UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Desarrollo de una Aplicación Móvil para la Evaluación de Riesgos de Ciberseguridad a Nivel de Activos

Trabajo Fin de Máster

Máster Universitario en Ciberseguridad y Ciberinteligencia

AUTOR/A: Jimenez Moreano, Anaid

Tutor/a: Esteve Domingo, Manuel

CURSO ACADÉMICO: 2023/2024

Resumen

El desconocimiento de los riesgos puede llegar a generar una amenaza ante ataques cibernéticos, y estos pueden generar posibles pérdidas físicas, financieras, de reputación y de datos. Con el trabajo siguiente se espera abordar esta problemática diseñando y desarrollando una aplicación móvil para el entendimiento de los riesgos de ciberseguridad que permita a los usuarios finales conocer mejor sus activos y los riesgos asociados a estos, así como generar informes rápidos y personalizados para mejorar la seguridad y solventar vulnerabilidades desde un plano general. Este objetivo abarca tanto el aspecto de concientizar al usuario sobre sus activos y los riesgos asociados, como proporcionar una herramienta práctica para mejorar la seguridad y mitigar posibles vulnerabilidades de manera eficaz, rápida y eficiente. La aplicación móvil serviría también como una herramienta integral para ayudar al usuario final a comprender y educarse manera intuitiva sobre los riesgos de ciberseguridad en su entorno digital.

Palabras clave: Integración de estándares de seguridad, Educación y sensibilización, amenazas, evaluación de riesgos.

Abstract

Ignorance of the risks can generate a threat of cyber attacks, and these can generate possible physical, financial, reputation and data losses. The following work hopes to address this problem by designing and developing a mobile application for understanding cybersecurity risks that allows end users to better understand their assets and the risks associated with them, as well as generate quick and personalized reports to improve security. security and solve vulnerabilities from a general level. This objective covers both the aspect of raising user awareness about their assets and the associated risks, as well as providing a practical tool to improve security and mitigate possible vulnerabilities in an effective, fast and efficient manner. The mobile application would also serve as a comprehensive tool to help the end user intuitively understand and educate themselves about cybersecurity risks in their digital environment.

Keywords: Integration of security standards, Education and awareness, threats, risk assessment.

Agradecimientos

Quisiera expresar mi más profundo agradecimiento a las personas que han sido fundamentalmente importantes en mi vida y en la culminación de esta tesis.

A mis queridos padres Juan y Claudia, cuyo amor, apoyo y sacrificio han sido la base sobre la que he construido mis logros. Gracias por inculcarme los valores de la perseverancia, la dedicación y el esfuerzo. Su fe inquebrantable en mí y su constante aliento me han permitido superar todos los obstáculos que se han presentado en mi camino.

A mi hermano Jürgen, por ser una fuente constante de inspiración y apoyo. Gracias por tu compañía en los momentos difíciles, por tus palabras de aliento y por siempre estar ahí para celebrar mis éxitos. Tu ejemplo de trabajo duro y determinación me ha motivado a seguir adelante y a dar lo mejor de mí en cada paso de este viaje académico.

A mi hermano Erwin, gracias a él siempre he sabido valorar lo frágil que puede ser la vida.

A mi tutor por estar ahí para poder aconsejarme y darse el tiempo de aportarme en este trabajo.

A mis amigos y compañeros que han estado apoyándome y brindándome todo momento apoyo emocional para continuar hasta aquí.

Este logro no habría sido posible sin el amor y el apoyo de todos. A ustedes les dedico esta tesis con gratitud y cariño eterno.

Tabla de contenidos

ÍNDICE DE TABLAS

ÍNDICE DE ILUSTRACIONES

1. Introducción

1.1 Presentación

Sobre el estudio del Esquema Nacional de Seguridad (ENS), el Sistema de Gestión de la seguridad de la información (SGSI) y el análisis de riesgos se tiene en verdad la documentación oficial, pero cabe recalcar que cuando se va estudiando no se llegan a entender bien los conceptos, adicionando a esto, muchas de las herramientas para optimizar procesos y tener un alcance general llegan a ser algo complejos de entender o tediosos de realizar, además de precisar de licencias que quizás como estudiantes no podemos solventar y que probablemente no necesitemos durante el proceso de aprendizaje, para ello el fin de este trabajo es el desarrollo de una aplicación móvil que pueda ayudar y apoyar en el proceso del aprendizaje y facilite a cualquier estudiante, empresa o Pyme pequeña a tener una idea general sobre los activos que va gestionando y la seguridad de la data que conlleva todo el sistema, apoyarle a solventar algunas deficiencias, la metodología que cubre el trabajo se basa netamente sobre Magerit V3.0, el contenido del temario y del desarrollo de la aplicación se basa sobre los fundamentos descritos en el Libro I, Libro II y Libro III de Magerit descritos por el portal de administración electrónica y el Centro Criptológico Nacional.

1.2 Motivación

Gracias al Master de Ciberseguridad y Ciberinteligencia de la Universidad Politécnica de Valencia, pude entender muchos procesos legales y diferencias del tratamiento de datos en diferentes países y circunstancias lo que me hizo pensar que sería una muy buena herramienta de desarrollo al facilitar al entendedor ejemplos o un entorno físico que le permita entender mejor la parte teórica legal, como informáticos muchas veces entendemos mejor los conceptos legales teóricos mediante la práctica y el ejercicio de estes. Por ello me veo motivada a brindar la herramienta y poder apoyar en este proceso al estudiante o usuario final que desee realizar o entender un análisis de riesgos básico de un sistema.

Citas: (*Qué es el ENS*, s. f.), (*Implantación de Sistemas de Gestión de la Seguridad de la Información (SGSI) según la norma ISO 27001*, s. f.), (*PAe - MAGERIT v.3*, s. f.)

1.3 Objetivos del trabajo

1.3.1 Objetivo General

La aplicación pretende ayudar, apoyar y hacer entender al usuario final sobre este cuidado de datos y activos, entendiendo los riesgos e interpretándolos adecuadamente, proporcionando una herramienta de apoyo fácil de utilizar y al alcance del móvil. Cabe recalcar que la información que vaya a aportar la aplicación no sirve para ser auditada y certificada, para ello se precisa pasar por un especialista en caso requiera o estime un análisis más profundo o una entidad certificadora aprobada por la ENAC y la ISO 27001.

Citas: (*2.- REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) | AEPD*, s. f.), (*Modificación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales | AEPD*, 2023), (*NQA-ISO-27001-Guia-de-implantacion.pdf*, s. f.), («Entidad Nacional de Acreditación», 2023)

1.3.2 Objetivos Específicos

Como bien describe las palabras claves de la introducción, los objetivos específicos se centran en:

1. La Integración de estándares de seguridad basados en la metodología Magerit V3.0.
2. La educación y sensibilización sobre el análisis de riesgos y el ENS.
3. El entendimiento de amenazas y la evaluación de riesgos sobre los activos de nuestro sistema a analizar.

1.4 Impacto esperado

La implementación y utilización de la aplicación, la cual ha sido desarrollada con inspiración y guía de la documentación de la metodología Magerit V.3 y el Esquema Nacional de Seguridad (ENS) pretende impactar significativamente en estudiantes de ciberseguridad y pequeñas empresas que necesitan o buscan realizar un análisis previo de sus activos. Su objetivo es facilitar la comprensión y el entendimiento de los lineamientos fundamentales que, en la actualidad, constituyen la base del conocimiento esencial para cualquier empresa, especialmente para aquellos que se desempeñan como especialistas en el área.

En la actualidad, es imprescindible que todas las organizaciones desarrollen y mantengan planes de seguridad que se alineen con el Esquema Nacional de Seguridad, adoptando metodologías reconocidas como MAGERIT para garantizar una gestión adecuada de los riesgos.

Pudiendo utilizar la base de datos y reportes para posibles auditorias futuras o análisis exhaustivos más profundos, esto genera una ventaja competitiva para la pequeña empresa y una manera intuitiva de educar al estudiante y o personal.

La aplicación se caracteriza por su bajo peso o tamaño reducido, lo cual optimiza su rendimiento y facilita su instalación en dispositivos con recursos limitados, además el uso eficiente de almacenamiento y tiempo de carga se ve reducido debido al uso de un webservice en la nube, facilita también el acceso en tiempo real desde cualquier ubicación geográfica, lo que la convierte en una herramienta ideal para usuarios que requieren movilidad y rapidez.

1.5 Estructura

El presente trabajo de fin de máster se organiza en varias secciones que abordan diferentes dimensiones del proyecto. En primer término, se presenta una visión general de su ejecución, en la que se describen la motivación subyacente, los objetivos propuestos y el impacto anticipado. Además, se exploran las potenciales aplicaciones futuras del proyecto, destacando su relevancia y perspectivas a largo plazo.

Se describe luego el análisis del problema que desea resolver, también se explica el proceso de análisis, diseño, planteamiento, desarrollo, pruebas y lanzamiento de la aplicación, se comenta la securización que se utilizó en la aplicación y se enfoca principalmente en describir el análisis que se hizo para generar los informes sobre las comparativas que se precisan para la comprensión del usuario final y la futura toma de decisiones al respecto.

En primer lugar, este trabajo aborda la parte teórica, describiendo los principios y fundamentos que sustentan la seguridad informática en el marco del Esquema Nacional de Seguridad (ENS), junto con el uso de metodologías específicas como MAGERIT. A partir de esta base conceptual, se analiza el desarrollo de las metodologías aplicadas tanto en la dimensión teórica como en la técnica del proyecto. En la parte teórica, se realiza una revisión exhaustiva de los estándares internacionales de seguridad, así como de las normativas del ENS, explicando su relevancia y aplicación en la gestión de riesgos. Por su parte, la metodología técnica se centra en la implementación práctica de estos conceptos, destacando la utilización de MAGERIT para el análisis y evaluación de los riesgos asociados a los activos de la organización.

Después, se describen detalladamente los pasos seguidos en el proceso de construcción del plan de seguridad, desde la identificación de activos y la valoración de los riesgos hasta la adopción de medidas de mitigación. A lo largo del desarrollo del proyecto, se presentaron diversos problemas, los cuales fueron abordados y resueltos mediante la aplicación de técnicas específicas que garantizan la coherencia entre los objetivos del plan de seguridad y los lineamientos del ENS. Este enfoque permitió no solo mitigar los problemas encontrados, sino también optimizar los resultados finales, alineando las soluciones propuestas con las mejores prácticas en gestión de riesgos

Finalmente se presenta conclusiones del trabajo, donde se evalúa si ha satisfecho los objetivos establecidos inicialmente y en qué medida. Se incluyen las referencias utilizadas a lo largo del documento, así como las citas.

2. Estado del arte

2.1 ENS-BOE-A-2022-7191

Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

El Esquema Nacional de Seguridad (ENS), que se publicó en el Boletín Oficial del Estado (BOE) con la referencia A-2022-7191, establece un conjunto de principios y requisitos para asegurar la adecuada protección de la información gestionada por las administraciones públicas en España. Esta normativa tiene como objetivo principal garantizar que los sistemas de información de estas entidades implementen medidas de seguridad apropiadas.

El ENS busca asegurar que la información se mantenga protegida en términos de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. De este modo, se pretende que los datos sean accesibles solo para quienes estén autorizados, que se mantengan precisos y completos, que se resguarden de accesos no autorizados, que se verifique su origen y que se pueda rastrear su uso y manejo a lo largo del tiempo.

2.2 Esquema Nacional de Seguridad (ENS)

El ENS se basa en una serie de principios fundamentales, entre los que se incluyen la gestión de riesgos, la prevención, la detección y la respuesta a incidentes de seguridad. Además, establece una categorización de los sistemas de información en función de su nivel de criticidad y riesgo, lo que permite adaptar las medidas de seguridad a las necesidades específicas de cada sistema.

Entre los aspectos clave del ENS se encuentran:

Gestión de Riesgos: Requiere que las administraciones públicas realicen análisis y evaluaciones de riesgos de manera continua, para identificar y mitigar posibles amenazas a la seguridad de la información.

Citas: (*BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.*, s. f.)

Medidas de Seguridad: Establece un conjunto de medidas de seguridad mínimas que deben implementarse en los sistemas de información, clasificadas en tres niveles (bajo, medio y alto).

Responsabilidades: Define las responsabilidades de las diferentes partes involucradas en la gestión de la seguridad de la información, incluyendo roles y funciones específicas.

Cumplimiento y Auditoría: Establece la necesidad de realizar auditorías periódicas para verificar el cumplimiento del ENS y asegurar la eficacia de las medidas de seguridad implementadas.

El ENS es una herramienta crucial para la protección de la información en el ámbito de las administraciones públicas españolas, alineándose con las mejores prácticas y normativas internacionales en materia de seguridad de la información.

Fuente: Ministerio de la Presidencia, Relaciones con las Cortes y Memoria Democrática. (2022). Esquema Nacional de Seguridad. Boletín Oficial del Estado. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191

2.3 Análisis de riesgos y evaluación de impacto

Con carácter previo a cualquier tratamiento de datos personales, es necesario realizar un análisis de riesgos que permita determinar las amenazas que pueden derivarse de dicho tratamiento y el nivel de riesgo si estas se materializan para los derechos y libertades de los interesados.

Al tratarse de datos especialmente protegidos, también será necesario realizar la correspondiente evaluación de impacto.

2.4 MAGERIT V3.0

MAGERIT versión 3 es una metodología para el análisis y gestión de riesgos que fue originalmente desarrollada por el antiguo Consejo Superior de Administración Electrónica. Actualmente, esta metodología es mantenida y actualizada por la Secretaría General de Administración Digital, del Ministerio de Asuntos Económicos y Transformación Digital, en colaboración con el Centro Criptológico Nacional (CCN) (CCN-CERT - Soluciones, s. f.).

Esta metodología se ofrece como una herramienta pública, lo que significa que puede ser utilizada de manera libre y sin necesidad de obtener una autorización previa. MAGERIT está diseñada principalmente para las entidades que operan bajo el marco del Esquema Nacional de Seguridad (ENS). Su propósito es facilitar el cumplimiento del principio de gestión de la seguridad basado en riesgos, así como del requisito de análisis y gestión de riesgos. La metodología toma en cuenta la dependencia creciente de las tecnologías de la información para llevar a cabo misiones, prestar servicios y alcanzar los objetivos estratégicos de las organizaciones.

Siguiendo la terminología establecida por la normativa ISO 31000, MAGERIT se alinea con el "Proceso de Gestión de los Riesgos," particularmente con la sección 4.4 ("Implementación de la Gestión de los Riesgos") dentro del "Marco de Gestión de Riesgos." Esto implica que MAGERIT se encuadra dentro de un proceso estructurado que facilita la identificación, evaluación y tratamiento de los riesgos. De esta manera, permite a los órganos de gobierno y a las entidades responsables tomar decisiones informadas y fundamentadas en relación con los riesgos derivados del uso de las tecnologías de la información. En resumen, MAGERIT proporciona un marco de trabajo sistemático para gestionar de manera eficaz los riesgos asociados, garantizando que las decisiones se tomen con una comprensión clara de las posibles amenazas y vulnerabilidades.

2.4.1 Magerit V3.0 Libro I

Se aborda los fundamentos y principios básicos de la metodología. Cubre aspectos generales esenciales como:

- Contexto y Objetivos: Explicación del marco regulatorio y los objetivos que busca cumplir la metodología.
- Ciclo de Vida de la Gestión de Riesgos: Detalla las fases del ciclo de vida, que incluyen la identificación de activos, evaluación de riesgos, tratamiento de riesgos y monitorización.
- Roles y Responsabilidades: Define los roles y responsabilidades de los actores involucrados en la gestión de riesgos dentro de una organización.
- Técnicas y Herramientas: Proporciona orientación sobre las técnicas y herramientas recomendadas para llevar a cabo la evaluación y gestión de riesgos de manera efectiva.
- Documentación y Reporte: Establece los requisitos para la documentación y el reporte de los resultados del análisis de riesgos.

Magerit V3.0 Libro I es fundamental para cualquier organización que desee implementar un enfoque estructurado y basado en riesgos para la gestión de la seguridad de la información, cumpliendo así con los estándares y normativas pertinentes.

Nos habla sobre los objetivos directos e indirectos, y detalle que para obtener los resultados debemos generar en cuestión de evaluación los siguientes informes, los cuales pretende incluir la aplicación mencionada en dicho trabajo:

1. Modelo de valor
2. Mapa de Riesgos
3. Declaración de aplicabilidad
4. Estado de riesgo
5. Informe de insuficiencias
6. Cumplimiento de la normativa
7. Plan de seguridad

2.4.2 Magerit V3.0 Libro II

Se centra en la gestión de riesgos de seguridad de la información y aborda diversos aspectos relacionados con los activos de información.

Definición de Activos

Los activos, en el contexto de MAGERIT v3, son todos aquellos elementos de la organización que tienen valor para la misma y cuya seguridad debe protegerse. Estos activos pueden ser de diferentes tipos, incluyendo:

- Activos de Información: Datos, documentos, bases de datos, sistemas informáticos, etc.
- Activos Físicos: Equipos, instalaciones, edificios, etc.
- Activos Humanos: Personal de la organización, usuarios, administradores, etc.
- Activos Intangibles: Propiedad intelectual, reputación, marca, etc.

Proceso de Identificación de Activos

propone un proceso estructurado para identificar todos los activos relevantes para la organización:

- Análisis de Contexto: Comprender el entorno organizacional y los objetivos de negocio para identificar qué activos son críticos.
- Inventario de Activos: Crear una lista detallada de todos los activos de la organización, categorizándolos por tipo y valor.
- Valoración de Activos: Evaluar la importancia y el valor de cada activo en función de su contribución a los objetivos y operaciones de la organización.

Valoración de Activos

La valoración de activos en MAGERIT v3 implica asignarles un nivel de importancia o criticidad mediante la evaluación de criterios como:

- Impacto en el Negocio: Qué tan crucial es el activo para la operación y continuidad del negocio.

- Sensibilidad de la Información: El grado de confidencialidad, integridad y disponibilidad que se requiere para proteger la información contenida en el activo.
- Vulnerabilidades y Amenazas: Identificar las posibles amenazas y vulnerabilidades que podrían afectar la seguridad del activo.

Gestión y Protección de Activos

Una vez identificados y valorados los activos, MAGERIT v3 propone estrategias y medidas para protegerlos adecuadamente:

- Medidas de Seguridad: Implementar controles y medidas de seguridad que mitiguen los riesgos identificados para cada activo.
- Monitoreo y Evaluación: Supervisar continuamente la efectividad de las medidas de seguridad implementadas y ajustarlas según sea necesario.
- Gestión de Incidentes: Preparar planes de respuesta a incidentes para actuar rápidamente en caso de que se produzcan amenazas o incidentes que afecten a los activos críticos.

2.4.3 Magerit V3.0 Libro III

Este está dedicado a la elaboración de informes y documentación en el proceso de gestión de riesgos de seguridad de la información. Su propósito principal es guiar a las organizaciones en la creación de reportes comprensibles y útiles que reflejen el estado de los riesgos y las medidas adoptadas para gestionarlos.

Tipos de Informes

- Informe de Riesgos: Documento que recoge los resultados del análisis y la valoración de riesgos, incluyendo la identificación de amenazas, vulnerabilidades y el impacto potencial sobre los activos.
- Informe de Tratamiento de Riesgos: Detalla las medidas y controles adoptados para mitigar los riesgos identificados. Incluye planes de acción y recursos necesarios.
- Informe de Seguimiento: Proporciona una actualización sobre el estado de los riesgos y la eficacia de las medidas implementadas. Se usa para monitorear y evaluar la evolución de los riesgos y los controles a lo largo del tiempo.
- Informe de Incidentes: Describe los incidentes de seguridad ocurridos, su impacto, las acciones tomadas para resolverlos y las lecciones aprendidas.

Estructura de los Informes

Cada tipo de informe debe tener una estructura clara y coherente, que generalmente incluye:

- Portada: Título, fecha, autor y destinatarios del informe.
- Índice: Lista de secciones y subsecciones del informe.
- Resumen Ejecutivo: Resumen conciso de los principales hallazgos y recomendaciones.
- Introducción: Contexto, objetivos y alcance del informe.
- Metodología: Descripción de los métodos y herramientas utilizados para el análisis de riesgos.
- Resultados: Presentación detallada de los hallazgos, incluyendo matrices de riesgo, gráficos y tablas.
- Conclusiones y Recomendaciones: Resumen de los riesgos más significativos y las acciones recomendadas para gestionarlos.
- Anexos: Información adicional que respalda el contenido del informe, como datos detallados, referencias y glosarios.

Buenas Prácticas para la Elaboración de Informes

- Claridad y Precisión: Los informes deben ser claros, concisos y precisos, evitando ambigüedades y tecnicismos innecesarios.
- Relevancia: Incluir información relevante y necesaria para los destinatarios del informe, enfocándose en los riesgos y medidas más críticos.
- Actualización Continua: Mantener los informes actualizados y reflejar los cambios en el entorno de riesgos y las medidas de control.
- Comunicación Efectiva: Utilizar gráficos, tablas y otros elementos visuales para facilitar la comprensión de la información.

Destinatarios de los Informes

Los informes de gestión de riesgos deben estar dirigidos a diferentes audiencias dentro de la organización, incluyendo:

- Alta Dirección: Para la toma de decisiones estratégicas sobre la gestión de riesgos y asignación de recursos.
- Equipos Técnicos: Para la implementación y monitoreo de medidas de seguridad específicas.
- Personal General: Para la concienciación y capacitación en aspectos de seguridad de la información.

El libro III de MAGERIT v3 proporciona una guía completa para la elaboración de informes de gestión de riesgos de seguridad de la información. Estos informes son fundamentales para comunicar el estado de los riesgos y las medidas de control a diferentes audiencias dentro de la organización, facilitando una gestión de riesgos informada y efectiva.

Fuente: Ministerio de Asuntos Económicos y Transformación Digital. (n.d.). MAGERIT versión 3: Metodología de análisis y gestión de riesgos. Secretaría General de Administración Digital.

2.5 MICROPILAR

Es una herramienta para el análisis de riesgos en la seguridad de la información, desarrollada por el Centro Criptológico Nacional de España. Su propósito es ofrecer un método claro y ágil para llevar a cabo evaluaciones de riesgos en sistemas de información. La herramienta se enfoca en aspectos esenciales de la seguridad, tales como la confidencialidad, la integridad y la disponibilidad de la información, permitiendo a las organizaciones identificar y gestionar de manera efectiva las amenazas y vulnerabilidades en sus sistemas.

Fuente: Centro Criptológico Nacional. µPILAR, (*PILAR - ¿Qué es el análisis de riesgos?*, s. f.)

2.6 UNE-EN-ISO/IEC 27001

Seguridad de la Información - Sistemas de Gestión

La norma UNE-EN-ISO/IEC 27001 especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Este estándar es aplicable a cualquier organización, independientemente de su tamaño, tipo o sector, y su objetivo es proteger la información de la organización mediante la adopción de un enfoque sistemático y estructurado. Los principales puntos incluyen:

- Evaluación y Tratamiento de Riesgos: Identificar, evaluar y tratar los riesgos de seguridad de la información.
- Política de Seguridad de la Información: Definir una política que establezca directrices y objetivos.
- Control de Acceso: Establecer controles para garantizar que el acceso a la información sea apropiado y autorizado.
- Seguridad de los Recursos Humanos: Asegurar que el personal entienda sus responsabilidades y roles en la seguridad de la información.
- Gestión de Incidentes de Seguridad: Implementar procedimientos para gestionar y reportar incidentes de seguridad.

- Continuidad del Negocio: Preparar planes para asegurar la continuidad de las operaciones en caso de una interrupción significativa.

Fuente: (Documento_Norma_UNE-EN_ISO-IEC_27001 MINTUR.pdf, s. f.)

2.7 UNE-EN-ISO/IEC 27002

Código de Buenas Prácticas para la Gestión de la Seguridad de la Información

La norma UNE-EN-ISO/IEC 27002 proporciona un conjunto de controles y directrices de seguridad de la información basados en las mejores prácticas internacionales. Es complementaria a la ISO/IEC 27001 y proporciona un marco detallado para ayudar a las organizaciones a seleccionar e implementar controles de seguridad adecuados. Los principales puntos incluyen:

- Control de Acceso: Directrices para implementar controles que restrinjan el acceso a la información.
- Seguridad en las Operaciones: Buenas prácticas para la gestión y control de las operaciones de TI.
- Seguridad Física y Ambiental: Medidas para proteger los activos físicos de la organización contra amenazas ambientales y físicas.
- Seguridad en las Comunicaciones: Directrices para asegurar la confidencialidad, integridad y disponibilidad de la información en tránsito.
- Adquisición, Desarrollo y Mantenimiento de Sistemas: Controles para asegurar que la seguridad esté integrada en los sistemas de información desde el inicio.
- Gestión de Incidentes de Seguridad de la Información: Procedimientos para la detección, reporte y respuesta a incidentes de seguridad.

Fuente: (Industria Conectada 4.0 - Normas UNE-EN ISO/IEC 27001 y UNE-EN ISO/IEC 27002 para la seguridad de la información, s. f.)

3. Análisis del Problema

3.1 Descripción del problema

Una de las principales dificultades que enfrentan los estudiantes de ingeniería informática y áreas afines radica en la comprensión de disciplinas complementarias a su campo de estudio, como el ámbito legal, que resulta fundamental en el contexto de la ciberseguridad y la Ciberinteligencia. Estos campos, que requieren un análisis y estudio exhaustivo en la actualidad, son especialmente relevantes para sectores críticos como el bancario, el sanitario, el alimentario y otros, donde la protección de los datos y activos se ha convertido en una prioridad estratégica.

El rol de un auditor, analista o responsable de seguridad recae en la protección de los datos y activos de una organización, asumiendo la gestión de los riesgos inherentes a un mal manejo de estos. Sin embargo, uno de los problemas más comunes reside en la falta de comprensión o en la inadecuada gestión de los activos, lo que puede derivar en riesgos significativos para la integridad de la información de los sistemas. Este desentendimiento subraya la importancia de una formación interdisciplinaria que integre aspectos técnicos y legales, esenciales para enfrentar los desafíos actuales en la gestión de la seguridad de la información

3.2 Identificación y análisis de posibles soluciones

Felizmente España ha desarrollado un esquema (ENS) sobre el cual las empresas y especialistas se pueden guiar además de la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) fue desarrollado por el Consejo Superior de Administración Electrónica (CSAE) del Gobierno de España dichos instrumentos de confianza se pueden utilizar para ejercer las mejores prácticas a la hora del análisis de los riesgos sobre nuestros activos. Así como guiar al usuario final a presentar de una forma inequívoca dichos activos.

3.3 INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE) es una entidad de referencia en ciberseguridad en España, dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. Su misión principal es mejorar la ciberseguridad de la sociedad, las empresas y las infraestructuras críticas del país.

Objetivos Principales del INCIBE:

- Protección y Prevención: Proteger los sistemas de información y las comunicaciones de los ciudadanos, empresas e instituciones.
- Respuesta ante Incidentes: Proporcionar una respuesta rápida y eficiente ante incidentes de ciberseguridad.
- Educación y Concienciación: Promover la cultura de la ciberseguridad a través de campañas de concienciación, formación y educación.
- Innovación y Desarrollo: Fomentar la innovación y el desarrollo en el ámbito de la ciberseguridad.

3.4 Resumen de la Aplicabilidad

Ambas normas son esenciales para cualquier organización que busque implementar un Sistema de Gestión de Seguridad de la Información (SGSI) robusto y alineado con las mejores prácticas internacionales. Mientras que la ISO/IEC 27001 proporciona el marco y los requisitos para un SGSI, la ISO/IEC 27002 ofrece una guía detallada sobre cómo implementar controles específicos para proteger la información

Fuente: Asociación Española de Normalización (UNE). (n.d.). Normas UNE-EN-ISO/IEC 27001 y UNE-EN-ISO/IEC 27002.

- Centro de Respuesta a Incidentes de Seguridad (CERT): Actúa como el CERT nacional, gestionando y coordinando la respuesta a incidentes de ciberseguridad.
- Servicios para Ciudadanos y Empresas: Ofrece servicios específicos de apoyo y asesoramiento en ciberseguridad para ciudadanos y pequeñas y medianas empresas (pymes).

- Colaboración con las Fuerzas y Cuerpos de Seguridad del Estado: Trabaja en estrecha colaboración con las fuerzas de seguridad para combatir el cibercrimen.
- Investigación y Desarrollo: Promueve y apoya proyectos de investigación y desarrollo en el campo de la ciberseguridad.
- Orientación del INCIBE al Desarrollo del ENS (Esquema Nacional de Seguridad)

(*CONAN móvil | Ciudadanía | INCIBE*, s. f.)

4. Solución Propuesta

4.1 Metodología

Como ya se ha expresado en párrafos previos, se ha detallado la metodología teoríca siendo MAGERIT y el ENS apoyándose sobre las ISOS 27001 y 27002, a continuación, se detalla la metodología de desarrollo para la aplicación.

4.1.1 Metodología Ágil rápida

La metodología ágil es un enfoque de gestión de proyectos que enfatiza la flexibilidad, la colaboración y la entrega continua de valor. Se originó en el desarrollo de software, pero sus principios pueden aplicarse a diversos tipos de proyectos.

Principios Fundamentales

Interacciones sobre Procesos y Herramientas: Valoración de la comunicación directa y la colaboración por encima de la rigidez de los procedimientos y el uso de herramientas específicas.

Software Funcional sobre Documentación Extensiva: Prioridad a la entrega de software que funcione, con documentación suficiente pero no excesiva.

Colaboración con el Cliente sobre la Negociación de Contratos: Trabajo cercano y continuo con el usuario final para adaptarse a sus necesidades y cambios de requerimientos.

Respuesta al Cambio sobre el Seguimiento de un Plan: Flexibilidad para adaptar el proyecto en función de los cambios y feedback recibido.

- Ciclos Iterativos e Incrementales
- Iteraciones Cortas (Sprints)
- Ciclos de trabajo breves y repetidos (generalmente de 2 a 4 semanas) en los que se desarrolla y se entrega una parte funcional del producto.

Incrementos Funcionales: Cada iteración produce un incremento del producto que se revisa y puede ser puesto en producción, asegurando así la entrega continua de valor.

Roles Clave

En este caso, yo hare de Product Owner, Scrum Máster y equipo de desarrollo debido a la envergadura del trabajo, siendo un trabajo personal.

- *Product Owner* (Propietario del Producto): Representa los intereses del cliente y prioriza el trabajo en función del valor de negocio.
- *Scrum Máster (*Facilitador): Facilita el proceso, elimina impedimentos y asegura que el equipo siga los principios ágiles.
- *Equipo de Desarrollo*: Grupo multifuncional encargado de entregar el producto en cada iteración.

Artefactos y Eventos

- *Product Backlog:* Lista priorizada de todas las funcionalidades y requisitos del producto.
- *Sprint Backlog*: Conjunto de tareas y objetivos específicos para la iteración actual.
- *Daily Stand-up* (Reunión Diaria): Reunión breve diaria para sincronizar al equipo y planificar el día.
- *Sprint Review* (Revisión del Sprint): Evaluación al final de cada sprint donde se presenta lo desarrollado y se recibe feedback.
- *Sprint Retrospective* (Retrospectiva del Sprint): Reflexión al final de cada sprint para identificar mejoras en el proceso.

Beneficios de la Metodología Ágil

- *Adaptabilidad*: Capacidad para responder rápidamente a los cambios en los requisitos y en el entorno.
- *Entrega Continua de Valor:* Proporciona incrementos funcionales del producto de manera frecuente.
- *Mejora Continua*: Enfoque en la revisión y mejora constante de procesos y productos.
- *Colaboración y Transparencia*: Fomenta una comunicación abierta y continua entre todos los involucrados en el proyecto.

La metodología ágil ofrece un marco flexible y eficiente para la gestión de proyectos, centrado en la entrega continua de valor y en la adaptación constante a las necesidades cambiantes del cliente. A través de iteraciones cortas, roles bien definidos y una comunicación constante, las metodologías ágiles permiten gestionar proyectos de manera efectiva, asegurando la satisfacción del cliente y la calidad del producto final.

Como el trabajo de tesis lo realizare solo yo, actuare en todos los ámbitos y roles descritos previamente.

Citas: (Cohn, 2010), (Layton & Ostermiller, 2017)

5. Cuerpo del trabajo

5.1 Sobre la parte teórica

Para entender mejor el trabajo se presenta en diferentes fases teóricas, las fases que se utilizó de referencia se basan en las fases del análisis de riesgo en seis sencillos pasos del Instituto Nacional de Ciberseguridad (INCIBE) aplicadas con Magerit, el que describe, estas mismas se plasman mediante formularios en la aplicación, la cuales el usuario final llenara, una vez haya entendido cada uno de los conceptos base.

Fase I: Definición del alcance

Fase II: Identificación de los activos

Fase III: Identificación de las amenazas

Fase IV: Identificación de las medidas de seguridad

Fase V: Identificación de las salvaguardas

Fase VI: Informes – base libro III de Magerit

5.1.1 Fase I: Definición del alcance

5.1.1.1 Alcance teórico

La aplicación pretende sobre todo orientar al usuario final sobre el ENS y Magerit V3, por lo ya descrito en el tópico del “estado del arte”, se limita a considerar estas bases teóricas y ninguna adicional a estas, se habla un poco de otras en el apartado “normativa”, como detalla adicional.

5.1.1.2 Alcance técnico

La aplicación ha sido concebida con el propósito de ofrecer una experiencia de usuario sencilla e intuitiva, orientada específicamente a dispositivos móviles con sistema operativo Android, desde la versión 11 (R, SDK 30) hasta la versión 14 (UpsideDown Cake, SDK 34). El desarrollo de la aplicación se ha llevado a cabo bajo lineamientos de seguridad conocidos, si bien no ha sido diseñada exhaustivamente para resistir pruebas

avanzadas de testing o vulnerabilidades. No obstante, se han implementado con esmero las mejores prácticas recomendadas en materia de seguridad durante su desarrollo, tales como el hasheo de contraseñas, el control de cabeceras, la configuración de CORS, entre otros aspectos que serán detallados en apartados posteriores.

5.1.2 Fase II: Identificación de los activos

Los servicios y activos se ven orientados a sistemas del Departamento Informática, Gestión, Servidor Principal, Almacén, Área común, Servidor Secundario y Ventas para este proceso se realizó una plantilla básica en Excel, para estudiar el comportamiento de los datos y obtener la mayoría de las áreas comunes que suelen tener las pymes y la generación de reportes, estas áreas son fácilmente editables sobre la base de datos en la tabla "área_pertenencia".

Para la identificación de estos activos se plantea obtener los siguientes datos:

- Nombre: Pone el nombre del activo o algún identificador.
- Descripción: Un detalle que podría incluir la versión de fábrica, compilación, última actualización u otro detalle relevante.
- Área de pertenencia: Área o espacio donde se halla el activo en uso.
- Valor de la Información: Se evalúa la importancia de la información que el dispositivo maneja, su confidencialidad, integridad y disponibilidad.
- Impacto en el Negocio: Se analiza el impacto que tendría el dispositivo en las operaciones de la organización si se viera comprometido o dejara de funcionar.
- Función y Criticidad del Dispositivo: Se considera el papel que desempeña el dispositivo en el cumplimiento de las funciones críticas de la organización y en el soporte de los procesos de negocio.
- Interconexión y Dependencias: Se evalúa cómo la interconexión del dispositivo con otros sistemas y su dependencia de otros servicios afecta a la seguridad y continuidad del negocio.
- Exposición a Amenazas: Se analizan las amenazas a las que está expuesto el dispositivo y su vulnerabilidad frente a estas amenazas.

- Costo de Recuperación o Sustitución: Se considera el costo asociado a la recuperación del dispositivo en caso de un incidente de seguridad o su sustitución en caso de fallo.
- Reputación y Cumplimiento: Se evalúa el impacto en la reputación de la organización y el cumplimiento de normativas y regulaciones relacionadas con la seguridad de la información.
- Factores Contextuales: Se tienen en cuenta otros factores específicos de la organización, como su tamaño, industria, entorno regulatorio, entre otros.
- Importancia: Hace un cálculo total aplicando los pesos ponderados con respecto al Valor de la Información, Impacto en el Negocio, Función y Criticidad del Dispositivo, Interconexión y Dependencias, Exposición a Amenazas, Costo de Recuperación o Sustitución, Reputación y Cumplimiento y Factores Contextuales.
- Código: Código identificativo sobre el activo puede ser número de serie, compilación o última fecha de instalación o fecha de recambio, dependiendo del tipo de activo que sea.
- Responsable: Persona que se hace cargo del activo.
- Incidencia: Posible incidencia o deterioro que podría afectar a su importancia
- Tipo de Activo: Basado sobre Magerit se define como activos esenciales, arquitectura del sistema, Datos/Información, Claves Criptograficas, Servicios, Software - Aplicaciones informáticas, Hardware - Equipamiento informatico, Redes de comunicaciones, Soportes de información, Equipamiento Auxiliar, Instalaciones y Personal, para mayor detalle revisar libro II de Magerit.
- Política de Seguridad: Aquí se definiría el lugar o el fichero donde se halla su política de seguridad para fácil acceso.
- En funcionamiento: 1 activo y 0 no activo.
- ID del proyecto: El identificador del proyecto al cual el activo que va relacionado.

A continuación, se muestra una tabla sobre los pesos de cada elemento, la valoración se puede ver desde la perspectiva de la "necesidad de proteger" siempre.

Valor de la Información:	20 %
Impacto en el Negocio:	20 %
Función y Criticidad del Dispositivo:	15 %
Interconexión y Dependencias:	15 %
Exposición a Amenazas:	10 %
Costo de Recuperación o Sustitución:	10 %
Reputación y Cumplimiento:	5 %
Factores Contextuales:	5 %

Tabla 1.- Pesos de diferentes cualidades para obtener la importancia del activo

5.1.3 Fase III: Identificación de las amenazas

Para la identificación de las amenazas se considera los activos agregados previamente en caso no haya ningún activo la aplicación generara un activo genérico sobre el cual trabajar, se elige la amenaza basada en Magerit sobre Amenazas, se identifica una descripción de la amenaza para mayor detalle, se define el impacto sobre el sistema de esta amenaza en el activo mencionado, luego la probabilidad que la amenaza pueda ocurrir al activo.

5.1.4 Fase IV: Identificación de las medidas de seguridad

Para la identificación de las medidas de seguridad se recolecta nuevamente los activos detallados anteriormente, mostrando una lista de los activos con los que queremos trabajar en el proyecto, las medidas de seguridad vienen de Magerit y finalmente se puede detallar una descripción más específica sobre esta medida.

5.1.5 Fase V: Identificación de las salvaguardas

Para la identificación de salvaguardas se recolecta nuevamente los activos detallados anteriormente, mostrando una lista de los activos con los que queremos trabajar en el proyecto, los salvaguardas vienen de Magerit y finalmente se puede detallar una descripción más específica sobre esta salvaguarda.

5.1.6 Fase VI: Informes

Los informes generados vienen algo relativos al libro I de Magerit con algunas interpretaciones propias un poco específicas para que el usuario final tenga un mejor alcance y entendimiento de estos, se tienen conformados de la siguiente manera:

5.1.6.1 Modelo de valor

Se detalla una gráfica del tipo de activo versus los valores de interés de los promedios ponderados del valor de la información, impacto en el negocio, función de criticidad, interconexiones y dependencias, exposición de amenazas, costo de recuperación, reputación y cumplimiento, factores contextuales e importancia. Ver anexo 10.a

5.1.6.2 Mapa de Riesgos

El mapa de riesgos compara las áreas donde se han detallado los activos y posibles riesgos tomando en cuenta el impacto promedio, probabilidad promedio y riesgo porcentual promedio. Ver anexo 10.b

5.1.6.1 Declaración de aplicabilidad

Se tiene una gráfica del total de salvaguardas según tipo de activo, adicional un gráfico del total de salvaguardas descritos en el proyecto por tipo de salvaguarda. Ver anexo 10.c

5.1.6.2 Evaluación de salvaguardas

Se ha generado tres graficas sobre la cantidad de salvaguardas en relación con el costo, la cantidad de salvaguardas en relación con el tiempo que toman implementarlas y finalmente una gráfica de la eficiencia versus el riesgo residual, para el cálculo de todas estas se ha considerado:

estándares como MAGERIT, NIST, e ISMS (ISO/IEC 27001). Estas estimaciones son aproximaciones comunes y pueden variar dependiendo de la implementación específica y el contexto. Ver anexo 10.d

Estimaciones de eficacia en porcentaje

Protecciones generales u horizontales: 80%

Son eficaces en un amplio rango de escenarios ya que cubren múltiples áreas de la organización.

Protección de datos / información: 85%

Fundamental para la confidencialidad e integridad de los datos, con medidas como cifrado, control de acceso, etc.

Protección de claves criptográficas: 90%

Crítica para la seguridad de la información, especialmente en sistemas que dependen del cifrado.

Protección de los servicios: 75%

Asegura la disponibilidad y continuidad de los servicios críticos, pero la eficacia puede verse afectada por la complejidad y dependencia de otros sistemas.

Protección de las aplicaciones (software): 70%

Incluye medidas como el parcheo y la seguridad en el desarrollo, pero depende de la regularidad y profundidad de las actualizaciones.

Protección de los equipos (hardware): 80%

Las medidas físicas y técnicas son generalmente efectivas para asegurar el hardware, aunque pueden fallar ante ataques físicos sofisticados.

Protección de las comunicaciones: 85%

Implica el uso de protocolos seguros y cifrado de extremo a extremo, generalmente muy eficaz.

Protección de los puntos de interconexión con otros sistemas: 75%

La eficacia depende de las medidas de control de acceso y la segmentación de red, pero puede ser un punto débil si no se maneja adecuadamente.

Protección de los soportes de información: 80%

Eficacia alta si se implementan controles como cifrado y gestión segura de los medios.

Protección de los elementos auxiliares: 70%

Incluye la seguridad de sistemas auxiliares como fuentes de energía, que, aunque críticas, pueden tener vulnerabilidades.

Protección de las instalaciones - Seguridad Física: 90%

Medidas físicas como vigilancia, controles de acceso, etc., son altamente efectivas.

Salvaguardas relativas al personal: 75%

Incluye formación y controles de acceso, pero la eficacia depende de la conducta humana.

Continuidad de operaciones: 85%

Planes de recuperación ante desastres y continuidad son generalmente efectivos si están bien diseñados y probados.

Externalización: 65%

La eficacia puede ser menor debido a la dependencia de terceros y la dificultad de control directo.

Adquisición y desarrollo: 70%

Eficacia moderada, depende de la inclusión de requisitos de seguridad desde el inicio del proceso de desarrollo y adquisición.

Salvaguardas del tipo organizativo: 80%

Incluyen políticas, procedimientos y gobernanza, siendo fundamentales pero su eficacia depende del cumplimiento y la adaptación continua.

Referencias generales:

Estas estimaciones están alineadas con las prácticas comunes de gestión de riesgos de seguridad de la información según estándares como NIST SP 800-53, MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), e ISO/IEC 27001. Es importante tener en cuenta que la eficacia real puede variar en función del contexto específico de implementación y de la organización.

5.1.6.3 Estado de riesgo

Para el estado de riesgo se ha definido un gráfico sobre la cantidad de activos afectados por su dimensionalidad versus el tipo de activo, la cantidad de activos afectados por su dimensionalidad versus área de pertenencia y la cantidad de activos afectados por si dimensionalidad versus la amenaza.

5.1.6.4 Informe de Insuficiencias

Se ha detallado un gráfico sobre la cantidad de medidas de seguridad por dimensión o categoría, la cantidad de medidas de seguridad en total por medida de seguridad y el promedio de seguridad porcentual según el área de pertenencia.

Estas dimensionalidades salen de la siguiente:

Valoración medidas de seguridad

Las valoraciones de seguridad que proporcioné se basan en una estimación general y representativa de cómo se podrían evaluar estas medidas de seguridad en el contexto de marcos normativos y estándares como ISO 27001, NIST, y las mejores prácticas de la industria.

- Relevancia de la medida dentro de marcos de ciberseguridad estándar (ej. ISO 27001, NIST SP 800-53).
- Impacto en la seguridad general de la organización si las medidas se implementan correctamente.
- Conocimiento común sobre la efectividad de las prácticas de seguridad.Es importante que las valoraciones específicas para un entorno particular se realicen mediante un análisis de riesgos detallado y en función de los requerimientos y condiciones de la organización en cuestión. Esto suele incluir auditorías, evaluaciones de riesgos, y la experiencia profesional en el área de ciberseguridad.

Si se necesitara realizar valoraciones más precisas y adaptadas a un entorno específico, recomiendo realizar un análisis basado en un marco como ISO 27001 o NIST SP 800-53, combinando evaluaciones cualitativas y cuantitativas basadas en datos reales de tu organización.

Para cuantificar el nivel de seguridad de una medida específica, se usa una fórmula basada en la combinación de factores clave, como el nivel de madurez, el riesgo asociado, y el impacto. Un enfoque común es utilizar una puntuación ponderada.

Fórmula General:

Seguridad = (Nivel de Madurez×0.4+Impacto×0.3+Probabilidad del Riesgo×0.3Puntaje Máximo) ×100

Donde:

- Nivel de Madurez: Evaluación de cuán desarrollada y efectiva es la medida de seguridad (puntuado en una escala de 1 a 5, donde 1 es inicial y 5 es optimizado).
- Impacto: El efecto que tendría un incidente relacionado con la medida (puntuado en una escala de 1 a 5, donde 1 es bajo y 5 es crítico).
- Probabilidad del Riesgo: La probabilidad de que ocurra un incidente si la medida no está implementada adecuadamente (puntuado en una escala de 1 a 5, donde 1 es baja probabilidad y 5 es alta probabilidad).
- Puntaje Máximo: En este caso sería 5, ya que cada factor se evalúa en una escala de 1 a 5.

Ejemplo de Aplicación:

Supongamos que para la Protección de claves criptográficas:

- Nivel de Madurez = 4 (gestionado cuantitativamente)
- Impacto = 5 (crítico)
- Probabilidad del Riesgo = 3 (moderada)

Sustituyendo en la fórmula:

$$\text{Seguridad} = ((4\times0.4) +(5\times0.3) +(3\times0.3)5) \times100=85\%$$

Se podría variar los pesos (0.4, 0.3, 0.3) según las prioridades estratégicas de seguridad.

5.1.6.5 Cumplimiento de normativa

Sobre el cumplimiento de la normativa se detalla los enlaces más usados y las normas que se precisó estudiar para entender todo este proceso como son Magerit, Norma UNE-EN ISO/IEC 27001, Norma UNE-EN ISO/IEC 27002, enlace a la ley orgánica de protección de datos, enlace a la agencia española de protección de datos, INCIBE, el Esquema Nacional de Seguridad y enlace al Centro Criptológico Nacional.

5.1.6.6 Plan de seguridad

El plan de seguridad detalla los pasos que el usuario final tendrá que aplicar sobre la información que obtuvo con la aplicación y orientarla mejor a sus objetivos.

5.2 Sobre la parte técnica

Para el desarrollo técnico del trabajo se utilizó la metodología de Desarrollo Ágil, adaptada para ser breve y sencillo, el cual cuenta con los pasos de:

I. Planeación: Definición de la idea y la enumeración de los requisitos básicos.
II. Diseño: Desarrollo de la estructura del BackEnd, desarrollo de Wireframes y UI/UX.
III. Desarrollo: Configuración del proyecto y programación básica.
IV. Pruebas: Pruebas funcionales:
    a. En debug
    b. En reléase
    c. De usuario.
V. Lanzamiento

Citas: (Blanco et al., s. f.), (Gironés, 2019), (*Kotlin y Android*, s. f.)

5.3 Desarrollo de la parte técnica

5.3.1 *Planeación*

Para comenzar se genera el esquema de la base de datos sobre la cual se va a trabajar dejando algunas tablas y campos vacíos para futuros trabajos de escala.

De primera mano se realizó una plantilla en Excel para evaluar el comportamiento natural de algunas empresas que mantendremos en la anonimidad sobre las cuales pudo realizar el estudio empírico.

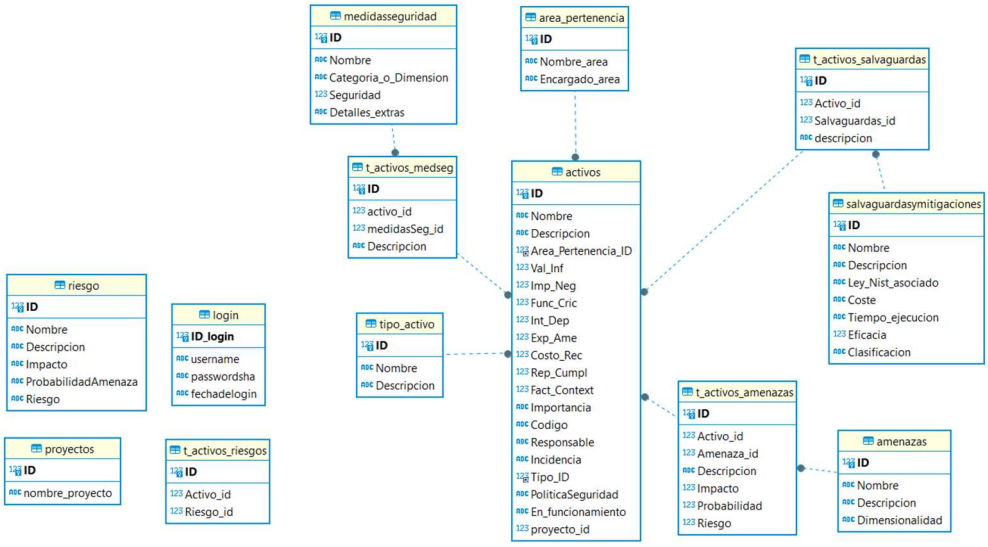


Ilustración 1.- Diagrama Entidad-Relación (ERD) de la aplicación "ARC"

5.3.2 Sobre el sistema de gestión de bases de datos (DBMS)

Sobre el sistema de gestión de bases de datos (DBMS): MariaDB 11.3.2, MariaDB Server es una de las bases de datos relacionales de código abierto más populares. Está creado por los desarrolladores originales de MySQL y se garantiza que seguirá siendo de código abierto. Es parte de la mayoría de las ofertas en la nube y el valor predeterminado en la mayoría de las distribuciones de Linux.

Se basa en los valores de rendimiento, estabilidad y apertura, y la Fundación MariaDB garantiza que las contribuciones se aceptarán según el mérito técnico. La nueva funcionalidad reciente incluye agrupación avanzada con Galera Cluster 4, funciones de compatibilidad con Oracle Database y tablas de datos temporales, lo que permite consultar los datos tal como estaban en cualquier momento del pasado.

Fuente: (*MariaDB Foundation*, s. f.)

5.3.3 Securización en el DBMS

Ejecuta el script de seguridad de MariaDB: MariaDB incluye un script de seguridad que se puede ejecutar para mejorar la seguridad de la instalación. Esto permitirá establecer una contraseña para el usuario root de MariaDB, eliminar usuarios anónimos, deshabilitar el inicio de sesión remoto para el usuario root, y eliminar la base de datos de prueba.

sudo mysql_secure_installation

Durante la ejecución de este script, se hace varias preguntas que se recomienda responder de la siguiente forma:

- Configurar la contraseña de root de MariaDB: Sí
- Eliminar usuarios anónimos: Sí
- Deshabilitar el inicio de sesión remoto para root: Sí
- Eliminar la base de datos de prueba y acceder a ella: Sí
- Recargar las tablas de privilegios: Sí

5.3.4 DBeaver V 23.2.3

DBeaver Community es una herramienta de gestión de bases de datos multiplataforma de código abierto, diseñada para desarrolladores, administradores de bases de datos, analistas y otros profesionales que trabajan con datos. Esta aplicación es compatible con una amplia gama de bases de datos SQL, incluyendo MySQL, MariaDB, PostgreSQL, SQLite, y las bases de datos de la familia Apache, entre otras.

En el contexto de la configuración del sistema, se ha creado un nuevo usuario específico para el webservice, con el propósito de asegurar que la conexión se realice utilizando credenciales dedicadas únicamente a esa base de datos en particular. Los permisos de este usuario se han restringido de manera rigurosa: se han denegado los permisos para operaciones potencialmente disruptivas, tales como DELETE y GRANT, y se han habilitado únicamente los permisos necesarios para el funcionamiento básico, que incluyen INSERT, SELECT y UPDATE. Esta configuración garantiza un control más granular y seguro sobre las operaciones realizadas en la base de datos, minimizando riesgos y protegiendo la integridad del sistema.

Fuente: (*DBeaver Community | Free Universal Database Tool*, s. f.)

5.3.5 Nginx Proxy Manager

Este proyecto se presenta como una imagen acoplable prediseñada que le permite reenviar fácilmente a sus sitios web que se ejecutan en casa o de otro modo, incluido SSL gratuito, sin tener que saber demasiado sobre Nginx o Letsencrypt.

Fuente: (*Nginx Proxy Manager*, s. f.)

El uso de Nginx facilita la integración de certificados SSL, lo que permite establecer conexiones seguras mediante HTTPS para realizar peticiones cifradas. Además, Nginx actúa como un proxy inverso, permitiendo el encaminamiento eficiente de las solicitudes mientras oculta datos sensibles, mejorando la seguridad general del sistema. Adicionalmente, Nginx permite configurar y gestionar cabeceras HTTP, lo que refuerza la protección frente a vulnerabilidades comunes, como ataques de tipo XSS o CSRF.

Una ventaja adicional de usar Nginx Proxy Manager es su interfaz gráfica simplificada, que facilita la configuración y administración del proxy inverso, incluyendo la gestión de

múltiples dominios y certificados SSL sin necesidad de una intervención avanzada en la línea de comandos. Esto lo convierte en una solución accesible para administradores que buscan simplificar tareas complejas en entornos de producción.

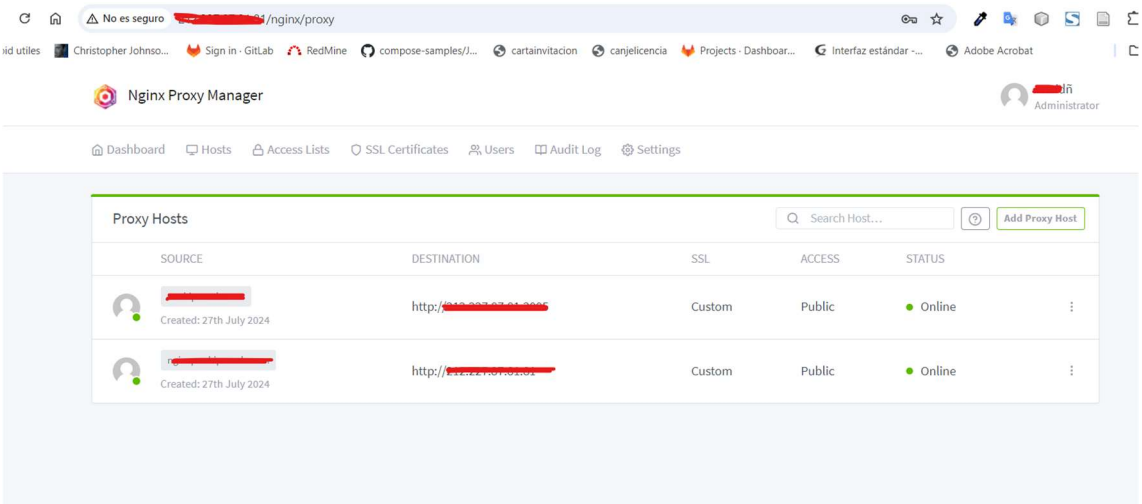


Ilustración 2.- Dashboard NGINX Proxy Manager muestra certificados SSL aplicados a servicios

5.3.6 Android Studio Giraffe 2022.3.1 Patch 3

Android Studio es el entorno de desarrollo integrado oficial para la plataforma Android. Fue anunciado el 16 de mayo de 2013 en la conferencia Google I/O, y reemplazó a Eclipse como el IDE oficial para el desarrollo de aplicaciones para Android. La primera versión estable fue publicada en diciembre de 2014.

Fuente: (*Cómo descargar Android Studio y App Tools*, s. f.)

5.3.7 Gradle V 8.1.1

Gradle es el sistema de compilación de código abierto elegido por los desarrolladores de Java, Android y Kotlin. Desde aplicaciones móviles hasta microservicios, desde pequeñas empresas emergentes hasta grandes empresas, ayuda a los equipos a ofrecer mejor software y más rápido.

Gradle es un sistema de automatización de construcción de código de software que construye sobre los conceptos de Apache Ant y Apache Maven e introduce un lenguaje específico del dominio basado en Groovy en vez de la forma XML utilizada por Apache Maven para declarar la configuración de proyecto.

Fuente: (*Gradle Build Tool*, 2024)

Para segurizar la aplicación se utilizó la última versión disponible de Gradle al momento de codificar el proyecto.

5.3.8 Kotlin V 1.9.22

Kotlin es un lenguaje de programación multiplataforma, estáticamente tipado, de alto nivel y propósito general con inferencia de tipos.

Fuente: (*Kotlin y Android*, s. f.)

5.3.9 Expresss framework 1.0.0

Express es una infraestructura de aplicaciones web Node.js mínima y flexible que proporciona un conjunto sólido de características para las aplicaciones web y móviles.

5.3.10 Securización en Express

las tecnologías y prácticas de securización utilizadas en el código de la aplicación Express:

5.3.10.1 *BodyParser*

Descripción: Middleware que analiza el cuerpo de las solicitudes entrantes en un formato JSON, lo que facilita la gestión de datos enviados a través de las solicitudes HTTP.

Securización: El límite de 10kb en el tamaño del cuerpo (limit: '10kb') ayuda a mitigar ataques como el denial-of-service (DoS), evitando que se envíen grandes volúmenes de datos que podrían sobrecargar el servidor.

5.3.10.2 Helmet

Descripción: Middleware que ayuda a proteger la aplicación Express estableciendo varios encabezados HTTP de seguridad.

Securización: Incluye protecciones contra vulnerabilidades comunes, como Clickjacking, Cross-Site Scripting (XSS) y MIME-type sniffing. Añade una capa de seguridad predeterminada, ajustando los encabezados HTTP de la respuesta.

5.3.10.3 Cors

Descripción: Middleware que permite controlar qué dominios pueden acceder a la API de tu aplicación mediante Cross-Origin Resource Sharing (CORS).

Securización: Al definir origin: 'https://arc.dominio.com', estás limitando las solicitudes CORS solo a este dominio, lo que ayuda a prevenir ataques CSRF (Cross-Site Request Forgery) al restringir quién puede hacer peticiones al servidor.

5.3.10.4 Crypto

Descripción: Módulo de Node.js que proporciona funcionalidades criptográficas como generación de hashes, cifrado, y otros algoritmos relacionados.

Securización: Utilizado correctamente, crypto permite cifrar datos sensibles y crear hashes seguros, esenciales para proteger contraseñas, tokens, y otros datos críticos.

5.3.10.5 Express-rate-limit

Descripción: Middleware que limita el número de solicitudes que un cliente puede hacer a la API en un tiempo determinado.

Securización: Protege contra ataques de fuerza bruta y denegación de servicio (DoS) al limitar el número de solicitudes permitidas desde una misma IP.

5.3.10.6 Morgan

Descripción: Middleware de registro de solicitudes HTTP para Node.js. Permite capturar y guardar detalles sobre cada solicitud que llega al servidor.

Securización: Aunque morgan en sí no es una medida de seguridad directa, el registro de solicitudes (log) es crucial para la detección y análisis de actividades sospechosas o maliciosas, facilitando la auditoría y el monitoreo.

5.3.10.7 Express-validator

Descripción: Conjunto de middlewares para validar y sanitizar los datos entrantes en las solicitudes HTTP.

Securización: Ayuda a prevenir ataques de inyección SQL, XSS y otras vulnerabilidades relacionadas con la entrada de datos al garantizar que los datos proporcionados por los usuarios cumplen con los criterios esperados y no contienen código malicioso.

5.3.10.8 App.disable('x-powered-by')

Descripción: Deshabilita el encabezado HTTP X-Powered-By que por defecto envía Express en las respuestas.

Securización: Eliminar este encabezado oculta el hecho de que tu aplicación está utilizando Express, lo que dificulta a los atacantes identificar el framework subyacente y explotar vulnerabilidades específicas conocidas

Fuente:

(*Security Best Practices for Express in Production*, s. f.)

(*Express - Infraestructura de aplicaciones web Node.js*, s. f.)

5.3.11 Chart.js V4.4.3

Chart.js proporciona un conjunto de tipos de gráficos, complementos y opciones de personalización de uso frecuente. Además de un conjunto razonable de tipos de gráficos integrados, puede utilizar tipos de gráficos adicionales mantenidos por la comunidad.

Además de eso, es posible combinar varios tipos de gráficos en un gráfico mixto (esencialmente, combinar varios tipos de gráficos en uno en el mismo lienzo).

Chart.js es altamente personalizable con complementos personalizados para crear anotaciones, hacer zoom o funcionalidades de arrastrar y soltar, por nombrar algunas cosas y demás.

Fuente: (*Chart.js | Chart.js*, s. f.)

5.3.12 VPS

En el contexto del alojamiento web, una máquina física robusta y de alto rendimiento suele hospedar múltiples servidores virtuales. Cada uno de estos servidores virtuales, conocidos como VPS (Virtual Private Server), opera con su propio sistema operativo y ofrece a los usuarios un acceso total con privilegios de administrador a través de Internet. Esto permite que cada administrador trabaje de manera autónoma, a pesar de compartir el mismo hardware subyacente con otros usuarios.

El hardware físico es gestionado por un componente de software denominado hipervisor. Este software es responsable de crear y gestionar los entornos virtuales, asignando a cada VPS una porción específica de los recursos físicos disponibles en el servidor, tales como la CPU, la memoria RAM y el espacio en disco. El hipervisor asegura que cada VPS funcione de manera aislada y eficiente, a pesar de compartir el mismo equipo físico.

Los privilegios de administrador, o acceso raíz, otorgados a los usuarios de un VPS permiten la instalación y configuración de una amplia variedad de aplicaciones compatibles con el sistema operativo seleccionado. Esto puede incluir software para servicios web, servidores de correo electrónico, y aplicaciones especializadas como sistemas de comercio electrónico o plataformas de blogs. En esencia, el acceso raíz proporciona a los usuarios la flexibilidad necesaria para personalizar y gestionar su entorno virtual según sus necesidades específicas.

Fuente: (*VPS*, 2023)

Para securizar el VPS se detalló algunas reglas sobre su firewall como la restricción de ciertos IPS para el acceso remoto y entre otras características de entrada y salidas de puertos, además rastreo de accesos y logs de cualquier modificación.

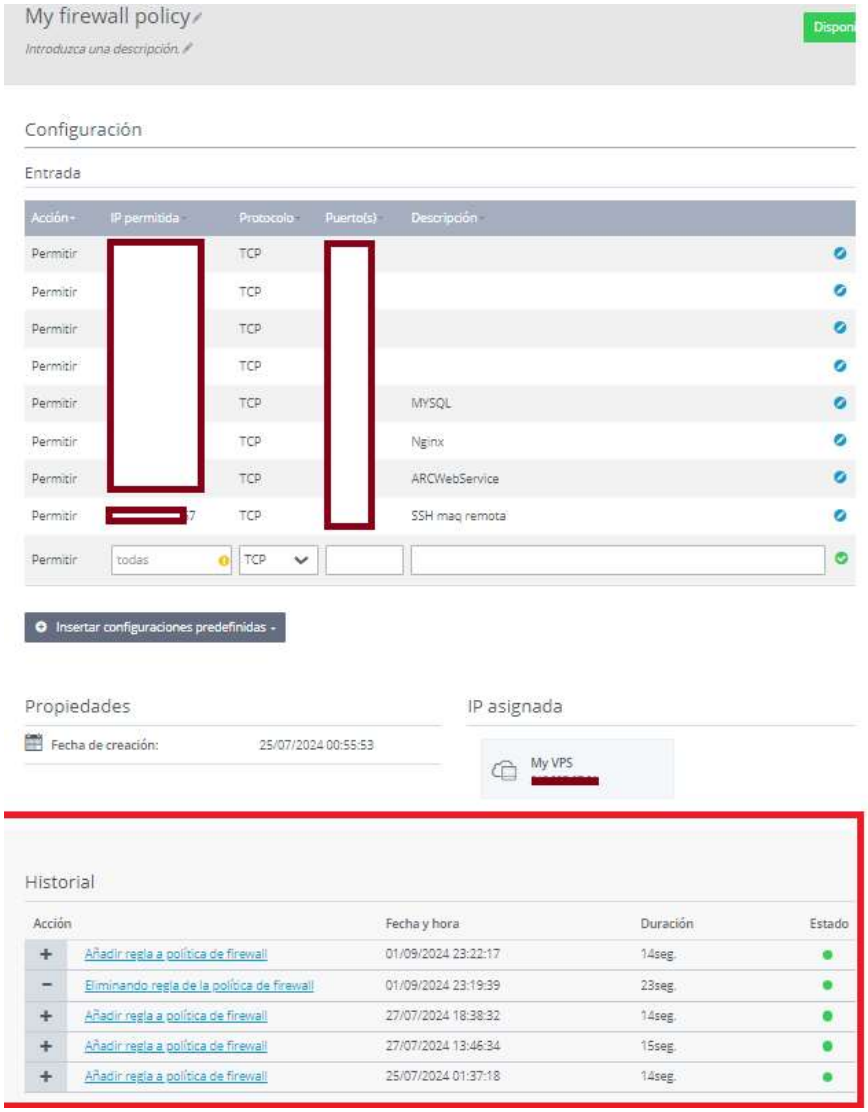


Ilustración 3.- Politicas de Firewall del VPS, muetra historial de modificación

5.3.13 Node V 20.15.1

Node.js es un entorno de ejecución de JavaScript multiplataforma, de código abierto y gratuito que permite a los desarrolladores crear servidores, aplicaciones web, herramientas de línea de comandos y scripts.

Fuente: (*Node.Js — Run JavaScript Everywhere*, s. f.)

La securización sobre node se hizo generando un entorno virtual para mantener el versionado e instalando la versión más reciente compatible con las herramientas de seguridad necesarias para el webservice en Express.

5.4 Topología de la aplicación

Entendiendo las tecnologías base que se han descrito anteriormente procedo a mostrar la topología de la aplicación.

Ilustración 4.- Topología de la aplicación

5.5 Desarrollo de la aplicación

5.5.1 Configuración del proyecto y programación básica

La aplicación utiliza el sistema de navigate para navegar entre fragmentos, usa JDK JAVA 17, sistema de binding y corountines para peticiones asincrónicas y controlar el buen funcionamiento de este.

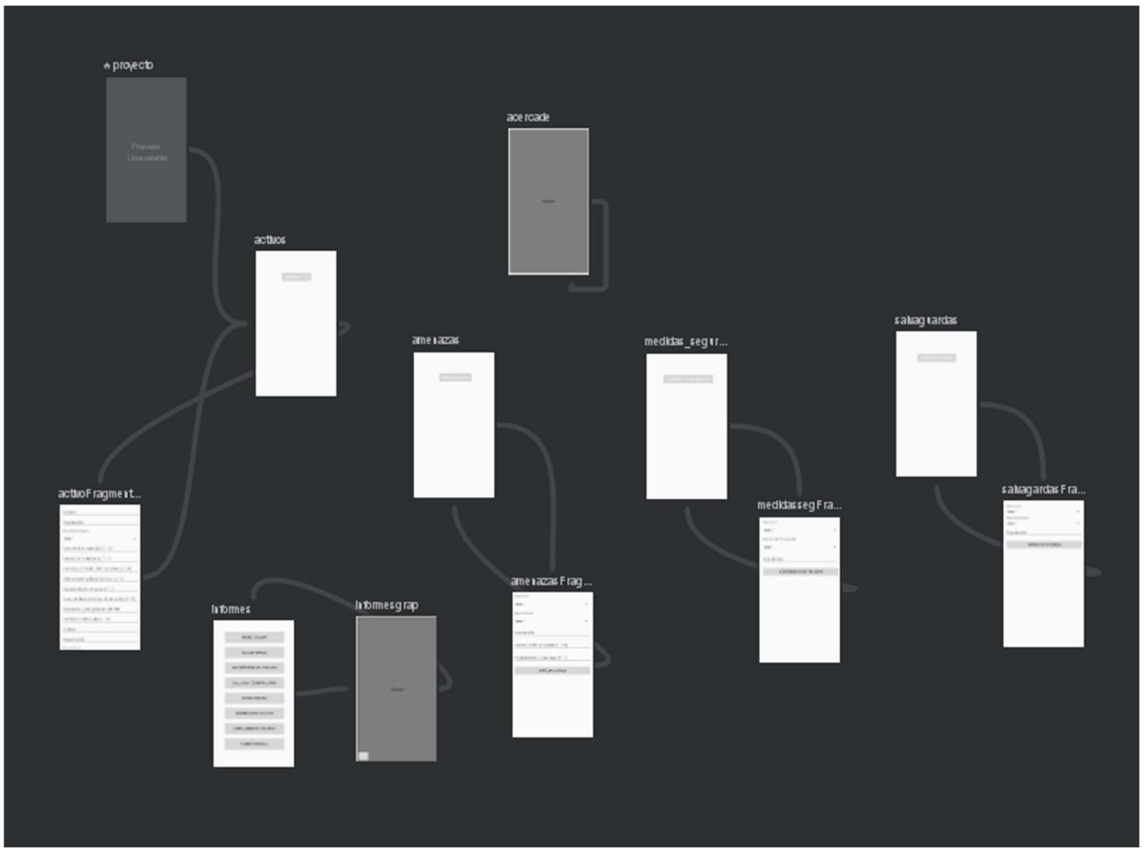


Ilustración 5.- Modelo de navegacion entre fragmentos

El modelo de Navigation en Android suele considerarse una mejora respecto a los Intents para la gestión de la navegación entre pantallas en una aplicación por varias razones:

a. Manejo de la pila de backstack
b. Simplificación de la navegación
c. Argumentos y datos entre pantallas
d. Integración con componentes modernos
e. Transiciones y animaciones

Al usar Navigation se reduce del riesgo de exposición de datos sensibles , el control centralizado de la navegación, gestión de datos de manera segura, ya que al pasar datos a través de extras en intents, hay un mayor riesgo de que datos sensibles puedan ser manipulados o interceptados si no se implementan medidas adecuadas de protección, evitar vulnerabilidades comunes, pues reduce la complejidad en el manejo de la navegación y los datos, lo que puede ayudar a evitar vulnerabilidades comunes asociadas con la gestión manual de la navegación y el paso de datos entre actividades como solían tener los Intents que por ser más susceptible a vulnerabilidades si los intents no se manejan correctamente, pueden ser vulnerables a ataques de inyección de generar intents o exposición accidental de datos sensibles.

5.5.2 Securización en Android y permisos

5.5.2.1 Introducción a los Permisos en Android

Permisos: Los permisos permiten a las aplicaciones acceder a recursos y datos sensibles del dispositivo. Android utiliza un sistema de permisos para proteger la privacidad y la seguridad del usuario.

Permisos de Nivel de Sistema: Algunos permisos afectan al sistema y se solicitan a nivel de sistema operativo. Estos permisos son críticos para el funcionamiento de la aplicación y pueden requerir aprobación especial.

5.5.2.2 Tipos de Permisos

- Permisos Normales: Son permisos que no afectan la privacidad del usuario. Las aplicaciones no necesitan solicitar la aprobación del usuario para estos permisos. Ejemplos incluyen el permiso para acceder al estado de la red.
- Permisos Peligrosos: Estos permisos afectan la privacidad del usuario o el funcionamiento del dispositivo. Requieren la aprobación explícita del usuario en tiempo de ejecución. Ejemplos incluyen el acceso a la cámara o a la ubicación.

5.5.2.3 Solicitud de Permisos

- Permisos en Tiempo de Ejecución: Desde Android 6.0 (API nivel 23), las aplicaciones deben solicitar permisos peligrosos en tiempo de ejecución. Los usuarios deben otorgar permisos explícitamente mientras usan la aplicación.
- Declaración de Permisos en el Manifiesto: Los permisos deben ser declarados en el archivo AndroidManifest.xml. Aunque no garantiza la concesión, es necesario para informar al sistema y al usuario sobre los permisos requeridos.

5.5.2.4 Manejo de Permisos

- Solicitar Permisos: Usa el método requestPermissions() para solicitar permisos peligrosos. Verifica si se han concedido con checkSelfPermission().
- Manejo de la Respuesta del Usuario: Implementa un método de callback, onRequestPermissionsResult(), para manejar la respuesta del usuario a las solicitudes de permisos.

5.5.2.5 Mejorar la Experiencia del Usuario

- Solicitar Permisos de Manera Contextual: Solicita permisos en el momento adecuado para mejorar la experiencia del usuario y la aceptación. Explica por qué se necesita el permiso antes de solicitarlo.
- Solicitudes de Permiso Graduales: Solicita permisos adicionales solo cuando sean necesarios para la funcionalidad específica.

5.5.2.6 **Actualización de Permisos y Versiones de Android**

- Compatibilidad hacia atrás: La compatibilidad con versiones anteriores de Android puede requerir el uso de métodos y permisos específicos.
- Permisos en Versiones Recientes: Las versiones recientes de Android pueden introducir cambios en los permisos, y los desarrolladores deben estar al tanto de estas actualizaciones.

5.5.2.7 Conclusión sobre los permisos

Los permisos en Android son una parte esencial para garantizar la privacidad y la seguridad del usuario. Las aplicaciones deben manejar los permisos con cuidado, solicitarlos de manera contextual y mantener la compatibilidad con las versiones del sistema operativo.

Este resumen cubre los puntos clave del artículo y proporciona una visión general de cómo manejar permisos en aplicaciones Android. Si necesitas más detalles o tienes preguntas específicas, no dudes en preguntar.

Fuente: (*Solicita permisos de tiempo de ejecución | Android Developers*, s. f.)

5.5.3 Consideraciones de Privacidad y Seguridad

- Uso Responsable: Usa permisos con responsabilidad y solo solicita los necesarios para la funcionalidad de tu aplicación.
- Educación al Usuario: Educa a los usuarios sobre el uso de permisos y cómo proteger su privacidad.

5.5.4 Seguridad con Protocolos de Red en Android

5.5.4.1 Introducción a SSL/TLS

SSL/TLS: SSL (Secure Sockets Layer) y su sucesor TLS (Transport Layer Security) son protocolos que proporcionan una capa de seguridad para las comunicaciones en redes. Se utilizan para cifrar los datos transmitidos entre clientes y servidores, garantizando que la información sea confidencial y no pueda ser manipulada o leída por terceros.

5.5.4.2 Configuración de Seguridad de Red

Configuración Básica: Android utiliza un archivo de configuración de seguridad de red (network-security-config.xml) para gestionar la seguridad de las conexiones de red. Este archivo permite especificar certificados, dominios y políticas de seguridad.

(*Configuración de seguridad de la red | App quality*, s. f.)

5.5.4.3 Pruebas: Pruebas funcionales de debug, en reléase y de usuario

Al desarrollar y desplegar una aplicación en Kotlin para Android, es crucial seguir buenas prácticas tanto en la fase de pruebas y depuración como en la de lanzamiento (release) para garantizar que la aplicación sea segura y eficiente como estas prácticas.

5.5.5 Pruebas y Debugging (Depuración)

5.5.5.1 Pruebas Unitarias y de Integración

Pruebas Unitarias: Asegúra de que las funciones y métodos individuales funcionencomo se espera.

Pruebas de Integración: Valida que los diferentes módulos de la aplicación interactúan correctamente.

5.5.5.2 Pruebas de UI

Pruebas de Interfaz de Usuario (UI): Garantiza que la experiencia del usuario sea fluida.

Pruebas de Compatibilidad: Asegura de que la aplicación funciona correctamente en diferentes versiones de Android y dispositivos.

5.5.6 Depuración Eficiente

Logs con Logcat: Usa Logcat para depurar y visualizar los registros de la aplicación, asegurándo de que no queden logs sensibles o innecesarios en el código de producción.

Puntos de Ruptura (Breakpoints): Utiliza breakpoints en Android Studio para detener la ejecución del código y analiza el estado del programa.

Depuración Remota: Si es necesario, usa herramientas como ADB (Android Debug Bridge) para depurar aplicaciones en dispositivos físicos.

5.5.7 Manejando Errores y Excepciones

Captura de Excepciones: Maneja correctamente las excepciones para evitar caídas inesperadas y proporcionar una experiencia de usuario robusta.

Informes de Errores: Implementa herramientas como Crashlytics para recibir informes detallados de errores en tiempo real.

5.5.8 Optimización para Release

5.5.8.1 Minimización y Ofuscación del Código

ProGuard/R8: Utiliza ProGuard o R8 para ofuscar el código en el APK final, lo que dificulta la ingeniería inversa y reduce el tamaño de la aplicación.

Shrink Resources: Activa la eliminación de recursos no utilizados (shrinkResources) para optimizar el tamaño del APK.

5.5.8.2 Configuraciones de Seguridad

Eliminar Debugging: Asegúra de deshabilitar cualquier opción de depuración en la versión de release (android:debuggable="false" en el AndroidManifest.xml).

Proteger Claves y Certificados: Utiliza el Android Keystore para gestionar claves criptográficas y evita almacenar claves sensibles en el código fuente.

Firmar el APK: Firma tu aplicación con una clave privada antes de lanzarla, asegurando la autenticidad y seguridad del APK.

5.5.9 Performance y Eficiencia

Perfilamiento de la Aplicación: Usa el profiler de Android Studio para detectar problemas de rendimiento, como consumo excesivo de memoria, CPU o batería.

Lazy Loading: Implementa el lazy loading para cargar recursos y datos solo cuando sean necesarios, mejorando la eficiencia y el tiempo de inicio de la aplicación.

Optimización de la Red: Usa bibliotecas eficientes como Retrofit y activa la compresión de datos para minimizar el consumo de datos y mejorar la velocidad.

5.5.10 Pruebas Funcionales y de Usuario Final

5.5.10.1 Pruebas Beta y A/B Testing

Pruebas Beta: Lanza versiones beta de la aplicación a un grupo selecto de usuarios para recibir retroalimentación antes del lanzamiento final.

A/B Testing: Realiza pruebas A/B para evaluar cómo diferentes versiones de la UI afectan el comportamiento del usuario.

5.5.10.2 Revisión de Permisos

Minimizar Permisos: Solicita solo los permisos estrictamente necesarios para el funcionamiento de la aplicación y explícalos claramente a los usuarios.

Verificación de Permisos: Usa el modelo de permisos en tiempo de ejecución de Android para manejar la concesión o denegación de permisos de manera adecuada.

5.6.1 Control de Versiones y Despliegue

Gestión de Versiones: Incrementa adecuadamente el número de versión y el código de la versión (versionCode y versionName) para cada nueva release.

CI/CD: Implementa pipelines de Integración Continua/Entrega Continua (CI/CD) para automatizar la construcción, pruebas y despliegue de tu aplicación

5.6 Lanzamiento

La generación del APK o Lanzamiento compilado final es firmado utilizando un. keystore y se compila en formato .apk para la instalación directa y una compilación tipo. aab para una versión futura que se pudiera incluir en el Google Play Store.

El sistema Android Keystore te permite almacenar claves criptográficas en un contenedor para que resulte más difícil extraerlas del dispositivo. Una vez que las claves se encuentran en el almacén de claves, puedes usarlas para operaciones criptográficas y el material de claves restante no se puede exportar. Además, el sistema Keystore te permite restringir cuándo y cómo se pueden usar las claves. Por ejemplo, cuando se solicita la autenticación del usuario para el uso de la clave o se restringen las claves para usarlas solo en ciertos modos criptográficos. Para obtener más información, consulta la sección Funciones de seguridad.

La API de KeyChain, que se introdujo en Android 4.0 (API nivel 14), y la función del proveedor de Android Keystore, que se introdujo en Android 4.3 (API nivel 18), usan el sistema Keystore. En este documento, se explica cómo y cuándo debe usarse el proveedor del sistema Android Keystore.

Fuente: (*Sistema Android Keystore | App quality*, s. f.)

6. Resultados

Los resultados obtenidos de la aplicación se reflejan de manera tangible a través de la aplicación compilada y testeada, con informes que proporcionan una representación detallada de una empresa hipotéticamente analizada. Estos informes destacan diversas áreas de deficiencia en relación con la gestión de activos, costos asociados y otros factores críticos. La información proporcionada es útil tanto para la toma de decisiones actuales como para la planificación estratégica futura.

Además, la aplicación ha demostrado ser efectiva en captar la atención del usuario final al ofrecer un entorno amigable y fácil de entender. Este aspecto contrasta positivamente con herramientas como MicroPilar, que, aunque potente, no ha logrado generar una impresión positiva entre diversos estudiantes del máster en ciberseguridad debido a su complejidad y falta de claridad.

Una validación adicional de la aplicación se ha llevado a cabo comparando los resultados generados con reportes reales. Los informes producidos por la aplicación han cumplido con éxito su propósito, proporcionando datos fiables que respaldan la toma de decisiones empíricas. Este proceso de comparación ha demostrado que la aplicación no solo es efectiva en la simulación y análisis de escenarios hipotéticos, sino que también ofrece resultados que se alinean con las expectativas y necesidades reales en la toma de decisiones empresariales de pequeñas PYMEs.

7. Conclusiones

La implementación y validación de los requisitos establecidos en los apartados previos han permitido concluir que la seguridad es un aspecto fundamental tanto en el desarrollo de aplicaciones como en su enseñanza. A través del proceso de construcción y evaluación de la aplicación, se ha adquirido un profundo conocimiento sobre los lineamientos de seguridad. Esta comprensión ha sido crucial para diseñar una herramienta que, se espera, pueda ser utilizada y mejorada en el futuro por la universidad, otros estudiantes, y potencialmente, contribuir al ámbito académico y a pequeñas PYMEs.

Las pruebas realizadas han generado informes satisfactorios que reflejan que las expectativas planteadas se han cumplido. Estos informes, elaborados con gran dedicación y esfuerzo, han demostrado la eficacia de las medidas de seguridad implementadas, garantizando una realidad confiable en cuanto a la protección de activos y la integridad del sistema. La aplicación no solo cumple con los estándares de seguridad exigidos básicos, sino que también ofrece una plataforma que apoya el aprendizaje en ciberseguridad, gestión, análisis de riesgos y cumplimiento de lineamientos legales.

8. Relación con los estudios

Para el desarrollo del trabajo he aplicado muchos conocimientos obtenidos durante la realización del Máster de Ciberseguridad y Ciberinteligencia (MUCC).

Sobre Aspectos Legales y Deontológicos de la Ciberseguridad, ha sido fundamental para realizar este trabajo, pues por fin he entendido la importancia de los temas legales sobre todo el tema de ciberseguridad y como es de crucial proteger los activos, más que todo los activos de información o relacionados a estos, un tema que se abordó bastante en el máster.

Gracias a la asignatura de CS (Ciberconciencia Situacional), he concientizado más el hecho de los objetivos de ciber inteligencia y como podrían ser afectos, al desarrollar los formularios se ha tomado muy en cuenta estos.

Usando como base la asignatura de Desarrollo y despliegue seguro es que se ha podido completar de manera adecuada y optima el despliegue de la aplicación, más que todo sobre la parte técnica.

Gracias a la asignatura de Informática Forense y análisis de Malware he considero el tema de los reportes como algo que podría utilizarse para una posible auditoria forense, siguiendo los lineamientos que me ofrecía la asignatura.

La formación proporcionada por la universidad, complementada con mi experiencia laboral y los conocimientos adquiridos a lo largo del máster, ha sido fundamental para la exitosa culminación de este trabajo. Esta formación ha constituido una base sólida que no solo ha facilitado la realización satisfactoria del proyecto actual, sino que también ha sentado las bases para futuros desarrollos profesionales. En particular, estos conocimientos y habilidades adquiridos abren la posibilidad de emprender nuevos proyectos, incluyendo, quien sabe, la realización de auditorías informáticas en el futuro.

9. Trabajo Futuro

Se confía en que la herramienta desarrollada servirá como un recurso educativo eficaz, facilitando el estudio y la aplicación de conceptos clave en estos campos críticos, además la aplicación tiene el potencial de convertirse en una herramienta valiosa para las PYMEs.

10. Glosario de términos

Activo: En Magerit y el ENS, un activo se refiere a cualquier elemento de valor para la organización que requiere ser protegido, como sistemas de información, datos, infraestructuras, recursos humanos, etc.

Amenaza: Una situación potencial que puede explotar una vulnerabilidad específica de un activo y causar daño o pérdida.

Medidas de Seguridad: Conjunto de controles y procedimientos implementados para proteger los activos de la organización contra amenazas y riesgos identificados.

Riesgo: La posibilidad de que una amenaza explote una vulnerabilidad específica y cause daño a un activo. Se calcula como la combinación de la probabilidad de ocurrencia y el impacto potencial.

Salvaguarda: Medidas específicas implementadas para reducir o mitigar un riesgo a un nivel aceptable para la organización.

Análisis de Riesgos: Proceso sistemático de evaluar los riesgos potenciales que enfrenta una organización, identificando amenazas, evaluando vulnerabilidades y determinando la probabilidad e impacto de los eventos adversos.

Impacto: La consecuencia o el efecto negativo resultante de la materialización de un riesgo en un activo de la organización.

Valoración: Evaluación del valor y la importancia de los activos de información para determinar la necesidad de protección y asignación de recursos.

Probabilidad de Amenaza: La posibilidad de que una amenaza específica ocurra y afecte a un activo.

Valor de la Información: Importancia y relevancia de la información para la organización en términos de su confidencialidad, integridad y disponibilidad.

Impacto en el Negocio: Evaluación de las consecuencias comerciales, operativas y financieras de la pérdida de un activo o interrupción de un proceso crítico.

Función y Criticidad del Dispositivo: Importancia y nivel de criticidad de un dispositivo dentro de la infraestructura tecnológica de la organización.

Interconexión y Dependencias: Relaciones y conexiones entre diferentes sistemas y procesos dentro de la organización que pueden afectar la seguridad de la información.

Exposición a Amenazas: El grado en el que un activo o sistema de información está expuesto a diferentes tipos de amenazas potenciales.

Costo de Recuperación o Sustitución: El gasto estimado para restaurar un activo dañado o reemplazarlo en caso de pérdida.

Reputación y Cumplimiento: Impacto en la reputación y las obligaciones legales o regulatorias que pueden surgir como resultado de una violación de la seguridad de la información.

Factores Contextuales: Variables externas e internas que influyen en el entorno de seguridad de la información de la organización, como el contexto operativo, la normativa legal, etc.

Contaminación Mecánica: Interferencias físicas que pueden afectar el funcionamiento correcto de los equipos y sistemas.

Contaminación Electromagnética: Interferencias eléctricas o magnéticas que pueden causar fallos en los sistemas electrónicos.

Emanaciones Electromagnéticas: Emisiones involuntarias de radiación electromagnética que pueden ser interceptadas y comprometer la seguridad de la información.

LOG: Registros o logs de eventos y actividades que pueden ser utilizados para la auditoría y la investigación de incidentes de seguridad.

Errores de Re-Encaminamiento: Fallos en el proceso de redireccionamiento de datos o tráfico que pueden resultar en la pérdida de información o exposición a amenazas.

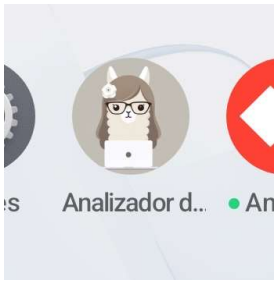
Ataques Intencionados - Repudio: Acciones maliciosas destinadas a negar la responsabilidad o el origen de una actividad específica en sistemas de información.

Claves Criptográficas: Códigos y algoritmos utilizados para cifrar y descifrar datos sensibles y asegurar la comunicación segura.

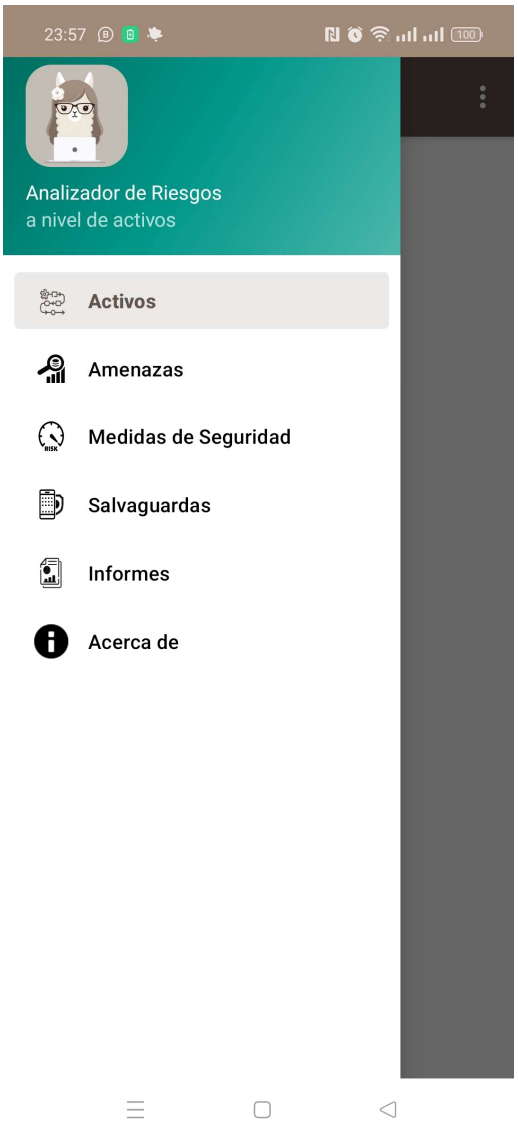
Equipamiento Auxiliar: Dispositivos y recursos adicionales utilizados para apoyar las operaciones de TI y comunicación dentro de la organización.

11. ANEXO I - Aplicación

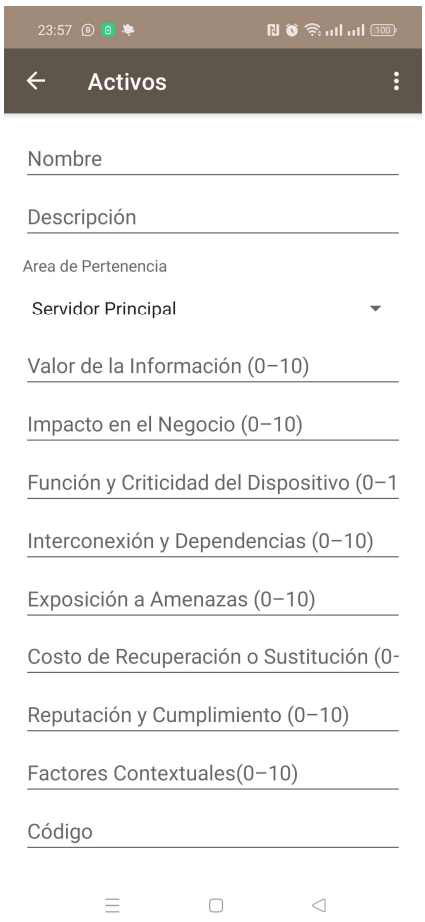
1.- Icono de la aplicación Análisis de Riesgos “ARC”



2.- Menú Principal de ARC



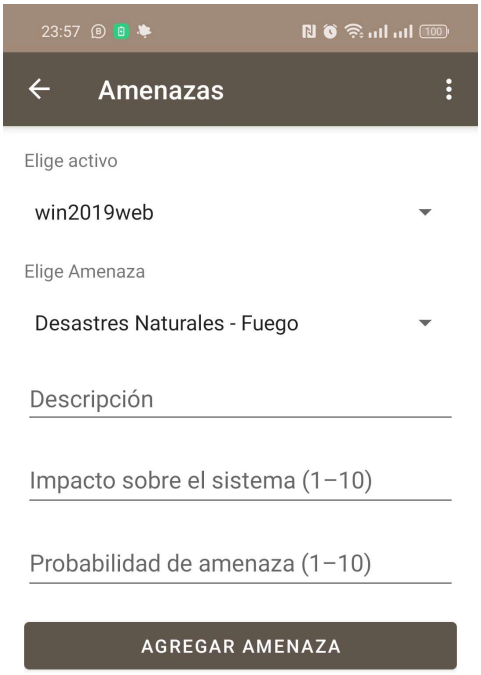
3.- Formulario de “Agregar Activo”



4.- Formulario de “Agregar Medidas de Seguridad”

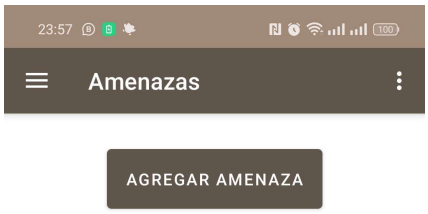
5.- Formulario de “Agregar Salvaguardas”

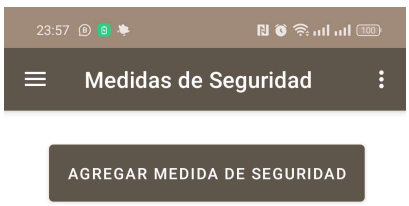
6.- Formulario de “Agregar Amenaza”

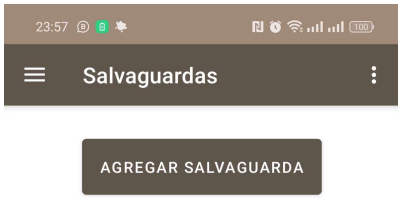


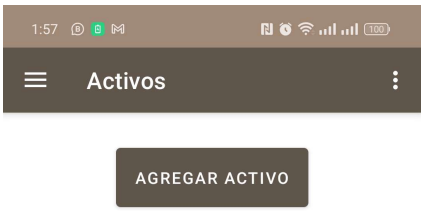
7.- Menu Informes

8.- Botones de acción para ir a los formularios

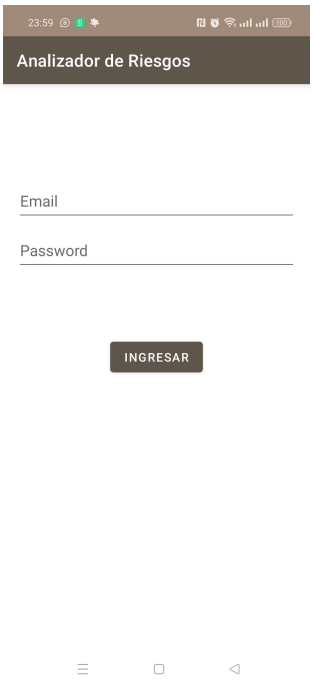


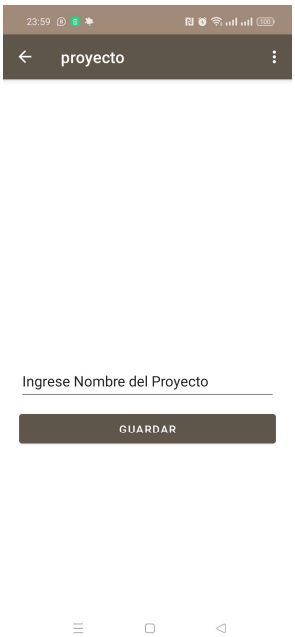






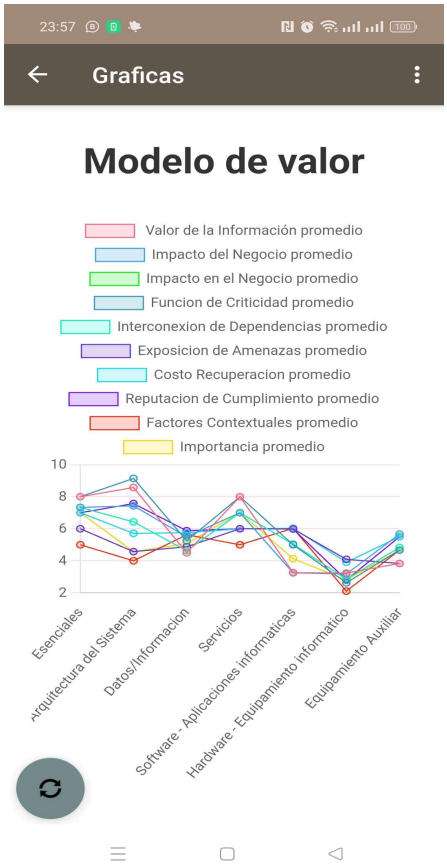
9.- Login y generacion o recuperacion de proyecto



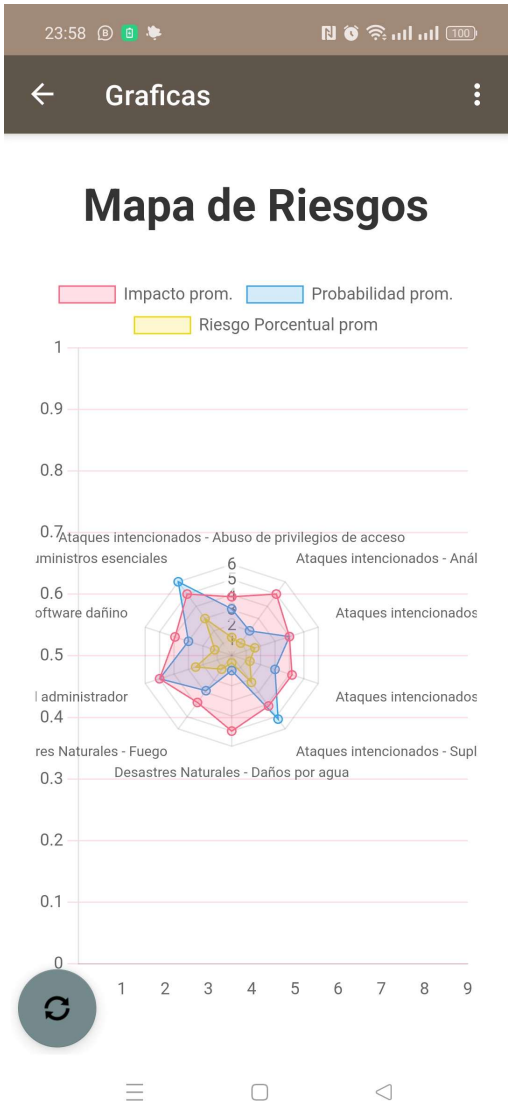


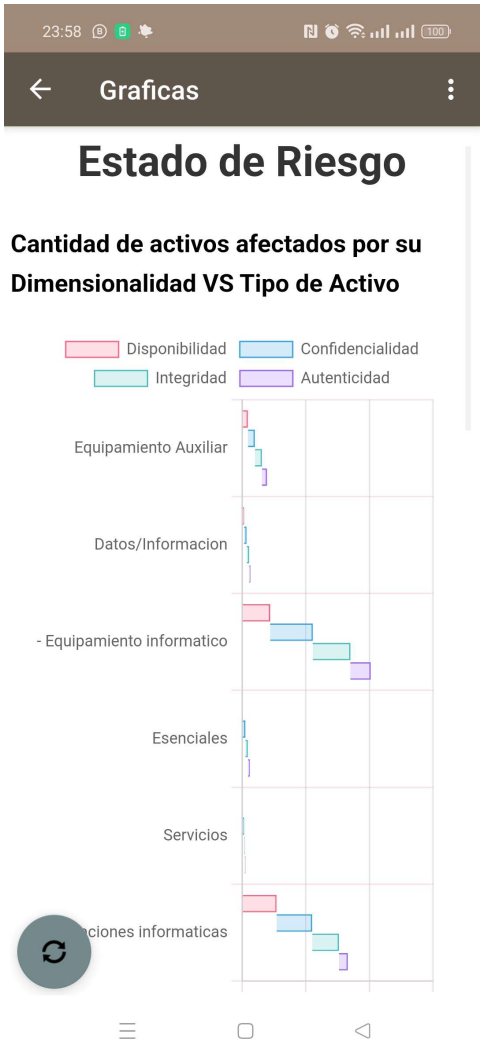
10.- Informes

10.a.- Modelo de Valor

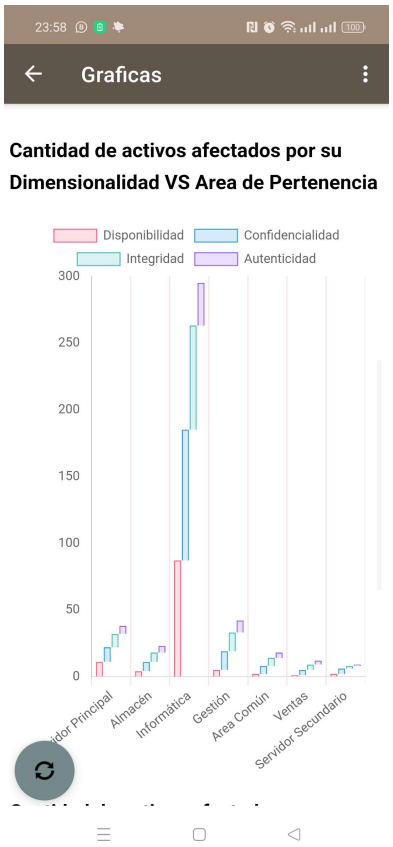


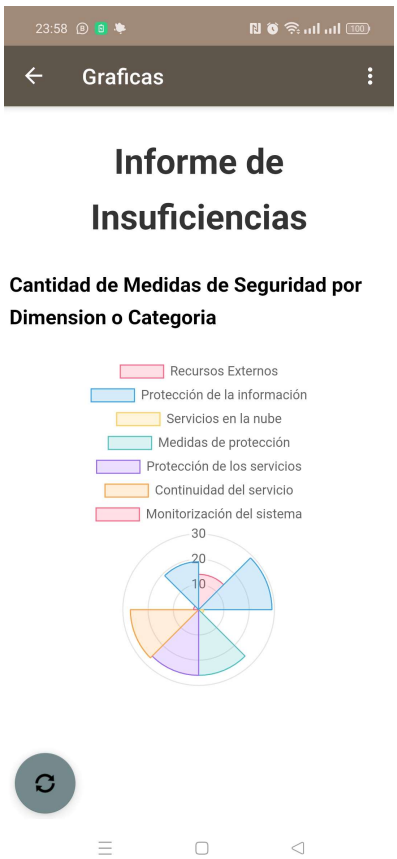
10.b.- Mapa de Riesgos

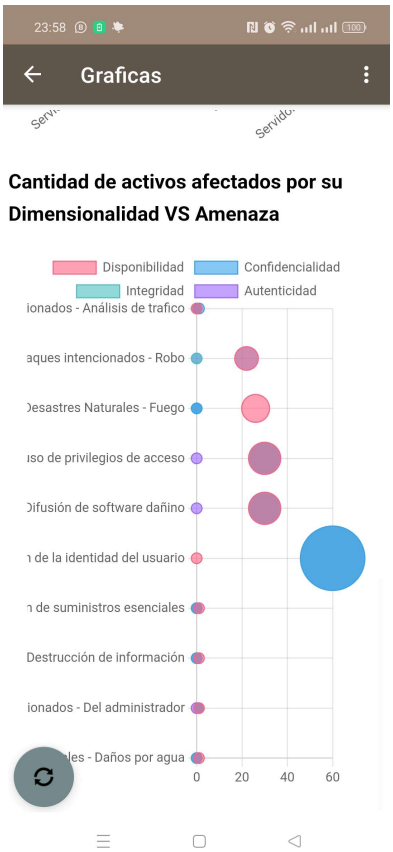




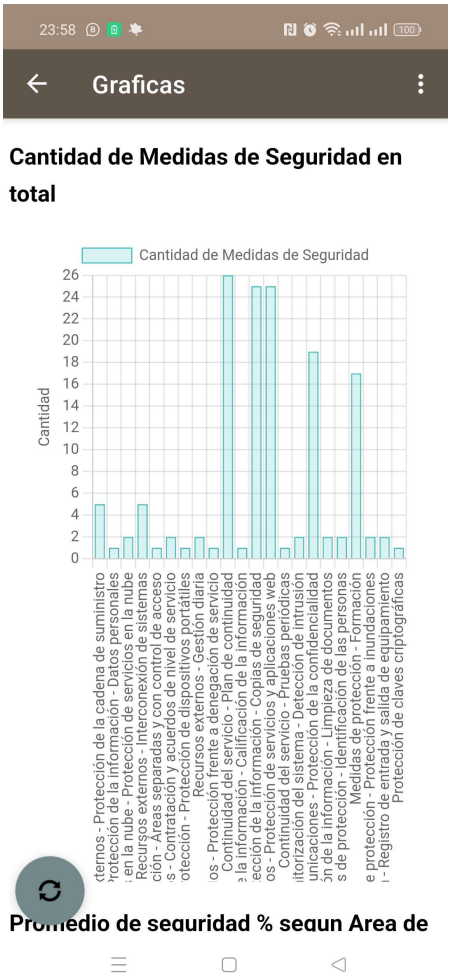
10 c.- Informes demás

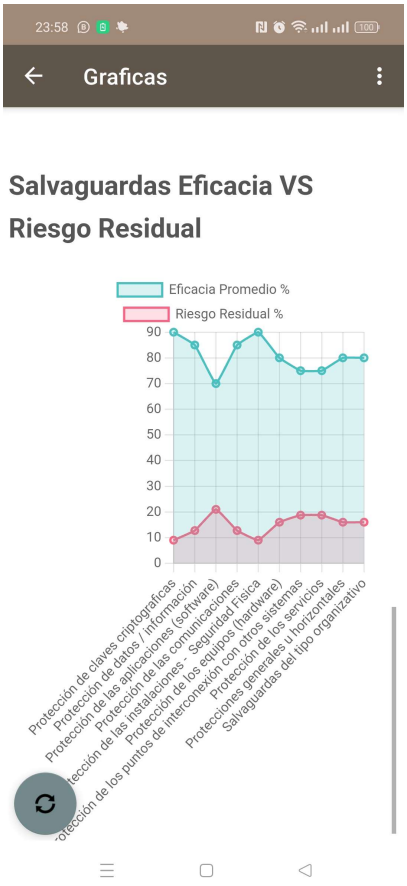


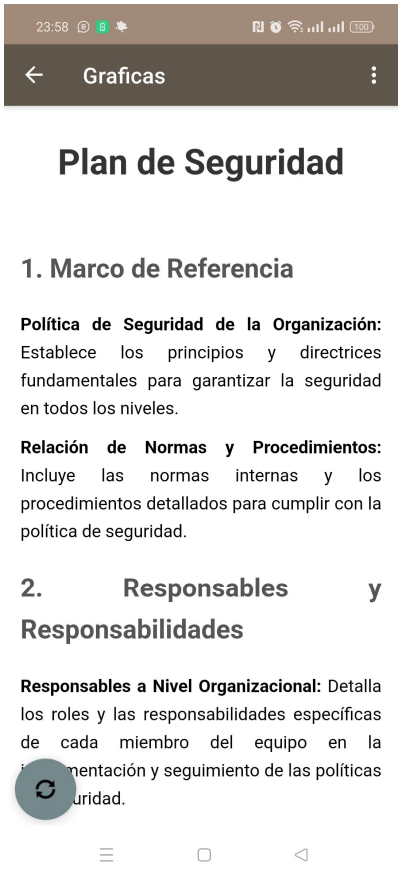


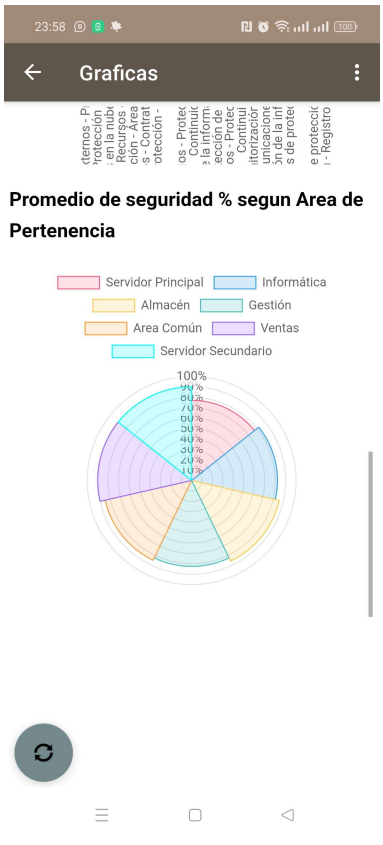


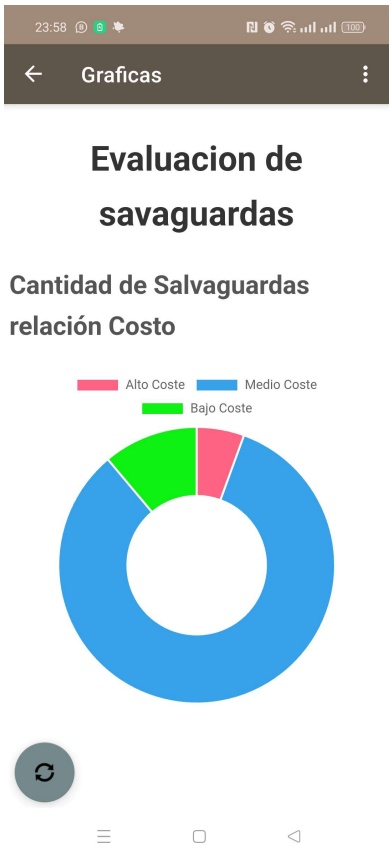

23:58
Graficas
Declaración de aplicabilidad
Por tipo de Activo
Total de Salvaguardas por tipo de activo
70
60
50
40
30
20
10
0
Equipamiento Auxiliar
Esenciales
Servicios

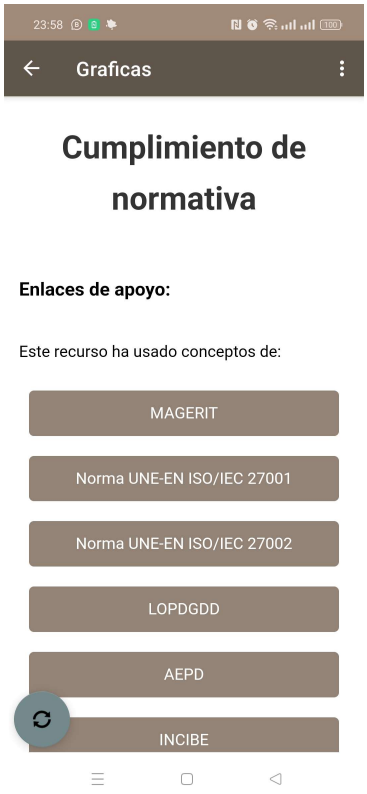

23:58
Graficas
Cantidad de Medidas de Seguridad en total
Cantidad de Medidas de Seguridad
Cantidad
26
24
22
20
18
16
14
12
10
8
6
4
2
0
Recursos externos - Gestión diaria
Continuidad del servicio - Plan de continuidad
Continuidad del servicio - Pruebas periódicas
Medidas de protección - Formación
Protección de claves criptográficas
Promedio de seguridad % segun Area de


23:58
Graficas
Salvaguardas Eficacia VS Riesgo Residual
Eficacia Promedio %
Riesgo Residual %
90
80
70
60
50
40
30
20
10
0
Protección de claves criptograficas
Protección de datos / información
Protección de las aplicaciones (software)
Protección de las comunicaciones
Protección de las instalaciones - Seguridad Física
Protección de los equipos (hardware)
Protección de los puntos de interconexión con otros sistemas
Protección de los servicios
Protecciones generales u horizontales
Salvaguardas del tipo organizativo


23:58
Graficas
Plan de Seguridad
1. Marco de Referencia
Política de Seguridad de la Organización: Establece los principios y directrices fundamentales para garantizar la seguridad en todos los niveles.
Relación de Normas y Procedimientos: Incluye las normas internas y los procedimientos detallados para cumplir con la política de seguridad.
2. Responsables y Responsabilidades
Responsables a Nivel Organizacional: Detalla los roles y las responsabilidades específicas de cada miembro del equipo en la

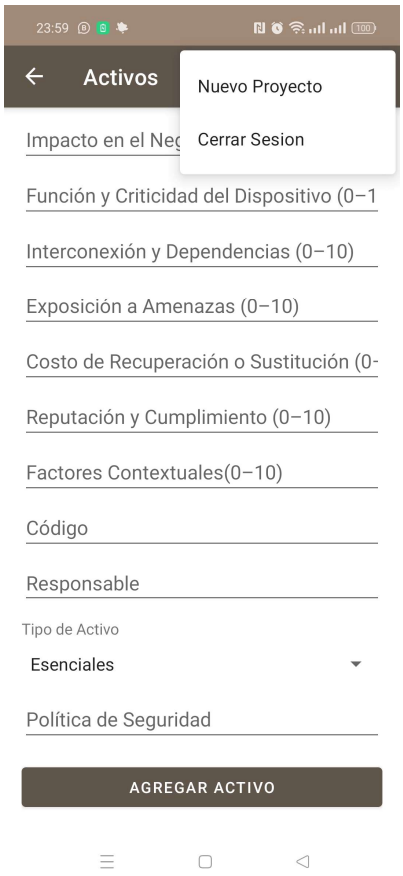

23:58
Graficas
Promedio de seguridad % segun Area de Pertenencia
Servidor Principal
Informática
Almacén
Gestión
Area Común
Ventas
Servidor Secundario
100%


23:58
Graficas
Evaluacion de savaguardas
Cantidad de Salvaguardas relación Costo
Alto Coste
Medio Coste
Bajo Coste


23:58
Graficas
Cumplimiento de normativa
Enlaces de apoyo:
Este recurso ha usado conceptos de:
MAGERIT
Norma UNE-EN ISO/IEC 27001
Norma UNE-EN ISO/IEC 27002
LOPDGDD
AEPD
INCIBE


23:58
Graficas
Enlaces de apoyo:
Este recurso ha usado conceptos de:
MAGERIT
Norma UNE-EN ISO/IEC 27001
Norma UNE-EN ISO/IEC 27002
LOPDGDD
AEPD
INCIBE
ENS
CCN

10.- Botones para cerrar sesión y generar nuevo proyecto



Recurso: Video demo, WebService y aplicación con extensión .apk:

https://upvedues-my.sharepoint.com/:f:/g/personal/ajimmor_upv_edu_es/Em2sJX8gp9FLqG8WEDX5jbABeruvggZN7ztaDyEZlBJltA?e=eN97vq

12. ANEXO II - Objetivos de Desarrollo Sostenible

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Procede**
ODS 1. **Fin de la pobreza.**				●
ODS 2. **Hambre cero.**				●
ODS 3. **Salud y bienestar.**				●
ODS 4. **Educación de calidad.**	●			
ODS 5. **Igualdad de género.**			●	
ODS 6. **Agua limpia y saneamiento.**				●
ODS 7. **Energía asequible y no contaminante.**	●			
ODS 8. **Trabajo decente y crecimiento económico.**	●			
ODS 9. **Industria, innovación e infraestructuras.**	●			
ODS 10. **Reducción de las desigualdades**.				●
ODS 11. **Ciudades y comunidades sostenibles**.		●		
ODS 12. **Producción y consumo responsables.**		●		
ODS 13. **Acción por el clima.**				●
ODS 14. **Vida submarina.**				●
ODS 15. **Vida de ecosistemas terrestres.**				●
ODS 16. **Paz, justicia e instituciones sólidas.**	●			
ODS 17. **Alianzas para lograr objetivos.**	●			

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

Con respecto a los objetivos de desarrollo sostenible he detallado de la forma mostrada en el cuadro anterior porque:

ODS 1.- No procede; La aplicación si bien apoya a la gestión mejor de recursos no se especifica que sean recursos de consumo humano sino mas bien a nivel de infrasestrtura informática de hardware y software.

ODS 2.- No procede; La aplicación no gestiona el hambre ni habla sobre el consumo de recursos para la salud o el consumo humano con respecto a la alimentación o similares.

ODS 3.- No procede; La salud es importante para gestionar diversos recursos de harware como tener precaución sobre elementos electromagnéticos o químicos pero la aplicación no se enfoca en ello especialmente.

ODS 4.- Alto; Pues la aplicación tiene como objetivo general apoyar la educación del estudiante sobre los temas que se infunden en el ámbito de la ciberseguridad y campos afines a este, por lo que la herramienta impulsaría claramente al objetivo de desarrollo sostenible sobre la educación de calidad, pues se espera como resultado que el estudiante o el usuario final tenga un concepto mucho más claro sobre la gestión de los activos en el ámbito empresarial, sobre el Esquema Nacional de Seguridad y la metodología que debería aplicar para llevar a cabo una auditoria (Magerit) o un control mejor de los recursos de hardware y software dentro de un ámbito privado comercial, alguna otra institución nacional, u otra que lo amerite así rigiéndose sobre los ISOS 27001 Y 27002.

ODS 5.- Bajo; En el área de la informática e ingenierías es bien sabido que el genero que se acostumbra observar o con el que se acostumbra estudiar es el género masculino, la aplicación no diferencia ni tiene relación alguna con el genero del cual vaya a usarlo pero, me parece que a nivel reflexivo que este creado por una ingeniera puede llegar a abrir puertas a muchas otras mujeres en el campo de la ciberseguridad y la Ciberinteligencia dándoles la oportunidad y mostrándoles que una mujer es capaz de trabajar en el área y desarrollar herramientas para el continuo aprendizaje desde un punto de vista quien sabe “femenino”.

OSD 6.- No procede; Simplemente porque no va relacionado de alguna forma con el tema del agua o el saneamiento.

ODS 7.- Alto; Una aplicación de reportes sobre energía asequible y no contaminante ofrece múltiples ventajas en términos de sostenibilidad y eficiencia. Al ser una herramienta digital, elimina la necesidad de generar reportes físicos, lo que reduce significativamente el consumo de papel y otros recursos asociados con la producción, impresión y distribución de documentos. Este enfoque no solo disminuye la deforestación y el uso de químicos tóxicos en la fabricación de papel, sino que también reduce la huella de carbono relacionada con el transporte y almacenamiento de esos informes.

Además, una aplicación digital puede proporcionar datos en tiempo real, lo que facilita una toma de decisiones más rápida y efectiva, permitiendo que los usuarios optimicen el uso de fuentes de energía más sostenibles. La accesibilidad de la información a través de una plataforma digital también promueve una mayor conciencia y educación sobre el consumo energético responsable, impulsando el cambio hacia prácticas más sostenibles.

La aplicación no solo evita la contaminación derivada del uso de materiales físicos, sino que también contribuye a la transición hacia un modelo energético más limpio y accesible al facilitar la gestión y el análisis eficiente de la energía, incluyendo a nivel de activos.

ODS 8.- Alto; Una aplicación que evalúa los riesgos asociados a activos es una herramienta clave para impulsar el trabajo decente y el crecimiento económico sostenible. Al identificar, monitorear y gestionar riesgos de manera eficiente, esta tecnología puede ayudar a las empresas a tomar decisiones informadas, protegiendo a los trabajadores y asegurando que las condiciones laborales sean más seguras y equitativas. Por ejemplo, la capacidad de predecir riesgos relacionados con la maquinaria, las instalaciones o los procesos productivos permite minimizar accidentes laborales, reducir el estrés de los empleados y promover un ambiente de trabajo más saludable.

Desde una perspectiva económica, una aplicación que gestiona los riesgos también contribuye al crecimiento económico al optimizar el uso de los activos empresariales. Al prevenir fallos costosos o incidentes que puedan interrumpir la producción, las empresas pueden operar de manera más eficiente, lo que se traduce en mayores ingresos, estabilidad económica y la creación de empleos de calidad. Al mejorar la seguridad y la estabilidad de las operaciones, se genera un entorno más atractivo para la inversión y se fortalece la capacidad de las empresas para expandirse y generar nuevas oportunidades laborales.

En resumen, esta aplicación no solo protege a los trabajadores al mitigar los riesgos inherentes a sus actividades, sino que también impulsa el crecimiento económico al asegurar que los activos sean gestionados de manera eficiente y responsable, lo que promueve un desarrollo más decente y justo.

ODS 9.- Alto; Cuando una persona busca información o alguna herramienta parecida en el Play Store o similares no se puede encontrar una que realmente ofrezca lo que esta aplicación promete, por lo que considero una herramienta innovadora y sencilla.

Ahora a nivel de industria, al identificar posibles riesgos en la gestión y operación de activos industriales e infraestructurales, la aplicación permite a las empresas anticiparse a fallos, reducir el tiempo de inactividad y optimizar el rendimiento de los recursos. Esto se traduce en operaciones más seguras y sostenibles, lo que impulsa tanto la innovación tecnológica como la mejora de las infraestructuras existentes, las empresas y gobiernos pueden planificar mejor las inversiones a largo plazo, optimizando los recursos y reduciendo los costos de mantenimiento no planificado. Esto fortalece la capacidad de crear infraestructuras más resilientes y adaptables a las necesidades futuras.

ODS 10.- No procede; La aplicación no tiene ningún fin sobre la reducción de las desigualdades al menos no en el uso y como va relacionado con los activos y no personas, no procedería en este caso.

ODS 11.- Medio; Si la aplicación se utilizara en una empresa que gestiona por ejemplo una smartcity o alguna parecida, es una herramienta valiosa para el desarrollo de ciudades y comunidades más sostenibles. Al monitorear y gestionar los activos urbanos, como edificios, redes de transporte, sistemas de energía y recursos hídricos, esta aplicación permite a los gestores urbanos identificar riesgos potenciales y tomar decisiones informadas que aseguren la resiliencia y sostenibilidad de la infraestructura. Esto reduce el impacto ambiental, optimiza el uso de los recursos y mejora la calidad de vida de los habitantes.

En el contexto de ciudades sostenibles, esta tecnología permite una gestión eficiente de los recursos y una planificación urbana más inteligente. Al prevenir fallos en infraestructuras críticas o desastres relacionados con la energía o el transporte, la aplicación ayuda a minimizar interrupciones en los servicios esenciales y evita el uso excesivo de materiales para reparaciones no planificadas.

ODS 12.- Medio; La aplicación que evalúa los riesgos asociados a activos es fundamental para promover una producción y consumo más responsable. Al proporcionar un análisis detallado y en tiempo real de los riesgos en la cadena de suministro, la manufactura y el uso de recursos, esta herramienta permite a las empresas optimizar sus procesos productivos, minimizar desperdicios y asegurar un uso más eficiente de los materiales. Esto no solo reduce el impacto ambiental, sino que también fomenta prácticas más sostenibles a lo largo del ciclo de vida de los activos.

En cuanto a la producción, esta tecnología facilita la transición hacia un modelo más circular, al identificar áreas donde se pueden reutilizar materiales o minimizar el uso de recursos naturales. Al anticipar fallos o ineficiencias en los activos, las empresas pueden reducir el desperdicio de energía, agua y otros insumos esenciales, alineándose con estándares más altos de sostenibilidad. Además, al mitigar los riesgos de fallos en la producción, se garantiza una operación más eficiente y segura, lo que contribuye a una menor huella ecológica.

ODS 13.- No procede; La aplicación no tiene relación alguna.

ODS 14.- No procede; La aplicación no tiene relación alguna.

ODS 15.- No procede; Si bien esta relacionada con los activos terrestres no procede sobre los "ecosistemas" mas sobre los sistemas tecnológicos e informáticos.

ODS 16.- Alto; La aplicación va fuertemente ligada al concepto del Esquema Nacional de Seguridad, cuyo motivo principal es promover la seguridad, la justicia y la paz sobre el control de los recursos de hardware y software para proteger así a sus usuarios finales en temas de información, datos y otros.

puede desempeñar un papel crucial en la promoción de la paz, la justicia y el fortalecimiento de las instituciones sólidas. Al proporcionar una evaluación precisa de los riesgos en infraestructuras críticas, recursos y procesos organizativos, esta herramienta contribuye a mejorar la transparencia, la responsabilidad y la eficiencia dentro de las instituciones, lo que a su vez refuerza la confianza pública y fomenta entornos más justos y equitativos.

Desde el punto de vista de la justicia, la aplicación puede ayudar a identificar posibles vulnerabilidades o irregularidades en la gestión de los recursos públicos y activos institucionales, lo que permite una mejor supervisión y control. Al prevenir el mal uso de los recursos o la corrupción dentro de las instituciones, se promueve un entorno donde la rendición de cuentas es una prioridad. Esto es fundamental para garantizar que los sistemas judiciales y gubernamentales actúen de manera justa y equitativa, apoyando la construcción de una sociedad más pacífica y transparente.

ODS 17.- Alto; Es una herramienta poderosa para fortalecer las alianzas entre diferentes sectores, fomentando la colaboración y facilitando el cumplimiento de objetivos comunes, como los ODS (Objetivos de Desarrollo Sostenible). Al proporcionar datos precisos y en tiempo real sobre la gestión de activos, la aplicación mejora la comunicación y coordinación entre gobiernos, empresas, ONGs y comunidades, permitiendo que los esfuerzos colectivos sean más eficientes y efectivos.

En el contexto de alianzas, esta herramienta digital promueve la transparencia y el intercambio de información clave entre los diferentes actores, lo que es esencial para generar confianza y construir relaciones sólidas. Al identificar riesgos compartidos, como los relacionados con infraestructuras, recursos naturales o la cadena de suministro, las organizaciones pueden colaborar para mitigar estos problemas de manera conjunta, optimizando recursos y maximizando el impacto de las soluciones.

13. Bibliografía y Referencias

2.- REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) | AEPD. (s. f.). Recuperado 8 de julio de 2024, de https://www.aepd.es/preguntas-frecuentes/2-rgpd

Blanco, P., Puras, J., Fumero, A., Werterski, A., & Rodríguez, P. (s. f.). *Metodología de desarrollo ágil para sistemas móviles Introducción al desarrollo con Android y el iPhone*.

BOE-A-2022-7191 Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. (s. f.). Recuperado 8 de julio de 2024, de https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191

CCN-CERT - Soluciones. (s. f.). Recuperado 6 de enero de 2024, de https://www.ccn-cert.cni.es/es/soluciones-seguridad?format=html

Cohn, M. (2010). *Succeeding with agile: Software development using Scrum*. Addison-Wesley.

Cómo descargar Android Studio y App Tools. (s. f.). Android Developers. Recuperado 2 de septiembre de 2024, de https://developer.android.com/studio?hl=es-419

CONAN mobile | Ciudadanía | INCIBE. (s. f.). Recuperado 8 de julio de 2024, de https://www.incibe.es/ciudadania/herramientas/conan-mobile

Configuración de seguridad de la red | App quality. (s. f.). Android Developers. Recuperado 2 de septiembre de 2024, de https://developer.android.com/privacy-and-security/security-config?hl=es-419

Documento_Norma_UNE-EN_ISO-IEC_27001 MINTUR.pdf. (s. f.). Recuperado 8 de julio de 2024, de https://www.industriaconectada40.gob.es/difusion/Documents/Documento_Norma_UNE-EN_ISO-IEC_27001%20MINTUR.pdf

Entidad Nacional de Acreditación. (2023). En *Wikipedia, la enciclopedia libre*. https://es.wikipedia.org/w/index.php?title=Entidad_Nacional_de_Acreditaci%C3%B3n&oldid=148527870

Express—Infraestructura de aplicaciones web Node.js. (s. f.). Recuperado 2 de septiembre de 2024, de https://expressjs.com/es/

Gironés, J. T. (2019). *El gran libro de Android*. Alpha Editorial.

Industria Conectada 4.0—Normas UNE-EN ISO/IEC 27001 y UNE-EN ISO/IEC 27002 para la seguridad de la información. (s. f.). Recuperado 8 de julio de 2024, de https://www.industriaconectada40.gob.es/difusion/noticias/Paginas/Normas-UNE-EN-ISOIEC-27001-UNE-EN-ISOIEC-27002-seguridad-de-informaci%C3%B3n.aspx

Kotlin y Android. (s. f.). Android Developers. Recuperado 8 de julio de 2024, de https://developer.android.com/kotlin?hl=es-419

Layton, M. C., & Ostermiller, S. J. (2017). *Agile project management* (2nd edition). Wiley.

MariaDB Foundation. (s. f.). MariaDB.Org. Recuperado 2 de septiembre de 2024, de https://mariadb.org/

Modificación de la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales | AEPD. (2023, mayo 9). https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/modificacion-ley-organica-proteccion-datos-personales-y-garantia-derechos-digitales

Nginx Proxy Manager. (s. f.). Recuperado 2 de septiembre de 2024, de https://nginxproxymanager.com/

Node.js—Run JavaScript Everywhere. (s. f.). Recuperado 2 de septiembre de 2024, de https://nodejs.org/en

Norma Internacional - ISO 31000, 31000.

PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. (s. f.). Recuperado 6 de enero de 2024, de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

PILAR - ¿Qué es el análisis de riesgos? (s. f.). Recuperado 8 de julio de 2024, de https://pilar.ccn-cert.cni.es/index.php/analisis-de-riesgos/analisis-de-riesgos-pilar

Qué es el ENS. (s. f.). Esquema Nacional de Seguridad. Recuperado 8 de julio de 2024, de https://ens.ccn.cni.es/es/que-es-el-ens

Sistema Android Keystore | App quality. (s. f.). Android Developers. Recuperado 1 de septiembre de 2024, de https://developer.android.com/privacy-and-security/keystore?hl=es-419

Solicita permisos de tiempo de ejecución | Android Developers. (s. f.). Recuperado 2 de septiembre de 2024, de https://developer.android.com/training/permissions/requesting?hl=es-419