 37

DFD Nivel 1 - Registro de Activos



Nota. Elaboración Propia

En este nivel, interactúan dos actores externos: el Usuario Normal y el Administrador, quienes tienen diferentes niveles de acceso y responsabilidades en el proceso de registro.

El proceso se inicia con la etapa de Ingresar información del activo. Tanto el Usuario Normal como el Administrador pueden ingresar información sobre un nuevo activo. Sin embargo, se indica una distinción en la cantidad y el detalle de la información proporcionada. El Usuario normal proporciona información básica, lo que sugiere un conjunto limitado de atributos esenciales para la identificación inicial del activo. Por otro lado, el Administrador proporciona

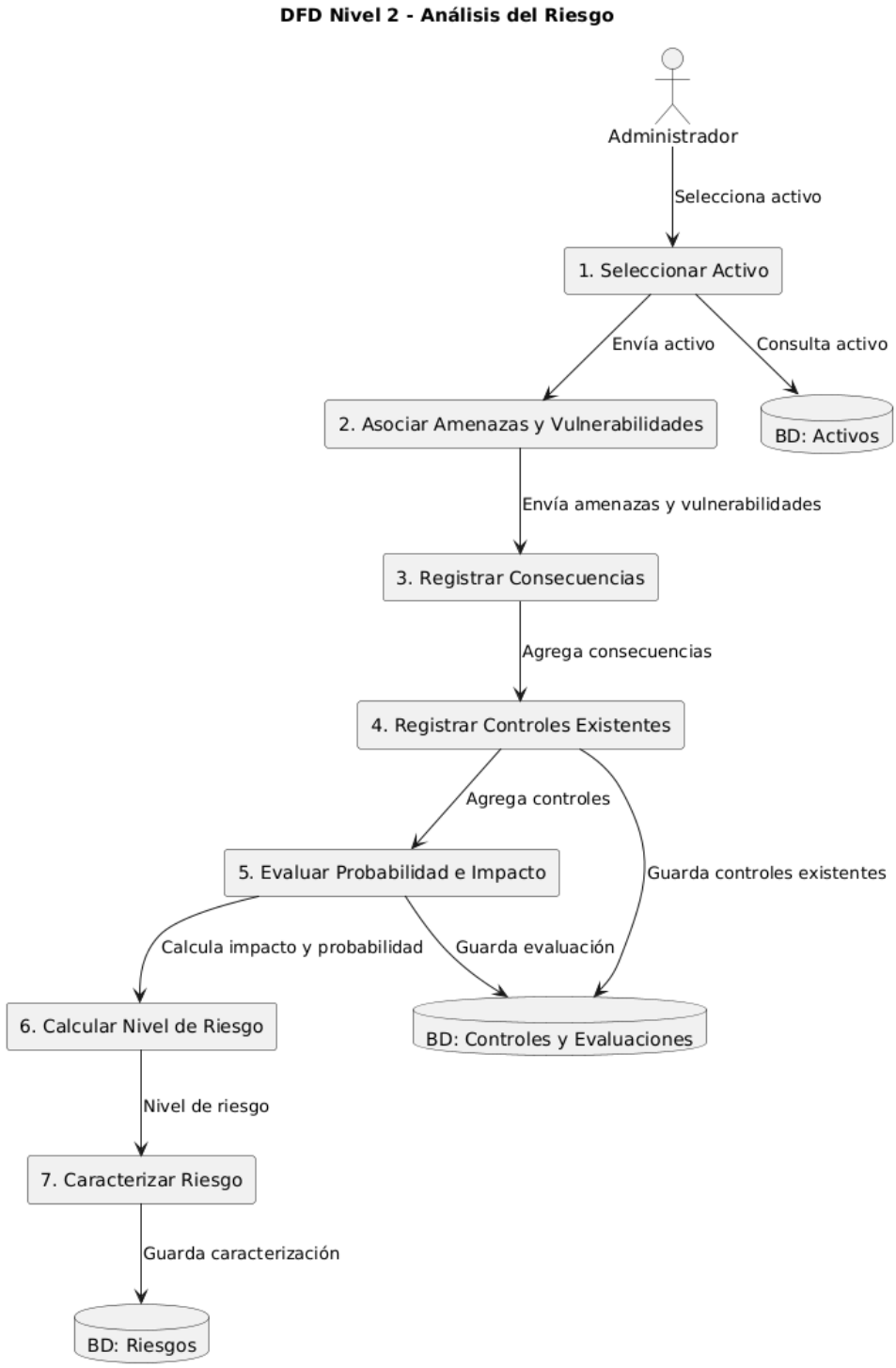
información completa, lo que implica el ingreso de un conjunto más extenso y detallado de características y metadatos relevantes para la gestión del activo.

Una vez que la información del activo ha sido ingresada por cualquiera de los dos actores, los datos se envían al proceso de validar datos del activo. Esta etapa es crucial para asegurar la calidad e integridad de la información que se almacena en el sistema. Durante la validación, se verifican aspectos como la completitud de los campos obligatorios, el formato de los datos ingresados y la coherencia con las reglas de negocio definidas para el registro de activos.

Si los datos del activo superan el proceso de validación, se genera un flujo de Datos validados que alimenta el proceso de registrar activo en la base de datos. En esta etapa, la información del activo validada se guarda de forma persistente en el almacén de datos BD: Activos. Este almacén constituye el repositorio central de todos los activos de información gestionados por el sistema.

Figura 38

DFD Nivel 2 Análisis del riesgo



Nota. Elaboración Propia

El Diagrama de Flujo de Datos de Nivel 2 profundiza en el proceso de Análisis de Riesgos identificado en el DFD de Nivel 0, detallando las sub-etapas y los flujos de información necesarios para llevar a cabo esta actividad crítica dentro del Sistema de Gestión de Riesgos de Seguridad de la Información. El actor externo en este nivel es el Administrador, quien se encarga de ejecutar el proceso de análisis de riesgos para los activos del sistema.

El proceso se inicia con la seleccionar Activo, donde el Administrador identifica el activo específico que será objeto de análisis. Para realizar esta selección, el sistema consulta la BD: Activos, el repositorio donde se encuentran registrados todos los activos de información. Una vez seleccionado el activo, el Administrador procede a asociar Amenazas y Vulnerabilidades, vinculando al activo las posibles amenazas que podrían explotar sus debilidades o vulnerabilidades.

A continuación, en el proceso de registrar Consecuencias, el Administrador define los posibles impactos o daños que podrían ocurrir si las amenazas se materializan y explotan las vulnerabilidades del activo. Posteriormente, en registrar Controles Existentes, se documentan las medidas de seguridad o controles que ya están implementados para mitigar las amenazas o reducir las vulnerabilidades del activo.

El núcleo del análisis de riesgos se encuentra en el proceso de evaluar Probabilidad e Impacto, donde el Administrador, basándose en la información recopilada sobre las amenazas, vulnerabilidades y controles, evalúa la probabilidad de ocurrencia del riesgo y la magnitud de su impacto potencial.

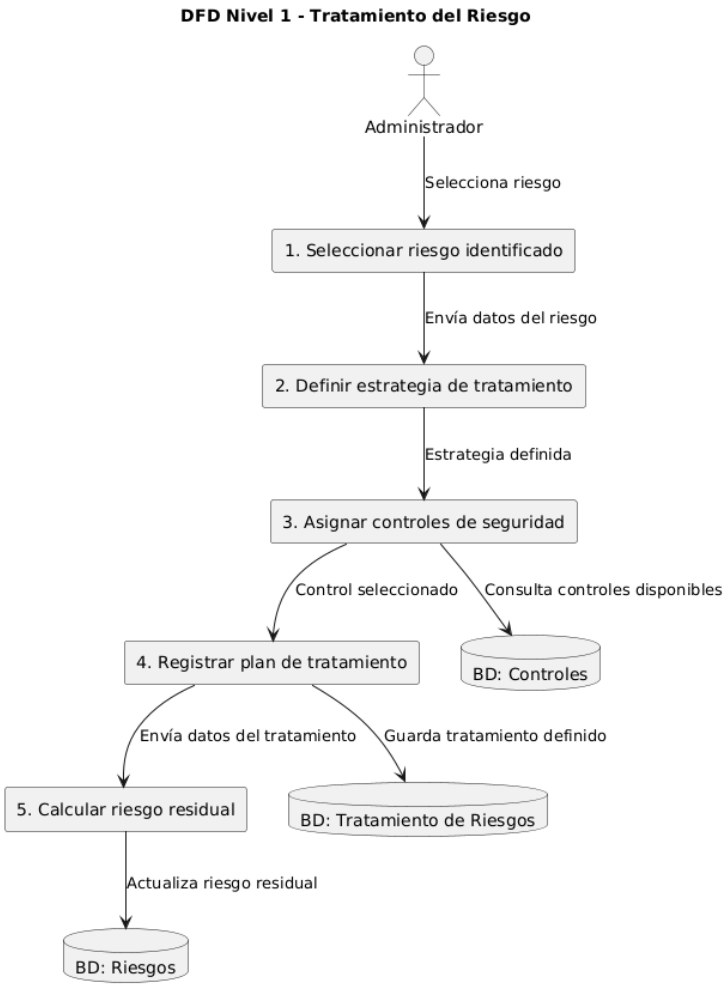
Con la probabilidad e impacto evaluados, el sistema ejecuta el proceso de calcular Nivel de Riesgo. Este proceso interno utiliza los valores de probabilidad e impacto para determinar el nivel de riesgo asociado al activo, aplicando una metodología predefinida (que podría estar

basada en matrices de riesgo o fórmulas específicas). El resultado de este cálculo es el Nivel de riesgo.

Finalmente, en el proceso Caracterizar Riesgo, el nivel de riesgo calculado se utiliza para categorizar o clasificar el riesgo (por ejemplo, como bajo, medio, alto). Esta caracterización proporciona una visión clara de la criticidad del riesgo y facilita la priorización de las acciones de tratamiento.

Figura 39

DFD Nivel 3- Tratamiento del Riesgo



Nota. Elaboración Propia

El Diagrama de Flujo de Datos de Nivel 3 detalla el proceso de Tratamiento de Riesgos identificado en el DFD de Nivel 0, exponiendo las sub-etapas y el flujo de información necesario para definir y registrar las acciones destinadas a gestionar los riesgos identificados dentro del Sistema de Gestión de Riesgos de Seguridad de la Información (ver Figura 1)El actor externo involucrado en este nivel es el Administrador, quien es responsable de la planificación y asignación de los tratamientos para los riesgos del sistema.

El proceso se inicia con la etapa de seleccionar riesgo identificado, donde el Administrador elige el riesgo específico que será objeto de tratamiento. Para llevar a cabo esta selección, el sistema consulta la BD: Riesgos, el repositorio donde se almacena la información consolidada sobre los riesgos previamente identificados y caracterizados. Una vez seleccionado el riesgo, el Administrador procede a definir estrategia de tratamiento, donde se determina el enfoque general para abordar el riesgo (por ejemplo, mitigar, evitar, transferir o aceptar).

A continuación, en el proceso Asignar controles de seguridad, el Administrador selecciona los controles de seguridad específicos que se implementarán para ejecutar la estrategia de tratamiento definida. Para facilitar esta selección, el sistema consulta la BD: Controles, que contiene un catálogo de los controles de seguridad disponibles en el sistema. El Administrador elige los controles pertinentes para el riesgo en cuestión.

Una vez definidos la estrategia y los controles asignados, se procede a Registrar plan de tratamiento. En esta etapa, se documenta formalmente el plan de tratamiento, incluyendo la estrategia seleccionada, los controles asignados y cualquier otra información relevante para la implementación del tratamiento. Los datos del tratamiento definido se guardan en la BD: Tratamiento de Riesgos, creando un registro de las acciones planificadas para cada riesgo.

Finalmente, el proceso de calcular riesgo residual evalúa el nivel de riesgo que persistirá después de la implementación de los controles definidos en el plan de tratamiento. Este cálculo se basa en la efectividad esperada de los controles asignados. El Riesgo residual calculado se utiliza para actualizar la información del riesgo original en la BD: Riesgos, proporcionando una visión del impacto de las acciones de tratamiento planificadas.

La arquitectura diseñada para la aplicación no solo responde a los requisitos técnicos del proyecto, sino que también garantiza una base sólida para su escalabilidad y seguridad. Gracias al uso del patrón MVC monolítico, se logró una organización clara de responsabilidades entre las capas del sistema, facilitando futuras modificaciones o ampliaciones funcionales. La elección de Laravel y React como tecnologías principales permite una integración fluida y mantenible entre frontend y backend, mientras que el uso de MySQL 8 como base de datos relacional asegura integridad y consistencia de la información. Por otro lado, la incorporación de Redis para manejo de sesiones y cache, junto con el despliegue en un entorno controlado como DigitalOcean, refuerzan la seguridad operativa del sistema. Esta arquitectura, documentada mediante diagramas claros (componentes, clases, despliegue, flujo de datos), no solo cumple con los objetivos planteados, sino que está preparada para soportar nuevas funcionalidades, adaptarse a las necesidades cambiantes del usuario y enfrentar los retos de seguridad de la información en el entorno real**.**

Crear una interfaz de usuario intuitiva y accesible, evaluada mediante pruebas de usabilidad, para facilitar la navegación y el uso de la aplicación por parte de los usuarios, independientemente de su nivel de experiencia técnica.

Para cumplir con este objetivo, se diseñó y desarrolló una interfaz de usuario web accesible e intuitiva, enfocada en la experiencia del usuario final. A continuación, se adjunta el código fuente completo de la aplicación:

Código Fuente: https://drive.google.com/file/d/1T3BETVRsy8cVoCErs-cd-4byWrKNBDlX/view?usp=drive_link

Realizar pruebas funcionales, de usabilidad y aceptación para validar el cumplimiento de los requerimientos definidos, garantizando la calidad del software y su adopción por parte de los usuarios.

Se creo un plan de pruebas que explica el paso a paso de las pruebas realizadas al software. A continuación, se adjunta el plan de pruebas:

https://docs.google.com/document/d/1justBQDtYrMgpEepQ5NioeMBlAIqkGjZ/edit?usp=sharing&ouid=104587354796030010275&rtpof=true&sd=true

Manual de Usuario

Se desarrolló un manual de usuario que explica paso a paso las funcionalidades del sistema. A continuación, se adjunta el manual de usuario en el que se describe el uso de cada módulo de la aplicación y se resuelven las dudas más comunes:

https://drive.google.com/file/d/1QXoOg6Y1L-QxQ-fA2H6jUpkR9bgyCGhh/view?usp=sharing

Impactos

El desarrollo de esta aplicación para la gestión de riesgos de seguridad de la información ha generado varios efectos positivos. En primer lugar, ha contribuido a que las empresas participantes sean más conscientes de los riesgos existentes en sus procesos y activos, fomentando una cultura organizacional orientada a la seguridad. En segundo lugar, la herramienta ha permitido estructurar de forma más ordenada la gestión de riesgos, lo cual mejora la gobernanza y la estructura organizacional al definir responsabilidades claras y procesos trazables.

Adicionalmente, el software soporta directamente los objetivos misionales y operacionales de las empresas al proteger la confidencialidad, integridad y disponibilidad de la información crítica, aspecto esencial para mantener la confianza de sus clientes y aliados. Asimismo, la aplicación promueve una mejora significativa en la toma de decisiones estratégicas y operativas, al proporcionar datos estructurados, reportes claros y evidencia objetiva para priorizar inversiones en seguridad.

A nivel regional, el desarrollo de este proyecto sienta un hito importante, pues constituye el inicio y cimiento para futuros estudios en seguridad de la información en el contexto local. La creación de una aplicación como esta y una base de datos estructurada sobre riesgos y activos abre la posibilidad de impulsar proyectos interdisciplinarios e innovadores, incluyendo el uso de inteligencia artificial para la detección proactiva de amenazas, algo que antes no era posible debido a la falta de información consolidada y estudios previos en el tema.

Finalmente, el proyecto también fomenta la profesionalización de la gestión de riesgos en las empresas de software de la región, ofreciendo un ejemplo replicable para otros sectores productivos que necesitan fortalecer sus prácticas de seguridad de la información de forma accesible y contextualizada.

Recomendaciones

Para garantizar la evolución continua y la máxima efectividad del software de gestión de riesgos de seguridad de la información, se probo el software final con las empresas y con usuarios finales (Ver anexo *O*) en una reunión final, se ofreció retroalimentación de las posibles mejoras al software:

1. ***Educación:*** Ofrecer una mayor explicación sobre los diferentes conceptos que se manejan y referencias a las normas que se están usando dentro la aplicación.
2. ***Personalización de Controles:*** Ampliar las capacidades de personalización de los controles de seguridad basados en ISO/IEC 27002 y permitir la importación de catálogos específicos según el sector o el marco normativo que aplique a cada organización.
3. ***Alertas y Notificaciones:*** Implementar un sistema robusto de notificaciones y alertas automáticas para informar a los responsables sobre cambios en el nivel de riesgo, vencimientos de planes de tratamiento o auditorías pendientes.
4. ***Adaptación normativa:*** Mantener actualizada la base normativa en la que se apoya la aplicación (ISO/IEC 27001, 27002, 27005, MAGERIT) incorporando futuras revisiones o versiones para asegurar su vigencia y relevancia además de metodologías como NIST.
5. ***Documentación y reportes periódicos:*** Establecer el hábito organizacional de generar y revisar reportes de riesgos de forma periódica (mensual o trimestral), utilizando las funcionalidades del software para informar a la alta dirección y apoyar la toma de decisiones estratégicas en materia de seguridad.

Cronograma de Actividades

El cronograma de actividades está distribuido en un total de 26 semanas de trabajo, organizadas de manera que se cubran los puntos clave relacionados con los objetivos planteados en el proyecto

Cuadro 2

Cronograma de actividades

N°	Actividad	Duracion (6 Meses) Fecha de Inicio : 1 de noviembre de 2024																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	Revisión bibliográfica sobre MAGERIT, ISO 27001 , ISO 27002, ISO 27005																										
2	Identificación de requerimientos de seguridad de la información basados en las normas mencionadas.																										
3	Entrevistas a Empresas de Software																										
4	Recopilacion de requerimientos Funcionales , No funcionales																										
5	Desarrollo de un informe con los requisitos del software basados en el análisis de las normas.																										
6	Desarrollo del diseño preliminar de la arquitectura del sistema basado en los requerimientos de seguridad																										
7	Desarrollo de Diagramas Clave																										
8	Diseño de la base de datos																										
9	Desarrollo(Backend y Frontend)																										
10	Pruebas de Integridad de datos,Calidad del Software Y Concurrencia																										
11	Pruebas de usabilidad con diferentes grupos de usuarios para validar la facilidad de uso de la interfaz.																										
12	Capacitación																										
13	Desarrollo del informe final del proyecto, que incluye la documentación del proceso completo, las pruebas realizadas y las recomendaciones de mejora																										
14	Manuales de usuario																										

Presupuesto

Tabla 22

Presupuesto de la Aplicación

No.	Componente / Documento de Referencia	Descripción / Justificacion	Cantidad	Valor unitario	Total
		Recursos Humanos			
1	Desarrollador	Se encarga del desarrollo, mantenimiento y actualización de la aplicación web de gestión de riesgos de seguridad de la información	1/mes	$ 3,000,000.00	**$ 18,000,000.00**
2	Auditor ISO 27001:2022	Asegura que Securisk cumpla con los estándares internacionales de seguridad de la información. Este rol implica realizar auditorías para evaluar el cumplimiento con los requisitos de la norma, identificar áreas de mejora, elaborar documentación y reportes detallados.	1/mes	$ 3,000,000.00	**$ 18,000,000.00**
3	Director de grado	Guia y supervisa el desarrollo del proyecto, asegurando que se cumplan los objetivos académicos y se mantenga la calidad del trabajo. Se encarga de proporcionar orientación técnica y metodológica, revisar y aprobar el avance del proyecto, ofrecer retroalimentación constructiva, y asegurar que el proyecto cumpla con los requisitos académicos y profesionales para la obtención del título de ingeniería de sistemas.	1/mes	$ 4,500,000.00	**$ 36,000,000.00**
		Equipos y Servicios			
4	Alquiler Computador	Intel Core i9-13900KF 3.0GHz, GeForce RTX 4070 12GB, 16GB DDR5, 1TB NVMe SSD	1	$ 200,000.00	**$ 1,200,000.00**
5	VPS(Virtual Private Server)	Máquina que aloja todo el software y los datos necesarios para ejecutar toda la aplicacion de Securisk , sirve para el lanzamiento de la aplicacion asi como para crear entornos de prueba	1/mes	$ 190,779.84	**$ 1,144,679.04**
8	Contingencias	Un fondo para imprevistos, generalmente un porcentaje del presupuesto total, para cubrir cualquier gasto inesperado que pueda surgir.	1	$ 7,434,679.00	**$ 7,434,680.00**
		Total del proyecto			**$ 81,779,359.04**

Conclusiones

El presente trabajo tuvo como propósito desarrollar una aplicación web que contribuyera a la gestión de riesgos de seguridad de la información en las empresas de desarrollo de software de Yopal, abordando una problemática crítica: la inexistencia de herramientas tecnológicas que guiaran a las organizaciones en la identificación, evaluación y tratamiento de riesgos. A partir de metodologías reconocidas, como MAGERIT, complementada por las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005, y bajo un enfoque de desarrollo en cascada, se logró materializar una solución funcional y adaptada a las necesidades reales del sector.

Analizar estas metodologías permitió no solo definir los requisitos funcionales y no funcionales del software, sino también construir una base sólida para un sistema que trasciende el cumplimiento normativo y busca generar conciencia en las organizaciones sobre la importancia de gestionar sus riesgos de seguridad de la información. A diferencia de otras metodologías, MAGERIT aportó un enfoque más completo, detallado y alineado con los principios de confidencialidad, integridad y disponibilidad, sirviendo como columna vertebral del proyecto.

Diseñar la arquitectura de la aplicación aseguró que la solución fuera escalable y segura. La selección de un modelo cliente-servidor y una arquitectura MVC monolítica no solo permitió cumplir con los requerimientos actuales, sino también sentar las bases para un crecimiento futuro del sistema. La integración de tecnologías modernas y diagramas arquitectónicos aportó claridad y robustez técnica, garantizando estabilidad y confiabilidad del software.

Crear una interfaz de usuario amigable y accesible fue clave para lograr que las empresas pudieran adoptar el sistema sin barreras técnicas. Las pruebas realizadas confirmaron que el software cumple con los objetivos de gestionar activos, analizar riesgos y definir planes de tratamiento de manera sencilla y ordenada, entregando información clara y reportes útiles para la toma de decisiones estratégicas.

Realizar pruebas de funcionalidad, usabilidad y aceptación permitió validar el cumplimiento de los requisitos definidos, demostrando que la solución propuesta es viable y efectiva para el propósito planteado. Si bien el proyecto no incluyó la implementación real en las empresas por limitaciones de alcance y recursos, los resultados obtenidos y el feedback recibido evidencian el potencial de esta herramienta para transformar la manera en que las organizaciones gestionan sus riesgos de seguridad.

En definitiva, este proyecto no solo cumplió con los objetivos establecidos, sino que también marca un precedente en la región al ofrecer un punto de partida para futuros desarrollos e investigaciones en materia de seguridad de la información. La aplicación diseñada no se limita a automatizar procesos, sino que impulsa un cambio cultural hacia la protección de los activos de información y la prevención de amenazas, contribuyendo a que las empresas de software de Yopal sean más resilientes y competitivas en un entorno digital cada vez más riesgoso.

Referencias Bibliográficas

Calle Herencia, C. A. (2022). La transformación digital y su importancia en las pymes. Iberoamerican Business Journal, 5(2), 64–81. https://doi.org/10.22451/5817.ibj2022.vol5.2.11059

SonicWall. (2024). 2024 SonicWall Cyber Threat Report. Recuperado de https://www.sonicwall.com/threat-report

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model for designing information technology security system based on risk analysis and cybersecurity framework. Egyptian Informatics Journal, 23(3), 383–404. https://doi.org/10.1016/j.eij.2022.03.001

AL-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. Electronics (Switzerland), 12(17). https://doi.org/10.3390/electronics12173629

Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. (2022). A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions. Applied Sciences (Switzerland), 12(8). https://doi.org/10.3390/app12084077

Alahmari, A., & Duncan, B. (2020). Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence. 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020, March. https://doi.org/10.1109/CyberSA49311.2020.9139638

Crespo-Martínez, E., & Cordero-Torres, G. (2018). Estudio Comparativo Entre Las Metodologías Cramm Y Magerit Para La Gestión De Riesgo De Ti En Las Mpymes. Uda Akadem, 1, 38–47. https://doi.org/10.33324/udaakadem.vi1.129

Kitsios, F., Chatzidimitriou, E., & Kamariotou, M. (2023). The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector. Sustainability (Switzerland), 15(7). https://doi.org/10.3390/su15075

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. In TQM Journal (Vol. 33, Issue 7, pp. 76–105). Emerald Group Holdings Ltd. https://doi.org/10.1108/TQM-09-2020-0202

Coello Yagual, R. R., & Pico Versoza, L. M. (2018). Análisis de las ventajas y desventajas del sistema de gestión de la seguridad de la información y su influencia en la competitividad de las empresas que utilizan Cloud Computing y Big Data en el Ecuador. INNOVA Research Journal, 3(4), 181–195. https://doi.org/10.33890/innova.v3.n4.2018.562

Franco-Ángel, M., & Urbano, D. (2019). Characteristics of Colombian SMEs and their founders: An analysis in two regions of that country. Estudios Gerenciales, 35(150), 81–91. https://doi.org/10.18046/j.estger.2019.150.2968

Banco Interamericano de Desarrollo. (2020). CIBERSEGURIDAD, Riesgos, Avances y el camino a seguir en America Latina y El Caribe. Bid- Oea, 1, 116–119. https://publications.iadb.org/es/reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe

Del Do, A. M., Villagra, A., & Pandolfi, D. (2023). Desafíos de la Transformación Digital en las PYMES. Informes Científicos Técnicos - UNPA, 15(1), 200–229. https://doi.org/10.22305/ict-unpa.v15.n1.941

Bautista García, F., & Aguilar, D. (2023). Estudio anual de ciberseguridad. In Comportamiento de las cifras del ciberdelito 2021-2023 (pp. 15–22).

National Quality Assurance. (s. f.). Guía de implantación ISO 27001. Recuperado de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Martínez, R., Palma, A., & Velásquez, A. (2020). Revolución tecnológica e inclusión social. Politicas Sociales, 233(0),9–87. https://repositorio.cepal.org/bitstream/handle/11362/45901/1/S2000401_es.pdf%0Ahttps://ideas.repec.org/p/ecr/col041/45901.html

SonicWall. (2023). 2023 SonicWall Cyber Threat Report. Recuperado de https://www.sonicwall.com/threat-report-2023

Universidad Católica de Cuenca. (2019). Transformación digital en las organizaciones. https://doi.org/10.29018/978-9942-823-15-1

Dane. (2023). Plan De Tratamiento De Riesgos De Seguridad Y Privacidad De La Información. 57(1). https://www.dane.gov.co/files/control_participacion/planes_institucionales/Plan_tratamiento_de_riesgos_de_seguridad_y_privacidad_de_la_informacion_2023.pdf

Universidad de Jaén, Servicio de Informática. (2018). Software malicioso (malware). Recuperado de https://www.ujaen.es/servicios/sinform/seguridad-informaticaNational, S (2019). La información.

Vega, E. (2021). Ciencias. Recuperado de https://3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACION.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (s. f.). Guía de gestión de riesgos. Recuperado de https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150516:Guia-de-gestion-de-riesgos

Departamento Administrativo Nacional de Estadística. (2023). Plan de tratamiento de riesgos de seguridad y privacidad de la información. Recuperado de https://www.dane.gov.co/files/control_participacion/planes_institucionales/Plan_tratamiento_de_riesgos_de_seguridad_y_privacidad_de_la_informacion_2023.pdf

Álvarez, J., Garzón, J. E., Ramírez, N., & Peña, Z. (2022). Análisis de la implementación tecnológica basada en la computación de la nube en Colombia para los períodos 2019 a 2021 [Tesis de grado inédita]. Universidad EAN. Recuperado de https://repository.universidadean.edu.co/bitstream/handle/10882/12470/GarzonJuan2022.pdf?sequence=2&isAllowed=y

Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia. (2018). Guía para la implementación de seguridad de la información en una MIPYME. Recuperado de https://gobiernodigital.mintic.gov.co/portal/Iniciativas/Seguridad-y-privacidad-de-la-informacion/

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Recuperado de https://www.iso.org/standard/75652.html

Instituto Colombiano de Normas Técnicas y Certificación, International Organization for Standardization, & International Electrotechnical Commission. (2009). NTC-ISO/IEC 27005:2009 Tecnología de la información — Técnicas de seguridad — Gestión de riesgos de seguridad de la información. ICONTEC.

Ruiz, P. (2018, 17 octubre). 1.4. Ventajas e inconvenientes de la arquitectura cliente/servidor. SomeBooks.es. https://somebooks.es/ventajas-e-inconvenientes-de-la-arquitectura-clienteservidor/

Amazon Web Services. (s.f.). Monolítico frente a microservicios: diferencia entre arquitecturas de desarrollo de software. https://aws.amazon.com/es/compare/the-difference-between-monolithic-and-microservices-architecture/

Sheldon, R. (2023, September 12). Model-view-controller (MVC). TechTarget. https://www.techtarget.com/whatis/definition/model-view-controller-MVC

Risso, D. (2022, August 30). ¿Cuáles son las novedades de MySQL 8? HostingMontevideo.com. https://www.hostingmontevideo.com/blog/cuales-son-las-novedades-de-mysql-8/

IBM. (2019). IBM InfoSphere Information Server 11.5.0: Referential integrity analysis. https://www.ibm.com/docs/es/iis/11.5.0?topic=overview-referential-integrity-analysis

Guia PHP. (2023, September 24). Tipos de bases de datos compatibles con Laravel. https://guiaphp.com/frameworks/tipos-de-bases-de-datos-compatibles-con-laravel/

Lucidchart. (2025, 26 de marzo). Tutorial de diagrama de clases UML. https://www.lucidchart.com/pages/es/tutorial-de-diagrama-de-clases-uml

Siriwardhana, S. (2022, 19 de octubre). La fácil guía de los diagramas de componentes. Creately Blog. https://creately.com/blog/es/diagramas/tutorial-de-diagrama-de-componentes/

ISO. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. https://www.iso.org/standard/82875.html

CSAE. (2012). Magerit: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro II: Catálogo de elementos. Ministerio de Hacienda y Administraciones Públicas. http://administracionelectronica.gob.es/

CSAE. (2012). Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro I: Método. Ministerio de Hacienda y Administraciones Públicas. http://administracionelectronica.gob.es/

CSAE. (2012). MAGERIT versión 3.0: Metodología de análisis y gestión de riesgos de los sistemas de información. Libro III: Guía de técnicas. Ministerio de Hacienda y Administraciones Públicas. http://administracionelectronica.gob.es/

Young, R. R. (2014). The requirements engineering handbook. Artech House.

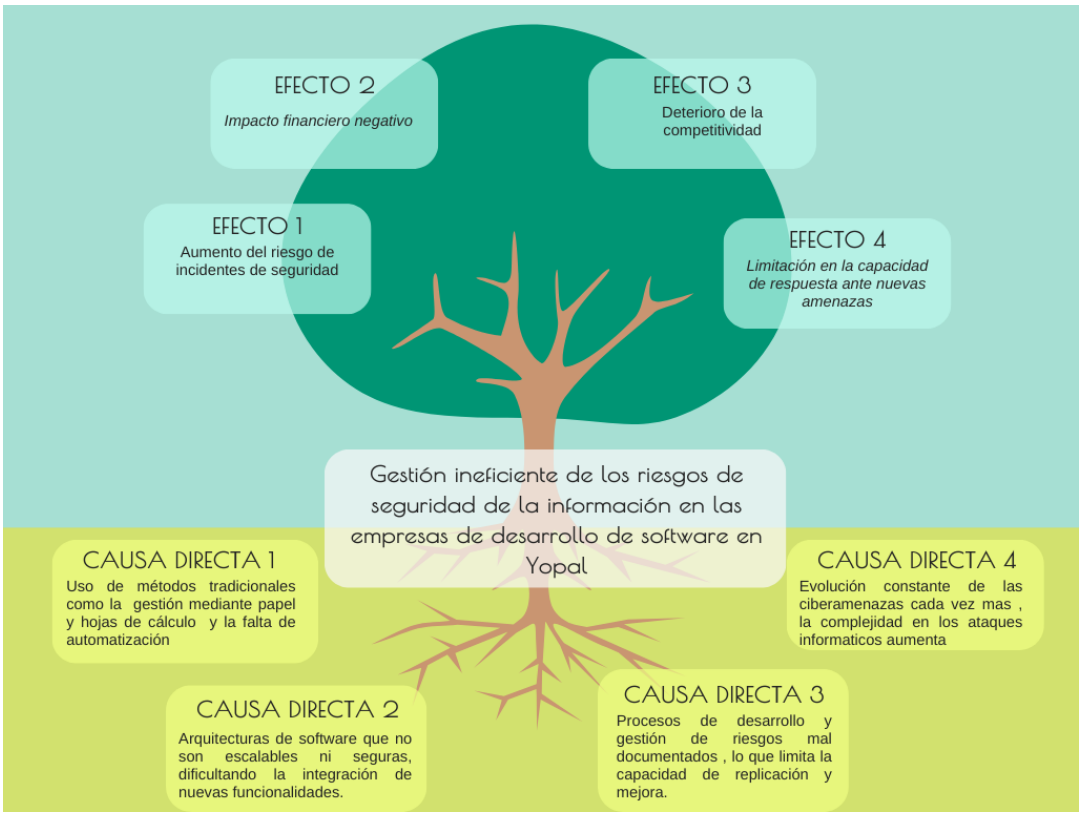
Velasco Elizondo, P., et al. (2015). *Arquitectura de software: Componentes 1-3* [Software architecture: Components 1-3]. Universidad Autónoma de Zacatecas.

Arsys. (2024, July 6). Ventajas de MySQL 8. https://www.arsys.es/blog/novedades-mysql-8

Anexos

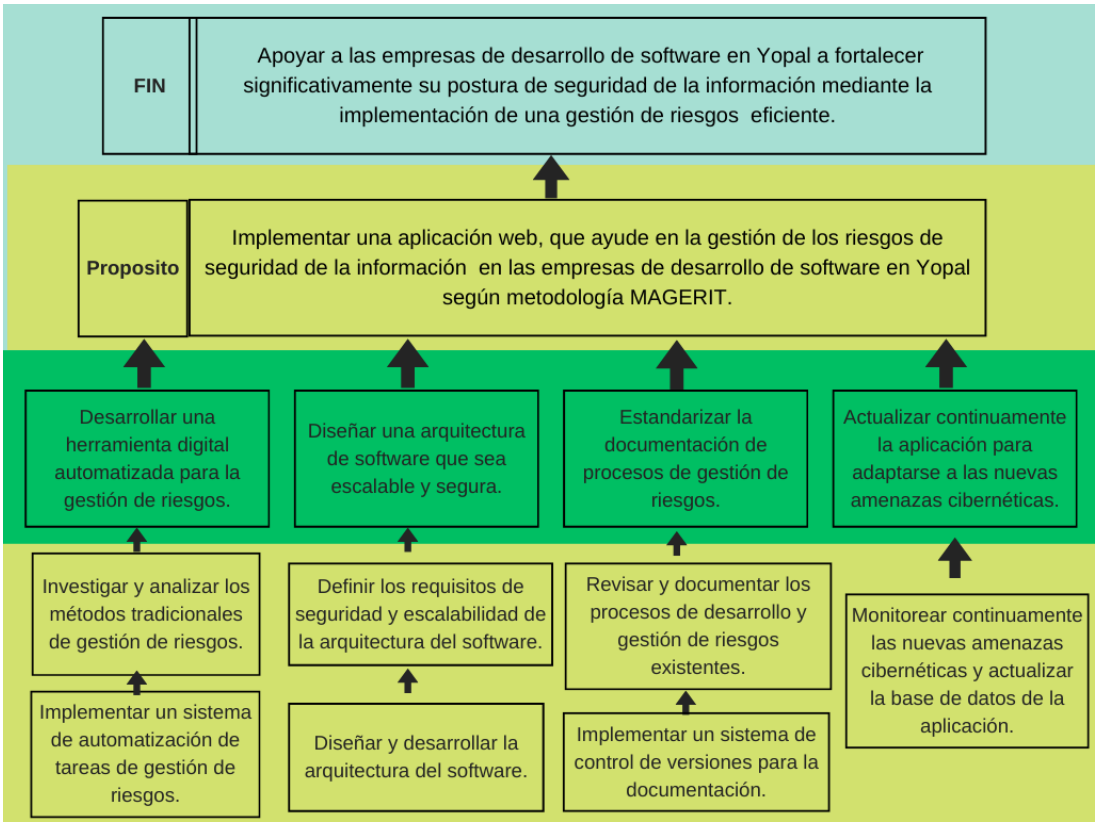
Anexo A

Árbol del problema



Anexo B

Árbol De Objetivos



Anexo C

Los 5 Por qué

1. **¿Por qué las PYMES en Colombia y de Yopal son vulnerables a las amenazas cibernéticas?**

Porque muchas PYMES no cuentan con procesos, tecnologías y entrenamientos robustos en seguridad de la información.

2. **¿Por qué las PYMES no cuentan con procesos, tecnologías y entrenamientos robustos en seguridad de la información?**

Porque la implementación de normas de seguridad de la información, como ISO 27001, puede ser compleja y costosa, especialmente para empresas con recursos limitados.

3. **¿Por qué es importante mejorar la gestión de riesgos de seguridad de la información en las PYMES y especialmente de empresas de Yopal?**

Porque sin una gestión eficaz, las PYMES están expuestas a ciberataques y brechas de seguridad que pueden causar pérdidas financieras, dañar la reputación, y afectar la continuidad del negocio, una gestión automatizada mejora la precisión, reduce el riesgo de omisiones y permite que las PYMES respondan más rápidamente a las amenazas emergentes.

4. **¿Por qué se necesita una aplicación de gestión de riesgos de seguridad de la información ?**

Porque la gestión manual de riesgos mediante métodos tradicionales, como hojas de cálculo y documentos en papel, es ineficaz y propensa a errores, estos métodos no permiten un seguimiento automatizado y centralizado de los riesgos, lo que dificulta la identificación oportuna de amenazas y la implementación de controles adecuados.

5. **¿Por qué esta aplicación de gestión de riesgos de seguridad de la información es una buena alternativa ?**

Porque Securisk está diseñado para ser una herramienta accesible, escalable y alineada con estándares internacionales, lo que permite a las PYMES gestionar eficazmente sus riesgos de seguridad, mejorar su competitividad, y aspirar a certificaciones como ISO 27001.

Anexo D

Cadena de Valor

A	B	C	D	E	F
CAUSAS DIRECTAS	**OBJETIVOS ESPECIFICOS**	**ACTIVIDADES**	**INDICADOR DE PRODUCTO**	**Medio de verificación**	**PRODUCTOS**
Uso de métodos tradicionales como la gestión mediante papel y hojas de cálculo y la falta de automatización	Desarrollar una herramienta digital automatizada para la gestión de riesgos en las empresas de desarrollo de software en Yopal.	Análisis de requisitos: Recolectar y documentar necesidades de automatización de los procesos de gestión de riesgos.	Porcentaje de procesos de gestión de riesgos automatizados.	Informe de implementación de la herramienta.	Herramienta digital para la gestión de riesgos.
		Diseño de la herramienta: Crear un diseño detallado de la herramienta.			
		Desarrollo del software: Codificación y desarrollo de la herramienta.			
		Pruebas de funcionalidad: Realizar pruebas para garantizar que la herramienta cumple con los requisitos.			
		Despliegue: Implementar la herramienta en las empresas.			
Arquitecturas de software que no son escalables ni seguras, dificultando la integración de nuevas funcionalidades	Diseñar una arquitectura de software que sea escalable y segura para, que permita la integración de nuevas funcionalidades y actualizaciones en el futuro.	Investigación de estándares: Revisar arquitecturas escalables y seguras existentes.	Nivel de escalabilidad y seguridad alcanzado.	Pruebas de seguridad y escalabilidad.	Arquitectura de software escalable y segura.
		Diseño de arquitectura: Crear un diseño detallado de la nueva arquitectura.			
		Desarrollo de componentes clave: Implementar componentes críticos de la arquitectura.			
		Pruebas de escalabilidad y seguridad: Realizar pruebas para validar el diseño.			
		Documentación de la arquitectura: Documentar el diseño y su implementación.			
Procesos de desarollo y gestión de riesgos mal documentados, lo que limita la capacidad de replicación y mejora	Estandarizar la documentación de procesos de gestión de riesgos para proporcionar un informe detallado que incluya recomendaciones para futuras mejoras y escalabilidad del proyecto.	Revisión de procesos actuales: Analizar y documentar los procesos de gestión de riesgos existentes.	Calidad y nivel de detalle de la documentación.	Revisión de la documentación estandarizada.	Informe detallado y estandarizado de procesos de gestión de riesgos.
		Establecimiento de estándares: Definir los estándares de documentación para los procesos.			
		Creación de plantillas y guías: Desarrollar plantillas para la documentación estandarizada.			
		Capacitación del equipo: Entrenar al equipo en el uso de los nuevos estándares y plantillas.			
		Documentación de procesos: Documentar los procesos siguiendo los nuevos estándares.			
Evoluación constante de las ciberamenazas cada vez mas, la complejidad en los ataques informáticos aumenta	Actualizar continuamente la aplicación para adaptarse a las nuevas amenazas cibernéticas.	Monitoreo de amenazas: Establecer un sistema de vigilancia para detectar nuevas ciberamenazas.	Frecuencia de actualizaciones y respuesta a nuevas amenazas.	Registro de actualizaciones realizadas.	Módulo de actualización continua para la aplicación.
		Desarrollo de actualizaciones: Crear actualizaciones de seguridad en respuesta a nuevas amenazas.			
		Pruebas de seguridad: Realizar pruebas para asegurar que las actualizaciones son efectivas.			
		Despliegue de actualizaciones: Implementar las actualizaciones en la aplicación.			
		Documentación de cambios: Registrar y documentar cada actualización realizada.			

Anexo E

Matriz de Expectativas y Necesidades de la Aplicación

PARTES INTERESADAS	FUNCIÓN	CATEGORIA	REQUISITO		NIVEL DE IMPORTANCIA		PRIORIZACION
			EXPECTATIVA	NECESIDADES	PODER	INTERES	
UNITRÓPICO	Institución que supervisa el trabajo de grado	Interno	Que el proyecto esté bien fundamentado, tenga impacto en la industria y pueda servir de referencia para futuros trabajos de grado relacionados con el area de ciberseguridad	Supervisar que el trabajo de grado cumpla con los requisitos académicos y científicos.	ALTO	ALTO	ALTO
Facultad de Ingeniería de Sistemas	Responsable de la validación académica y evaluación del proyecto.	Interno	Que el trabajo de grado refleje el uso adecuado de metodologías de desarrollo de software y seguridad de la información.	Garantizar que el proyecto tenga relevancia en el campo de la ingeniería de sistemas y que cumpla con los estándares de calidad académica.	ALTO	ALTO	ALTO
Director de trabajo de grado	Persona encargada de orientar, revisar y aprobar el desarrollo del proyecto.	Interno	Que los estudiantes sigan un proceso estructurado, documenten adecuadamente el proyecto y logren resultados aplicables.	Asegurar que el proyecto sea viable, tenga un desarrollo metodológico sólido y aporte soluciones a problemas reales.	ALTO	ALTO	ALTO
Empresas de desarrollo de software en Yopal	Responsables de la toma de decisiones estratégicas sobre seguridad de la información. Beneficiarios directos	Externo	Que la aplicación sea fácil de usar, adaptada a sus necesidades y compatible con normativas como ISO 27001.	Implementar una herramienta que les ayude a gestionar los riesgos de seguridad de la información de manera eficiente.	MEDIO	ALTO	ALTO
Consultores y Auditores de Ciberseguridad	Profesionales que revisan y validan la implementación de normativas como ISO 27001, ademas de expertos que pueden recomendar el uso de la aplicacion en empresas del sector	Externo	Que la aplicación permita evaluaciones de riesgos precisas que permitan asi una auditoria eficaz a los sistemas optimizando recursos.	Contar con herramientas que faciliten la auditoría y validación de la seguridad en las empresas.	MEDIO	MEDIO	MEDIO
Clientes y Proveedores de las Empresas de Software (Usuarios indirectos y afectados por la seguridad de los datos) SC	Empresas o individuos que esperan que sus datos sean protegidos.	Externo	Que las empresas con las que trabajan implementen medidas de seguridad confiables y verificables.	Garantizar que su información esté protegida cuando contratan servicios de software.	BAJO	ALTO	MEDIO
Comunidad Académica y Científica	Estudiantes e investigadores en ciberseguridad que pueden aprovechar los resultados del proyecto para futuras investigaciones.	Interno	Que el proyecto genere publicaciones científicas o documentación útil para la comunidad.	Obtener un referente académico que sirva como base para futuras investigaciones en ciberseguridad y desarrollo de software.	BAJO	MEDIO	BAJO

Anexo F

Solicitud de Información sobre empresas de Software

CÁMARA DE COMERCIO
CASANARE

CAMARA DE COMERCIO DE CASANARE CONTACTENOS <contactenos@cccasanare.co>

Solicitud de información sobre empresas de desarrollo de software en Yopal

Fabian David Guevara Bello <fabiandavidguevarabello@gmail.com> 10 de marzo de 2025, 15:10
Para: contactenos@cccasanare.co

Estimados representantes de la Cámara de Comercio de Casanare,

Cordial saludo.

Mi nombre es Fabian David Guevara Bello y actualmente me encuentro realizando un trabajo de grado en la Universidad UNITROPICO, enfocado en el desarrollo de una aplicación web para la gestión de riesgos de seguridad de la información en empresas de desarrollo de software.

En este sentido, me gustaría solicitar su apoyo con información sobre el número de empresas dedicadas al desarrollo de software registradas en Yopal, así como cualquier dato relevante sobre su clasificación y actividad económica. Esta información es clave para contextualizar nuestro estudio y analizar el impacto de nuestra propuesta en la industria local.

Agradecemos de antemano su colaboración y quedamos atentos a su pronta respuesta.

Atentamente,

Fabian David Guevara Bello

3223296487

Anexo G

Respuesta por parte de la Cámara de Comercio

CÁMARA DE COMERCIO CASANARE	**CARTA O SOLICITUD**	**FOR-GEA-049 Versión: 06**

del Departamento de Casanare, ya que según la "Clasificación Industrial Internacional Uniforme de todas las actividades económicas Revisión 4 Adaptada para Colombia CIIU Rev. 4 A.C. (2022) – DANE (PDF adjunto)", según la cual los empresarios inscriben la actividad ante Cámara de Comercio, no existe un CIIU específico de "desarrollo de software", información con corte a 31 de diciembre de 2024, para los fines pertinentes:

CIIU 1 - ACTIVIDAD	TOTAL
J6201 ** Actividades de desarrollo de sistemas informáticos (planificación análisis diseño programación pruebas)	29
J5820 ** Edición de programas de informática (software)	4
TOTAL	**33**

Así mismo, envío documento Clasificación Industrial Internacional Uniforme de todas las actividades económicas Revisión 4 Adaptada para Colombia CIIU Rev. 4 A.C. (2022) – DANE (PDF adjunto), según la cual los empresarios inscriben la actividad ante Cámara de Comercio, donde puede consultar los códigos de las actividades (estructura detallada páginas 90 a la 133 – columna clase) en el caso que desee aclarar el oficio de su solicitud o incluir otros CIIU relacionados con su petición.

Espero de esta forma haber atendido su solicitud.

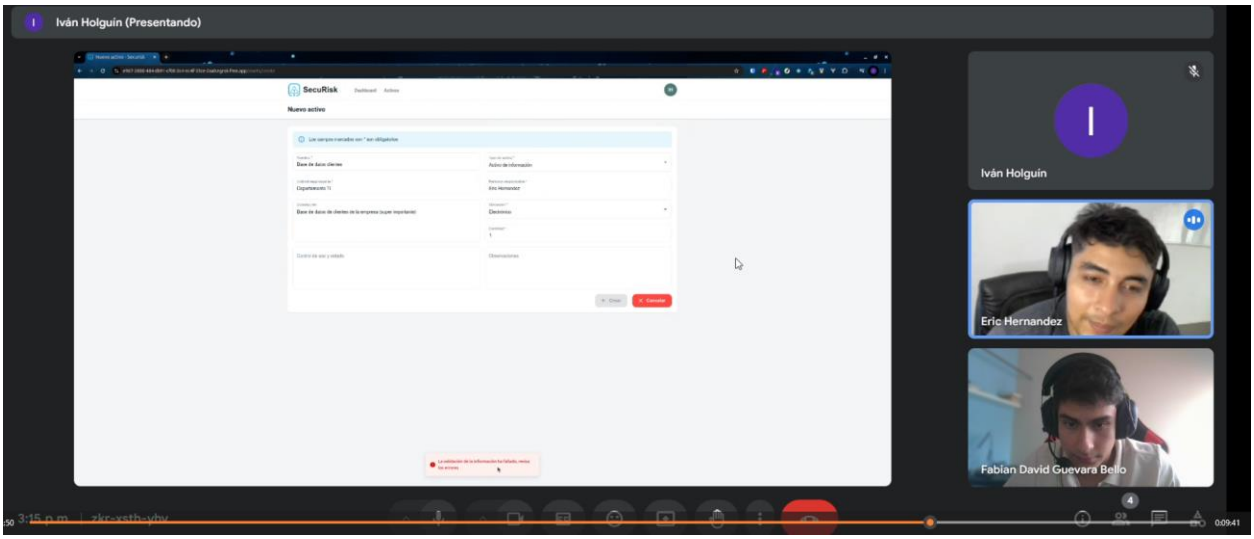
Cordialmente,

PILAR BENÍTEZ LÓPEZ
Directora de Estadísticas e Información Empresarial
V.P. de Desarrollo Regional y Atracción de Inversión
Cámara de Comercio de Casanare
https://cccasanare.co/serviciobasesdedatos/

Anexo: Un (1) archivo en PDF.

Anexo H

Video Entrevista Empresa Delta Solutions



Nota. El link completo de la entrevista se encuentra en el siguiente enlace https://drive.google.com/file/d/1DTRdQen5DDetSuF8Cf1uYX1EKYib65RF/view?usp=drive_link

Anexo I

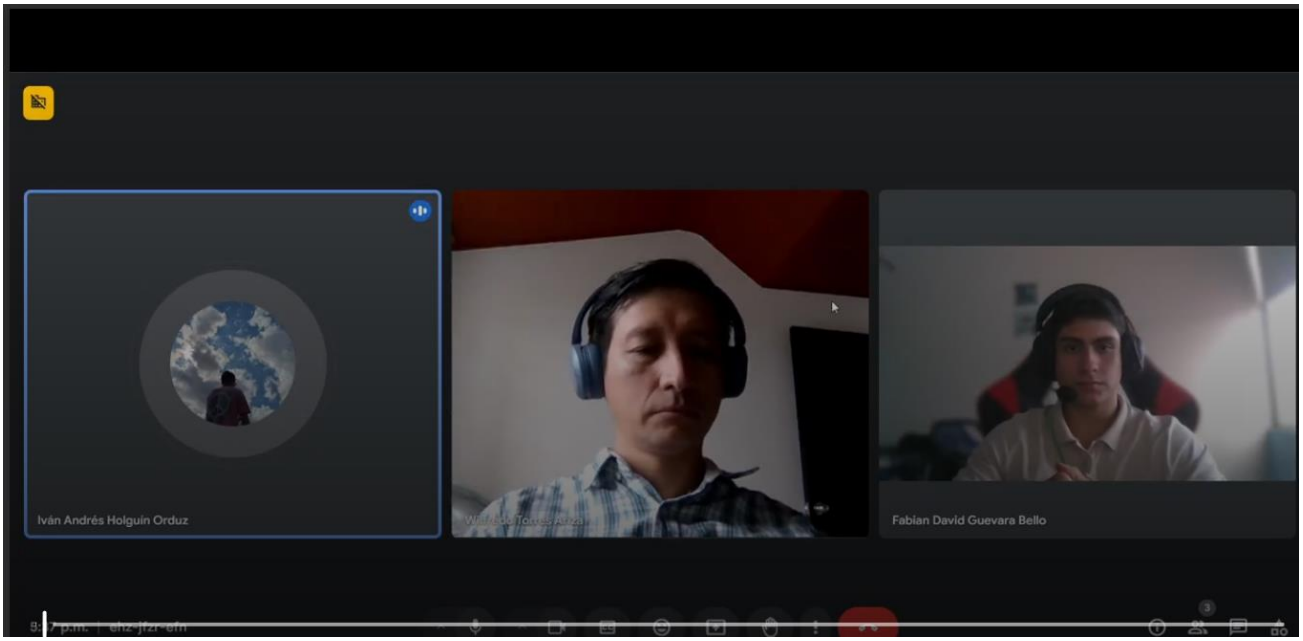
Información Recopilada Delta Solutions

N°	NOMBRE DE LA EMPRESA	DELTA SOLUTIONS	ENTREVISTADO	Eric Hernandez	FECHA	12/03/2025
CONTEXTUALIZACION INICIAL						
1	**¿Implementan prácticas de seguridad de la información en su proceso de desarrollo de software? (Sí/No). En caso afirmativo, ¿cuáles y cómo las aplican? Si la respuesta es no, ¿por qué no han adoptado estas prácticas?**					
Si, usan las ultimas versiones de cada framework en el cual trabaja, enfocan su desarrollo a un estructura serverless						
2	**¿Utilizan alguna herramienta para la gestión de riesgos de seguridad de la información en su empresa? (Sí/No). En caso afirmativo, ¿cuál(es) y cómo las utilizan? Si la respuesta es no, ¿qué les ha impedido implementarlas?**					
No, porque no los han atacado aún.						
3	**¿Enfrentan dificultades para identificar, evaluar y tratar los riesgos de seguridad de la información en su empresa? (Sí/No). Si la respuesta es afirmativa, ¿cuáles son los principales desafíos que han encontrado y qué impacto han tenido en su organización?**					
Si , no tienen la suficiente experticia para saber como gestionar los riesgos de seguridad de la informacion						
4	**¿Han sido víctimas de ataques de ciberseguridad y/o seguridad de la información? En caso contrario, ¿cómo llevan el registro o monitoreo para saber si han sido atacados o si han sufrido incidentes de seguridad?**					
No, no han sufrido ataques directamente a la organizacion pero si al software desarrollado para terceros, son victimas de phishing constante y llevan un registro al "ojo"						
5	**¿Cuentan con algún sistema automatizado o software específico para la gestión de riesgos de seguridad de la información en su empresa? (Sí/No). Si la respuesta es afirmativa, ¿qué funcionalidades consideran más útiles y cuáles son sus principales limitaciones?**					
No no cuentan con un software para la gestion de riesgos de seguridad de la informacion						
NECESIDADES FUNCIONALES DEL SOFTWARE						
6	**¿Qué funcionalidades considera indispensables en una aplicación para la gestión de riesgos de seguridad de la información? (Ejemplo: identificación de activos, evaluación de riesgos, monitoreo de controles, reportes automatizados, etc.)**					

Nota. El link completo de la información se encuentra en el siguiente enlace: https://docs.google.com/spreadsheets/d/1-31fcfKpI66u1qOO-fmAdIHqYiheq6zKc7dSGnYpnuw/edit?usp=sharing

Anexo J

Video Entrevista Empresa Puntualtic



Nota. El link completo de la entrevista se encuentra en el siguiente enlace

https://drive.google.com/file/d/18MPjskF_0v6rf_IMBUs3Wp4XKinOuolr/view?usp=drive_link

Anexo K *Información Recopilada Puntualtic*

Información Recopilada Puntualtic

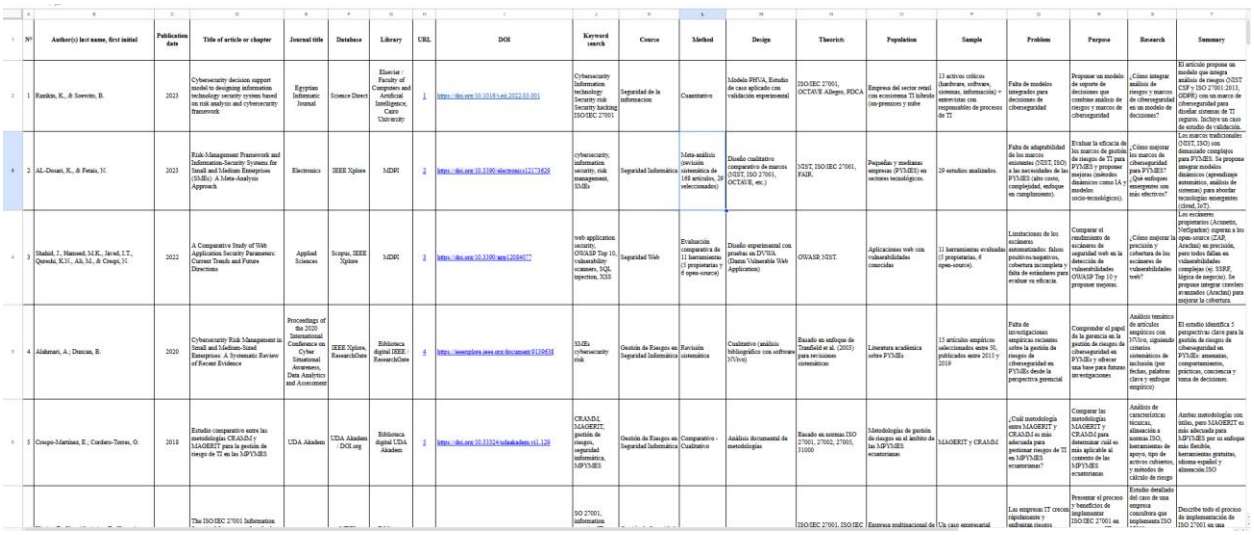
N°	NOMBRE DE LA EMPRESA	PUNTUALTIC	ENTREVISTADO		FECHA	12/03/2025
CONTEXTUALIZACION INICIAL						
1	**¿Implementan prácticas de seguridad de la información en su proceso de desarrollo de software? (Sí/No). En caso afirmativo, ¿cuáles y cómo las aplican? Si la respuesta es no, ¿por qué no han adoptado estas prácticas?**					
Si , pero no tienen una politica de seguridad de la informacion, cuentan con politicas generales a nivel empresas , dentro de los controles que implementan implementan acceso restringido , medidas de seguridad y algo imporatante aplican la metodologia OWASP en el desarrollo de sus productos.						
2	**¿Utilizan alguna herramienta para la gestión de riesgos de seguridad de la información en su empresa? (Sí/No). En caso afirmativo, ¿cuál(es) y cómo las utilizan? Si la respuesta es no, ¿qué les ha impedido implementarlas?**					
No, la seguridad no es una prioridad en la empresa , estan enfocados en la rapidez con la cual se entrega el producto						
3	**¿Enfrentan dificultades para identificar, evaluar y tratar los riesgos de seguridad de la información en su empresa? (Sí/No). Si la respuesta es afirmativa, ¿cuáles son los principales desafíos que han encontrado y qué impacto han tenido en su organización?**					
No, no enfrentan dificultades una vez se entrega el producto parte de la responsabilidad, es del cliente.						
4	**¿Han sido víctimas de ataques de ciberseguridad y/o seguridad de la información? En caso contrario, ¿cómo llevan el registro o monitoreo para saber si han sido atacados o si han sufrido incidentes de seguridad?**					
Si ,han sido victimas de ataques pero los productos que desarrollan para las empresas, directamente a la empresa no, ellos monitorean los logs en busca de un rastreo de vulnerabilidades.						
5	**¿Cuentan con algún sistema automatizado o software específico para la gestión de riesgos de seguridad de la información en su empresa? (Sí/No). Si la respuesta es afirmativa, ¿qué funcionalidades consideran más útiles y cuáles son sus principales limitaciones?**					
No, no cuentan						
NECESIDADES FUNCIONALES DEL SOFTWARE						
6	**¿Qué funcionalidades considera indispensables en una aplicación para la gestión de riesgos de seguridad de la información? (Ejemplo: identificación de activos, evaluación de riesgos, monitoreo**					

Nota. El link completo de la información se encuentra en el siguiente enlace:

https://docs.google.com/spreadsheets/d/1-31fcfKpI66u1qOO-fmAdIHqYiheq6zKc7dSGnYpnuw/edit?usp=sharing

Anexo L

Matriz de Revisión de Literatura



Nº	Author(s) last name, first initial	Publication date	Title of article or chapter	Journal title	Database	Library	URL	DOI	Keyword search	Course	Method	Design	Theorich	Population	Sample	Problem	Purpose	Research	Summary
1	Ramkin, K., & Sorentn, B.	2023	Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework	Egyptian Informatic Journal	Science Direct	Elsevier / Faculty of Computers and Artificial Intelligence, Cairo University	1	https://doi.org/10.1016/j.eij.2022.03.001	Cybersecurity Information technology Security risk Security hacking ISO/IEC 27001	Seguridad de la información	Cuantitativo	Modelo PHVA, Estudio de caso aplicado con validación experimental	ISO/IEC 27001, OCTAVE Allegro, PDCA	Empresa del sector retail con ecosistema TI híbrido (on-premises y nube	13 activos críticos (hardware, software, sistemas, información) + entrevistas con responsables de procesos de TI	Falta de modelos integrados para decisiones de ciberseguridad	Proponer un modelo de soporte de decisiones que combine análisis de riesgos y marcos de ciberseguridad	¿Cómo integrar análisis de riesgos y marcos de ciberseguridad en un modelo de decisiones?	El artículo propone un modelo que integra análisis de riesgos (NIST CSF y ISO 27001:2013, GDPR) con un marco de ciberseguridad para diseñar sistemas de TI seguros. Incluye un caso de estudio de validación.
2	AL-Dosari, K., & Fetais, N.	2023	Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach	Electronics	IEEE Xplore	MDPI	2	https://doi.org/10.3390/electronics12173624	cybersecurity, information security, risk management, SMEs	Seguridad Informática	Meta-análisis (revisión sistemática de 146 artículos, 20 seleccionados)	Diseño cualitativo comparativo de marcos (NIST, ISO 27001, OCTAVE, etc.)	NIST, ISO/IEC 27001, FAIR.	Pequeñas y medianas empresas (PYMES) en sectores tecnológicos.	20 estudios analizados.	Falta de adaptabilidad de los marcos existentes (NIST, ISO) a las necesidades de las PYMES (alto costo, complejidad, enfoque en cumplimiento).	Evaluar la eficacia de los marcos de gestión de riesgos de TI para PYMES y proponer mejoras (métodos dinámicos como IA y modelos socio-tecnológicos).	¿Cómo mejorar los marcos de ciberseguridad para PYMES? ¿Qué enfoques emergentes son más efectivos?	Los marcos tradicionales (NIST, ISO) son demasiado complejos para PYMES. Se propone integrar modelos dinámicos (aprendizaje automático, análisis de sistemas) para abordar tecnologías emergentes (cloud, IoT).
3	Shahid, J., Hameed, M.K., Javed, I.T., Qureshi, K.N., Ali, M., & Crespi, N.	2022	A Comparative Study of Web Application Security Parameters: Current Trends and Future Directions	Applied Sciences	Scopus, IEEE Xplore	MDPI	3	https://doi.org/10.3390/app12094077	web application security, OWASP Top 10, vulnerability scanners, SQL injection, XSS	Seguridad Web	Evaluación comparativa de 11 herramientas (5 propietarias y 6 open-source)	Diseño experimental con pruebas en DVWA (Damn Vulnerable Web Application)	OWASP, NIST.	Aplicaciones web con vulnerabilidades conocidas	11 herramientas evaluadas (5 propietarias, 6 open-source).	Limitaciones de los escáneres automatizados: falsos positivos/negativos, cobertura incompleta y falta de estándares para evaluar su eficacia.	Comparar el rendimiento de escáneres de seguridad web en la detección de vulnerabilidades OWASP Top 10 y proponer mejoras.	¿Cómo mejorar la precisión y cobertura de los escáneres de vulnerabilidades web?	Los escáneres propietarios (Acunetix, NetSparker) superan a los open-source (ZAP, Arachni) en precisión, pero todos fallan en vulnerabilidades complejas (ej. SSRF, lógica de negocio). Se propone integrar crawlers avanzados (Arachni) para mejorar la cobertura.
4	Alahmari, A.; Duncan, B.	2020	Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence	Proceedings of the 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment	IEEE Xplore, ResearchGate	Biblioteca digital IEEE, ResearchGate	4	https://ieeexplore.ieee.org/document/9139638	SMEs cybersecurity risk	Gestión de Riesgos en Seguridad Informática	Revisión sistemática	Cualitativo (análisis bibliográfico con software NVivo)	Basado en enfoque de Stanfield et al. (2002) para revisiones sistemáticas	Literatura académica sobre PYMEs	15 artículos empíricos seleccionados entre 50, publicados entre 2015 y 2019	Falta de investigaciones empíricas recientes sobre la gestión de riesgos de ciberseguridad en PYMEs desde la perspectiva gerencial	Comprender el papel de la gerencia en la gestión de riesgos de ciberseguridad en PYMEs y ofrecer una base para futuras investigaciones	Análisis temático de artículos empíricos con NVivo, siguiendo criterios sistemáticos de inclusión (por fechas, palabras clave y enfoque empírico)	El estudio identifica 5 perspectivas clave para la gestión de riesgos de ciberseguridad en PYMEs: amenazas, comportamientos, prácticas, conciencia y toma de decisiones.
5	Crespo-Martínez, E.; Cordero-Torres, O.	2018	Estudio comparativo entre las metodologías CRAMM y MAGERIT para la gestión de riesgo de TI en las MPYMES	UDA Akademi	UDA Akademi / DOI.org	Biblioteca digital UDA Akademi	5	https://doi.org/10.33324/udaakdem.vi1.129	CRAMM, MAGERIT, gestión de riesgo, seguridad informática, MPYMES	Gestión de Riesgos en Seguridad Informática	Comparativo - Cualitativo	Análisis documental de metodologías	Basado en normas ISO 27001, 27002, 27005, 31000	Metodologías de gestión de riesgos en el ámbito de las MPYMES ecuatorianas	MAGERIT y CRAMM	¿Cuál metodología entre MAGERIT y CRAMM es más adecuada para gestionar riesgos de TI en MPYMES ecuatorianas?	Comparar las metodologías MAGERIT y CRAMM para determinar cuál es más aplicable al contexto de las MPYMES ecuatorianas	Análisis de características técnicas, alineación a normas ISO, herramientas de apoyo, tipo de activos cubiertos, y métodos de cálculo de riesgo	Ambas metodologías son útiles, pero MAGERIT es más adecuada para MPYMES por su enfoque más flexible, herramientas gratuitas, idioma español y alineación ISO
			The ISO/IEC 27001 Information						ISO 27001, information				ISO/IEC 27001, ISO/IEC	Empresa multinacional de	Un caso empresarial	Las empresas IT crecen rápidamente y enfrentan riesgos	Presentar el proceso y beneficios de implementar ISO/IEC 27001 en	Estudio detallado del caso de una empresa consultora que implementa ISO	Describe todo el proceso de implementación de ISO 27001 en una

Nota. Para acceder al link lo podrá hacer desde el siguiente enlace:

https://docs.google.com/spreadsheets/d/1BJvYZFwXUc7G1yZEU2Hnj8omFjt93KtxR2nnQ_XU1Uo/edit?usp=sharing

Anexo M

Acta de Reunión Inicial Delta Soluciones

ACTA DE REUNIÓN	Unitrópico Universidad Internacional del Trópico Americano

ACTA REUNIÓN No. 01

LUGAR:	**VIRTUAL MEDIANTE APLICACION GOOGLE MEET**	**FECHA:**	**11/03/2025**
HORA INICIO:	**03:00 pm**	**HORA FIN:**	**04:00 pm**

I. OBJETO DE LA REUNION

DAR A CONOCER LA IDEA DEL APLICATIVO PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ASÍ COMO EL PROYECTO DE GRADO TITULADO **"Aplicación web para la gestión de riesgos de seguridad de la información en empresas de software de Yopal - Casanare" A LA EMPRESA DELTA SOLUCIONES TI LIDERADA POR ERIC HERNANDEZ.**

II. TEMAS A TRATAR

NIVEL DE CONOCIMIENTO DE CIBERSEGURIDAD Y GESTION DE ACTIVOS DE INFORMACION EN LA ORGANIZACION.

PROCESOS DE GESTION DE ACTIVOS DE INFORMACION EN LA ORGANIZACION.

NECESIDAD DE SISTEMATIZAR LOS PROCESOS DE GESTION DE ACTIVOS.

POSIBLE IMPACTO QUE PODRIA TENER EL USO DE UN APLICATIVO QUE PERMITA GESTIONAR LOS ACTIVOS DE INFORMACION.

III. ANTECEDENTES

N/A

IV. SEGUIMIENTO A COMPROMISOS ANTERIORES

ACTIVIDAD	FECHA DE ENTREGA	RESPONSABLE	SEGUIMIENTO
N/A	N/A	N/A	N/A

V. DESARROLLO

A LAS 03:00 PM DEL DIA 11 DE MARZO DEL 2025 SE DIO INICIO A LA REUNION CONVOCADA PREVIAMENTE MEDIANTE MEDIO VIRTUAL.

SE INICIA CON LA PRESENTACION DE LA EMPRESA DELTA SOLUCIONES TI ASI COMO DE SU REPRESENTANTE. SEGUIDAMENTE SE PROCEDE A REALIZAR PREGUNTAS REFERENTES A LOS PROCESOS DE CIBERSEGURIDAD Y GESTION DE ACTIVOS DE INFORMACION EN LA ORGANIZACION ASI COMO PREGUNTAS VARIAS SOBRE EL POSIBLE IMPACTO QUE PODRIA TENER LA IMPLEMENTACION DE UN APLICATIVO QUE AUTOMATIZARA DICHOS PROCESOS. PORTERIOR A LO CUAL SE PROCEDIO A MOSTRAR LA VERSION INICIAL DEL PROYECTO PARA FINALIZAR CON EL FEEDBACK DEL LIDER DE LA EMPRESA RESPECTO AL APLICATIVO PRESENTADO Y EL PROYECTO DE GRADO EN SI.

SE FINALIZA LA REUNION A LAS 04:00 PM.

ACTA DE REUNIÓN	Unitrópico Universidad Internacional del Trópico Americano

VI. OBSERVACIONES Y RECOMENDACIONES

N/A

VII. TAREAS Y COMPROMISOS

ACTIVIDAD	RESPONSABLE	FECHA DE ENTREGA
N/A	N/A	N/A

VIII. DOCUMENTACION Y/O ARCHIVOS SOPORTE

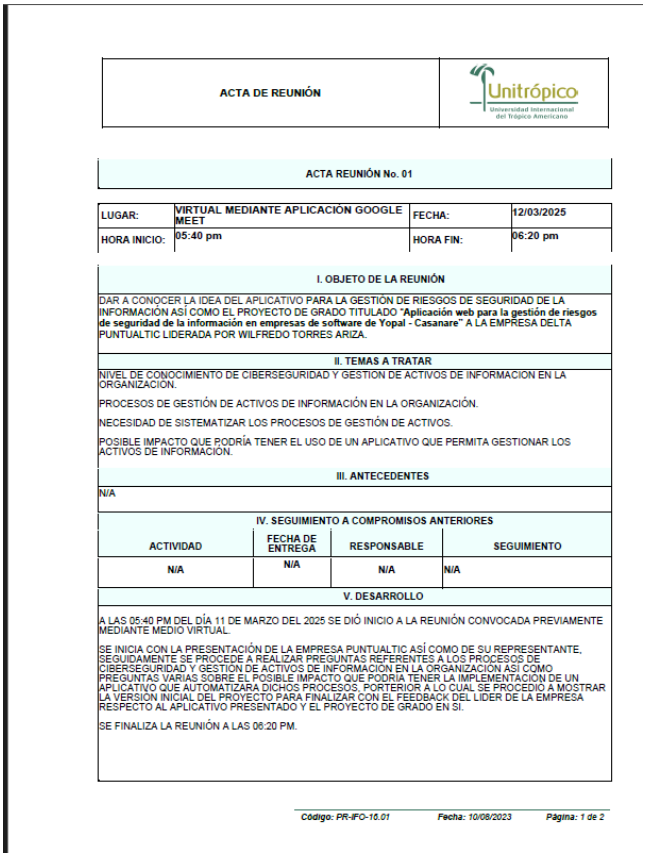
IX. ASISTENTES

NOMBRE	ENTIDAD QUE REPRESENTA	*TELEFONO DE CONTACTO	*CORREO ELECTRONICO	FIRMA
ERIC SANTIAGO HERNANDEZ	DELTA SOLUCIONES	3207675724	COMERCIAL@DELTASOLUCIONES.TECH	

**Diligenciar solo por personal ajeno a Unitrópico*

Anexo N

Acta de Reunión Inicial Puntualtic



ACTA DE REUNIÓN	Unitrópico

ACTA REUNIÓN No. 01

LUGAR:	VIRTUAL MEDIANTE APLICACIÓN GOOGLE MEET	FECHA:	12/03/2025
HORA INICIO:	05:40 pm	HORA FIN:	06:20 pm

I. OBJETO DE LA REUNIÓN

DAR A CONOCER LA IDEA DEL APLICATIVO PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ASÍ COMO EL PROYECTO DE GRADO TITULADO **"Aplicación web para la gestión de riesgos de seguridad de la información en empresas de software de Yopal - Casanare"** A LA EMPRESA DELTA PUNTUALTIC LIDERADA POR WILFREDO TORRES ARIZA.

II. TEMAS A TRATAR

NIVEL DE CONOCIMIENTO DE CIBERSEGURIDAD Y GESTIÓN DE ACTIVOS DE INFORMACIÓN EN LA ORGANIZACIÓN.

PROCESOS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN EN LA ORGANIZACIÓN.

NECESIDAD DE SISTEMATIZAR LOS PROCESOS DE GESTIÓN DE ACTIVOS.

POSIBLE IMPACTO QUE PODRÍA TENER EL USO DE UN APLICATIVO QUE PERMITA GESTIONAR LOS ACTIVOS DE INFORMACIÓN.

III. ANTECEDENTES

N/A

IV. SEGUIMIENTO A COMPROMISOS ANTERIORES

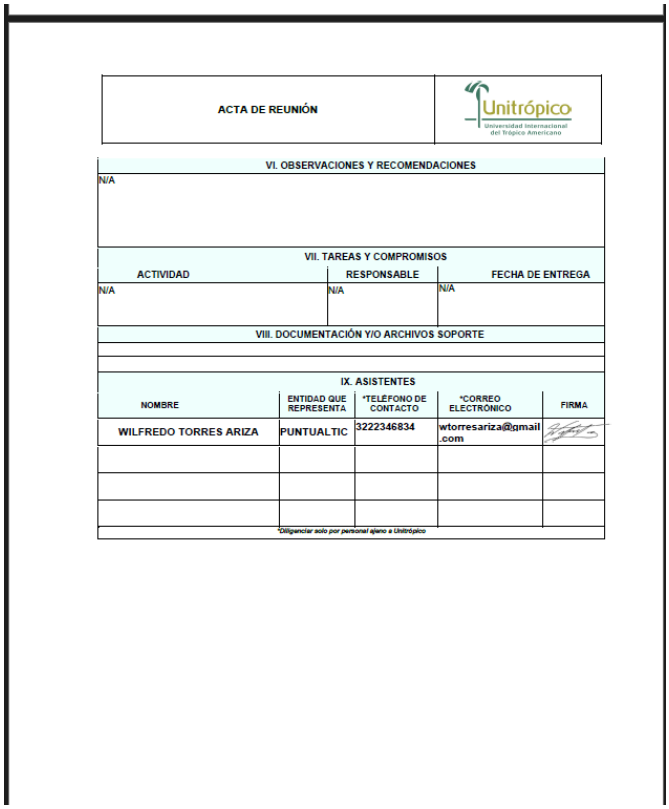
ACTIVIDAD	FECHA DE ENTREGA	RESPONSABLE	SEGUIMIENTO
N/A	N/A	N/A	N/A

V. DESARROLLO

A LAS 05:40 PM DEL DÍA 11 DE MARZO DEL 2025 SE DIÓ INICIO A LA REUNIÓN CONVOCADA PREVIAMENTE MEDIANTE MEDIO VIRTUAL.

SE INICIA CON LA PRESENTACIÓN DE LA EMPRESA PUNTUALTIC ASÍ COMO DE SU REPRESENTANTE, SEGUIDAMENTE SE PROCEDE A REALIZAR PREGUNTAS REFERENTES A LOS PROCESOS DE CIBERSEGURIDAD Y GESTIÓN DE ACTIVOS DE INFORMACIÓN EN LA ORGANIZACIÓN ASÍ COMO PREGUNTAS VARIAS SOBRE EL POSIBLE IMPACTO QUE PODRÍA TENER LA IMPLEMENTACIÓN DE UN APLICATIVO QUE AUTOMATIZARA DICHOS PROCESOS, PORTERIOR A LO CUAL SE PROCEDIO A MOSTRAR LA VERSIÓN INICIAL DEL PROYECTO PARA FINALIZAR CON EL FEEDBACK DEL LÍDER DE LA EMPRESA RESPECTO AL APLICATIVO PRESENTADO Y EL PROYECTO DE GRADO EN SI.

SE FINALIZA LA REUNIÓN A LAS 06:20 PM.



ACTA DE REUNIÓN	Unitrópico

VI. OBSERVACIONES Y RECOMENDACIONES

N/A

VII. TAREAS Y COMPROMISOS

ACTIVIDAD	RESPONSABLE	FECHA DE ENTREGA
N/A	N/A	N/A

VIII. DOCUMENTACIÓN Y/O ARCHIVOS SOPORTE

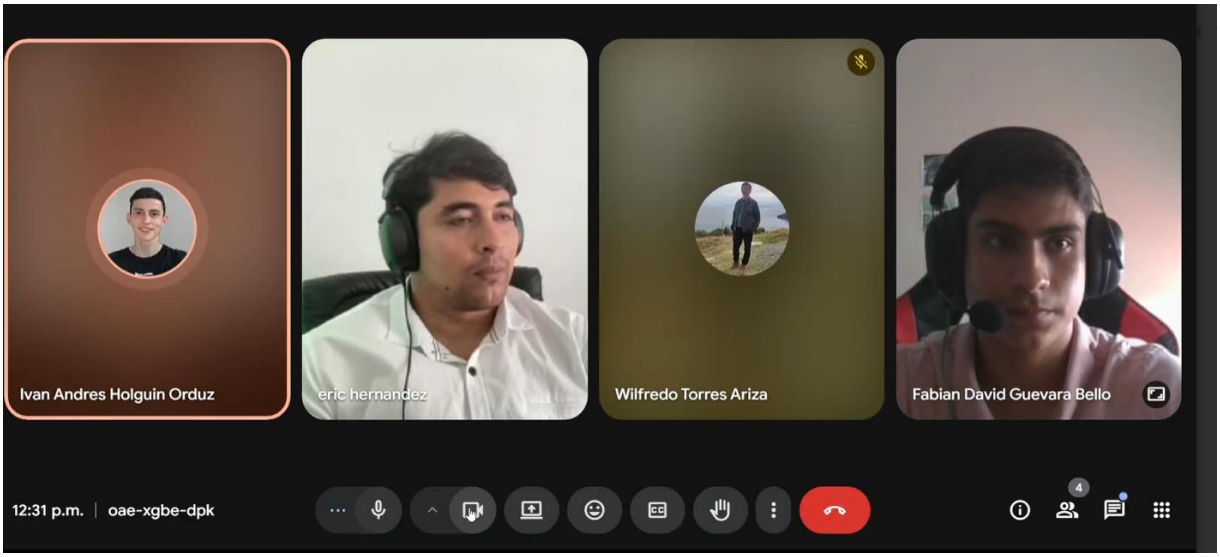
IX. ASISTENTES

NOMBRE	ENTIDAD QUE REPRESENTA	*TELÉFONO DE CONTACTO	*CORREO ELECTRÓNICO	FIRMA
WILFREDO TORRES ARIZA	PUNTUALTIC	3222346834	wtorresariza@gmail.com	

**Diligenciar solo por personal ajeno a Unitrópico*

Anexo O

Socialización Final del Software



Nota. Para acceder al link de la reunión lo puede hacer desde el siguiente enlace:

https://drive.google.com/drive/u/2/folders/1fqHaRH1SuVTVUp0R2FEGom1Ezw5qoHxk

Anexo P

Validación Final del Software Puntualtic

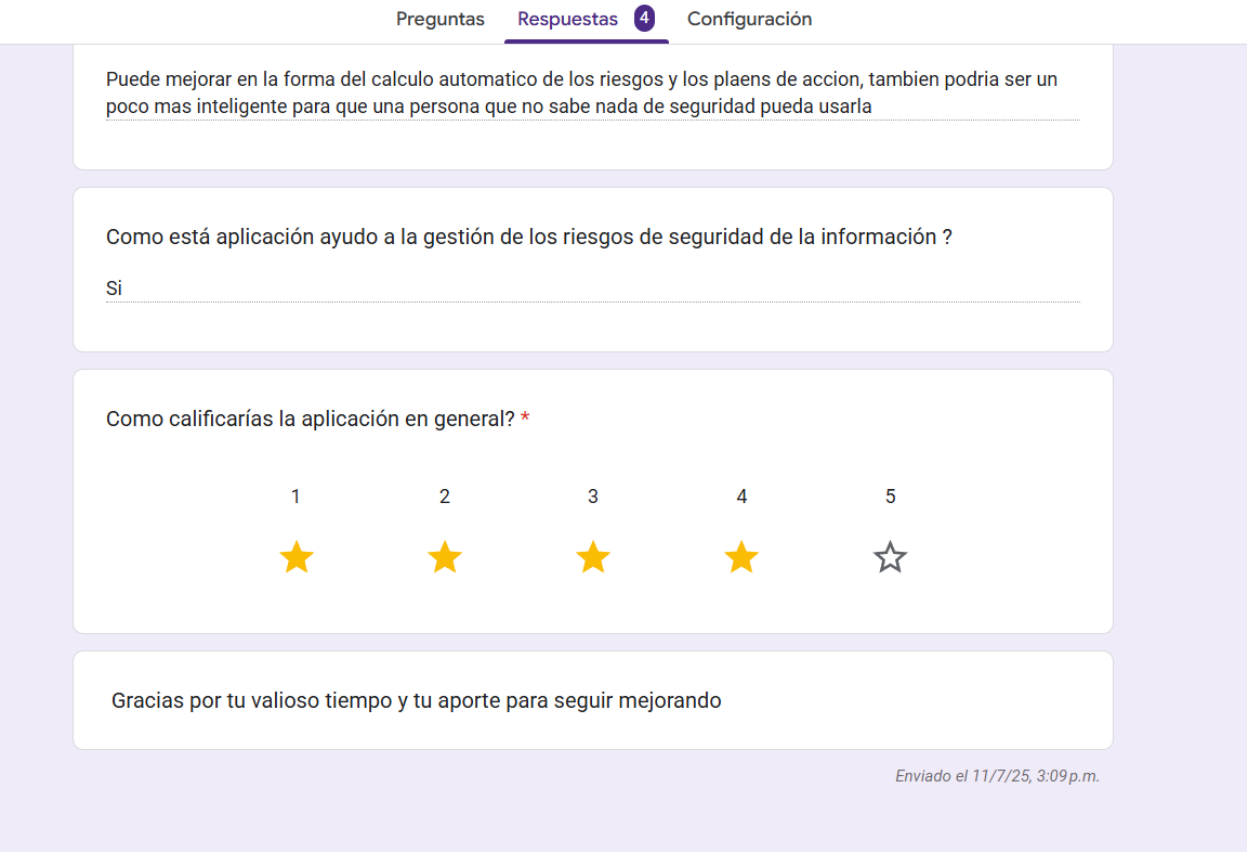


Nota. Para acceder al link del formulario lo puede hacer desde el siguiente enlace:

https://drive.google.com/file/d/13pggWpsONNKHgdBGdnCeP4OtIFRlMFBw/view?usp=drive_link

Anexo Q

Validación Final del Software Delta Soluciones



Nota. Para acceder al link de la reunión lo puede hacer desde el siguiente enlace:

https://docs.google.com/document/d/1aF7GnmSp-wIjchmDUv3cL6sgNcxJVqVeGOrq-Avt-sA/edit?usp=sharing