ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA DE SISTEMAS

DESARROLLO DE APLICACIÓN WEB PARA ANÁLISIS DE RIESGOS EN HOGARES INTELIGENTES CON ECOSISTEMAS IoT

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS INFORMÁTICOS Y DE COMPUTACIÓN

ALEX MARCELO AREVALO PROAÑO
alex.arevalo03@epn.edu.ec

MARCO PATRICIO PARCO GUALPA
marco.parco@epn.edu.ec

DIRECTOR: ING. ROBERTO OMAR ANDRADE PAREDES
roberto.andrade@epn.edu.ec

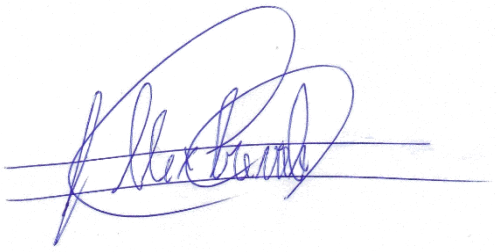
CODIRECTOR: DR. SANG GUUN YOO
sang.yoo@epn.edu.ec

Quito, enero 2022

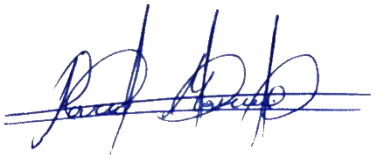
DECLARACIÓN

Nosotros, Alex Marcelo Arevalo Proaño y Marco Patricio Parco Gualpa, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.



Alex Marcelo Arevalo Proaño



Marco Patricio Parco Gualpa

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Alex Marcelo Arevalo Proaño y Marco Patricio Parco Gualpa bajo nuestra supervisión.

Ing. Roberto Omar Andrade Paredes

DIRECTOR DE PROYECTO

Ing. Sang Guun Yoo, PhD.

CODIRECTOR DE PROYECTO

DEDICATORIA – ALEX AREVALO

A mis padres y hermanos por quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo, valentía y de no temer las adversidades.

Alex

DEDICATORIA – MARCO PARCO

A mis padres, hermanos, a mi abuelita y a todos los que confiaron en mi fueron un pilar importante en la trayectoria de este importante logro académico, gracias por ser fuente de inspiración, de valores y sobre todo la perseverancia.

Marco P. (MP)

AGRADECIMIENTOS – ALEX AREVALO

El presente trabajo agradezco a mis padres por ser mi pilar fundamental y haberme apoyado incondicionalmente, pese a las adversidades e inconvenientes que se presentaron.

Agradezco a mi director de tesis Ing. Roberto Andrade por su ayuda con su experiencia, conocimiento y motivación durante la investigación de este proyecto de titulación.

A mis amigos que gracias a su apoyo me permitieron permanecer con empeño y dedicación durante toda mi carrera universitaria.

Por último, pero no menos importante quiero agradecerme a mí por creer en mí, por hacer todo este trabajo duro, por nunca renunciar y por ser alguien que siempre busca dar lo mejor.

Alex

AGRADECIMIENTOS – PARCO MARCO

A Dios por darme la oportunidad de tener salud y vida.

A mi mami Pascuala Gualpa quien es fuente de amor, compresión y sobre todo por confiar en mí que a pesar de la circunstancia de la vida siempre estuvo junto a mí creyendo que todo se puede lograr con esfuerzo, perseverancia y humildad. Por el ahincó de guiarme por el camino del bien y sobre todo también por no darse por vencida en mi educación prescolar. Gracias por todo mami.

A mi papi Fausto Parco quien es un pilar fundamental en la familia y ser fuente de enseñanza de trabajo, perseverancia y humildad. El tiempo que me brindo para enseñarme y guiarme por el camino del bien. Gracias por todo papi.

A mi mamita Elena Tupiza quien siempre estuvo ahí aconsejándome en la importancia de la educación, que me preguntaba cómo iba todos los días que salía a estudiar. Quien me daba la inspiración para no decaer en este importante camino académico. Ser ejemplo de carácter, valores y sobre todo el espíritu de trabajo.

A mis hermanos Aldahir y Natasha quien fueron la inspiración para esforzarme todos los días.

A mi tía Elena Ulco quien fue apoyo en todo este lapso académico quien ha expresado su apoyo y confianza en mí.

A todos mis amigos quien fueron parte de esta experiencia en la vida académica.

A mi amigo y compañero de tesis Alex Arevalo por su colaboración y esfuerzo para llevar a cabo este trabajo de titulación.

Al mi director de tesis Ing. Roberto Andrade por su paciencia y colaboración en el desarrollo de este trabajo de titulación

A Marco Parco por nunca haberse rendido.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El ecosistema de Internet de las Cosas (IoT) presente en hogares inteligentes genera gran cantidad de datos sensibles que se ven comprometidos al aumento de ciberataques encaminados a esta tecnología, afectando la privacidad y seguridad de los hogares. El análisis de riesgos permitirá estimar el estado del riesgo al que se encuentra expuesto el hogar inteligente logrando informar al usuario con la finalidad de tomar decisiones para reducir el riesgo.

En la actualidad existen escasas herramientas de software que permiten obtener un valor estimado del riesgo de seguridad informática en ecosistemas IoT; las existentes están dirigidas únicamente a infraestructuras de tecnologías de la información (TI) tradicional.

En el presente trabajo se desarrolla una aplicación web para análisis de riesgos cualitativo en hogares inteligentes con ecosistemas IoT, utilizando el método de análisis de riesgo basado en la metodología Magerit versión 3.0. La aplicación permite automatizar el proceso de recolección de información para posterior estimar automáticamente con criterios de la metodología el valor del riesgo logrando agilizar el proceso manual como se lo realiza comúnmente. Lo que conlleva que el cálculo del estado del riesgo sea eficiente y con mayor rapidez logrando así en el mejoramiento de toma de decisiones para asegurar el hogar inteligente.

El proyecto fue desarrollado bajo el estándar ISO/IEC 29110 y el marco de trabajo Scrum con la finalidad que el desarrollo sea de calidad, ordenado y pueda ser replicado con mejoras para próximas implementaciones futuras.

Palabras Clave: Análisis de Riesgos, Internet de las Cosas, automatizar, Magerit versión 3.0, Estándar ISO/IEC 29110, Scrum.

ABSTRACT

The Internet of Things (IoT) ecosystem present in smart homes generates a large amount of sensitive data that is compromised by the increase in cyberattacks aimed at this technology, affecting the privacy and security of homes. The risk analysis will allow estimating the state of the risk to which the smart home is exposed, managing to inform the user to make decisions to reduce the risk.

Currently there are few software tools that allow an estimated value of the computer security risk in IoT ecosystems to be obtained; the existing ones are aimed solely at traditional information technology (IT) infrastructures.

In the present work, a web application is developed for qualitative risk analysis in smart homes with IoT ecosystems, using the risk analysis method based on the Magerit version 3.0 methodology. The application allows to automate the information collection process to estimate the value of the risk later automatically with criteria of the methodology, speeding up the manual process as it is commonly done. This means that the calculation of the risk status is efficient and faster, thus achieving the improvement of decision-making to ensure the smart home.

The project was developed under the ISO/IEC 29110 standard and the Scrum framework with the aim that the development is of quality, orderly and can be replicated with improvements for future implementations.

Keywords: Risk Analysis, Internet of Things, automate, Magerit version 3.0, ISO/IEC 29110 Standard, Scrum.

1 INTRODUCCIÓN

1.1 Planteamiento del problema

En América Latina y el Caribe, el mercado de Internet de las Cosas (IoT) es todavía pequeño, pero muestra un fuerte crecimiento; se proyecta 1,000 millones de dispositivos para 2023 [1]. Gran parte de los dispositivos de IoT, se encuentran en el dominio de hogares inteligentes (*Smart Home*), las cuales están compuestos de software, hardware, sensores, actuadores y conectividad en el ecosistema del hogar [2]. Y aunque la implementación de esta nueva tecnología ha traído grandes beneficios, la interconectividad de los dispositivos inteligentes al internet ha dado paso a la aparición de nuevos y sustanciales riesgos de ciberseguridad [3].

Los ciberataques se producen con mayor frecuencia y cada vez más están siendo encaminados a dispositivos IoT [4]. El ecosistema IoT presente en hogares inteligentes genera gran cantidad de datos sensibles que pueden verse comprometidos afectando la privacidad y seguridad de los hogares. Si un atacante toma el control sobre un dispositivo IoT puede espiar lugares restringidos, recopilar información confidencial, deshabilitar dispositivos o producir una red de robots (por ejemplo: el ataque *botnet* DDoS Mirai) [2] [4] .

La reducción de los riesgos de seguridad tanto en infraestructuras de Tecnologías de la Información (TI) tradicional como en ecosistemas de IoT es notable cuando existe una estructura para la evaluación y gestión de riesgos [3]. La gestión de riesgos implica un análisis de riesgos, proceso encargado en identificar vulnerabilidades y amenazas con el objetivo de cuantificar el impacto de eventos negativos exitosos que afecten la disponibilidad, integridad y confidencial de los activos críticos como son en este caso los dispositivos IoT inmersos en el hogar.

El propósito del análisis de riesgos en ecosistemas IoT para hogares es comprender la naturaleza del riesgo y sus características, con la finalidad de establecer el nivel de riesgo existente al que se encuentra expuesto el hogar inteligente y finalmente dar a conocer al usuario para que él mismo tome decisiones con el propósito de reducir el riesgo [5].

En la actualidad existen escasas herramientas de software que permiten obtener un valor estimado del riesgo de seguridad informática; las existentes están dirigidas a infraestructuras de TI tradicional y se apoyan en metodologías de análisis de riesgo como: MAGERIT, OCTAVE e

ISO 27005 [6]. A pesar de que exista la gestión de riesgos únicamente orientada a infraestructuras de TI tradicional, este puede ser adaptado a ecosistemas IoT, debido a que se basan en los mismos principios utilizados para proteger activos críticos [7].

Las herramientas comerciales presentes en el mercado como Pilar, GxSGSI, R-BOX realizan la gestión de riesgos en infraestructuras de TI tradicional y no se enfocan en ecosistemas con dispositivos IoT, presentes en el hogar y considerados también activos críticos. Es por tal motivo que el presente proyecto de titulación propone desarrollar una aplicación web para el análisis de riesgos en ecosistemas IoT para hogares inteligentes; la misma se desarrollará aplicando la metodología Magerit debido a que ofrece un método sistemático y concreto para analizar los riesgos derivados del uso de información digital y sistemas informáticos.

1.2 Justificación practica

En las últimas dos décadas el Internet moderno está expandiéndose a la vida cotidiana a través del IoT, entre los dominios destacados se encuentra los hogares inteligentes [8]. Sin embargo, detrás de la perspectiva optimista, existe la sombra de una amenaza inminente que son ciberdelincuentes, quienes intentan sabotear el correcto funcionamiento del ecosistema IoT. En general, entre los fabricantes de dispositivos IoT para hogares inteligentes, la seguridad en los dispositivos es casi inexistente o se minimiza significativamente. En consecuencia, las vulnerabilidades desestimadas y no resueltas en estos dispositivos exponen ampliamente a los usuarios y familias a ataques cibernéticos [9].

Los hogares inteligentes son una innovación esencial que ayudan a resolver varios desafíos urgentes en la sociedad; analizar los posibles riesgos en los dispositivos de los hogares inteligentes es un procedimiento clave hacia la construcción de un futuro de IoT más seguro para la sociedad [10].

Por tal motivo, el presente trabajo de titulación permitirá desarrollar una herramienta de software que apoye en los procedimientos de análisis de riesgos existentes en el ecosistema IoT inmersos en hogares inteligentes, y de esta forma mitigar las posibles vulnerabilidades encontradas por la aplicación promoviendo un desarrollo eficiente, escalable y seguro del ecosistema IoT.

1.3 Justificación teórica

El crecimiento a la par de dispositivos IoT y amenazas que atentan contra los mismos, han impulsado el análisis de riesgos en infraestructuras de IoT, a pesar de la complejidad del ecosistema IoT, es necesaria una evaluación continua de riesgos en los hogares inteligentes, debido a que los datos que se generan en este ambiente son sensibles consiguiendo afectar la vida de las personas y la seguridad de sus hogares [11] [12].

Los procesos de análisis de riesgos de seguridad informática hasta la actualidad son procesos llevados a cabo manualmente por un oficial de seguridad bajo la guía de metodologías o estándares de análisis de riesgos, con el objetivo de estimar la magnitud de riesgos a la que está expuesta una organización [13] [14].

Rawat [3] y Malik [12] mencionan que el análisis de riesgos IoT mejora sustancialmente si se convierte en un proceso continuo. Por tanto, disponer de una herramienta de software que automatice los procesos de análisis de riesgos permitiría un aumento en el ciclo de ejecución de este proceso y su eficiencia [15]. Además, con un software que facilite el análisis de riesgos de IoT en los hogares que cuentan con un número considerable de dispositivos interconectados, permitiría que el proceso manual de reconocimiento de amenazas y vulnerabilidades sobre estos activos dentro del hogar se vuelva más llevadero.

Una investigación previa realizada acerca de software existentes, enfocados en ejecutar el análisis de riesgos de seguridad informática proporcionó como resultado la Tabla 1, donde se describen 4 software existentes de análisis de riesgos, pero están enfocados en análisis los riesgos en activos de TI tradicional.

Tabla 1 Software de Análisis de Riesgos

Software / Características	EAR / PILAR	GxSGSI	R-BOX	Counter Measures
Análisis de Riesgo	Si	Si	Si	Si
Metodología de Análisis	MAGERIT	MAGERIT	MAGERIT	NIST-800-53
Análisis Cuantitativo	Si	Si	Si	Si
Análisis Cualitativo	Si	No	Si	Si
Inventario de activos	Si	Si	Si	Si
Valoración de activos	Si	Si	Si	Si
Identificación y valoración de las amenazas	Si	Si	Si	Si
Generador de Reportes	Si	Si	Si	Si
Tipo de Software	Escritorio	Escritorio	Escritorio	Web
Tipo de Licencia	Comercial	Comercial	Comercial	Comercial

La información recabada en la Tabla 1 muestra que 3 de los softwares existentes son herramientas de escritorio, lo que implica que el usuario descargue e instale una aplicación. A diferencia de las aplicaciones de escritorio, las aplicaciones web son independientes del sistema operativo. La mayoría de las aplicaciones web funcionan en cualquier navegador web estándar conectado a Internet, independientemente del sistema operativo subyacente [16].

Por consiguiente, para el proceso de codificación de la aplicación web se utilizará un stack JavaScript y tecnologías de código abierto (*Open Source*) que en conjunto proporcionan un marco de trabajo de extremo a extremo para desarrollar aplicaciones web dinámicas [17]. El stack está compuesto por MongoDB, Strapi, ReactJS y NodeJS con estas tecnologías se desarrollará el frontend y backend de la aplicación de manera rápida y con una gran robustez ya que soporta la arquitectura Modelo-Vista-Controlador (MVC) para que el proceso de desarrollo fluya sin problemas [17].

1.4 Objetivos

1.4.1 Objetivo General

Desarrollar una aplicación web para análisis de riesgos en hogares inteligentes con ecosistemas de IoT utilizando la norma ISO/IEC 29110 con una orientación al ciclo de vida ágil Scrum.

1.4.2 Objetivos Específicos

- Comprender la metodología de análisis de riesgo Magerit para definir los módulos a implementar en la aplicación web.
- Adaptar la metodología de Magerit para el análisis de riesgos de un hogar inteligente.
- Diseñar la arquitectura de la aplicación.
- Implementar la aplicación web para análisis de riesgos IoT.
- Verificar el funcionamiento de la aplicación desarrollada para el análisis de riesgos de un hogar inteligente.

1.5 Análisis de Riesgo

1.5.1 Proceso de análisis de riesgos basado en la Magerit versión 3.0

El análisis de riesgos basado en la metodología Magerit versión 3.0 tiene como objetivo ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones llevando un control de los riesgos presentes en el sistema de información. [14]

En un sistema de información el crecimiento tanto de activos como de las amenazas ligadas al mismo exige una revisión continua de todo el contexto debido a la presencia de acciones malintencionadas que afectan la disponibilidad, integridad, confidencialidad, trazabilidad y autenticidad de los datos almacenados o transmitidos por el sistema. [14]

El análisis de riesgos propuesta por la metodología Magerit considera los siguientes elementos: activos, amenazas y salvaguardas, mediante la valoración dada a los mismos consecuentemente se estima el valor de impacto y el riesgo al que se encuentra expuesto el sistema. Este proceso se encuentra formalizado en el método de análisis de riesgos. El método de análisis de riesgos cuenta con las siguientes tareas:

1. Caracterización de los activos
    a. Identificación de los activos
    b. Dependencias entre activos
    c. Valoración de los activos
2. Caracterización de las amenazas
    a. Identificación de las amenazas
    b. Valoración de las amenazas
3. Caracterización de las salvaguardas
    a. Identificación de las salvaguardas pertinentes
    b. Valoración de las salvaguardas
4. Estimación del estado de riesgo
    a. Estimación del impacto
    b. Estimación del riesgo

A continuación, se detallan cada una de las tareas a desarrollar en cada una de las actividades del proceso de análisis de riegos:

1.5.1.1 MAR.1 – Caracterización de los activos

Actividad encargada de identificar los activos relevantes que son parte del sistema de información caracterizándolo por el tipo de activo, relaciones entre los diferentes activos e identificando y valorando en que dimensiones de seguridad son importantes. El resultado de esta actividad es el informe denominado modelo de valor. Consta de dos subtareas:

a. Identificación de los activos
b. Dependencias entre activos
c. Valoración de los activos

a. Identificación de los activos

Esta actividad identifica los activos esenciales que componen el sistema de información y son valiosos para la organización, reconociendo las características (atributos) esenciales que definen al activo. La denominación de los activos no debe ser ambigua y debe ser recogida en terminología habitual a la organización.

En la identificación de activos existe dos cosas esenciales en el sistema que son la información que maneja y los servicios que presta permitiendo clasificar más a detalle los activos en grupos diferentes como son datos, servicios, aplicaciones informáticas, equipos informáticos, soportes de información, equipamiento auxiliar, redes de comunicaciones, instalaciones y personas.

Los atributos sugeridos por la metodología son:

- Código
- Nombre
- Descripción
- Tipo (o tipos) que caracterizan el activo (*)
- Unidad responsable
- Persona responsable
- Ubicación técnica o geográfica
- Cantidad (En caso de equipos idénticos en configuración y datos que manejan)

(*) En el registro del atributo tipo hace referencia al tipo de activo según la clasificación que propone la metodología Magerit en el Libro de “Catalogo de Elementos” sección 2, es preciso recalcar que esta clasificación no es exhaustiva ni peor aún válida para siempre. Además, un activo no es excluyente a un solo tipo, un activo puede ser simultáneamente de varios tipos. [14]

Para esta actividad es recomendable tener a la mano toda la información disponible como:

- Inventario de datos manejados por el sistema,
- Inventario de servicios prestados por el sistema,
- Procesos de negocio,
- Diagramas de uso,
- Diagramas de flujo de datos,
- Inventarios de equipamiento lógico,
- Inventarios de equipamiento físico,
- Locales y sedes de la Organización,
- Caracterización funcional de los puestos de trabajo. [14]

El correcto levantamiento de información de los activos es importante debido a que fija el alcance del proyecto y logra que todos los usuarios comprendan un lenguaje común logrando facilitar las

siguientes gestiones como: determinar las dependencias entre activos, valorar los activos, identificar y valorar las amenazas, y determinar las salvaguardas necesarias para proteger el sistema.

b. Dependencias entre activos

En esta actividad se identifica y valora la dependencia entre activos, es decir la medida en que un activo de orden superior se puede ver afectado por una amenaza materializada sobre un activo de orden inferior. [18]

Al ser considerado un sistema de información se debe tratar cada uno de los activos como un todo lo que implica considerar la dependencia entre cada uno de los activos debido a que si uno de ellos es afectado en la seguridad puede propagarse al resto de activos poniendo en aprietos a toda la organización. [14]

Los documentos en donde podemos encontrar información acerca de las dependencias pueden ser:

- Procesos de negocio
- Diagramas de flujo de datos
- Diagramas de uso

La documentación y entrevistas facilitan la estimación del grado de dependencias entre activos valorándolo de una escala de 0 a 100 por ciento, adicional es recomendable registrar una explicación breve de dicha valoración

El resultado de esta actividad es el Diagrama de dependencias entre activos.

c. Valoración de los activos

En esta actividad se identifica y valora en que dimensión de seguridad es valioso el activo y el coste que supondría la destrucción del activo para la organización. La valoración de cada uno de los activos nace de la necesidad de protegerlo por lo que vale pues cuanto más valioso, mayor será la necesidad de protección en la dimensión de seguridad pertinente.

Las dimensiones que se toman en cuenta son confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Una vez identificadas las dimensiones que se verán afectadas en el

activo se registra el valor en cada dimensión con valores cuantitativos (valor numérico) o cualitativos (valor en una escala de nivel). [14]

La información importante a ser registrar en cada valoración son las dimensiones en las que el activo es relevante, la valoración en cada dimensión y una breve explicación de la valoración.

La valoración de los activos implica un alto grado de subjetividad de parte de los responsables del sistema de información de la organización para lo cual será necesario entrevistar a varios de ellos (gerencia, responsable de datos, responsable de servicios, responsable de operación) debido a que conocen las consecuencias que acarrea si llegará a suceder un incidente. [18]

El resultado de esta actividad es la obtención del Modelo de valor de los activos.

1.5.1.2 MAR.2 – Caracterización de las amenazas

En esta actividad se analiza al enemigo que se encuentra en el entorno del sistema de información, realizando las siguientes preguntas: ¿qué puede suceder si se lleva a cabo?, ¿cuáles son las consecuencias en las que puede derivar?, ¿cuán probable es que ocurra? Mediante esto logramos identificar las amenazas relevantes que pueden acechar al sistema y por consiguiente tomar en consideración su probabilidad ocurrencia y el daño que causa a cada activo.

a. Identificación de las amenazas

Se identifican las amenazas más importantes que pueden actuar sobre los activos registrados en tareas previas. La identificación de amenazas por activo se realiza con la ayuda del catálogo de amenazas debido a que existe amenazas específicas para cierto tipo de activo por tanto se debe recurrir al catálogo del libro catálogo de elementos para ver que amenaza puede actuar sobre dicho activo.

Las amenazas pueden ser:

- **De origen natural. -** Son accidentes causados por fenómenos naturales (terremotos, inundaciones, fuego, etc.), el sistema de información es víctima pasiva.
- **Del entorno. -** Son desastres industriales (contaminación, fallos eléctricos, humedad, etc.), el sistema es víctima pasiva, pero se deben tomar medidas.

- **Defectos de aplicaciones. -** Defectos de diseño o implementación son denominadas vulnerabilidades técnicas, pueden acarrear consecuencias graves sobre el sistema.
- **Causadas por las personas de forma accidental. -** Personas que tienen acceso en el sistema de información que cometen errores no intencionados.
- **Causadas por las personas de forma deliberada. -** Personas que tienen acceso al sistema de información que comenten ataques deliberados con el ánimo de causar daño u obtener beneficio.

. Las características importantes por tomar en cuenta en cada amenaza son:

- Amenazas que actúan sobre cierto tipo de activo,
- Las dimensiones que afectan en cada tipo activo y
- Breve descripción del efecto que puede causar la amenaza.

Las fuentes de información necesarias para esta actividad son:

- El resultado de la actividad de Caracterización de los activos,
- Informes de vulnerabilidades de los activos,
- Historial de incidentes de la organización u otras organizaciones referentes,
- Catálogo de amenazas y
- Entrevistas.

En esta actividad se obtiene un Informe de relación de amenazas posibles.

b. Valoración de las amenazas

En esta actividad se estima el valor de la frecuencia (probabilidad) de cada amenaza y el valor del daño (degradación) que causaría la amenaza en cada dimensión de seguridad si llega a suceder.

La degradación es el porcentaje que resultaría afectado el activo si ocurre la amenaza. La probabilidad es la frecuencia de que esta amenaza se materialice. Tanto la probabilidad y la degradación se puede modelar cualitativamente mediante la escala nominal de la Tabla 2 o cuantitativamente como una frecuencia de ocurrencia tomando de referencia de 1 año para la probabilidad y de 0 a 100 porciento el grado de degradación.

Tabla 2 Escala nominal

Representación	Valor
MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Tomado de [14].

Para cada una de las amenazas se registra la frecuencia, degradación y una breve descripción de las estimaciones valoradas.

La valoración de cada amenaza debe considerar:

- la experiencia (historia) universal,
- la experiencia (historia) del sector de actividad,
- la experiencia (historia) del entorno en que se ubican los sistemas,
- la experiencia (historia) de la propia Organización y
- los informes anexos a los reportes de defectos proporcionados por los fabricantes y organismos de respuesta a incidentes de seguridad (CERTS). [14]

Los documentos que se deben tener presente son:

- Resultados obtenidos de la tarea identificación de las amenazas,
- Series históricas de incidentes,
- Informes de defectos en los productos y
- Informes históricos de incidentes en la Organización.

El resultado de la actividad llevada a cabo es un mapa de riesgos, informe que contiene las amenazas posibles de cada activo, la probabilidad y la degradación que provocarían en los activos.

1.5.1.3 MAR.3 – Caracterización de las salvaguardas

En esta actividad se busca las medidas necesarias para proteger y verificar con que cuenta el sistema de información para afrontar los diferentes incidentes que pueden causar las amenazas.

Cuenta con dos subtareas:

a. Identificación de las salvaguardas pertinentes
b. Valoración de las salvaguardas

a. Identificación de las salvaguardas pertinentes

En esta actividad se identifica las salvaguardas pertinentes que protejan el sistema de información, para determinar las salvaguardas se recurre a diferentes catálogos de salvaguardas o a consejos de personas expertas, luego de obtener un conjunto de salvaguardas se realiza un proceso de descarte y se selecciona las óptimas para reducir el riesgo.

La selección de cada una de las salvaguardas del catálogo propuesto debe ser relevante para lo que hay que proteger por tal es preciso realizar una lista de las salvaguardas tomando en cuenta que activos se va a proteger, cuáles son las dimensiones que requieren protección, que amenazas se debe contrarrestar y si existe una salvaguarda alternativa. Es importante centrar nuestra atención en salvaguardas valiosas y obviar las irrelevantes conllevando excluir ciertas salvaguardas de forma que no aplica o no se justifica.
Las razones para descartar una salvaguarda son:

- No es apropiada para el activo a proteger,
- No es apropiada para dimensión de seguridad a proteger,
- No es efectiva a la amenaza que se pretende contrarrestar,
- El valor por invertir en la salvaguarda es mucho mayor a lo que hay que proteger y
- Existe medidas alternativas [14]

Existe varios tipos de salvaguardas como se puede ver en la Tabla 3 que se encargan de reducir la probabilidad de que una amenaza ocurra o si ya ocurrió reducir la degradación.

Tabla 3 Tipos de salvaguardas

Efecto	Tipo	Descripción
Preventivas: reducen la probabilidad	[PR] preventivas	Reduce que el incidente no ocurra
	[DR] disuasorias	Actúa antes de que ocurra el incidente, reduce la probabilidad de que ocurra
	[EL] eliminatorias	Impide que ocurra el incidente
Acotan la degradación	[IM] minimizadoras	Acota las consecuencias de un incidente
	[CR] correctivas	Ocurrido el incidente repara el daño
	[RC] recuperativas	Regresa al estado anterior al ocurrido el incidente

Consolidan el efecto de las demás	[MN] de monitorización	Monitoriza lo que ocurre y ocurrió para atajar el incidente y limitar el impacto
	[DC] de detección	Detecta e informa que el ataque está ocurriendo
	[AW] de concienciación	Capacitación de personas anexas al sistema. Efecto preventivo
	[AD] administrativas	Administración en los componentes de seguridad del sistema.

La información importante por registrar en cada salvaguarda es:

- Descripción de la salvaguarda y el estado de implantación,
- Que amenazas pretende hacer frente.

El resultado de esta actividad son la Declaración de aplicabilidad de las salvaguardas y la Relación de salvaguardas desplegadas. [14]

b. Valoración de las salvaguardas

El objetivo de esta actividad es determinar cuan eficaz es la salvaguarda es decir si realiza el procedimiento con el que fue considerado para reducir el riesgo presente en el activo. [14]

La estimación del valor de la eficacia se basa en que una salvaguarda bien implementada y que reduce el riesgo a 0 es una salvaguarda ideal y su valor de eficacia es 100 por ciento, eficacia que combina factores técnicos y operacionales de la salvaguarda. La eficacia puede ser de 0 a 100 por ciento siendo 0 por ciento que no existen o que faltan ser elaboradas mientras que el 100 por ciento se refiere que están perfectamente implementadas. Para establecer el valor de la eficacia en la salvaguarda se empleará una escala de madurez como la Tabla 4.

Tabla 4 Eficacia y madurez de las salvaguardas

Factor	Nivel	Significado
0%	L0	Inexistente
	L1	Inicial / ad hoc
	L2	Reproducible pero intuitivo
	L3	Proceso definido
	L4	Gestionado y medible
100%	L5	Optimizado

Tomado de [14].

El inventario de salvaguardas obtenido en la actividad anterior es el paso previo para valorar la eficacia, tomando en consideración:

- Idoneidad de la salvaguarda para objetivo que se quiere contrarrestar,
- la calidad de implantación,
- la formación de los responsables de su configuración y operación,
- la formación de los usuarios, si tienen un papel activo,
- la existencia de controles de medida de su efectividad y
- la existencia de procedimientos de revisión regular

Las características que se deben tomar en cuenta en las salvaguardas es el valor de su eficacia para contrarrestar las amenazas y la explicación breve de la estimación de eficacia.
Al finalizar de esta actividad se obtiene como resultado un informe de salvaguardas desplegadas caracterizándola por el grado de efectividad y un informe de insuficiencias (o vulnerabilidades) describe que salvaguardas deberían implementar o mejorar. [14]

1.5.1.4 MAR.4 – Estimación del estado de riesgo

La última actividad estima un valor que puede ocurrir (impacto) y probablemente ocurra (riesgo), no es posible llegar a esta actividad sin previo realizar las tareas anteriores (MAR.1, MAR.2 y MAR.3) debido a que los cálculos de estas estimaciones se derivan de estas tareas previas.
La actividad consta de dos subtareas:

a. Estimación del impacto
b. Estimación del riesgo

a. Estimación del impacto

En esta tarea se estima el valor de impacto al que están expuestos los activos del sistema de información, existe dos tipos de impacto potencial y residual.
El impacto potencial es aquel al que se encuentra expuesto el sistema de información tomando en cuenta el valor de los activos, valor de las amenazas sin ser considerado las salvaguardas implementadas. [14] El impacto potencial se obtiene del producto del valor del activo y la degradación que causa la amenaza.

El impacto residual es aquel que se encuentra expuesto el sistema de información tomando en cuenta la valoración de los activos, valoración de las amenazas y la eficacia de las salvaguardas implementadas actualmente. [14] El impacto residual se obtiene del producto del valor del activo y la degradación que causa la amenaza después de implementar la salvaguarda.
El resultado de esta actividad es la obtención de un informe de impacto potencial e impacto residual por activo.

b. Estimación del riesgo

En esta actividad se determina el valor de riesgo al que están expuestos los activos del sistema de información, existe dos tipos de riesgo el riesgo potencial y residual.

El riesgo potencial es aquel que se encuentra expuesto el sistema de información tomando en cuenta la valoración de los activos, la valoración de las amenazas sin considerar las salvaguardas implementadas. [14] El riesgo potencial se obtiene del producto del impacto potencial y la probabilidad de ocurrencia de la amenaza.

El riesgo potencial es aquel que se encuentra expuesto el sistema de información tomando en cuenta la valoración de los activos, la valoración de las amenazas y la eficacia de las salvaguardas implementadas actualmente. [14] El riesgo residual se obtiene del producto del impacto residual y la probabilidad de ocurrencia luego de implementar la salvaguarda.

1.5.2 Módulos para el Análisis de Riesgo

La comprensión del método de análisis de riesgos es clave para la ejecución de este proyecto debido a que la aplicación web se basa en la metodología Magerit siguiendo cada una de sus actividades para estimar el valor de riesgo. Por tal motivo se diseñó en BPMN (*Business Process Model and Notation*) el diagrama de proceso del método de análisis de riesgos.

En la Figura 1, se muestra el método de análisis de riesgos completo como lo describe la metodología, cuenta con cinco actividades cuatro de ellos son subprocesos (Figura 2, 3, 4, 5) y una actividad agregada para el cálculo del valor acumulado. El cálculo de valor acumulado sirve para determinar el impacto y riesgo acumulado, esta actividad fue introducida debido a requisitos del cliente.

El diagrama de procesos del método de análisis de riesgos realizado facilitará el desarrollo de los Mockups de la aplicación a desarrollar. Mediante este diagrama se obtiene la secuencia de la aplicación y los usuarios quien manejara la aplicación. El desarrollo de las actividades de todo el proceso tiene dos responsables el usuario encargado en ingresar toda la información del sistema a analizar y el analista de seguridad que se encarga de realizar los cálculos de estimación del riesgo.

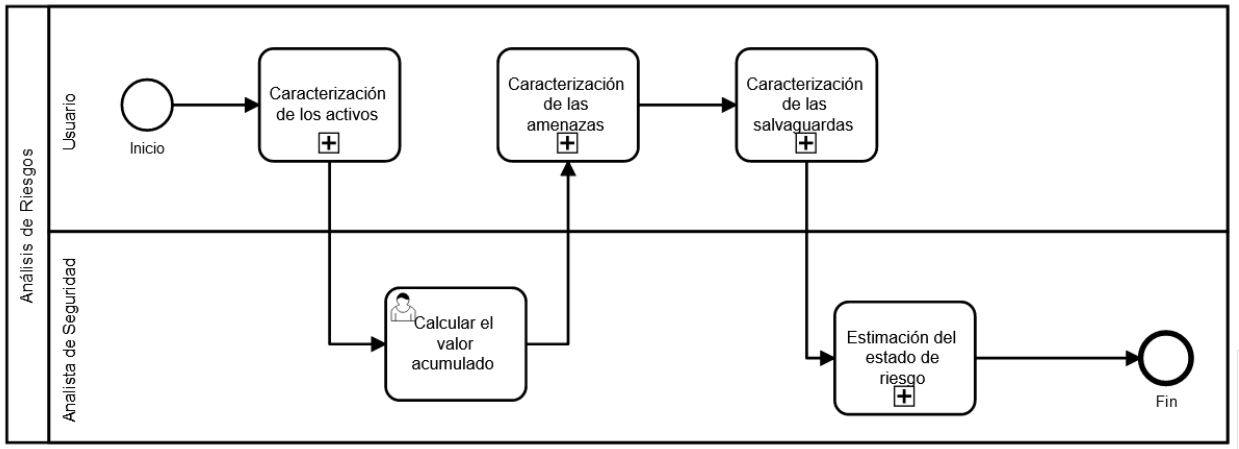


Figura 1 Método de análisis de riesgos.

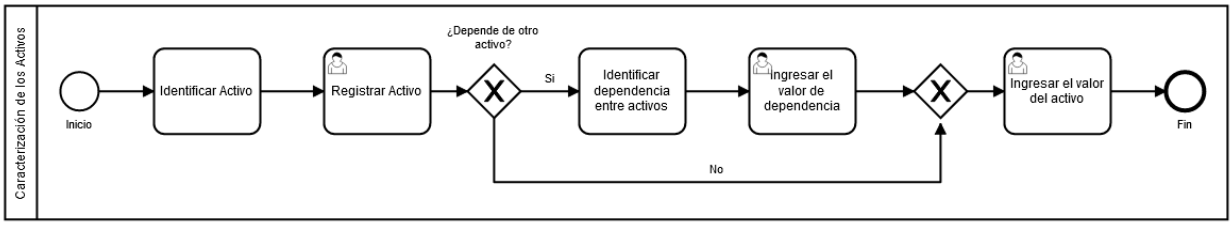


Figura 2 Subproceso caracterización de los activos.

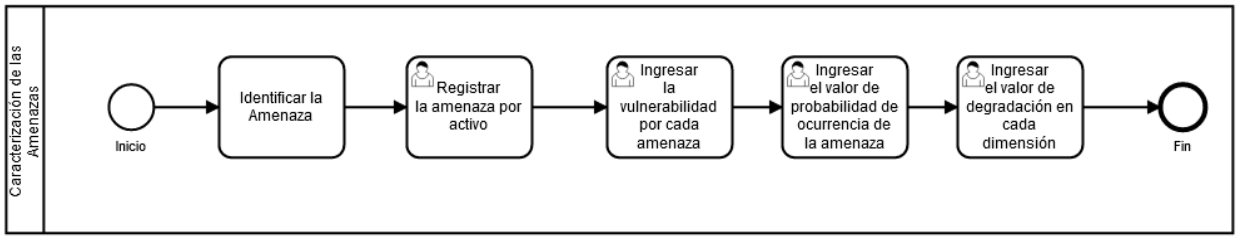


Figura 3 Subproceso caracterización de las amenazas.

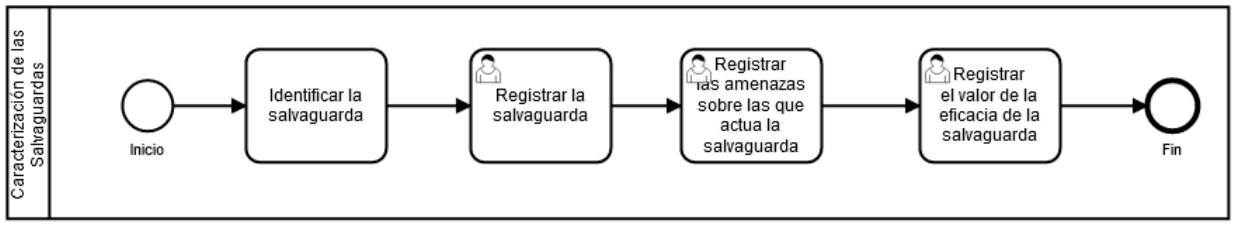


Figura 4 Subproceso caracterización de salvaguardas.

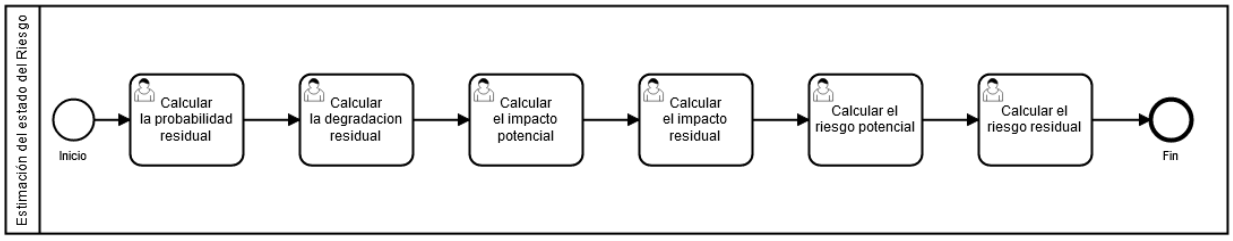


Figura 5 Subproceso estimación del estado del riesgo

1.5.3 Aplicaciones de Análisis de Riesgo

La automatización del proceso de análisis de riesgos mediante la utilización de software que facilite el manejo de gran cantidad de información de los ecosistemas de tecnologías de la información y comunicación para la estimación de riesgo viene dada por un sinfín de software propietario de uso comercial presente en el mercado. Se ha identificado varios softwares entre estos son: EAR / PILAR, GxSGSI, R-BOX y CheckPoint.

La evaluación de cada uno de los softwares reconocidos orientados al análisis de riesgos y que se basan en la metodología Magerit son tres EAR / PILAR, GxSGSI, R-BOX, a diferencia de *CheckPoint IoT Protect* es un software orientado al análisis de riesgos en ecosistemas IoT (*Internet of things*) y se basa de forma dinámica de varias políticas para establecer la estimación del riesgo.

1.5.3.1 EAR / PILAR

Es un software de análisis y gestión de riesgos para sistemas de información y comunicación, esta implementado bajo la metodología Magerit versión 3.0. Los riesgos se analizan en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. Es un software propietario de uso comercial y está dirigido para empresas pequeñas y medianas. [19]

1.5.3.2 GxSGSI

Es un software de escritorio completo que automatiza el análisis y gestión de los riesgos de sistemas de información y comunicación, permite el cálculo de riesgo intrínseco y residual, de la misma forma está basado en la metodología Magerit permitiendo así lograr la certificación de un sistema de gestión de seguridad de la información, bajo las normas ISO 27001 e 27002. El

software es propietario y se encuentra a la fecha del desarrollo de este documento descontinuado. [20]

1.5.3.3 R-BOX

Software comercial propietario de escritorio para el análisis y gestión de riesgos en sistemas de información y comunicación. Esta solución está basada en la metodología Magerit. Además, cuenta con algoritmos de cálculo de riesgo documentada y disponible que permite cálculos robustos, también permite múltiples integraciones con los sistemas de las organizaciones. [21]

1.5.3.4 CheckPoint IoT Protect

Es un software comercial propietario de escritorio para el análisis de riesgos de IoT (Internet of Things) que permite el "análisis de riesgo en tiempo real basado en descubrimiento del IoT, evaluación de riesgos de firmware e inteligencia de amenazas" [22]. Permite visualizar en tiempo real el nivel de riesgo por dispositivo.

La revisión de las diferentes soluciones de software muestra que gran parte de ellas se basan en la metodología Magerit debido a que esta tiene sus procesos bien establecidos entorno a activos, amenazas, salvaguardas o contramedidas y la estimación del riesgo. Finalmente, esta revisión de soluciones facilita la comprensión de la secuencia de navegación contrastado con el proceso de análisis de riesgos y así poder enfocarlo a ecosistemas con dispositivos IoT que se encuentran dentro del gran conjunto que es el de tecnologías de la información y comunicación.

2 METODOLOGÍA

La aplicación web para el análisis de riesgos en hogares inteligentes con ecosistemas IoT fue desarrollada bajo el estándar ISO/IEC 29110 utilizando la metodología ágil con el marco de trabajo Scrum. La fusión del estándar y la metodología establece un proceso de implementación ordenada del proyecto lo que ayuda a desarrollar una aplicación web de calidad y el mismo sea llevado a cabo en el costo y tiempo esperado.

El estándar ISO/IEC 29110: 2016 facilita el desarrollo de software de calidad así abriéndose a suministrar un producto software competitivo y de confianza que puede solventar el problema del cliente a pesar de ser desarrollado por un grupo reducido de personas, al ser un estándar

muy amplio y estar enfocado a pequeñas y medianas empresas existen perfiles específicos, en este proyecto se utilizó el perfil de entrada. [23]

El perfil de entrada ISO/IEC 29110-5-1-1: 2012 está orientado a entidades muy pequeñas que trabajan en solo un pequeño proyecto de software y cuentan con hasta 6 o menos personas al mes. [24] El perfil de entrada se implementará utilizando una metodología ágil que en este caso es Scrum debido a que los requisitos del software definidos al principio son incompletos por parte del cliente.

El marco de trabajo Scrum permitirá el desarrollo continuo en colaboración con el cliente e interesados del proyecto, la colaboración permite que los diferentes incrementos entregados al cliente sea un producto funcional y a la par pueda ir mejorando las irregularidades que se presentan en los requisitos a medida que estos evolucionan en comparación con los requisitos definidos al principio. [23]

Scrum se encarga en el desarrollo de productos complejos en donde los requisitos son cambiantes y poco definidos al principio es por tal que fue utilizado en este proyecto debido a que los requisitos de software no estaban definidos completamente al principio por el cliente y debía adaptarse a nuevos cambios propuestos logrando obtener un producto software competitivo y fácil de usar para el usuario.

El estándar ISO/IEC 29110-5-1-1:2012 cuenta con dos fases la gestión de proyecto y la implementación de software. La gestión del proyecto tiene como propósito planificar y documentar todo el proceso implementación de software. La implementación de software se encarga del proceso de análisis, identificación de los componentes, desarrollo, integración, evaluación y entrega de producto software acorde a los requisitos. [24]

Scrum trabaja mediante ciclos llamados sprint que tiene una duración de un mes o menos, esta iteración tiene como finalidad entregar un resultado de software funcional en base a una lista de producto (*Product Backlog*). Al ser un marco de trabajo se encarga de guiar para obtener un producto funcional con el mayor valor posible, mas no es un proceso prescriptivo. [25]

La composición del estándar ISO/IEC 29110 del perfil de entrada y la metodología ágil Scrum se muestra la Figura 6 donde describe todo el proceso combinado del estándar y Scrum.

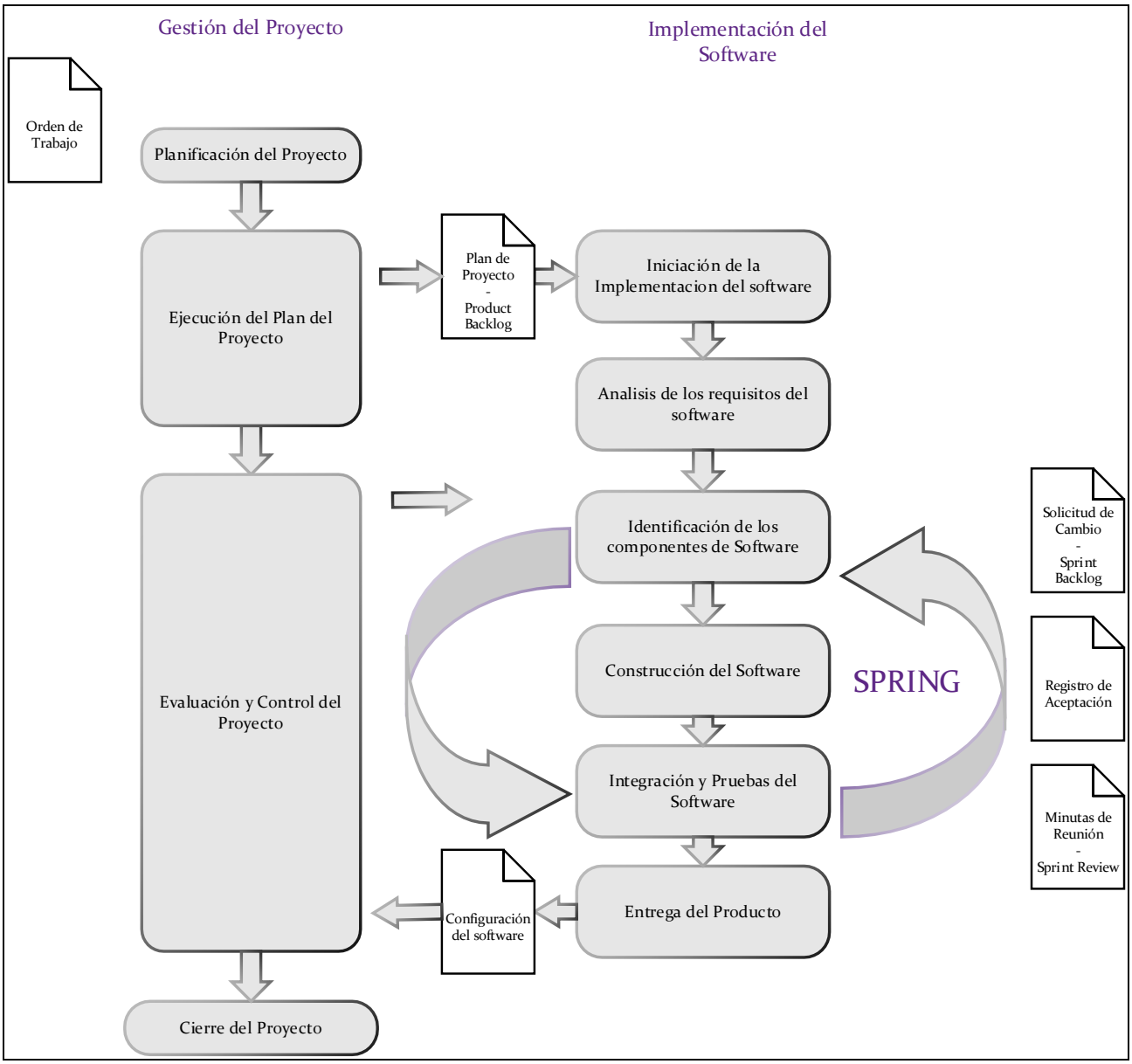


Figura 6 Combinación de ISO/IEC 29110-5-1-1:2012 y SCRUM

El proceso implementación de software es donde mayoritariamente se aplica el marco de trabajo Scrum. Scrum está presente en cada iteración desde la parte del análisis de los requisitos del software hasta la integración y pruebas del software que pertenece al proceso de implementación en el estándar.

La entrada y salida de documentos de cada actividad del proceso comparte por así decir documentos similares tanto en Scrum como en el estándar, los siguientes documentos tienen

el mismo objetivo: Plan de proyecto – *Product Backlog*, Solicitud de cambio – *Spring Backlog,* Minutas de reunión – *Spring Review*. Es por tal que se ajustará estos documentos tomando en cuenta el objetivo con el que fueron creados.

A continuación, se describe el proceso completo de la aplicación del estándar con Scrum al proyecto de implementación de la aplicación web de análisis de riesgos en hogares inteligentes con ecosistemas IoT que se desarrolló en este tema de tesis.

2.1 Aplicación del estándar ISO/IEC 29110-5-1-1:2012 y SCRUM

2.1.1 Proceso de administración del proyecto

Este proceso tiene como propósito establecer y ejecutar las tareas del proyecto de implementación software que permitan cumplir con los objetivos del proyecto en la calidad, tiempo y costos esperados [23]. Se encuentra definido por las siguientes fases:

- **Planeación del proyecto**

La actividad inicia con la declaración de trabajo donde el cliente menciona que necesita una "aplicación de análisis de riesgos en hogares inteligentes con ecosistemas IoT, y el análisis de riesgos debe seguir el proceso de la metodología Magerit versión 3.0". En consecuencia, se elabora el documento Declaración de Trabajo de manera formal, el mismo que se lo encontrará en el Anexo 1.

Además, se elabora la primera versión del documento del Plan de proyecto ahí se describe la planificación del cronograma de las actividades que se llevaran a cabo, los responsables y la documentación a realizar desde el inicio hasta la entrega del software funcional terminado al cliente.

- **Ejecución del plan de proyecto**

En esta actividad se lleva un control y registro del progreso del documento plan de proyecto realizando acercamientos con el cliente el cual se va registrando en el documento de Registro de Minutas y si existe algún cambio se da el seguimiento del cambio en el

documento Solicitud de Cambio. Obtenido el Plan de Proyecto ya se puede iniciar con el proceso de la implementación del software como se puede ver en la Figura 6.

- **Evaluación y control del proyecto**

Una vez ya iniciado la implementación de la aplicación web se revisa si se ha cumplido lo planificado en el documento plan de proyecto, existió varias modificaciones lo que provoco el cambio de fechas debido a retrasos. Todas las modificaciones durante el desarrollo del proyecto fueron registradas en las diferentes versiones del documento plan de proyecto. El documento de plan de proyecto y sus diferentes versiones se encuentran en el Anexo 2.

Esta actividad únicamente tiene como finalidad dar seguimiento del progreso del proyecto y si existen cambios son registrados con la finalidad de no desviarse del objetivo del proyecto.

- **Cierre del Proyecto**

La actividad de cierre del proyecto es donde se formalizo la finalización del proyecto y la entrega de toda la documentación de entregables finales de acuerdo con el plan de proyecto, esto se dio una vez que el cliente dio su aceptación del producto final obtenido. Finalmente se cierra el proyecto y se informa a todos los interesados.

2.1.2 Proceso de implementación del software

Este proceso tiene como propósito realizar las actividades de análisis, diseño, construcción, integración y pruebas para el producto de software de acuerdo con los requerimientos especificados [23]. Está definido por las siguientes fases:

- **Inicio de la Implementación del Software**

En esta actividad el equipo de trabajo constituido por tres personas Roberto Andrade (Cliente), Alex Arevalo y Marco Parco (Equipo de desarrollo) se comprometen a llevar a cabo lo establecido en el documento Plan de Proyecto con la finalidad de revisar y asignar tareas según el alcance del proyecto e iniciar el entorno de implementación. El resultado de la revisión es la comprensión de todos los participantes en los objetivos del proyecto.

El plan del Proyecto cuenta con varias versiones la versión inicial es el documento PlanDeProyecto-v1.0, pueden existir modificaciones en el mismo y la versión incrementara según corresponda a cambios sustanciales. El documento Plan de Proyecto y todas sus versiones son incluidas en el Anexo 2.

- **Análisis de requisitos del software**

En esta actividad el equipo de trabajo identifica los requisitos clave mencionados por el cliente en el documento de declaración de trabajo y recolecta información acerca del dominio de desenvolvimiento del proyecto con la finalidad de identificar el alcance del proyecto, estructurar y priorizar los requisitos.

El estándar ISO/IEC 29110 utiliza la metodología ágil SCRUM para la implementación del software por lo tanto la recolección de requisitos se lo realiza mediante historias de usuarios que se adaptan al desarrollo ágil. En los documentos declaración del trabajo y plan de proyecto se describen los requisitos claves y mejor conocidos del software que debe ser entregado al cliente, por lo tanto, en base a estos documentos se elaboró la lista de producto (*Product Backlog*) que es dinámico debido a que cambia constantemente para ser adecuada a las necesidades del cliente. La lista de producto se presenta en las siguientes secciones de este documento.

Una vez ya identificado los requisitos iniciamos con la revisión del entorno donde se desenvuelve el proyecto. La revisión iniciara con la comprensión del análisis de riesgos basado en la metodología Magerit versión 3.0 y la adaptación de esta para el análisis de riesgos en dispositivos de internet de las cosas.

Finalmente, la estructuración y priorización de los requisitos identificados en la lista de producto deben contar con la prioridad como alto, medio, bajo con la finalidad de priorizar las funcionalidades a ser implementadas.

- **Identificación de los componentes de software**

La identificación de los componentes del software es una pieza clave en el desarrollo del proyecto debido a que responden a los requisitos del cliente, para la identificación de los componentes de software se realizó tres actividades importantes: caso de estudio de análisis de riesgos, diseño del diagrama de procesos del análisis de riesgos orientado a ecosistemas inteligentes y el diseño de interfaces de usuario.

El caso de estudio se realizó de forma manual todo el proceso de análisis de riesgos basado en la metodología Magerit aplicado a un hogar con dispositivos inteligentes esto con la finalidad de comprender cada actividad a realizarse para determinar el riesgo. Una vez comprendido cada una de las actividades a realizarse en el proceso de análisis de riesgos en ecosistemas inteligentes se diseñó un diagrama de procesos de todas las actividades y tareas que implica este proceso (Figura 1 hasta Figura 5).

Finalmente, el equipo de trabajo comprendido el análisis de riesgos procede a diseñar en interfaces de usuario de todo el proceso que antes se realizó de forma manual para poder automatizarla en la aplicación a desarrollar en el proyecto. El diseño de interfaces de usuario se adjunta en el Anexo 3.

- **Construcción del software**

La construcción del producto de software se desarrolló utilizando la metodología ágil Scrum bajo la planificación del plan de proyecto propuesta por el estándar ISO 29110, allí se describe los recursos, responsables, calendario y presupuesto del desarrollo de la aplicación, el plan de proyecto se encuentra en el Anexo 2.

El desarrollo del software inició con la recolección de requisitos del software logrando obtener la lista de producto (Spring Backlog) que recolecta los requisitos mejor conocidos y comprendidos al principio, en la lista de producto se identificó los módulos importantes de la aplicación web estos son: autenticación, proyecto, caracterización de activos, caracterización de amenazas, caracterización de salvaguardas y estimación del estado del riesgo.

Los módulos encontrados en la lista de producto son seis los mismos que en la planificación de Sprint (*Spring Planning*) fueron divididos en cinco. El primer sprint abarco el módulo de autenticación y proyecto los posteriores Sprint abarcaron cada uno de los módulos subsiguientes. En la planificación de Sprint de cada uno de los Sprint se registró las historias de usuario que fueron desarrolladas.

El desarrollo de cada Sprint tuvo una duración de un mes aproximadamente el mismo que desembocaba en la entrega de un producto funcional al culminar el mes, la codificación de las historias de usuario se guio mediante mockups de la aplicación web. Los lenguajes utilizados en la aplicación web es JavaScript, HTML y CSS. Una vez culminado el Sprint se realizaba una revisión con el cliente e interesados.

La revisión de Sprint (*Sprint Review*) con el cliente permitió verificar si las historias de usuario planificadas han terminado o tienen cambios por parte del cliente, los cambios por parte del cliente fueron planificadas y agregados para el siguiente Sprint.

- **Integración y Pruebas de Software**

La integración y pruebas de software se dividió en tres partes esenciales para poder determinar que la aplicación cumpla con los requerimientos y se encuentre en un nivel adecuado para su utilización.

La primera parte fue realizar pruebas de funcionalidad las cuales nos permitieron validar la aplicación web frente a los requerimientos funcionales. Para esta fase se crearon 9 casos de pruebas diferentes los cuales cubrieron las principales funcionalidades de la aplicación y fueron probadas por usuarios externos al desarrollo de la aplicación.

Una vez terminada las pruebas funcionales pasamos a las pruebas de usabilidad del producto las cuales nos permitieron obtener resultados cualitativos acerca del nivel de satisfacción del usuario con el producto y la facilidad de completar tareas utilizando la interfaz de usuario. Se efectúo una encuesta a 16 personas con las principales interfaces de usuario de la aplicación y de esta manera se obtuvieron resultados satisfactorios en cuanto a las pruebas de usabilidad.

Finalmente, se realizaron pruebas de rendimiento las cuales permitieron conocer la estabilidad, la velocidad, la escalabilidad y la capacidad de respuesta que tiene la aplicación web bajo una carga de trabajo determinado. Se realizo un análisis estático de código utilizando la herramienta SonarQube y un análisis de rendimiento con la herramienta JMeter obteniendo resultados satisfactorios en cada uno de los análisis realizados.

- **Entrega del producto**

Una vez finalizado la implementación de los requerimientos de la aplicación web se realizó el proceso de entrega del producto para lo cual se procedió con un despliegue final del frontend y backend de la aplicación en los servidores de Netlify y Heroku respectivamente verificando que la aplicación se encuentre activa y pueda recibir peticiones de usuarios. Con el proceso de despliegue concluido se procedió a la entrega de la siguiente dirección web

https://app.smartrisk.tech/ la cual dirige hacia la aplicación web para que pueda ser utilizada por la parte interesada.

Finalmente se procedió con la entrega del backlog de requerimientos concluido, así como los resultados de las pruebas de funcionalidad, usabilidad y rendimiento para que pueda ser analizado por la parte interesada cada uno de estos ítems, de esta manera se finalizó con el proceso de entrega del producto.

2.2 Ambiente de desarrollo

2.2.1 Arquitectura de la aplicación

Para el desarrollo del presente proyecto se optó por la utilización de la arquitectura cliente-servidor bajo el patrón arquitectónico Modelo-Vista-Controlador (MVC). El patrón arquitectónico MVC proporciona una forma eficaz de generar aplicaciones modulares organizadas en tres componentes principales los cuales son Modelo, Vista y Controlador [26]. MVC define estos tres componentes de forma independiente con separación completa y proporciona una conexión integrada entre ellos [27].

- **Modelo:** Responsable de manejar la interacción de la base de datos con el controlador.
- **Vista:** Responsable de mostrar el contenido del usuario.
- **Controlador:** Responsable de actuar según la acción del usuario.

En la Figura 7, se puede observar la separación de los tres componentes del patrón MVC y su interacción [28].

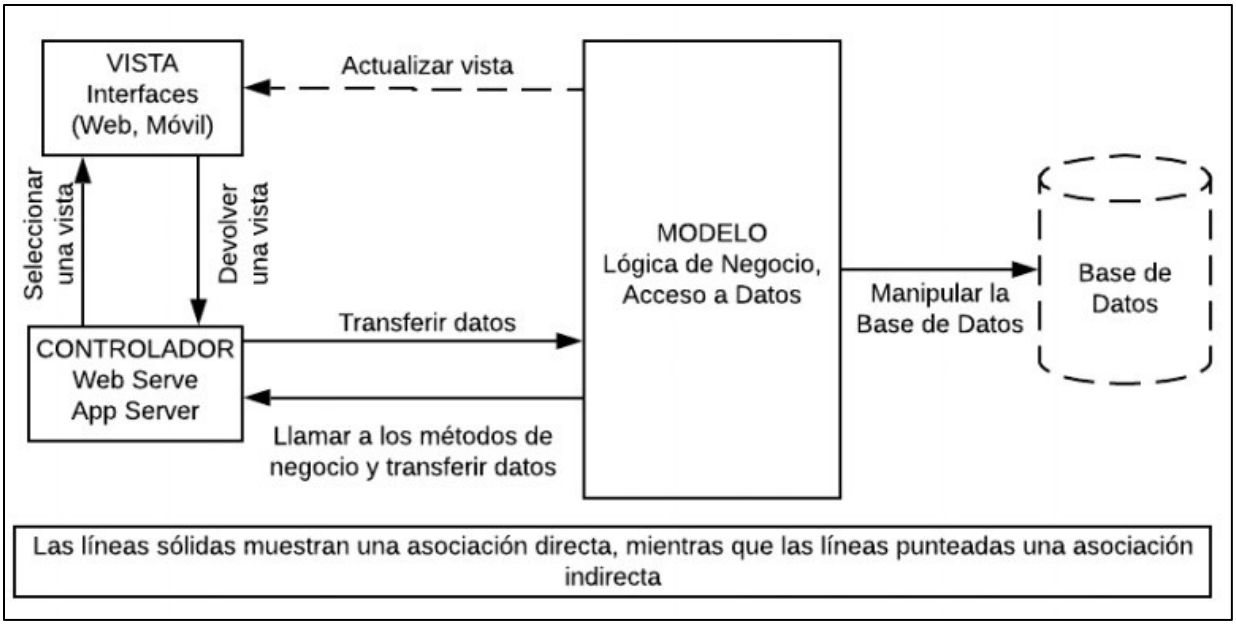


Figura 7 Patrón Arquitectónico MVC

Tomado de [28]

Los beneficios que brinda el patrón arquitectónico MVC son los siguientes [29]:

- **Varias vistas utilizando el mismo modelo:** la separación de modelo y vista permite que varias vistas utilicen el mismo modelo.
- **Soporte más fácil para nuevas clases de clientes:** para soportar una nueva clase de cliente, todo lo que se necesita es desarrollar una vista y el controlador para dicha clase y conectarlo al modelo existente.
- **Modularidad eficiente:** los componentes se pueden agregar o quitar muy fácilmente, sin influencia negativa en la aplicación. Los cambios realizados en un componente de la aplicación no se combinan con otros componentes.
- **Facilidad de crecimiento:** la aplicación puede incorporar un número indefinido de módulos, junto con componentes antiguos, sin interferencias.

La comunicación cliente-servidor tiene lugar en el patrón arquitectónico MVC para lo cual se ha hecho uso de una arquitectura de dos niveles en donde el componente de vista se encuentra en el lado del cliente, mientras que los componentes de controlador y modelo se encuentran en el lado del servidor y sobre esta arquitectura se ha implementado el stack de tecnologías [27].

A continuación, en la Figura 8, se muestra la arquitectura de la aplicación Web.

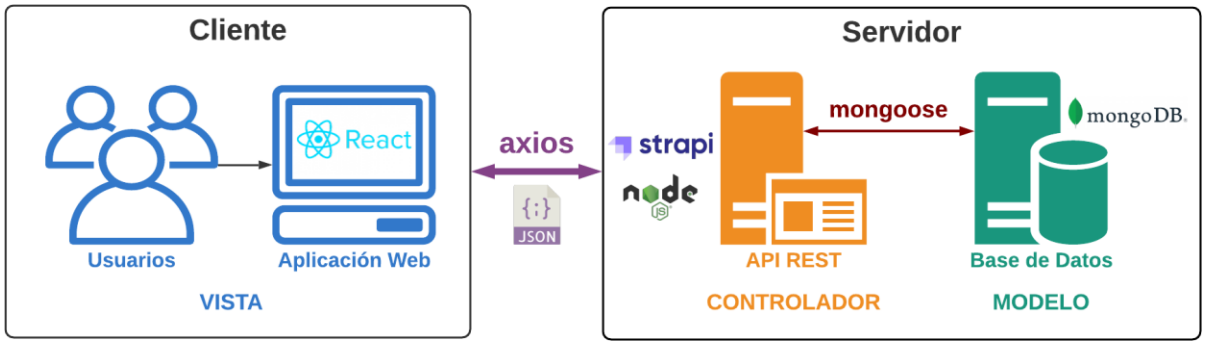


Figura 8 Arquitectura de la Aplicación Web

Elaborado por: Arevalo & Parco

Utilizando esta arquitectura logramos la separación de responsabilidades entres los componentes de MVC, así como una estructura bien definida que será clave para un menor costo de desarrollo de la aplicación. En siguientes párrafos se definen los conceptos claves utilizados en la definición de la arquitectura de la aplicación.

2.2.2 Tecnologías Utilizadas

En el desarrollo del presente proyecto de titulación, se utilizó: lenguajes de programación, marcos de trabajo(*frameworks*), herramientas de prototipado, repositorio para alojar el proyecto, administrador de base de datos y entornos de desarrollo que son descritos a más destalle a continuación:

2.2.2.1 Prototipado de Interfaces de Usuario

Tabla 5 Herramienta utilizada para el prototipado de interfaces de usuario.

Nombre	Uso	Descripción
Figma	Diseño de Mockups	Figma es una herramienta de diseño y creación de prototipos, es una aplicación de diseño de interfaz de usuario (UI - *User Interface*) y experiencia de usuario (UX - *User Experience*) utilizada para crear sitios web, aplicaciones o componentes de interfaz de usuario más pequeños que se pueden integrar en otros proyectos [30].

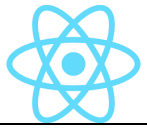
2.2.2.2 Lenguajes de Programación

Tabla 6 Lenguajes de Programación utilizados

Nombre	Uso	Descripción
JavaScript 	Desarrollo de Aplicación Web	JavaScript es un lenguaje de programación de alto nivel que permite implementar características complejas en una página web. JavaScript es una de las tecnologías centrales de la *World Wide Web* ya que hace posible páginas web interactivas y es una parte esencial de las aplicaciones web [31].
HTML 	Desarrollo de Aplicación Web	Lenguaje de Marcado de Hipertextos (HTML - *HyperText Markup Language*) es un lenguaje de marcado que consiste en una serie de elementos que definen la estructura y contenido de un documento para mostrarse en un navegador web [32].
CSS 	Desarrollo de Aplicación Web	Hojas de Estilo en Cascada (CSS - *Cascading Style Sheets*) es un lenguaje simple para agregar estilo a los documentos web escritos en HTML o XML [33].

2.2.2.3 Marcos de Trabajo (Frameworks) y Bibliotecas

Tabla 7 Framework y Bibliotecas utilizadas.

Nombre	Uso	Descripción
Desarrollo del Frontend		
ReactJS 	Frontend de la Aplicación Web	ReactJS es una librería de JavaScript de código abierto que permite el desarrollo de interfaces de usuario interactivas basado en componentes encapsulados y reutilizables [34].
Ant Design 	Estilos de la Aplicación Web	Ant Design es una biblioteca React UI que tiene una gran cantidad de componentes fáciles de usar que son útiles para crear interfaces de usuario elegantes. [35].
Desarrollo del Backend		

Nombre	Uso	Descripción
NodeJS 	Desarrollo del Backend	NodeJS es un entorno de ejecución para JavaScript fuera del navegador, trabaja en tiempo de ejecución y permite el desarrollo de servidores web asincrónicos controlados por eventos y sin bloqueo [36].
Strapi 	Desarrollo del Backend	Strapi es un sistema de gestión de contenidos (*CMS - Content Management System*) *headless* de código abierto basado en NodeJS, totalmente personalizable y orientado al desarrollador [37].
Base de Datos		
MongoDB 	Base de Datos	MongoDB es una base de datos NoSQL orientada a documentos en formato JSON que se utiliza para el almacenamiento de datos de gran volumen. En lugar de usar tablas y filas como en las bases de datos relacionales tradicionales, MongoDB hace uso de colecciones y documentos [38].
Robo 3T 	Gestión de Base de Datos	Robo 3T es una interfaz gráfica de usuario (GUI) de escritorio para implementaciones de MongoDB que permite interactuar con los datos a través de indicadores visuales en lugar de una interfaz basada en texto. Es una herramienta de código abierto, tiene soporte multiplataforma e incorpora el shell mongo dentro de su interfaz para proporcionar interacción basada tanto en shell como en GUI [39].
Mongoose 	Biblioteca para MongoDB	Mongoose es una biblioteca de modelado de datos de objetos para MongoDB y Node.js. Gestiona las relaciones entre los datos, proporciona validación de esquemas y se utiliza para traducir entre objetos en código y la representación de esos objetos en MongoDB [40].
Comunicación entre Frontend y Backend		
AXIOS 	Comunicación entre cliente y servidor	Axios es un cliente HTTP ligero basado en el servicio XMLHttpRequests y en promesas de JavaScript que funciona tanto en el navegador como en un entorno Node.js. Es similar a la API *Fetch* y se utiliza para realizar solicitudes HTTP [41].

Nombre	Uso	Descripción
API 	Comunicación entre cliente y servidor	Interfaz de programación de aplicaciones (API - *Application Programming Interface*) es un conjunto de funciones y librerías que permite a las aplicaciones acceder a datos e interactuar con componentes de software externos, sistemas operativos o establecer comunicación entre microservicios [42].
REST 	Comunicación entre cliente y servidor	Transferencia de Estado Representacional (REST - *Representational State Transfer*) es un estilo de arquitectura de software que define un conjunto de restricciones utilizadas para crear servicios web, facilitando que los sistemas se comuniquen entre sí usando el protocolo HTTP. Los sistemas que cumplen con REST, a menudo se denominan RESTful [43]. Los servicios web RESTful permiten que los sistemas solicitantes accedan y manipulen datos en varios formatos (siendo JSON el más usado) mediante el uso de un conjunto uniforme y predefinido de operaciones sin estado [43].
Archivos JSON 	Formato de datos entre frontend y backend	Notación de Objetos de JavaScript (JSON - *JavaScript Object Notation*) es un estándar abierto de formato de archivo y de intercambio de datos basado en JavaScript, consta de pares atributo-valor y tipos de datos de matriz. JSON es una notación de fácil lectura y escritura para los humanos de igual forma también fácil para las máquinas analizar y generar [44].

2.2.2.4 Entornos de Desarrollo y Repositorios de Código

Tabla 8 Entornos de Desarrollo y Repositorios de Código utilizados.

Nombre	Uso	Descripción
Visual Studio Code 	Entorno de Desarrollo Integral	Visual Studio Code es un editor de código fuente gratuito creado por Microsoft para Windows, Linux y macOS. Las características incluyen soporte para depuración, resaltado de sintaxis, finalización inteligente de código, refactorización de código y Git integrado [45].

GitHub 	Alojamiento y Control de Versiones	GitHub es un servicio de alojamiento de repositorios y control de versiones basado en Git, proporciona una interfaz web gráfica. También proporciona control de acceso y varias funciones de colaboración, como wikis y herramientas básicas de gestión de tareas para cada proyecto [46].
Sourcetree 	Gestión de Repositorios	Sourcetree es un cliente GUI de Git que permite la gestión de repositorios a través de una interfaz simplificada con las funciones de crear y clonar repositorios, así como realizar *commit*, *push*, *pull*, *merge*, resolver conflictos y manejar repositorios remotos [47].

2.3 Desarrollo de la aplicación web

El desarrollo de la aplicación web se inicia con la definición de los requerimientos funcionales por parte de los interesados del proyecto, se describen en la lista de productos (*Product backlog*) que se muestra a continuación.

2.3.1 Lista de Productos - *Product Backlog*

Tabla 9 Lista de Productos de la Aplicación

Código	Nombre	Descripción	Prioridad
Autenticación			
AU01	Registro en el sistema	**Como** usuario **quiero** registrarme en el sistema de forma rápida sin llenar formularios complejos.	Alta
AU02	Inicio de sesión en el sistema	**Como** usuario **quiero** ingresar al sistema de forma fácil para hacer uso de la aplicación	Alta
Proyecto			
PR01	Registrar un proyecto	**Como** usuario **quiero** registrar un proyecto en el sistema.	Alta
PR02	Consultar datos de proyectos	**Como** usuario **quiero** consultar datos de los proyectos ingresados.	Alta
PR03	Modificar datos del proyecto	**Como** usuario **quiero** modificar los datos ingresados de un proyecto	Media
PR04	Eliminar un proyecto	**Como** usuario **quiero** eliminar un proyecto.	Media
Caracterización de Activos			

Código	Nombre	Descripción	Prioridad
CA01	Registrar activos	***Como*** usuario ***quiero*** registrar los activos ***para*** tener una lista con los activos críticos del hogar inteligente.	Alta
CA02	Consultar datos de activos	***Como*** usuario ***quiero*** consultar datos de los activos ingresados	Alta
CA03	Modificar datos del activo	***Como*** usuario ***quiero*** modificar los datos ingresados anteriormente de un activo.	Media
CA04	Eliminar un activo	***Como*** usuario ***quiero*** eliminar un activo	Media
CA05	Registrar un grupo de activos	***Como*** usuario ***quiero*** registrar un grupo de activos para no tener que registrar uno por uno.	Media
CA06	Registrar la dependencia existente de un activo con otro	***Como*** usuario ***quiero*** registrar la dependencia que existe de un activo con otro.	Alta
CA07	Registrar el valor del activo	***Como*** usuario ***quiero*** registrar el valor del activo en cada dimensión de seguridad	Alta
Caracterización de Amenazas			
CAM01	Visualizar las amenazas del activo	***Como*** usuario ***quiero*** observar las amenazas a las que está ligado el activo.	Alta
CAM02	Registrar vulnerabilidades en cada amenaza	***Como*** usuario ***quiero*** registrar información de vulnerabilidades ligadas a las amenazas.	Media
CAM03	Registrar el valor del porcentaje de degradación de la amenaza	***Como*** usuario ***quiero*** registrar el valor del porcentaje de degradación de la amenaza en cada dimensión de seguridad.	Alta
CAM04	Registrar el valor del porcentaje de probabilidad de ocurrencia de la amenaza.	***Como*** usuario ***quiero*** ingresar la probabilidad de ocurrencia cuando una amenaza se lleve a cabo.	Alta
Caracterización de Salvaguardas			
CS01	Seleccionar una salvaguarda	***Como*** usuario ***quiero*** seleccionar las salvaguardas para reducir riesgo en las amenazas.	Alta
CS02	Registrar características de las salvaguardas	***Como*** usuario ***quiero*** registrar características adicionales de la salvaguarda seleccionada.	Alta
CS03	Consultar datos de las salvaguardas	***Como*** usuario ***quiero*** consultar datos de los activos ingresados	Media
CS04	Modificar datos de las salvaguardas	***Como*** usuario ***quiero*** modificar los datos anteriormente registrados de las salvaguardas.	Media
CS05	Eliminar una salvaguarda	***Como*** usuario ***quiero*** eliminar una salvaguarda	Alta
CS06	Registrar el valor de eficacia frente al	***Como*** usuario ***quiero*** ingresar el valor de eficacia frente al impacto y probabilidad.	Alta

Código	Nombre	Descripción	Prioridad
	impacto y a la probabilidad.		
Estimación de Estado de Riesgo			
ER01	Consultar el valor de la probabilidad y degradación residual.	***Como*** usuario ***quiero*** observar el valor de la probabilidad y degradación residual frente a la eficacia de las salvaguardas.	Alta
ER02	Consultar el valor del impacto potencial acumulado y repercutido	***Como*** usuario ***quiero*** observar el impacto potencial acumulado y repercutido del hogar inteligente	Alta
ER03	Consultar el valor del impacto residual acumulado y repercutido.	***Como*** usuario ***quiero*** observar el impacto residual acumulado y repercutido del hogar inteligente una vez consideradas las salvaguardas.	Alta
ER04	Consultar el valor del riesgo potencial acumulado y repercutido.	***Como*** usuario ***quiero*** observar el riesgo potencial acumulado y repercutido del hogar inteligente.	Alta
ER05	Consultar el valor del riesgo residual acumulado y repercutido.	***Como*** usuario ***quiero*** observar el riesgo residual acumulado y repercutido del hogar inteligente una vez considerada las salvaguardas.	Alta

Una vez definido el *Product Backlog* y los requerimientos funcionales con los que debe contar la aplicación web, se procede con la ejecución de los Sprint, los cuales estarán compuestos por las siguientes fases:

- Planificación del Sprint - *Sprint Planning*
- Codificación
- Revisión del Sprint - *Sprint Review*
- Despliegue

2.3.2 Sprint 1

La primera iteración presenta la estructura del proyecto en donde abarca los módulos de autenticación y proyecto, se consideró iniciar por tales módulos debido a su alta prioridad y dependencia a módulos siguientes.

2.3.2.1 Planificación del Sprint

La Tabla 10 muestra la lista de requerimientos a implementar en el primer Sprint.

Tabla 10 Planificación del Sprint para el primer Sprint.

Código	**Nombre**	**Descripción**	**Prioridad**	**Estimación** (Story Points)
Autenticación				
AU01	Registro en el sistema	**Como** usuario **quiero** registrarme en el sistema de forma rápida sin llenar formularios complejos.	Alta	5
AU02	Inicio de sesión en el sistema	**Como** usuario **quiero** ingresar al sistema de forma fácil para hacer uso de la aplicación.	Alta	8
Proyecto				
PR01	Registrar un proyecto	**Como** usuario **quiero** registrar un proyecto en el sistema.	Alta	8
PR02	Consultar datos de proyectos	**Como** usuario **quiero** consultar datos de los proyectos ingresados.	Alta	3
PR03	Modificar datos del proyecto	**Como** usuario **quiero** modificar los datos ingresados de un proyecto	Media	3
PR04	Eliminar un proyecto	**Como** usuario **quiero** eliminar un proyecto.	Media	3
Total				**30**

A continuación, en la Tabla 11 hasta la Tabla 16 se detallan las historias de usuario de la primera iteración:

Tabla 11 Historia de usuario AU01

Historia de Usuario	**AU01**
Fecha:	28/9/2021
Código:	AU01
Requisito:	Registro en el sistema
Puntos estimados:	5
Prioridad:	Alta
Descripción:	Como usuario quiero registrarme en el sistema de forma rápida sin llenar formularios complejos.
Justificación:	Permite controlar al usuario del sistema la utilización de información confidencial a suministrar
Dependencia:	No aplica
Usuario(s):	Usuario general
Responsable:	Alex Arevalo

Historia de Usuario	AU01
Criterios de aceptación:	1. El sistema permitirá registrar un usuario ingresando los siguientes datos. - Nombre - Apellido - Correo - Contraseña 2. El sistema validará que todos los campos (nombre, apellido, correo y contraseña) no estén vacíos, si algún campo esta vació mostrará el mensaje de error en cada campo: "Ingrese su [nombre, apellido, correo, contraseña]" 3. El sistema validará que la contraseña ingresada cumpla con los siguientes requisitos: mínimo de 6 caracteres, al menos que cuente con: una letra mayúscula, una letra minúscula y un número. 4. El sistema validará que el correo ingresado cumpla con el formato válido de un correo, si el correo no cumple mostrará el mensaje de error: "Escribe la dirección de correo electrónico con el formato alguien@example.com."

Tabla 12 Historia de usuario AU02

Historia de Usuario	AU02
Fecha:	28/09/2021
Código:	AU02
Requisito:	Inicio de sesión en el sistema
Puntos estimados:	8
Prioridad:	Alta
Descripción:	Como usuario quiero ingresar al sistema de forma fácil para hacer uso de la aplicación
Justificación:	Permite identificar y autorizar que usuario utilizará el sistema
Dependencia:	AU01
Usuario(s):	Usuario general
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema debe solicitar el correo y contraseña para la autenticación del usuario. 2. El sistema validará que el correo y contraseña no estén vacíos y los mismos ya se encuentren registrados en el sistema. Si el usuario no se encuentra registrado en el sistema este mostrará un mensaje de error: "Usuario o contraseña incorrectos"

Tabla 13 Historia de usuario PR01

Historia de Usuario	**PR01**
Fecha:	28/9/2021
Código:	PR01
Requisito:	Registrar un proyecto
Puntos estimados:	8
Prioridad:	Alta
Descripción:	**Como** usuario **quiero** registrar un proyecto en el sistema.
Justificación:	Inicia con la creación de un proyecto que registra los datos de la casa inteligente
Dependencia:	No aplica
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá registrar un proyecto ingresando los siguientes datos: - Nombre del proyecto - Descripción del proyecto 2. El sistema validará que los campos: nombre del proyecto y descripción del proyecto no estén vacíos, si algún campo esta vació mostrará el mensaje de error en cada campo: "Ingrese el [nombre del proyecto, descripción del proyecto]"

Tabla 14 Historia de usuario PR02

Historia de Usuario	**PR02**
Fecha:	28/9/2021
Código:	PR02
Requisito:	Consultar datos de proyectos
Puntos estimados:	3
Prioridad:	Media
Descripción:	**Como** usuario **quiero** consultar datos de los proyectos ingresados.
Justificación:	Listar todos los proyectos que se ha creado por parte del usuario
Dependencia:	PR01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo

Historia de Usuario	**PR02**
Criterios de aceptación:	1. El sistema mostrará una tabla con todos los proyectos registrados por el usuario en el sistema, la cual estará distribuida en una tabla con las siguientes columnas: - Nombre - Descripción - Acción 2. La columna acción mostrará la función de editar y/o eliminar. - Editar está representado por un icono de lápiz que permitirá abrir un formulario para editar los campos del proyecto. - Eliminar está representado por un ícono de basurero que permitirá abrir un cuadro de confirmación para eliminar el proyecto. 3. El sistema permitirá buscar un proyecto mediante un buscador que filtrará mediante el nombre del proyecto.

Tabla 15 Historia de usuario PR03

Historia de Usuario	**PR03**
Fecha:	28/9/2021
Código:	PR03
Requisito:	Modificar datos del proyecto
Puntos estimados:	3
Prioridad:	Media
Descripción:	**Como** usuario **quiero** modificar los datos ingresados de un proyecto
Justificación:	El usuario puede modificar los valores de los datos registrados por cada proyecto debido a una equivocación o cambio de valores.
Dependencia:	PR02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá modificar datos del proyecto, para el cual se muestra un formulario completo con los datos antes ingresados, donde se pueden cambiar los siguientes datos: - Nombre del proyecto - Descripción del proyecto 2. Al modificar la información del proyecto el sistema validará: - Los campos código del proyecto, nombre del proyecto y fecha del proyecto que no se encuentren vacíos al guardar los cambios realizados, si el campo está vacío mostrará el mensaje de error: *¡Ingrese el [nombre del proyecto, descripción del proyecto]!*

Tabla 16 Historia de usuario PR04

Historia de Usuario	**PR04**
Fecha:	28/9/2021
Código:	PR04
Requisito:	Eliminar un proyecto
Puntos estimados:	2
Prioridad:	Media
Descripción:	**Como** usuario **quiero** eliminar un proyecto.
Justificación:	El sistema permitirá al usuario eliminar un proyecto de su lista de proyectos
Dependencia:	PR02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá eliminar un proyecto creado por el usuario, antes de eliminar se presentará una notificación de aviso *¿Desea eliminar el proyecto [nombre del proyecto]?,* si el usuario desea eliminar debe aceptar caso contrario debe cancelar esta notificación.

2.3.2.2 Implementación

A continuación, se describe la implementación de las historias de usuarios de la primera iteración.

AU01: Registro en el sistema

La Figura 9 muestra el formulario de registro de usuarios para autorizar el ingreso y uso del sistema, en el formulario se ingresará los campos nombre, apellido, correo electrónico, contraseña.

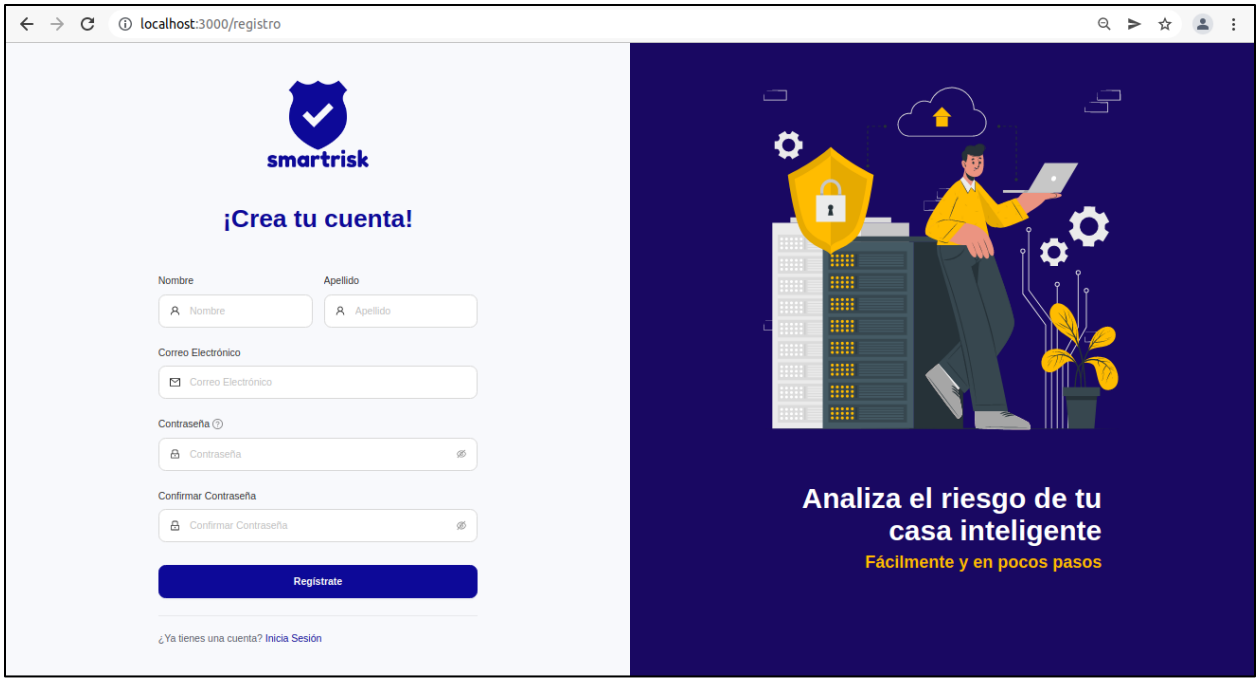


Figura 9 AU01 Formulario de registro de usuarios

Una vez ya registrado los campos solicitados, el sistema procede a la validación de campos vacíos, validación de correo electrónico y de contraseña. Finalmente, si algún campo validado tiene algún inconveniente se muestra un mensaje de error como se puede ver en la Figura 10.

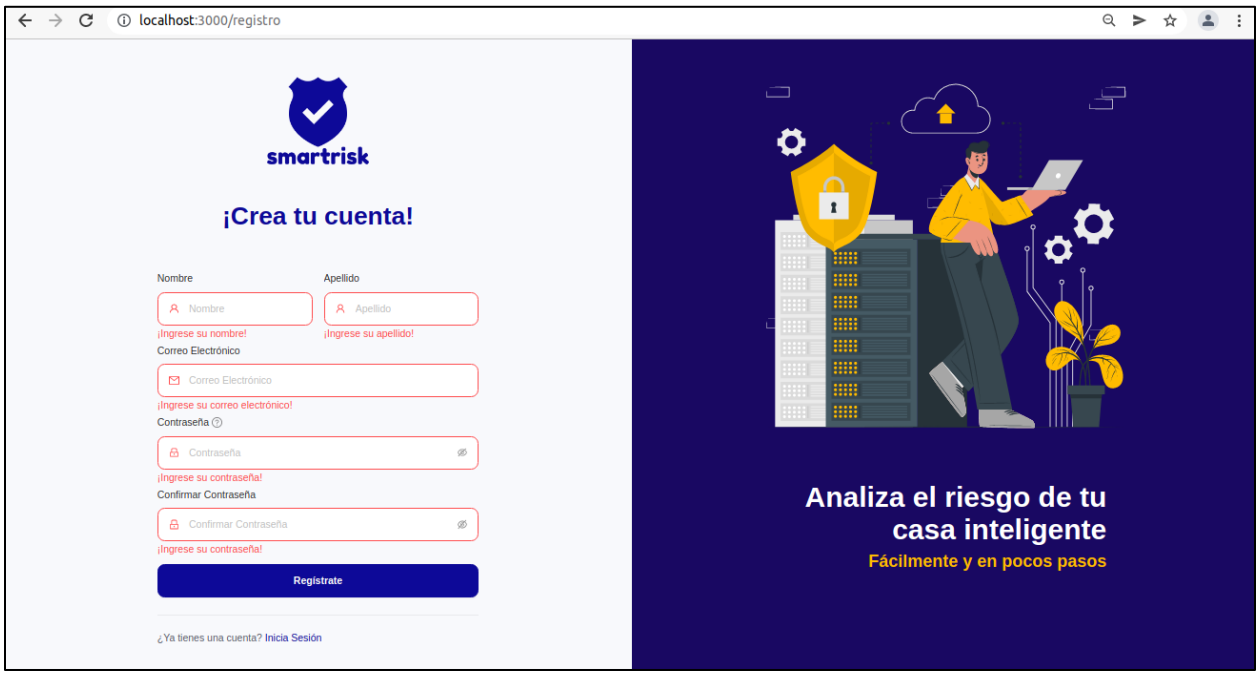


Figura 10 Validación de campos en el formulario de registro de usuarios

AU02: Inicio de sesión en el sistema

El formulario de inicio de sesión para autenticación de la aplicación se muestra en la Figura 11, para iniciar sesión en la aplicación el usuario debe ingresar el correo electrónico y contraseña. Finalmente dar clic en el botón “Iniciar Sesión”.

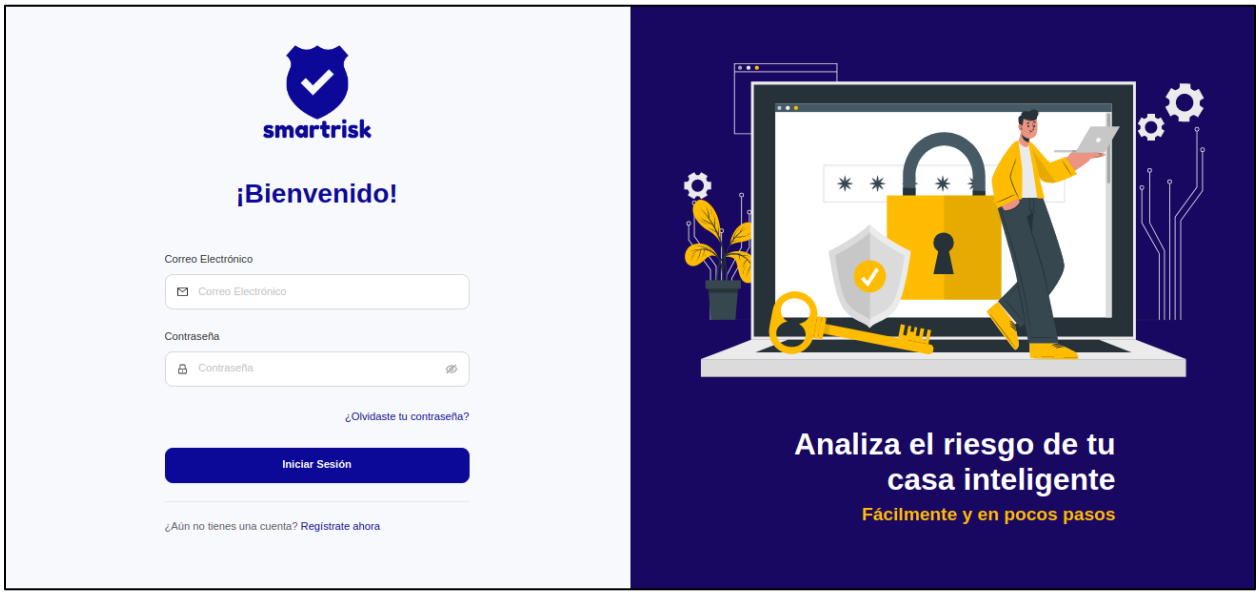


Figura 11 AU02 Formulario de inicio de sesión.

El formulario de inicio de sesión cuenta con una validación de campos vacíos y correo electrónico como se muestra en la Figura 12.

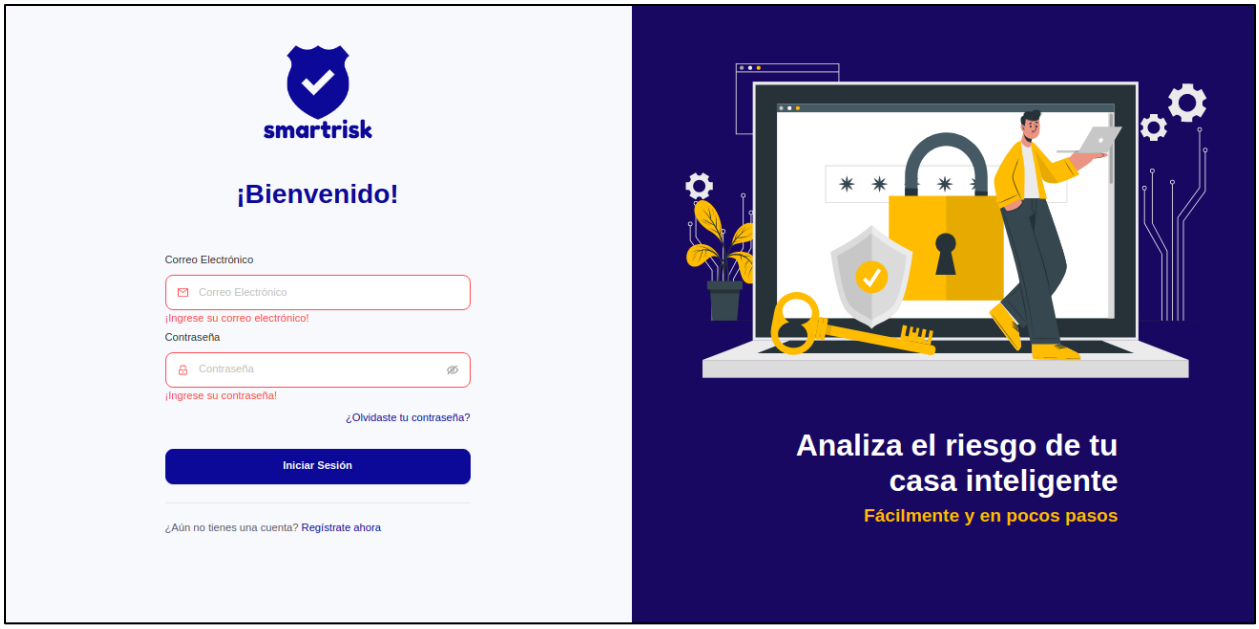


Figura 12 Validación de campos en el formulario de inicio de sesión.

Es importante considerar que el usuario para ingresar las credenciales de inicio de sesión previamente debe estar registrado en la aplicación. En caso de que el usuario no se haya registrado previamente le mostrará un mensaje de error de inicio sesión fallido como se muestra en la Figura 13. De igual manera un mensaje similar se mostrará si el usuario o contraseña ingresadas son incorrectas.

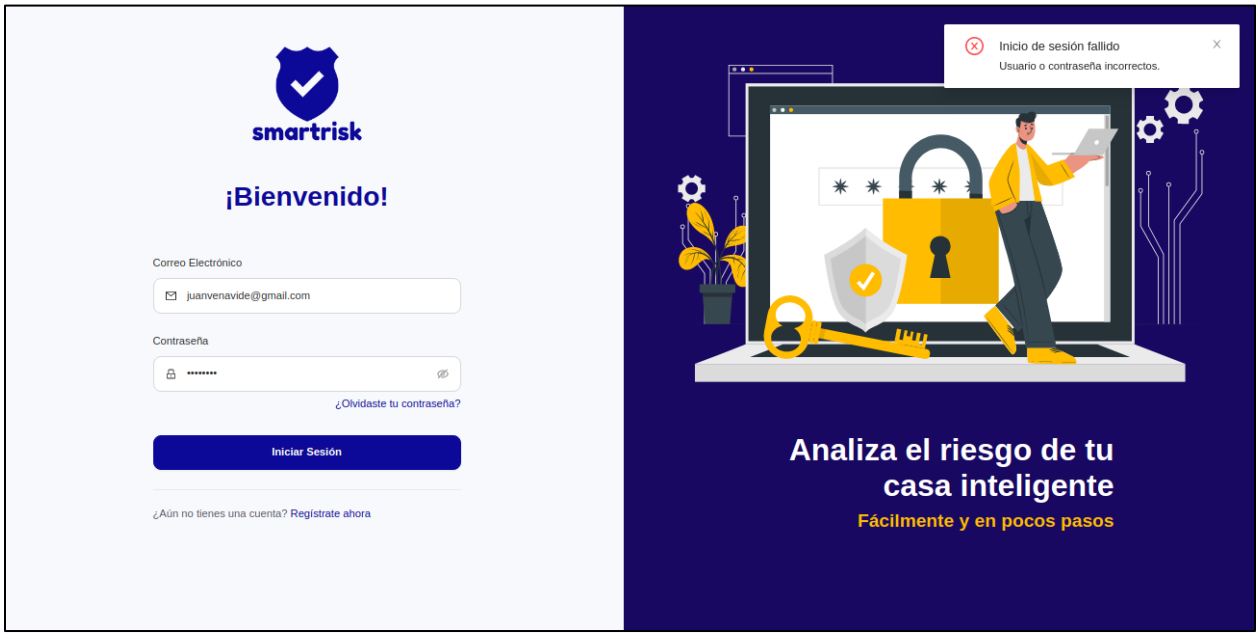


Figura 13 Inicio de sesión caso fallido.

El caso de éxito se lleva a cabo cuando el usuario se ha registrado previamente y tanto el correo electrónico y la contraseña ingresada sean correctas, lo cual conlleva que una vez ingresado las credenciales en la Figura 14 subsiguiente se muestra la Figura 15 que es la página web principal.

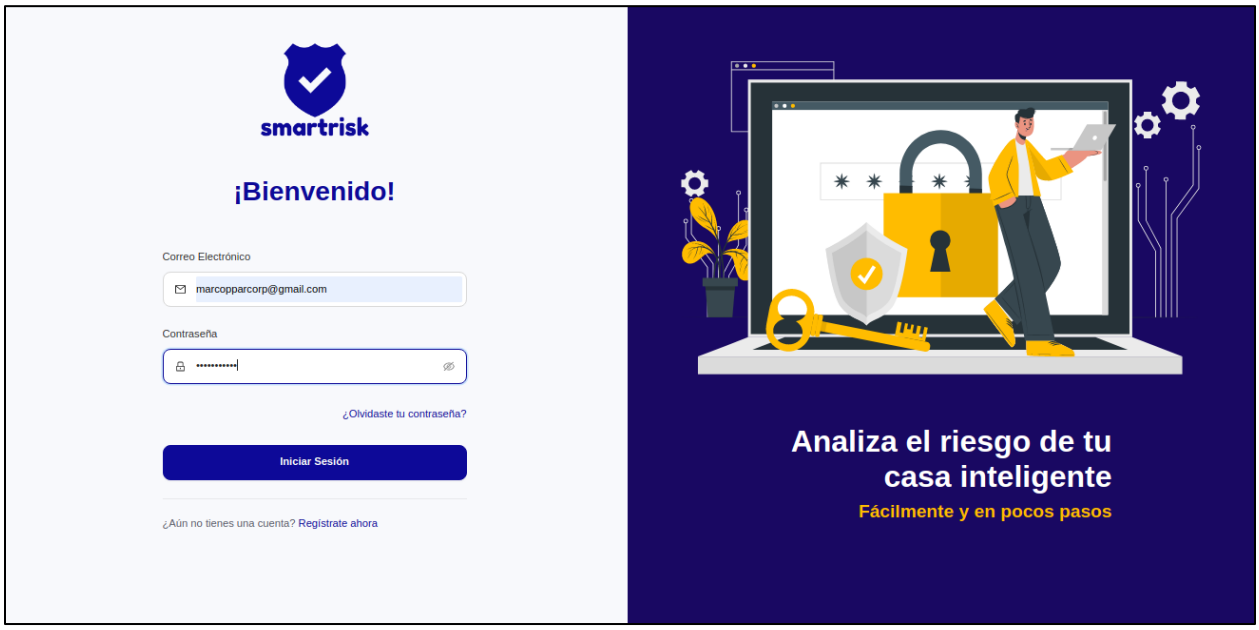


Figura 14 Inicio de sesión caso de éxito

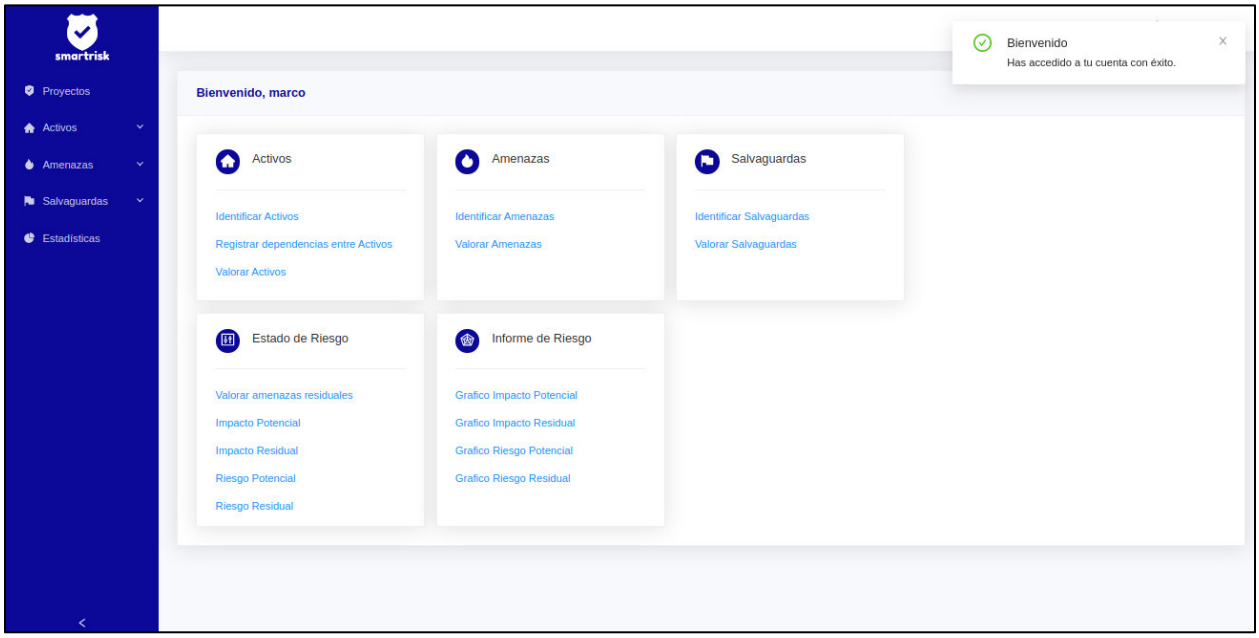


Figura 15 Pagina web principal después del inicio sesión exitoso.

PR01: Registrar un proyecto

El registro de un proyecto se lo realiza con el ingreso de información en un formulario como se muestra en la Figura 16, la información a ingresar son nombre de proyecto y descripción del proyecto. El formulario cuenta con una validación de campos vacíos donde no se puede crear un proyecto si los campos tanto el nombre del proyecto y descripción del proyecto están vacíos, lo campos deben estar con información para posterior crear un proyecto dando clic en el botón “Crear Proyecto”.

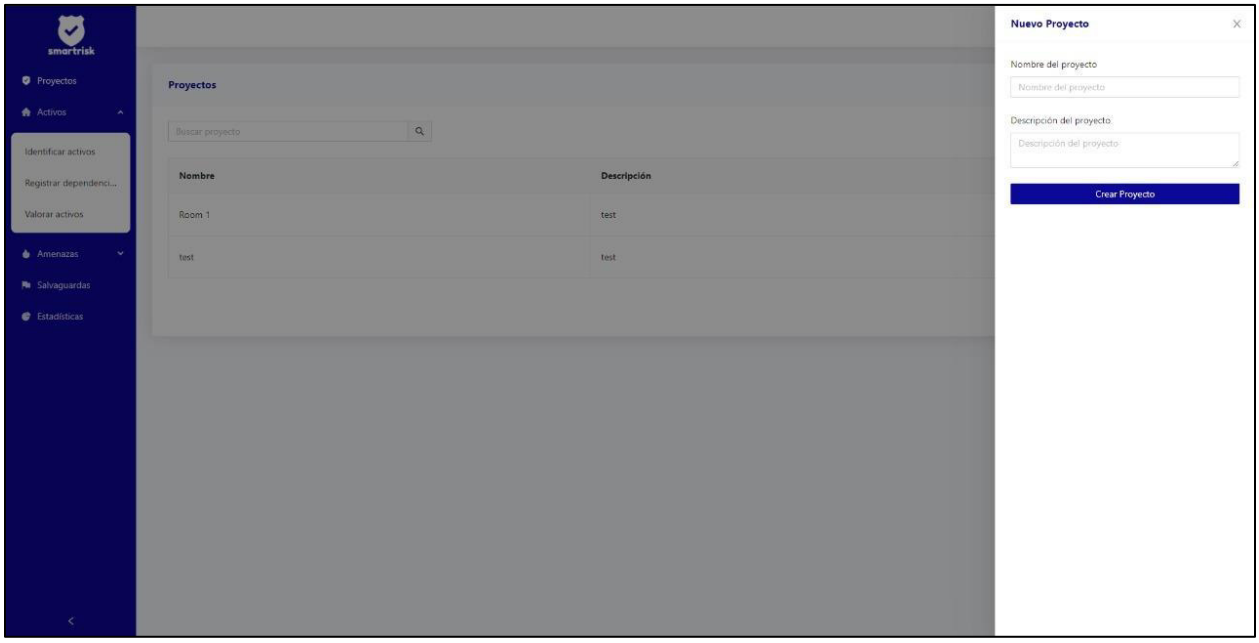


Figura 16 Formulario de registro de proyecto Spring 1

PR02: Consultar datos de proyectos

Los proyectos registrados en el sistema por el usuario se muestran en una tabla como se muestra en la Figura 17, la columna acción no es un dato si no es una acción que se puede hacer sobre dicha fila que representa a un proyecto, las acciones que se pueden realizar son editar (icono lápiz) y eliminar (icono basurero). Además, cuenta con un buscador que sirve para filtrar y buscar un proyecto en específico.

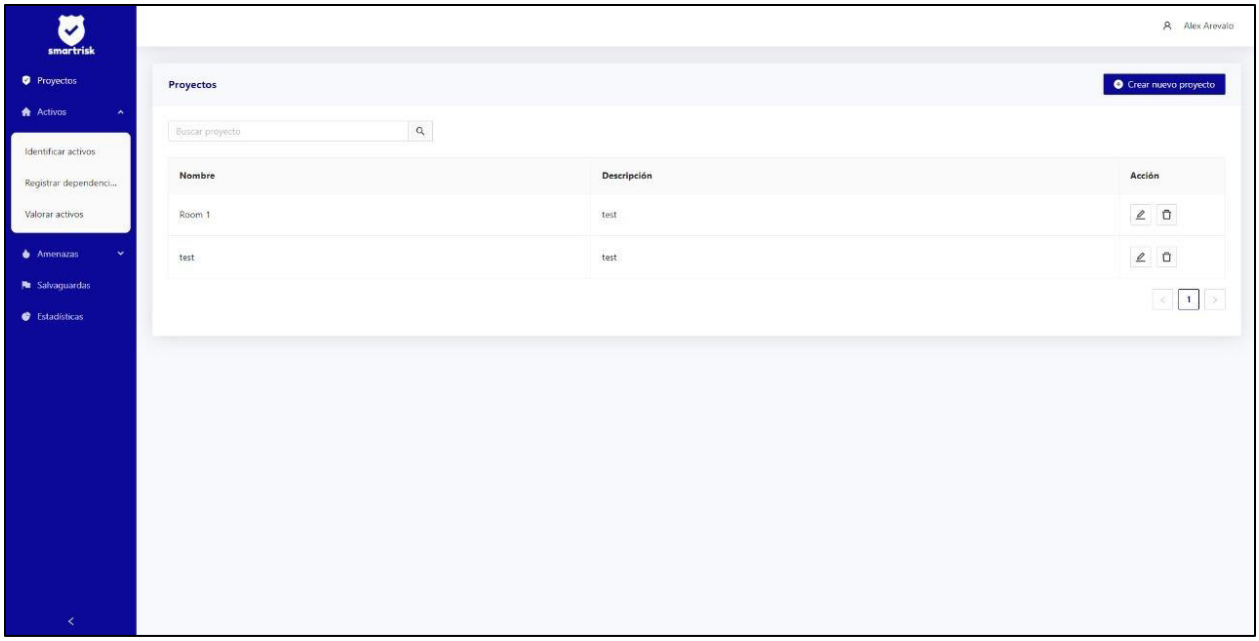


Figura 17 Tabla de datos de proyecto registrados.

PR03: Modificar datos del proyecto

El formulario para editar los datos de un proyecto previamente registrado se muestra en la Figura 18, en este formulario se puede modificar los datos de los campos antes ingresados, una vez finalizado la edición debe dar clic en “Guardar Cambios” para guardar los cambios.

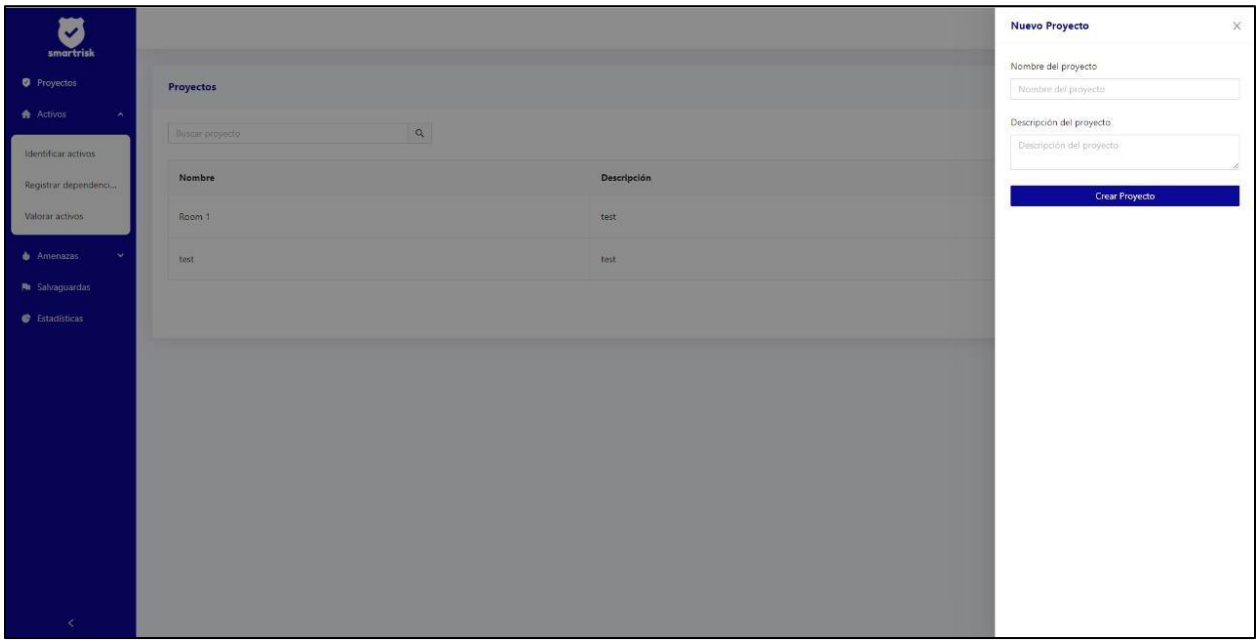


Figura 18 Formulario de edición de proyecto antes registrado

PR04: Eliminar un proyecto

La eliminación de un proyecto inicia en el momento en que da clic en el icono del basurero como se muestra en la Figura 19, para confirmar la eliminación se muestra una notificación donde si da clic en aceptar el proyecto se eliminará caso contrario se cancela.

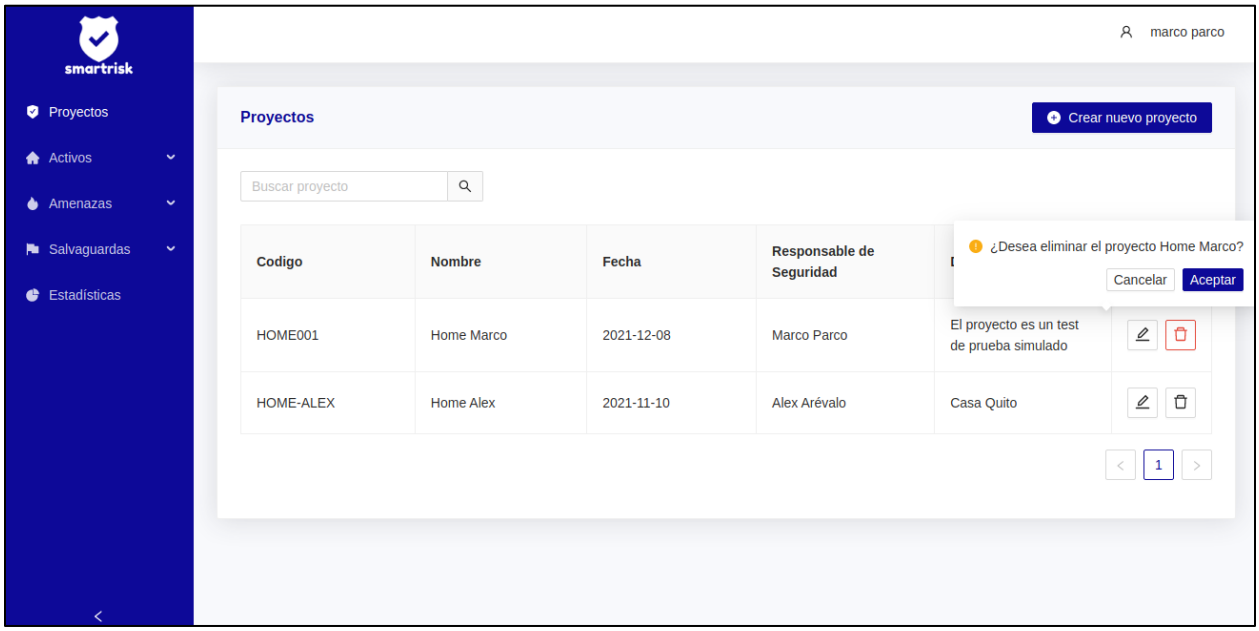


Figura 19 Eliminar Proyecto

2.3.2.3 Revisión del Spring

Una vez realizadas las historias de usuario en la primera iteración se realiza la presentación del producto funcional, logrando así obtener la retroalimentación de los interesados del producto y siendo esta resumida en la Tabla 17 (*Spring Review*) donde se detallan las observaciones realizadas por los interesados.

Tabla 17 Revisión de la iteración de la primera iteración

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
AU01	Registro en el sistema	Ninguna	5	5	0

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
AU02	Inicio de sesión en el sistema	Ninguna	8	8	0
PR01	Registrar un proyecto	1.- El formulario de registro del proyecto debe contar con información mínima como así lo requiere la metodología Magerit (nombre del proyecto, fecha, responsable y descripción)	8	8	0
PR02	Consultar datos de proyectos	1.- Desplegar la información adicional de los campos agregados en el requisito PR01.	3	3	0
PR03	Modificar datos del proyecto	1.- Modificar la información adicional de los campos agregados en el requisito PR01	3	3	0
PR04	Eliminar un proyecto	Ninguna	3	3	0
Total			**30**	**30**	**0**

2.3.2.4 Despliegue

Para el despliegue de la aplicación web en un ambiente real se utilizaron varios servicios web gratuitos que se describen en la Tabla 18, con los cuales se logró obtener un ciclo de despliegue continuo para ser utilizado durante todos los Sprint.

Tabla 18 Servicios Web utilizados para el despliegue de la aplicación

Servicios Web		
Servicio	**Descripción**	**Características**
Netlify	Despliegue del frontend	Hosting estático con un ancho de banda de 100GB y despliegues automáticos desde GitHub.
Heroku	Despliegue del backend	Servidor Web con 512 MB de memoria RAM y despliegues automáticos desde GitHub.
GitHub Actions	Despliegue del backend	Workflows de integración continua para sincronizar la base de datos a través de migraciones.
MongoDB Atlas	Base de datos	Base de datos MongoDB en la nube con 5GB de almacenamiento y memoria ram compartida.

Los servicios de Netlify y Heroku realizan un despliegue continuo cada vez que detecta nuevos cambios en la rama desarrollo (*develop)* de los repositorios del frontend y backend respectivamente, esto ayuda a que se pueda visualizar los nuevos cambios en la aplicación a medida que se vaya desarrollando los requerimientos de cada Sprint.

2.3.3 Spring 2

2.3.3.1 Planificación del Spring

Tabla 19 Planificación del Sprint para el segundo Sprint.

Código	**Nombre**	**Descripción**	**Prioridad**	**Estimación** (*Story Points*)
Proyecto				
PR01	Registrar un proyecto	[Procedente de la Iteración 1] Registrar un proyecto con los siguientes datos: nombre del proyecto, fecha, responsable y descripción.	Alta	3
PR02	Consultar datos de proyectos	[Procedente de la Iteración 1] Mostrar en una tabla los proyectos registrados con los siguientes datos: nombre del proyecto, fecha, responsable y descripción	Media	1

PR03	Modificar datos del proyecto	[Procedente de la Iteración 1] Modificar los datos de un proyecto que incluyan los siguientes campos: nombre del proyecto, fecha, responsable y descripción.	Media	1
Caracterización de activos				
CA01	Registrar activos	***Como*** usuario ***quiero*** registrar los activos ***para*** tener una lista con los activos críticos del hogar inteligente.	Alta	8
CA02	Consultar datos de activos	***Como*** usuario ***quiero*** consultar datos de los activos ingresados	Alta	3
CA03	Modificar datos del activo	***Como*** usuario ***quiero*** modificar los datos ingresados anteriormente de un activo.	Media	3
CA04	Eliminar un activo	***Como*** usuario ***quiero*** eliminar un proyecto	Media	3
CA05	Registrar un grupo de activos	***Como*** usuario ***quiero*** registrar un grupo de activos para no tener que registrar uno por uno.	Media	5
CA06	Registrar la dependencia existente de un activo con otro	***Como*** usuario ***quiero*** registrar la dependencia que existe de un activo con otro.	Alta	5
CA07	Registrar el valor del activo	***Como*** usuario ***quiero*** registrar el valor del activo en cada dimensión de seguridad	Alta	5
Total				**37**

A continuación, en la Tabla 20 hasta la Tabla 29 se detallan las historias de usuario del primer Spring:

Tabla 20 Historia de usuario PR01 – Procedente del Sprint 1

Historia de Usuario	**PR01**
Fecha:	28/9/2021
Código:	PR01
Requisito:	Registrar un proyecto
Puntos estimados:	3
Prioridad:	Alta

Historia de Usuario	**PR01**
Descripción:	**Como** usuario **quiero** registrar un proyecto en el sistema. [Procedente de la Iteración 1] Registrar un proyecto con los siguientes datos nombre del proyecto, fecha, responsable y descripción
Justificación:	Inicia con la creación de un proyecto que registra los datos de la casa inteligente
Dependencia:	No aplica
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá registrar un proyecto ingresando los siguientes datos: - Código del proyecto - Nombre del proyecto - Fecha del proyecto - Responsable de seguridad - Descripción del proyecto 2. El sistema validará que los campos: código del proyecto, nombre del proyecto, fecha del proyecto no estén vacíos, si algún campo esta vació mostrará el mensaje de error en cada campo: "Ingrese el [código del proyecto, nombre del proyecto, fecha del proyecto]" 3. Los campos responsables de seguridad y descripción del proyecto son campos opcionales, permitirá guardar un proyecto sin datos en estos campos.

Tabla 21 Historia de usuario PR02 – Procedente del Sprint 1.

Historia de Usuario	**PR02**
Fecha:	28/9/2021
Código:	PR02
Requisito:	Consultar datos de proyectos
Puntos estimados:	1
Prioridad:	Media
Descripción:	**Como** usuario **quiero** consultar datos de los proyectos ingresados. [Procedente de la Iteración 1] Mostrar en una tabla los proyectos registrados con los siguientes datos: nombre del proyecto, fecha, responsable y descripción
Justificación:	Listar todos los proyectos que se ha creado por parte del usuario
Dependencia:	PR01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo

Historia de Usuario	PR02
Criterios de aceptación:	1. El sistema mostrará una tabla con todos los proyectos registrados por el usuario en el sistema, la cual estará distribuida en una tabla con las siguientes columnas: - Código - Nombre - Fecha - Responsable de seguridad - Descripción - Acción 2. La columna acción mostrará la función de editar y/o eliminar. - Editar está representado por un icono de lápiz que permitirá abrir un formulario para editar los campos del proyecto. - Eliminar está representado por un ícono de basurero que permitirá abrir un cuadro de confirmación para eliminar el proyecto. 3. El sistema permitirá buscar un proyecto mediante un buscador que filtrará mediante el nombre del proyecto.

Tabla 22 Historia de usuario PR03 – Procedente del Sprint 1

Historia de Usuario	PR03
Fecha:	28/9/2021
Código:	PR03
Requisito:	Modificar datos del proyecto
Puntos estimados:	1
Prioridad:	Media
Descripción:	**Como** usuario **quiero** modificar los datos ingresados de un proyecto [Procedente de la Iteración 1] Modificar los datos de un proyecto que incluyan los siguientes campos: nombre del proyecto, fecha, responsable y descripción.
Justificación:	El usuario puede modificar los valores de los datos registrados por cada proyecto debido a una equivocación o cambio de valores.
Dependencia:	PR02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo

Historia de Usuario	**PR03**
Criterios de aceptación:	1. El sistema permitirá modificar datos del proyecto, para el cual se muestra un formulario completo con los datos antes ingresados, donde se pueden cambiar los siguientes datos: - Código del proyecto - Nombre del proyecto - Fecha del proyecto - Responsable de seguridad - Descripción del proyecto 2. Al modificar la información del proyecto el sistema validará: - Los campos código del proyecto, nombre del proyecto y fecha del proyecto que no se encuentren vacíos al guardar los cambios realizados, si el campo este vacío mostrará el mensaje de error: *¡Ingrese el [código del proyecto, nombre del proyecto y fecha del proyecto]!* 3. Al modificar la información de los campos responsable de seguridad y descripción del proyecto son campos opcionales, permitirá guardar un proyecto sin datos en estos campos.

Tabla 23 Historia de usuario CA01

Historia de Usuario	**CA01**
Fecha:	28/9/2021
Código:	CA01
Requisito:	Registrar activos
Puntos estimados:	8
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** registrar los activos ***para*** tener una lista con los activos críticos del hogar inteligente.
Justificación:	Permitirá registrar los activos de la casa inteligente para conocer qué clase de activos hay en la casa inteligente.
Dependencia:	No aplica
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo y Marco Parco

Criterios de aceptación:	1. El sistema permitirá registrar activos ingresando los siguientes datos: - Identificación del activo - Nombre del activo - Modelo del activo - Clase del activo 2. El sistema validará que los campos identificación del activo, nombre del activo no estén vacíos, si alguno de los campos se encuentra vacío mostrará el mensaje de error en cada campo: *"¡Ingrese el/la [identificación del activo, nombre del activo]!"* 4. El sistema permitirá seleccionar uno o varios tipos de activo al cuál pertenezca el activo. 5. El sistema validará que los campos identificación del activo, nombre del activo no estén vacíos antes de registrar el activo, si alguno se encuentra vacío mostrará un mensaje de error como se mencionó en 2.

Tabla 24 Historia de usuario CA02

Historia de Usuario	**CA02**
Fecha:	28/9/2021
Código:	CA02
Requisito:	Consultar datos de activos
Puntos estimados:	3
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** consultar datos de los activos ingresados
Justificación:	Permitirá visualizar los datos que se han ingresado de los activos registrados
Dependencia:	CA01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo y Marco Parco

Criterios de aceptación:	1. El sistema mostrará una tabla con la lista de activos registrados previamente por el usuario en el sistema, la cual estará distribuida en una tabla con las siguientes columnas: - Identificación - Nombre - Modelo - Acción 2. La columna acción mostrará la función de editar y/o eliminar un activo. - Editar está representado por un icono de lápiz que permitirá abrir un formulario para editar los campos del activo. - Eliminar está representado por un ícono de basurero que permitirá abrir un cuadro de confirmación para eliminar el activo. 3. El sistema permitirá buscar un activo mediante un buscador que filtrará mediante el nombre del activo.

Tabla 25 Historia de usuario CA03

Historia de Usuario	**CA03**
Fecha:	28/9/2021
Código:	CA03
Requisito:	Modificar datos del activo
Puntos estimados:	3
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** modificar los datos ingresados anteriormente de un activo.
Justificación:	El usuario podrá modificar los valores de los datos registrados anteriormente por cada activo debido a una equivocación o cambio de valores.
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo y Marco Parco

Historia de Usuario	**CA03**
Criterios de aceptación:	1. El sistema permitirá modificar datos del activo registrados anteriormente, para el cuál se muestra un formulario completo con los datos antes ingresados, donde se pueden cambiar los siguientes datos: - Identificación del activo - Nombre del activo - Modelo del activo - Clase de activo 2. Al modificar la información del proyecto el sistema validará: - Los campos identificación del activo, nombre del activo y que no se encuentren vacíos, previos al guardar los cambios realizados, si el campo está vacío mostrará el mensaje de error: *¡Ingrese el/la [identificación del activo, nombre del activo]!* 3. Al modificar la información de modelo del activo al ser un campo opcional el sistema permitirá guardar un activo sin datos en este campo.

Tabla 26 Historia de usuario CA04

Historia de Usuario	**CA04**
Fecha:	28/9/2021
Código:	CA04
Requisito:	Eliminar un activo
Puntos estimados:	3
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** eliminar un proyecto
Justificación:	El usuario podrá eliminar un proyecto de la lista de activos registrados anteriormente
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá eliminar un activo creado previamente por el usuario, antes de eliminar se presentará una notificación de aviso *¿Desea eliminar el activo [nombre del activo]?*, si el usuario desea eliminar debe aceptar caso contrario debe cancelar la notificación que se muestra.

Tabla 27 Historia de usuario CA05

Historia de Usuario	**CA05**
Fecha:	28/9/2021
Código:	CA05

Historia de Usuario	**CA05**
Requisito:	Registrar un grupo de activos
Puntos estimados:	5
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** registrar un grupo de activos para no tener que registrar uno por uno.
Justificación:	El usuario podrá registrar un grupo de activos en una sola carga lo que facilitará el registro del activo.
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá cargar un archivo de extensión xlsx, el cual debe contener 7 columnas denominadas: - ID - NAME - MODEL , donde; - ID corresponde a la identificación del activo - NAME corresponde al nombre del activo - MODEL corresponde al modelo del activo

Tabla 28 Historia de usuario CA06

Historia de Usuario	**CA06**
Fecha:	28/9/2021
Código:	CA06
Requisito:	Registrar la dependencia existente de un activo con otro
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** registrar la dependencia que existe de un activo con otro.
Justificación:	El registro de la dependencia entre activos permite simular el entorno de funcionamiento del ecosistema IoT
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema mostrará una matriz donde se puede ingresar la dependencia de un activo con otro en la celda de intersección. 2. El usuario podrá ingresar si existe dependencia entre activos únicamente cuatro tipos de dependencia: - 1 o Servicio - 2 o Aplicación - 3 o Equipo - 4 o Instalación

Tabla 29 Historia de usuario CA07

Historia de Usuario	**CA07**
Fecha:	28/9/2021
Código:	CA07
Requisito:	Registrar el valor del activo
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** registrar el valor del activo en cada dimensión de seguridad
Justificación:	El valor del activo permite realizar cálculos posteriores para evaluar el riesgo.
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá registrar el valor del activo en cada dimensión para la cual se mostrará una ventana donde el usuario puede valorar el activo de tres formas: - NA. Es decir, no se valora el activo - Una escala de 0 a 10. - Un valor de 0 a 10 dependiendo a criterios como propone la metodología Magerit.

2.3.3.2 Implementación

A continuación, se describe la implementación de las historias de usuarios de la segunda iteración, además incluye historias de usuario que proceden de la primera iteración que tuvieron observaciones.

PR01: Registrar un proyecto

El registro de proyecto se lo realiza mediante un formulario como se muestra en la Figura 20, donde se ingresa todos los campos necesarios código del proyecto, nombre del proyecto, fecha del proyecto, responsable del proyecto y descripción del proyecto. Una vez registrados los campos para guardar se debe dar clic en el botón “Crear Proyecto” y el proyecto será registrado.

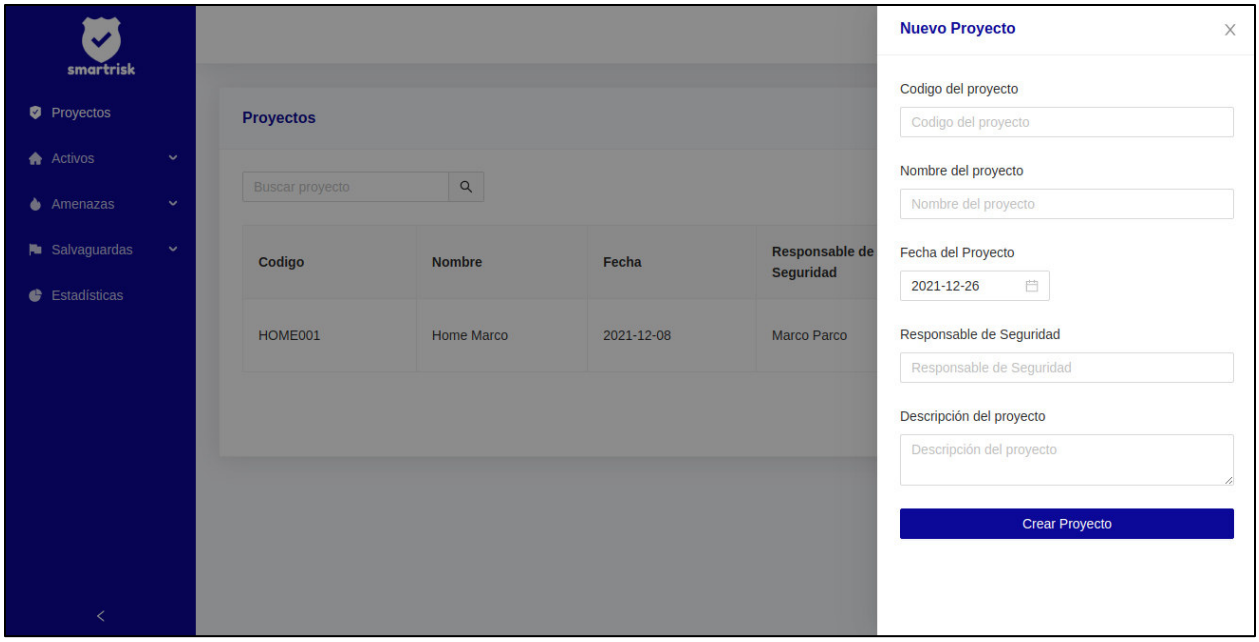


Figura 20 Formulario de registro de un proyecto – Spring 2.

Antes de crear un proyecto el sistema valida el formulario y verifica si los campos obligatorios código del proyecto, nombre del proyecto y fecha del proyecto no estén vacíos caso contrario no se podrá crear el proyecto y se muestra mensaje de error como se muestra en la Figura 21.

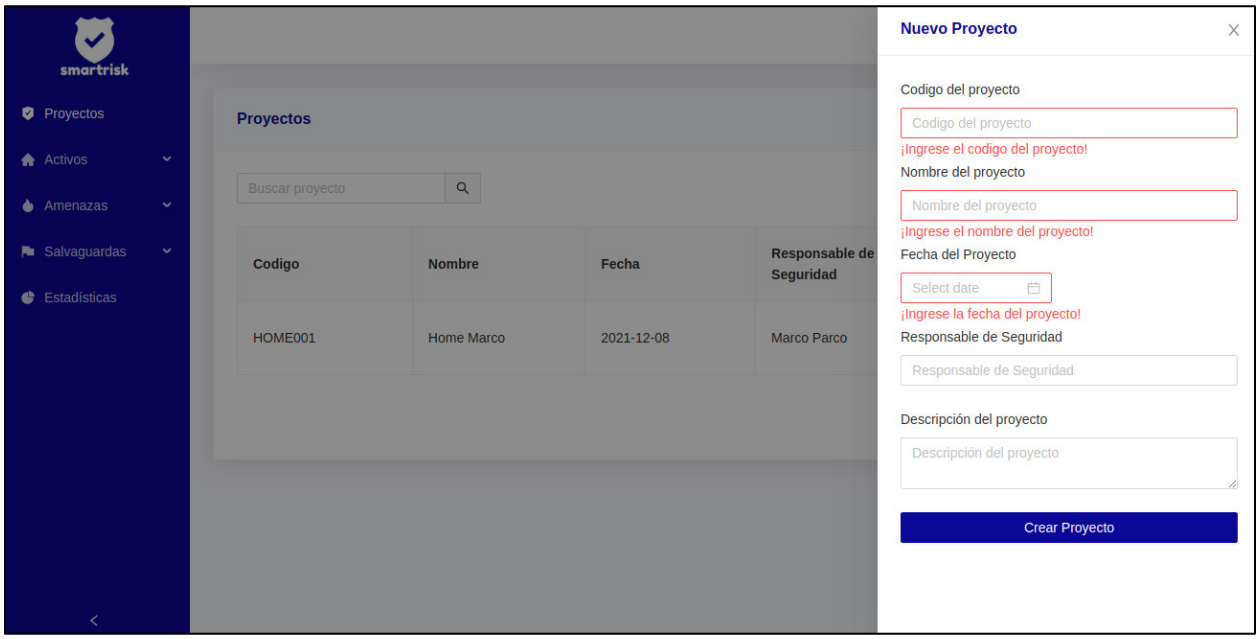


Figura 21 Validación del formulario de registro de un proyecto

PR02: Consultar datos de proyectos

Los proyectos registrados se muestran en una tabla como se muestra en la Figura 22, la columna acción cuenta con las funciones de editar (icono de lápiz) y eliminar (icono de basurero). Además, al ser una tabla que maneja gran cantidad de datos tiene un cuadro para buscar un proyecto en específico con tan solo ingresar el nombre de proyecto el sistema filtrara el proyecto a buscar.

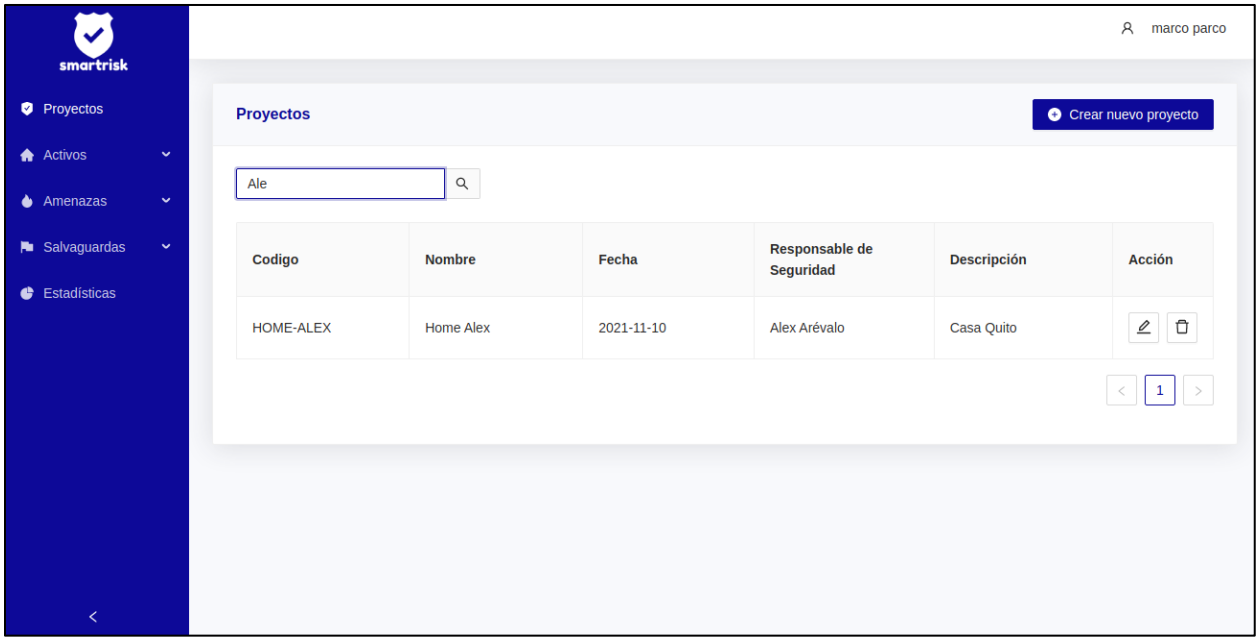


Figura 22 Tabla de datos proyectos registrados – Spring 2

PR03: Modificar datos del proyecto

La edición de los datos de un proyecto ya ingresados anteriormente que se encuentra en la tabla de proyecto (Figura 22), para modificar cualquier dato únicamente debe dar clic en editar (icono lápiz) y se mostrará el formulario de la Figura 23, en este formulario el usuario puede modificar la información antes ingresada. Es importante tomar en cuenta que los campos obligatorios son: código del proyecto, nombre del proyecto, fecha del proyecto lo cual no se podrá guardar el proyecto si estos campos están vacíos.

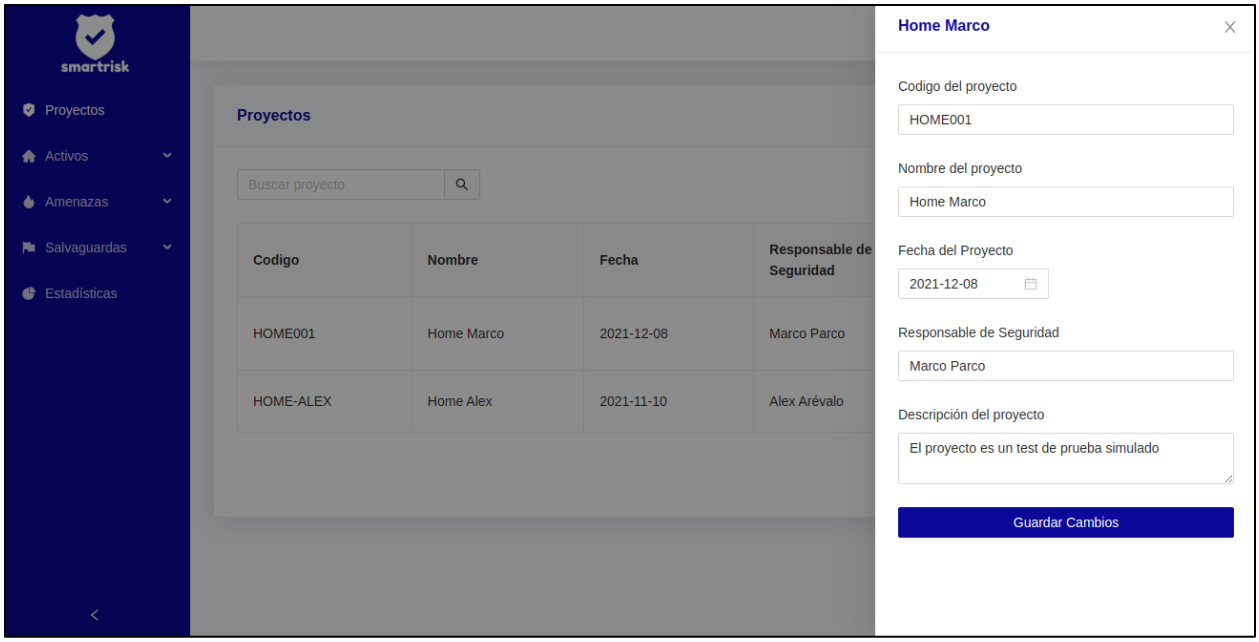


Figura 23 Formulario para modificar de un proyecto - Spring 2

CA01: Registrar activos

El ingreso de activos se lo realiza mediante un formulario como se muestra en la Figura 24, los datos necesarios para ingresar un activo son: identificación del activo, nombre del activo, modelo del activo y clase de activo. Ya ingresado todos los datos en los campos se procede a validar los campos en donde la identificación del activo y nombre del activo no pueden ser campos vacíos lo cual no permitirá crear un nuevo activo. Para crear un nuevo activo se debe dar clic en el botón “Crear Activo”.

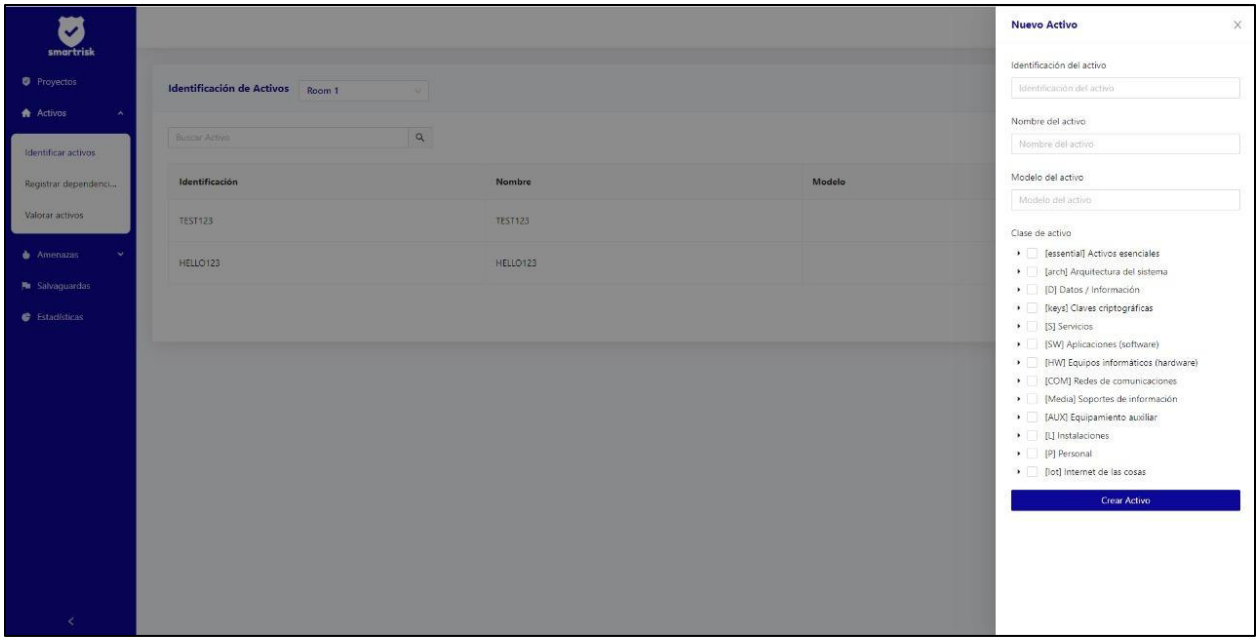


Figura 24 Formulario de registro de un activo.

CA02: Consultar datos del activo

Una vez ya registrados los activos se muestran en una tabla como en la Figura 25, la columna Acción son las funciones que el usuario puede realizar sobre ese activo editar (icono de lápiz) y eliminar (icono de basurero). Al ser una tabla que maneja gran cantidad de datos cuenta con filtro en donde se puede buscar un activo especifico únicamente buscándolo por el nombre del activo.

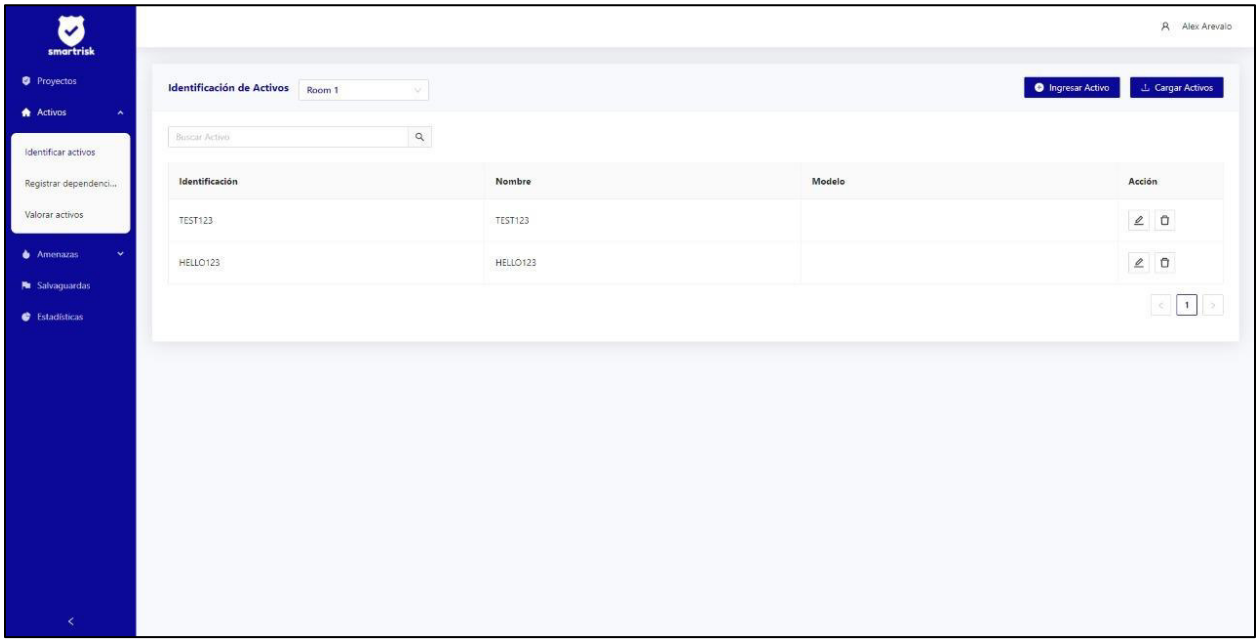


Figura 25 Tabla de datos de activos ya ingresados.

CA03: Modificar datos del activo

La edición de los datos de activos ya ingresados se lo realiza dando clic en el icono de lápiz de la tabla de activos (Figura 25), posterior se muestra un formulario donde se editan los campos de todos los activos (Figura 26) una vez ya modificado para guardar los cambios se debe dar clic en “Guardar Cambios”.

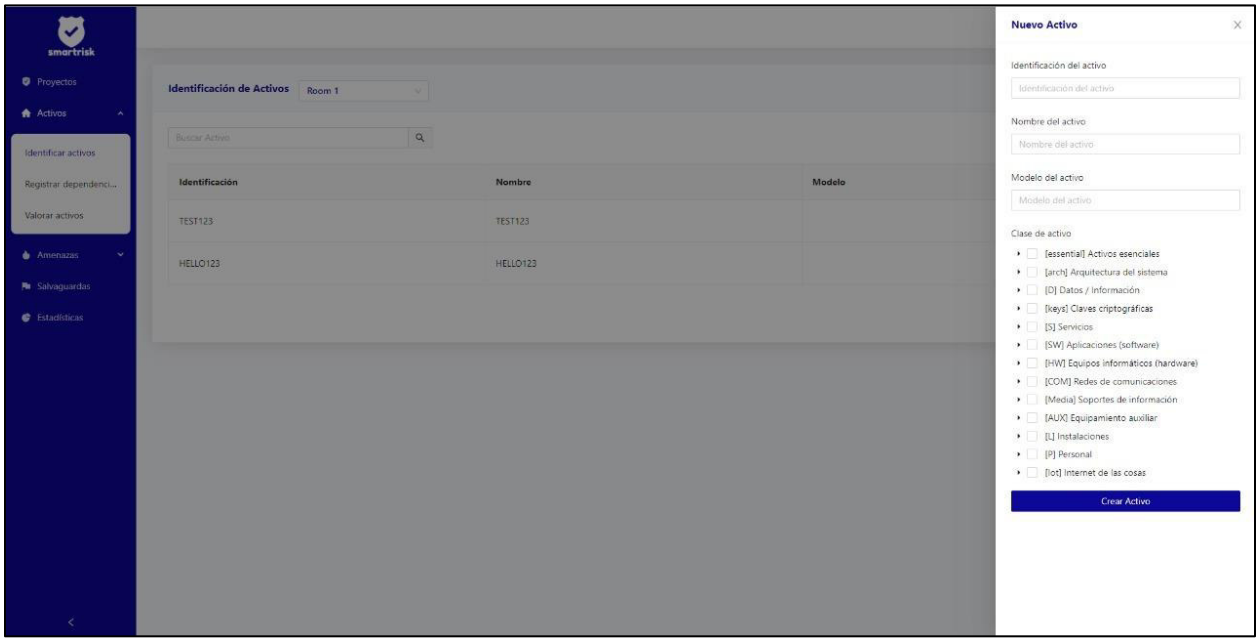


Figura 26 Formulario de edición de un activo

CA04: Eliminar un activo

La eliminación de un activo registrado se efectuará al momento de dar clic en el icono de basurero en la columna de acción de cada activo, antes de eliminar el activo el sistema muestra una notificación de confirmación si está seguro de eliminar el mismo. (Figura 27)

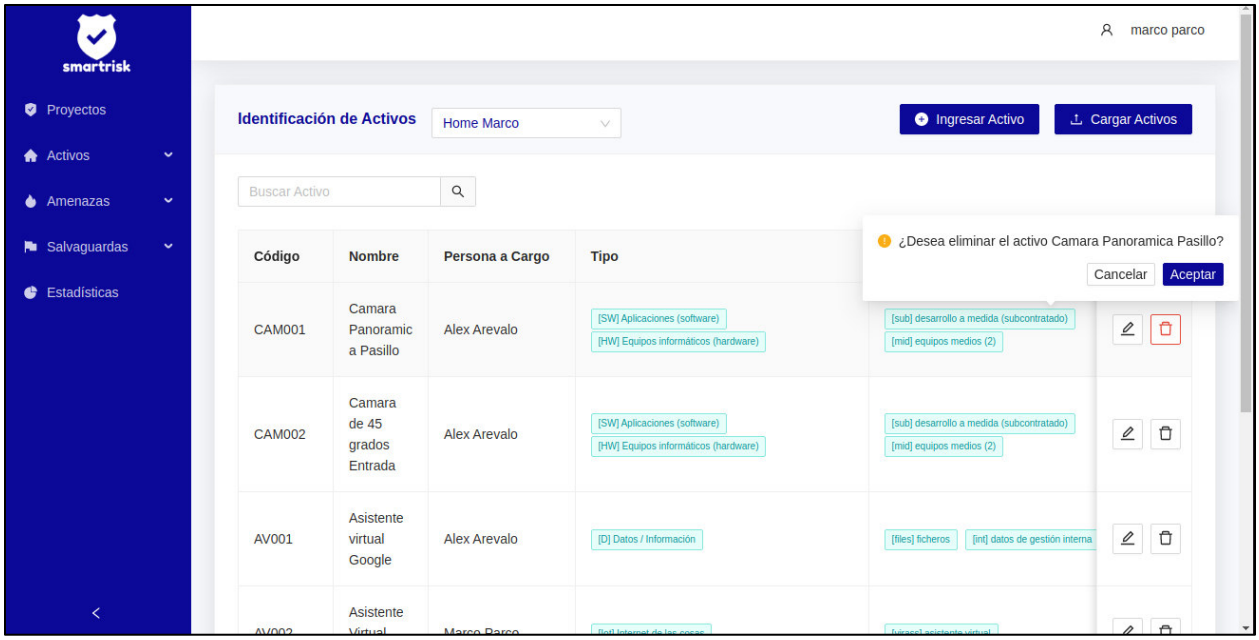


Figura 27 Eliminar un activo

CA05: Registrar un grupo de activos

El registro de un grupo de activos se lo realiza mediante la carga de un archivo de extensión .xlsx (Figura 28), el sistema permitirá que el usuario pueda cargar un grupo de activos ya registrados en una hoja de cálculo.

ID	NAME	MODEL
CAM004	Refrigeradora	Modelo:Samsung
CAM005	Termostato	Modelo:Samsung
CAM006	Microondas	Modelo:Samsung
CAM007	Foco	Modelo:Samsung
CAM008	Cafetera	Modelo:Samsung
CAM009	Televisor	Modelo:Samsung

Figura 28 Formato de archivo estándar

Con el archivo estándar a la mano el sistema permitirá cargar mediante el explorador de archivos o arrastrando el archivo hasta la posición de icono de carga como se muestra en la Figura 29, ya cargado el archivo para que se ingresen los activos se debe dar clic en el botón “Cargar” y automáticamente se mostraran en la tabla de activos.

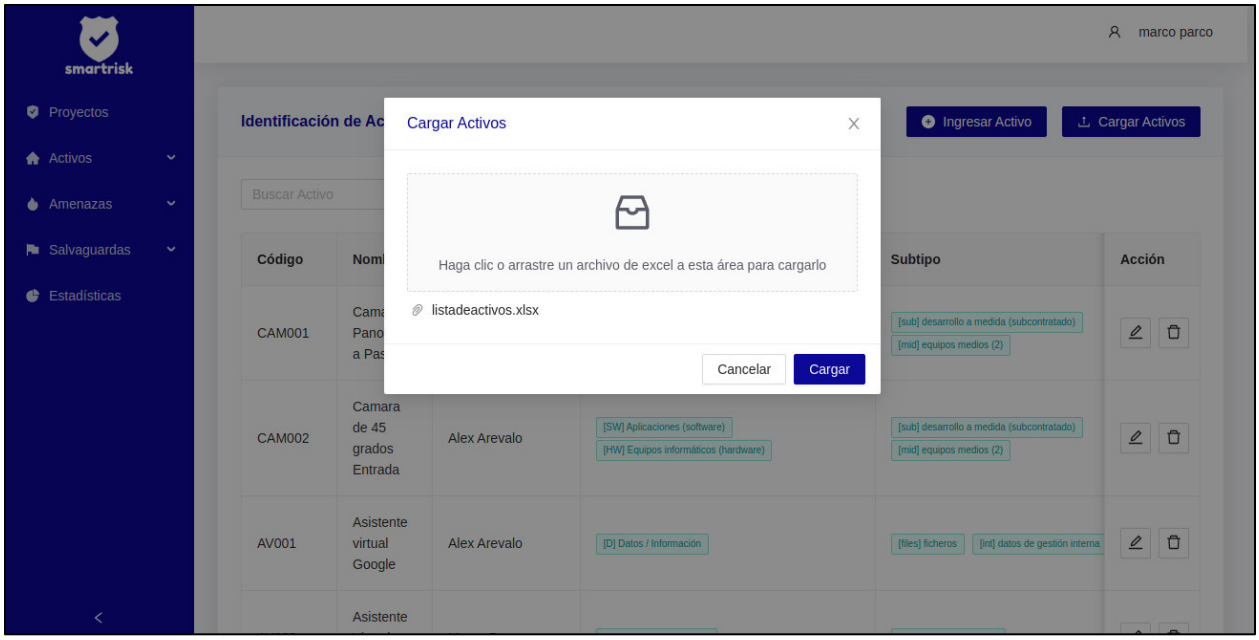


Figura 29 Cargar un archivo para ingreso de un grupo de activos

CA06: Registrar la dependencia existente de un activo con otro

La dependencia de un activo con otro se lo realiza mediante una matriz donde la celda de intersección muestra esta relación y en la misma se registrará el número de dependencia que tiene un activo con otro. (Figura 30)

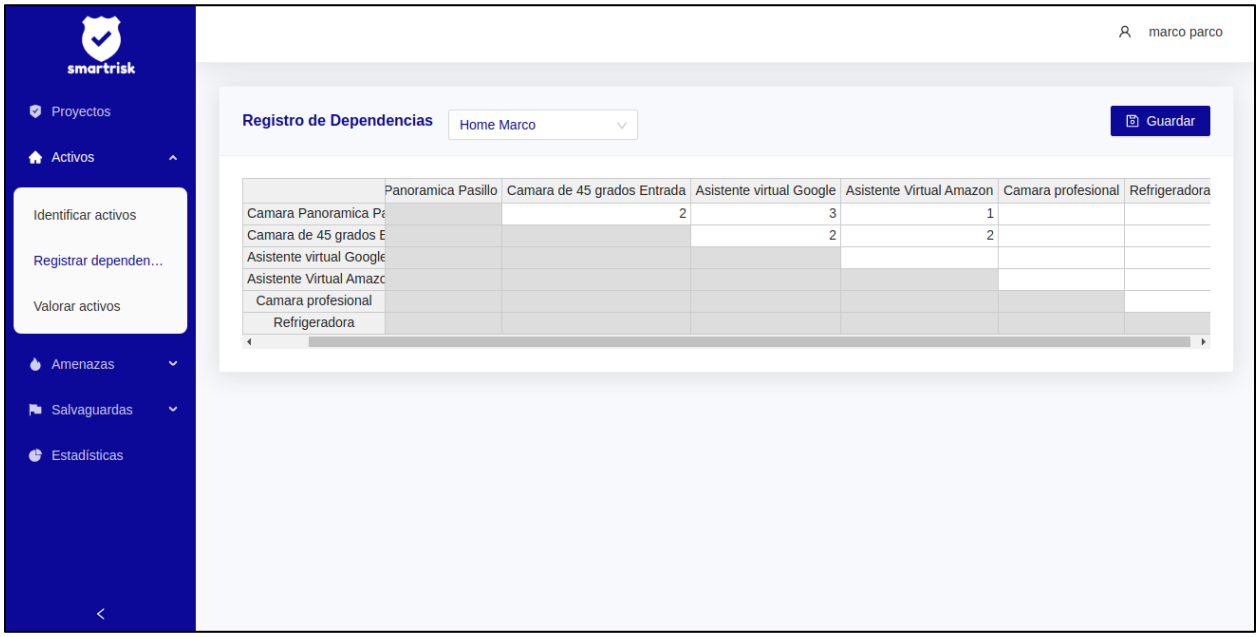


Figura 30 Matriz para registro de dependencias entre activos

CA07: Registrar el valor del activo

El registro del valor del activo se lo realiza en varias dimensiones de seguridad (Figura 31), un activo puede ser valorado en todas las dimensiones o no debido a que depende a criterios del usuario a que tan valioso es el activo, esta valoración no es referido al costo sino a la importancia que tiene el activo en el ecosistema del internet de las cosas.

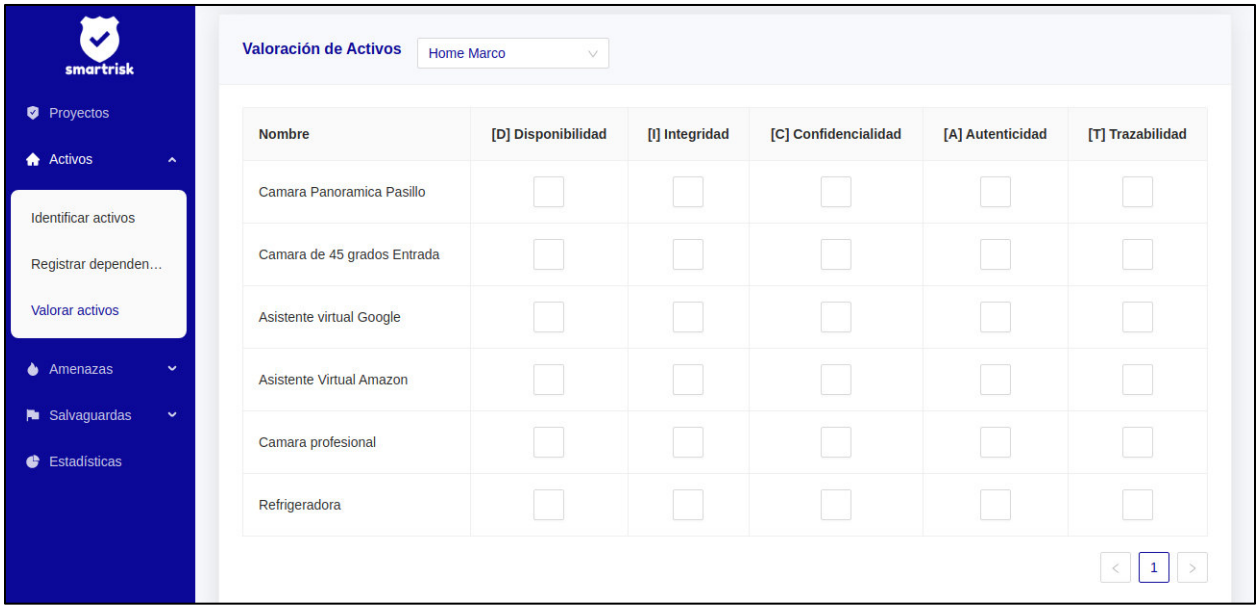


Figura 31 Tabla de registro del valor del activo

La valoración de un activo se lo realiza mediante escalas como indica la metodología Magerit de donde se basa la lógica del software es por tal que el usuario para valorar un activo tiene tres opciones:

a.- No aplica

b.- Escala numérica de 1 al 10, y

c.- Escala numérica con criterios técnicos de 1 al 10.

Como se muestra en la Figura 32, el usuario valorará el activo en cada dimensión de seguridad y debe dar clic en el botón “Guardar” para que se refleje el valor del activo guardado en esa dimensión como se muestra en la Figura 33.

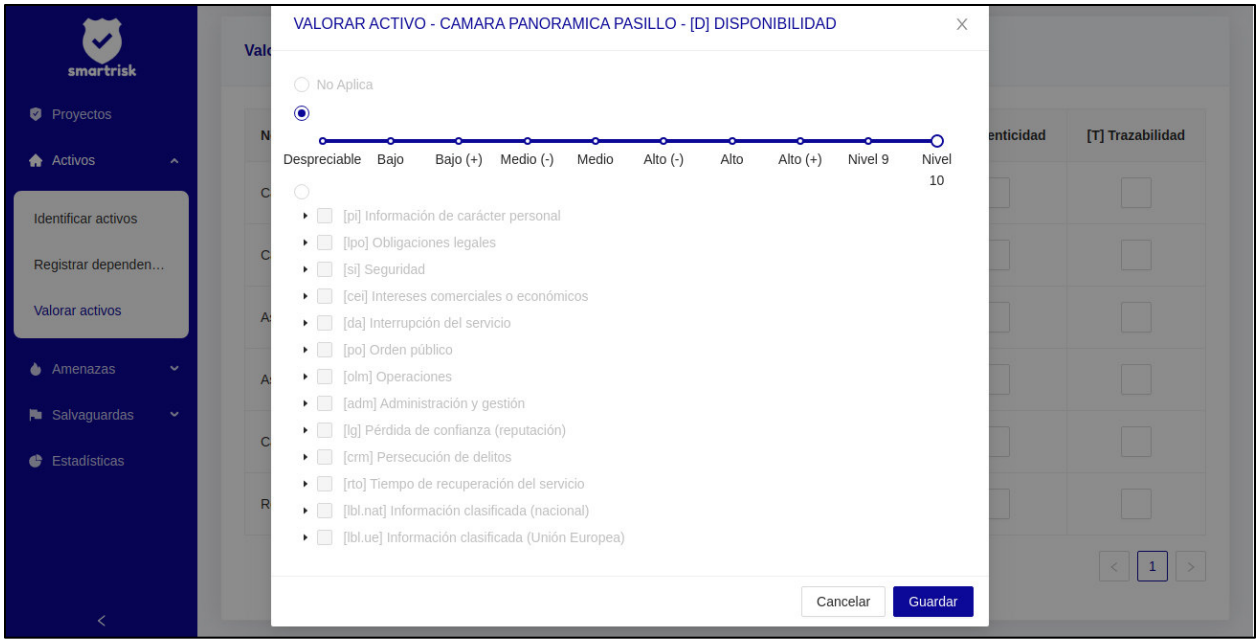


Figura 32 Opciones de valoración de un activo

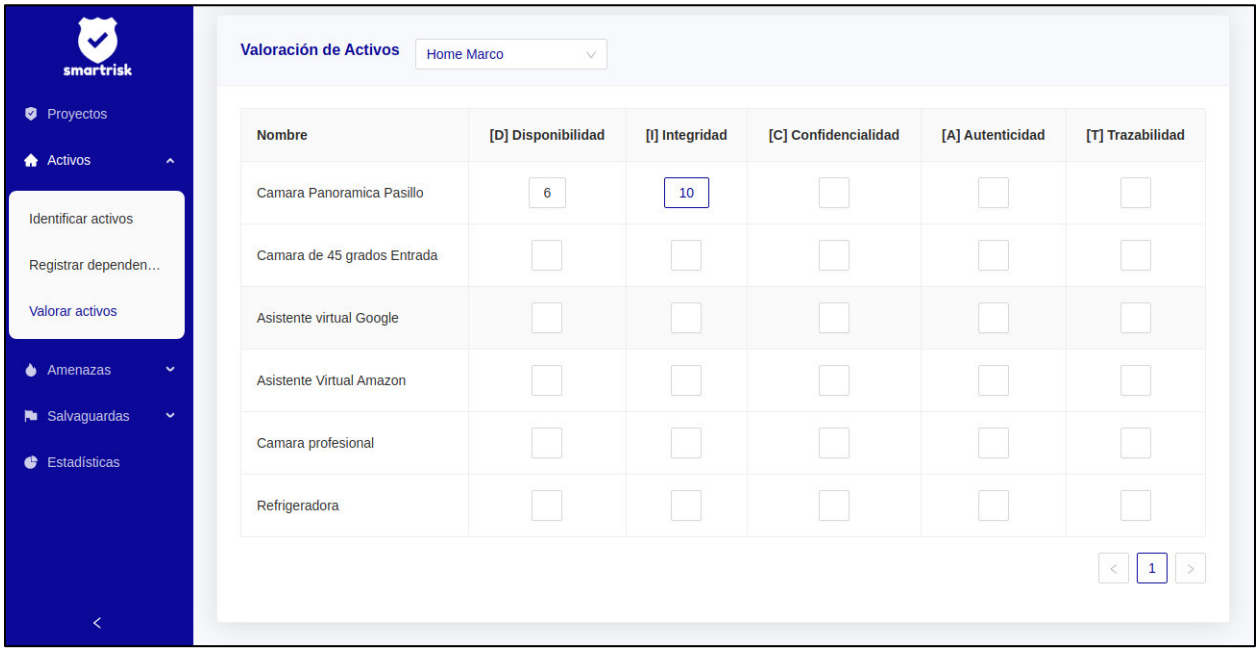


Figura 33 Registro del valor de un activo.

2.3.3.3 Revisión del Spring

Una vez finalizado el desarrollo de las historias de usuario de la segunda iteración se procede a entregar al interesado el producto funcional. La retroalimentación del producto funcional se resume en la Tabla 30 (*Spring Review*), aquí se detallan las observaciones con relación al producto de la segunda iteración.

Tabla 30 Revisión de la iteración de la segunda iteración.

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
PR01	Registrar un proyecto	Ninguna	3	3	0
PR02	Consultar datos de proyectos	Ninguna	1	1	0
PR03	Modificar datos del proyecto	Ninguna	1	1	0
CA01	Registrar activos	1.- Al registrar un activo se debe registrar con los campos mínimos que requiere la metodología Magerit estos campos son: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.	8	8	0
CA02	Consultar datos de activos	1.- La información del tipo y subtipo al que pertenece el activo es importante que se	3	3	0

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
		muestre debido a que ayuda a identificar las amenazas ligadas al activo.			
CA03	Modificar datos del activo	1. Al modificar el CA01 también cambia este requisito.	3	3	0
CA04	Eliminar un activo	Ninguna	3	3	0
CA05	Registrar un grupo de activos	1. Al modificar el CA01 también cambia este requisito.	5	5	0
CA06	Registrar la dependencia existente de un activo con otro	Ninguna	5	5	0
CA07	Registrar el valor del activo	Ninguna	5	5	0
Total			**37**	**37**	**0**

2.3.3.4 Despliegue

Para el despliegue de esta iteración se utilizó la misma configuración de despliegue continuo que se detalló en el primer Sprint.

2.3.4 Spring 3

2.3.4.1 Planificación del Spring

Tabla 31 Planificación para la tercera iteración

Código	Nombre	Descripción	Prioridad	Estimación (*Story Points*)
Caracterización de activos				
CA01	Registrar activos	[Procedente de la Iteración 2] Registrar los campos mínimos que requiere la metodología Magerit estos campos son: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.	Alta	3
CA02	Consultar datos de activos	[Procedente de la Iteración 2] La información del tipo y subtipo al que pertenece el activo es importante que se muestre debido a que ayuda a identificar las amenazas ligadas al activo.	Alta	2
CA03	Modificar datos del activo	[Procedente de la Iteración 2] Al modificar un activo se debe considerar los campos: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.	Media	2
CA05	Registrar un grupo de activos	[Procedente de la Iteración 2] Al cargar un lote de un grupo de activos se debe considerar los campos: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.	Media	2
Caracterización de Amenazas				
CAM01	Visualizar las amenazas del activo	***Como*** usuario ***quiero*** observar las amenazas a las que está ligado el activo.	Alta	8
CAM02	Registrar vulnerabilidades en cada amenaza	***Como*** usuario ***quiero*** registrar información de vulnerabilidades ligadas a las amenazas.	Media	5

Código	Nombre	Descripción	Prioridad	Estimación (*Story Points*)
CAM03	Registrar el valor del porcentaje de degradación de la amenaza	***Como*** usuario ***quiero*** registrar el valor del porcentaje de degradación de la amenaza en cada dimensión de seguridad.	Alta	3
CAM04	Registrar el valor del porcentaje de probabilidad de ocurrencia de la amenaza.	***Como*** usuario ***quiero*** ingresar la probabilidad de ocurrencia cuando una amenaza se lleve a cabo.	Alta	3
Total				**28**

A continuación, en la Tabla 32 hasta la Tabla 39 se detallan las historias de usuario de la tercera iteración:

Tabla 32 Historia de usuario CA01 – Precedente del Spring 2.

Historia de Usuario	**CA01**
Fecha:	28/9/2021
Código:	CA01
Requisito:	Registrar activos
Puntos estimados:	3
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** registrar los activos ***para*** tener una lista con los activos críticos del hogar inteligente. [Procedente de la Iteración 2] Registrar los campos mínimos que requiere la metodología Magerit estos campos son: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.
Justificación:	Permitirá registrar los activos de la casa inteligente para conocer qué clase de activos hay en la casa inteligente.
Dependencia:	No aplica
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo y Marco Parco

Historia de Usuario	**CA01**
Criterios de aceptación:	1. El sistema permitirá registrar activos ingresando los siguientes datos: - Código del activo - Nombre del activo - Persona a cargo del activo - Ubicación - Cantidad - Descripción - Características Específicas - Clase del activo 2. El sistema validará que los campos código del activo, nombre del activo, cantidad del activo no estén vacíos, si alguno de los campos se encuentra vacío mostrará el mensaje de error en cada campo: *"¡Ingrese el/la [código del activo, nombre del activo, cantidad]!"* 3. El sistema validará que el campo cantidad únicamente son valores numéricos enteros positivos de 1 hasta 100. 4. El sistema permitirá seleccionar uno o varios tipos de activo al cuál pertenezca el activo. 5. El sistema validará que los campos código del activo, nombre del activo, cantidad del activo no estén vacíos antes de registrar el activo, si alguno se encuentra vacío mostrará un mensaje de error como se mencionó en 2.

Tabla 33 Historia de usuario CA02 – Precedente del Spring 2.

Historia de Usuario	**CA02**
Fecha:	28/9/2021
Código:	CA02
Requisito:	Consultar datos de activos
Puntos estimados:	2
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** consultar datos de los activos ingresados [Procedente de la Iteración 2] La información del tipo y subtipo al que pertenece el activo es importante que se muestre debido a que ayuda a identificar las amenazas ligadas al activo.
Justificación:	Permitirá visualizar los datos que se han ingresado de los activos registrados
Dependencia:	CA01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo y Marco Parco

Historia de Usuario	**CA02**
Criterios de aceptación:	1. El sistema mostrará una tabla con la lista de activos registrados previamente por el usuario en el sistema, la cual estará distribuida en una tabla con las siguientes columnas: - Código - Nombre - Persona a cargo - Tipo - Subtipo - Ubicación - Cantidad - Descripción - Características específicas 2. La columna acción mostrará la función de editar y/o eliminar un activo. - Editar está representado por un icono de lápiz que permitirá abrir un formulario para editar los campos del activo. - Eliminar está representado por un ícono de basurero que permitirá abrir un cuadro de confirmación para eliminar el activo. 3. El sistema permitirá buscar un activo mediante un buscador que filtrará mediante el nombre del activo.

Tabla 34 Historia de usuario CA03 – Precedente del Spring 2

Historia de Usuario	**CA03**
Fecha:	28/9/2021
Código:	CA03
Requisito:	Modificar datos del activo
Puntos estimados:	2
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** modificar los datos ingresados anteriormente de un activo. [Procedente de la Iteración 2] Al modificar un activo se debe considerar los campos: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.
Justificación:	El usuario podrá modificar los valores de los datos registrados anteriormente por cada activo debido a una equivocación o cambio de valores.
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo y Marco Parco

Historia de Usuario	**CA03**
Criterios de aceptación:	1. El sistema permitirá modificar datos del activo registrados anteriormente, para el cuál se muestra un formulario completo con los datos antes ingresados, donde se pueden cambiar los siguientes datos: - Código del activo - Nombre del activo - Persona a cargo del activo - Ubicación - Cantidad - Descripción - Características Específicas - Clase del activo 2. Al modificar la información del proyecto el sistema validará: - Los campos código del activo, nombre del activo y cantidad del activo que no se encuentren vacíos, previo al guardar los cambios realizados, si el campo está vacío mostrará el mensaje de error: *¡Ingrese el/la [código del activo, nombre del activo, cantidad]!* 3. Al modificar la información de los campos persona a cargo del activo, ubicación, descripción, características específicas y clase del activo y al ser campos opcionales el sistema permitirá guardar un activo sin datos en estos campos.

Tabla 35 Historia de usuario CA05 – Precedente del Spring 2

Historia de Usuario	**CA05**
Fecha:	28/9/2021
Código:	CA05
Requisito:	Registrar un grupo de activos
Puntos estimados:	2
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** registrar un grupo de activos para no tener que registrar uno por uno. [Procedente de la Iteración 2] Al cargar un lote de un grupo de activos se debe considerar los campos: código, nombre, persona a cargo, ubicación, cantidad, descripción, características específicas.
Justificación:	El usuario podrá registrar un grupo de activos en una sola carga lo que facilitará el registro del activo.
Dependencia:	CA02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo

Historia de Usuario	CA05
Criterios de aceptación:	1. El sistema permitirá cargar un archivo de extensión xlsx, el cual debe contener 7 columnas denominadas: - ID - NAME - PERSON_CHARGE - LOCATION - QUANTITY - DESCRIPTION - SPECIFIC_CHARACTERISTICS , donde; - ID corresponde al código del activo - NAME corresponde al nombre del activo - PERSON_CHARGE corresponde a la Personas a cargo del activo - LOCATION corresponde a la ubicación - QUANTITY corresponde a la cantidad - DESCRIPTION corresponde a la descripción - SPECIFIC_CHARACTERISTICS corresponde a las características específicas

Tabla 36 Historia de usuario CAM01

Historia de Usuario	CAM01
Fecha:	28/9/2021
Código:	CAM01
Requisito:	Visualizar las amenazas del activo
Puntos estimados:	8
Prioridad:	Alta
Descripción:	Como usuario quiero observar las amenazas a las que está ligado el activo.
Justificación:	Verificar cuales son las amenazas que están ligadas a un determinado activo para posterior poder cuantificar su implicación que puede tener sobre el activo.
Dependencia:	CA01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo

Historia de Usuario	CAM01
Criterios de aceptación:	1. El sistema mostrará una tabla con la lista de activos y sus respectivas amenazas que actúan sobre dicho activo, las amenazas se mostrarán bajo el activo en una tabla la cual estará distribuida en una tabla con las siguientes columnas: - Amenazas - Vulnerabilidades - Acción 2. La columna acción mostrará la función de editar. - Editar está representado por un icono de lápiz que permitirá abrir un formulario para agregar vulnerabilidades o un comentario de dicha amenaza.

Tabla 37 Historia de usuario CAM02

Historia de Usuario	CAM02
Fecha:	28/9/2021
Código:	CAM02
Requisito:	Registrar vulnerabilidades en cada amenaza
Puntos estimados:	5
Prioridad:	Media
Descripción:	Como usuario quiero registrar información de vulnerabilidades ligadas a las amenazas.
Justificación:	Permite ingresar información adicional de cada amenaza
Dependencia:	CAM01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá registrar vulnerabilidades en amenazas ingresando los siguientes datos: - Vulnerabilidades - Comentario 2. Los campos vulnerabilidades y cometario son campos opcionales, permitirá guardar un proyecto sin datos en estos campos.

Tabla 38 Historia de usuario CAM03

Historia de Usuario	CAM03
Fecha:	28/9/2021
Código:	CAM03
Requisito:	Registrar el valor del porcentaje de degradación de la amenaza
Puntos estimados:	3
Prioridad:	Alta

Historia de Usuario	CAM03
Descripción:	Como usuario quiero registrar el valor del porcentaje de degradación de la amenaza en cada dimensión de seguridad.
Justificación:	Permite registrar el valor del porcentaje de degradación en cada dimensión que influye la amenaza sobre el activo en el que actúa.
Dependencia:	CAM01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá registrar el valor de degradación en cada dimensión de seguridad ingresando el porcentaje en un intervalo de números de 0 a 100. 2. El campo para registrar el valor de porcentaje únicamente aceptará números de 0 a 100. 3. El valor de degradación podrá ser registrado si el campo se encuentra habilitado en cada dimensión de seguridad, si se encuentra inhabilitado no se podrá registrar ningún valor.

Tabla 39 Historia de usuario CAM04

Historia de Usuario	CAM04
Fecha:	28/9/2021
Código:	CAM04
Requisito:	Registrar el valor del porcentaje de probabilidad de ocurrencia de la amenaza.
Puntos estimados:	3
Prioridad:	Alta
Descripción:	Como usuario quiero ingresar el valor de la probabilidad de ocurrencia cuando una amenaza se lleve a cabo.
Justificación:	Permite registrar el valor de la probabilidad de ocurrencia de una amenaza
Dependencia:	CAM01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema permitirá registrar el porcentaje de probabilidad de ocurrencia de una amenaza ingresando el valor del porcentaje en un intervalo de numero de 0 a 100 por ciento. 2. La celda de ingreso del valor de porcentaje únicamente aceptará número de 0 a 100.

2.3.4.2 Implementación

A continuación, se describe la implementación de las historias de usuarios de la tercera iteración, además incluye historias de usuario que proceden de la segunda iteración que tuvieron observaciones.

CA01: Registrar activos

El registro de activos se lo realiza mediante el formulario que se muestra en la Figura 34 y Figura 35, el usuario deberá ingresar los datos requeridos para registrar un activo.

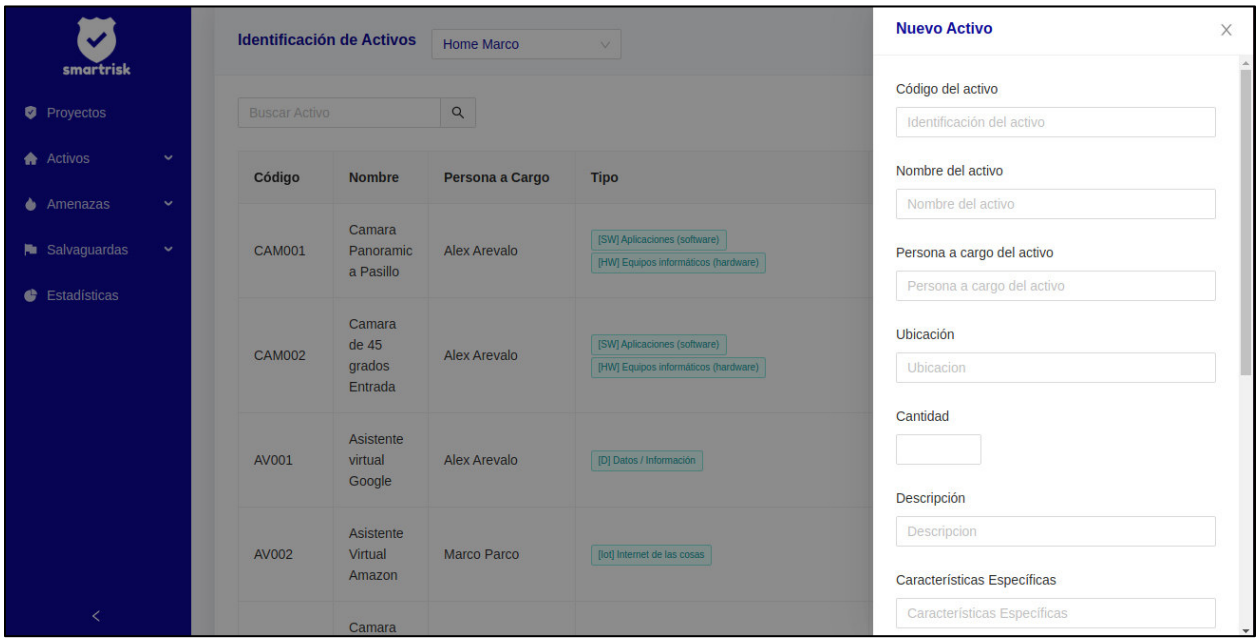


Figura 34 Formulario de registro de activos – Spring 3

En el registro de un activo se debe seleccionar el tipo de activo el mismo puede ser de uno o varios tipos por tal se puede seleccionar varias casillas, una vez ingresado los datos para registrar el activo el usuario debe dar clic en “Crear activo” (Figura 35).

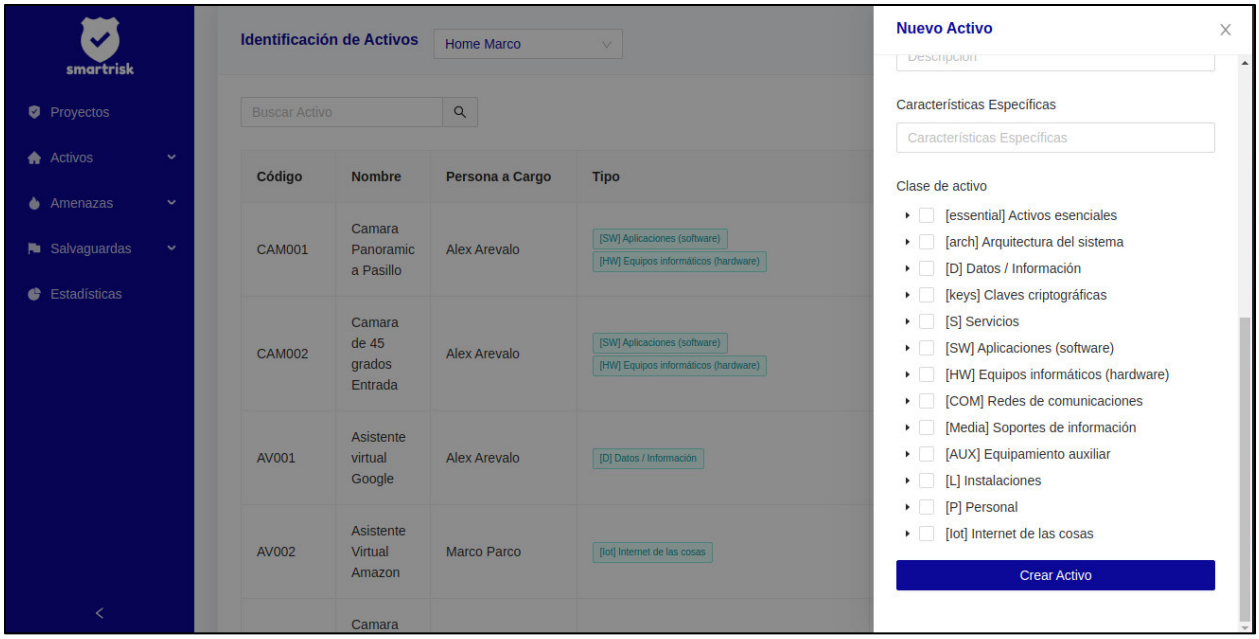


Figura 35 Formulario de registro de activos (continuación) – Spring 3

El formulario cuenta con una validación (Figura 36), donde los campos código del activo, nombre del activo, cantidad no pueden ser vacíos.

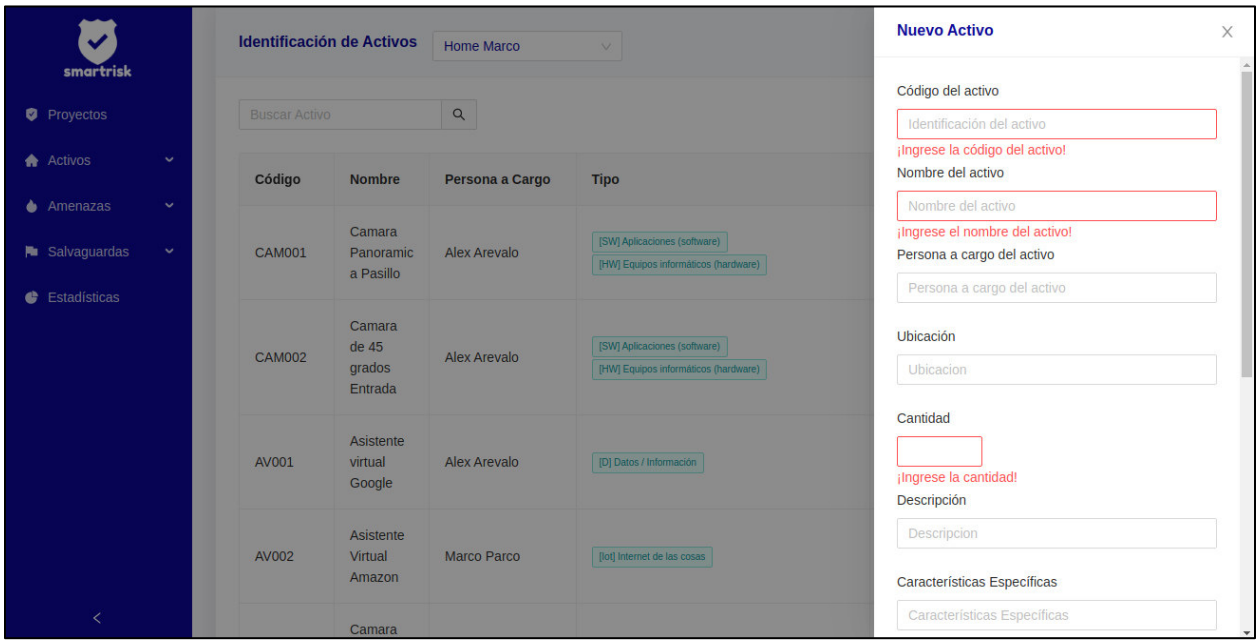


Figura 36 Validación del formulario de registro de activos.

CA02: Consultar datos de activos

Una vez que se han registrados los activos los mismos se mostraran en una tabla como en la Figura 37. Al ser una tabla que maneja gran cantidad de activos existe un cuadro de búsqueda (icono de lupa) que permite filtrar por el nombre del activo.

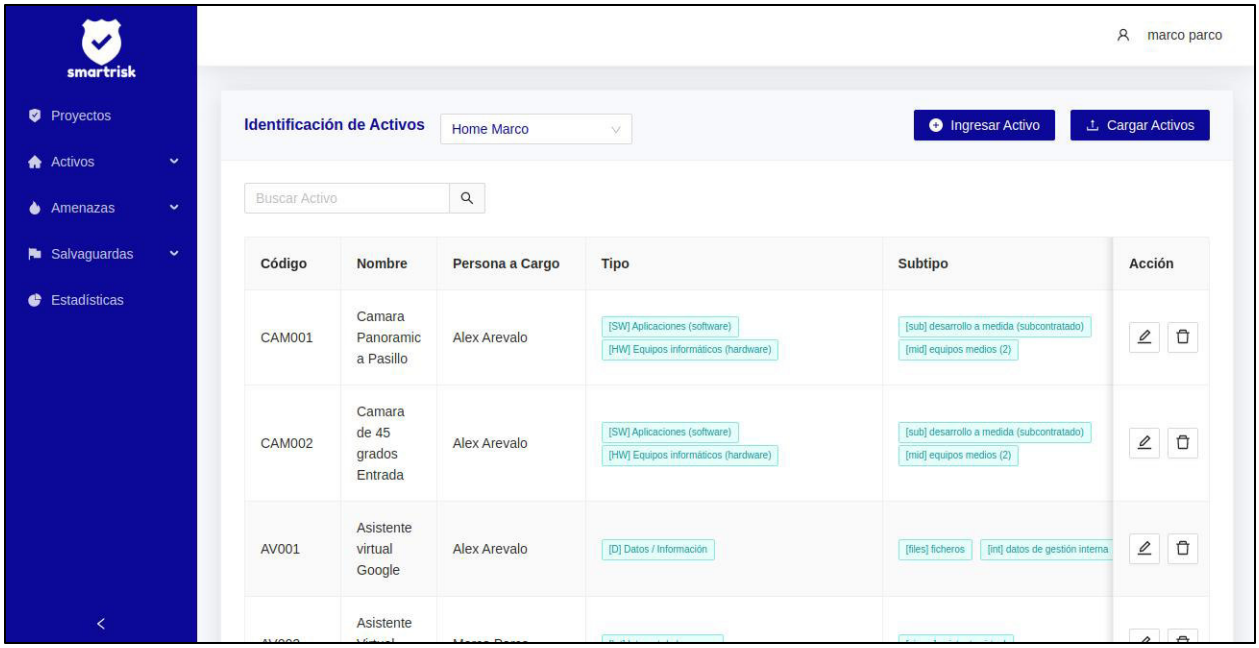
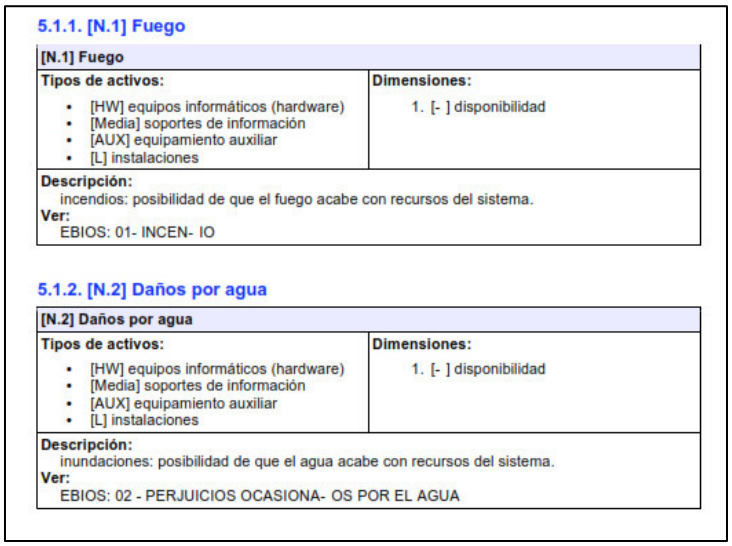


Figura 37 Tabla de datos de activos registrados – Spring 3

CAM01: Visualizar las amenazas del activo

Las amenazas ligadas al activo se mostrarán automáticamente en base al catálogo de amenazas planteado por la metodología Magerit versión 3, para lo cual para automatizar este proceso de identificación de amenazas que actúan sobre un activo se revisó el catálogo de amenazas como se muestra en el libro de catálogos de elementos (Figura 38).



5.1.1. [N.1] Fuego

[N.1] Fuego	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [-] disponibilidad
Descripción: incendios: posibilidad de que el fuego acabe con recursos del sistema. **Ver:** EBIOS: 01- INCEN- IO	

5.1.2. [N.2] Daños por agua

[N.2] Daños por agua	
Tipos de activos: • [HW] equipos informáticos (hardware) • [Media] soportes de información • [AUX] equipamiento auxiliar • [L] instalaciones	**Dimensiones:** 1. [-] disponibilidad
Descripción: inundaciones: posibilidad de que el agua acabe con recursos del sistema. **Ver:** EBIOS: 02 - PERJUICIOS OCASIONA- OS POR EL AGUA	

Figura 38 Vista del catálogo de amenazas

Tomado de [48]

Una vez examinado el catálogo de amenazas lo copiamos en un archivo JSON (Figura 39), servirá para automatizar la identificación de que amenazas afectan al activo dependiendo a que grupo de tipo de activo pertenece este.

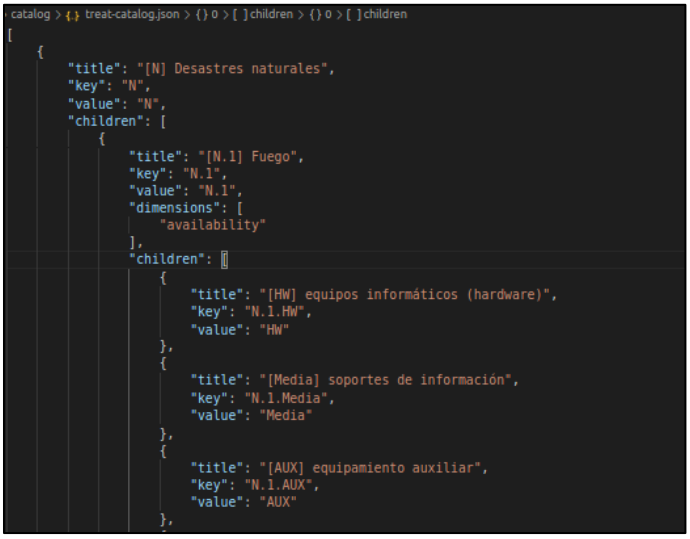


Figura 39 Archivo JSON del catálogo de amenazas

El sistema automáticamente mostrará las amenazas ligadas al activo como se muestra en la Figura 40, el sistema automatiza este proceso gracias al tipo de activo que se registra en la identificación del activo. El proceso de identificación de amenazas es transparente para el usuario, pero está basado en el catálogo de amenazas planteado por la metodología Magerit.

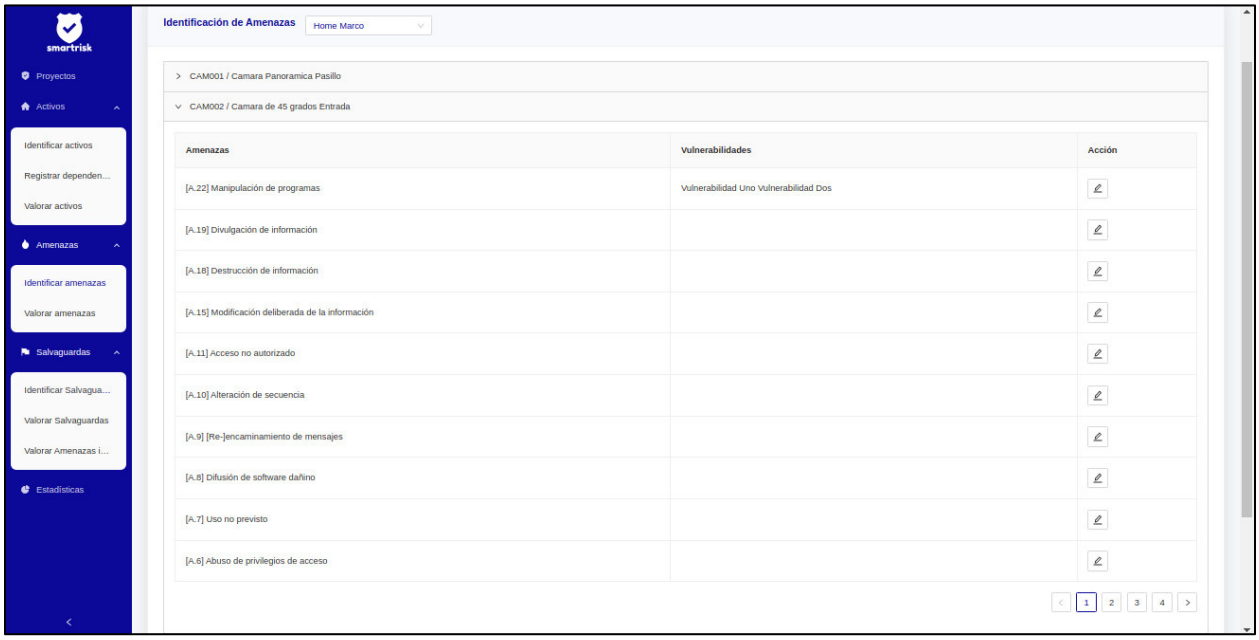


Figura 40 Lista de amenazas ligadas a cada activo.

CAM02: Registrar vulnerabilidades en cada amenaza

El registro de vulnerabilidades puede ser o no escrito en cada una de las amenazas vinculadas a un activo, para ingresar tanto las vulnerabilidades y el comentario se debe dar clic en el icono de lápiz ubicada en la columna de acción la que posterior desplegará un formulario como se muestra en la Figura 41.

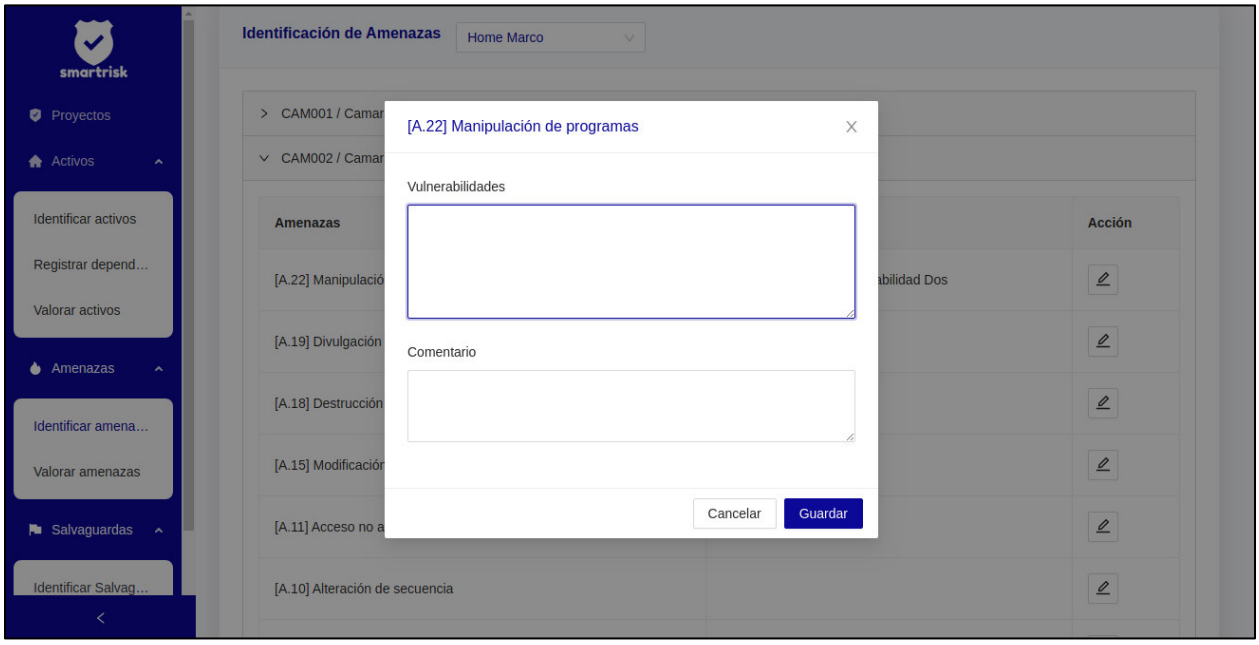


Figura 41 Formulario de ingreso de vulnerabilidades.

CAM03: Registrar el valor del porcentaje de degradación de la amenaza

El registro del valor del porcentaje de degradación de igual forma se lo realiza mediante el nivel de afectación que tiene en cada dimensión de seguridad, el valor que se puede registrar es un número de 0 a 100 si se intenta ingresar valores fuera del intervalo el sistema cambiará automaticamente a un valor dentro del intervalo. Para ingresar el valor del porcentaje el usuario debe dar clic en el icono de lápiz (Figura 42) posterior se habilita las casillas en cada dimensión de seguridad (columna 3 a la columna 7) donde es posible ingresar el valor de degradación, si las casillas están deshabilitadas quiere decir que esta amenaza no afecta dicha dimensión de seguridad.

La habilitación y deshabilitacion de las celdas dependerá de la amenaza y las dimensiones de seguridad en la que puede causar degradación, de igual manera esto es basado en el catálogo de amenazas propuesto por la metodología Magerit.

CAM04: Registrar el valor del porcentaje de probabilidad de ocurrencia de la amenaza.

El registro del valor de la probabilidad de ocurrencia de la amenaza se lo realiza dando clic en el icono de lápiz el cual permitirá registrar la probabilidad, la celda para ingresar la probabilidad de

cada una de las amenazas está ubicada en la primera columna de la tabla después del nombre de la amenaza como muestra la Figura 42. Los valores permitidos son números en el intervalo de 0 a 100 por ciento. Es importante considerar que una vez habilitado para ingresar la probabilidad también se deshabilita el ingreso del valor de la degradación.

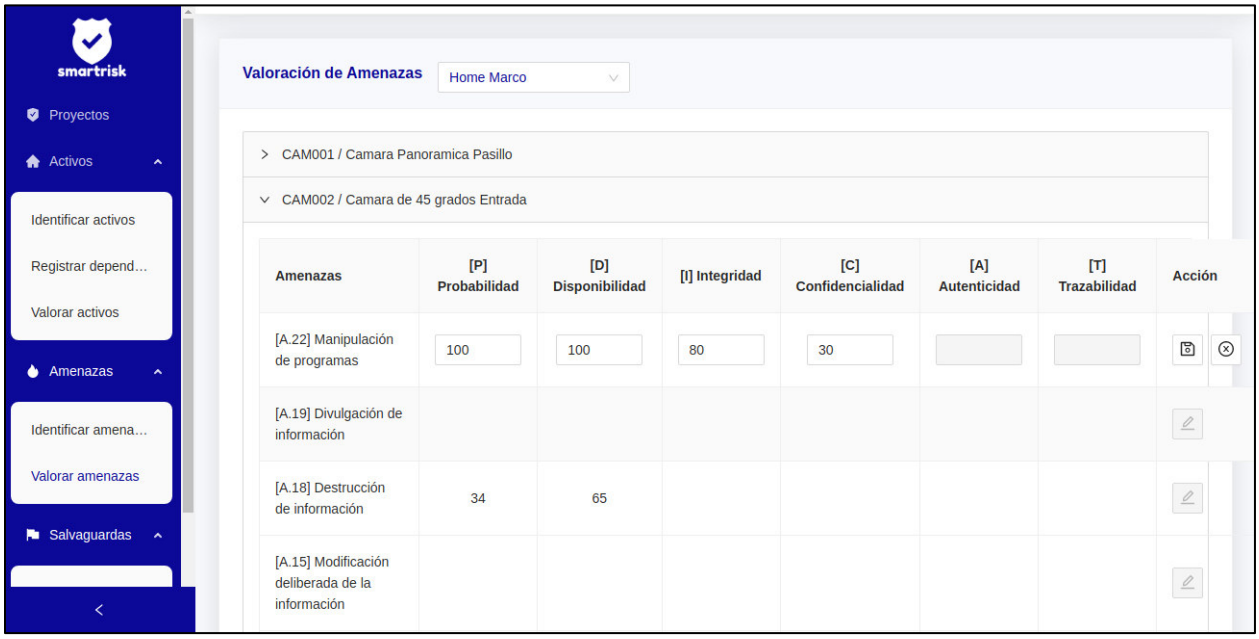


Figura 42 Tabla de registro del valor de degradación

2.3.4.3 Revisión del Spring

Una vez finalizado el desarrollo de las historias de usuario de la segunda iteración se procede a entregar al interesado el producto funcional. La retroalimentación del producto funcional se resume en la Tabla 40 (*Spring Review*) aquí se detallan las observaciones con relación al producto del segundo Spring.

Tabla 40 Revisión del Spring del segundo Spring.

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
CA01	Registrar activos	Ninguna	3	3	0
CA02	Consultar datos de activos	Ninguna	2	2	0
CA03	Modificar datos del activo	Ninguna	2	2	0

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
CA05	Registrar un grupo de activos	Ninguna	2	2	0
CAM01	Visualizar las amenazas del activo	Ninguna	8	8	0
CAM02	Registrar vulnerabilidades en cada amenaza	Ninguna	5	5	0
CAM03	Registrar el valor del porcentaje de degradación de la amenaza	Ninguna	3	3	0
CAM04	Registrar el valor del porcentaje de probabilidad de ocurrencia de la amenaza.	Ninguna	3	3	0
Total			**28**	**28**	**0**

2.3.4.4 Despliegue

Para el despliegue de esta iteración se utilizó la misma configuración de despliegue continuo que se detalló en el primer Sprint.

2.3.5 Spring 4

2.3.5.1 Planificación del Sprint

Tabla 41 Planificación del Sprint para el Sprint 4.

Código	Nombre	Descripción	Prioridad	Estimación (*Story Points*)
Caracterización de Salvaguardas				
CS01	Seleccionar una salvaguarda	***Como*** usuario ***quiero*** seleccionar las salvaguardas para reducir riesgo en las amenazas.	Alta	13
CS02	Registrar características de las salvaguardas	***Como*** usuario ***quiero*** registrar características adicionales de la salvaguarda seleccionada.	Alta	5
CS03	Consultar datos de las salvaguardas	***Como*** usuario ***quiero*** consultar datos de los activos ingresados	Media	3
CS04	Modificar datos de las salvaguardas	***Como*** usuario ***quiero*** modificar los datos anteriormente registrados de las salvaguardas.	Media	3
CS05	Eliminar una salvaguarda	***Como*** usuario ***quiero*** eliminar una salvaguarda	Alta	3
CS06	Registrar el valor de eficacia frente al impacto y a la probabilidad.	***Como*** usuario ***quiero*** ingresar el valor de eficacia frente al impacto y probabilidad.	Alta	5
CS07	Registrar el valor de eficacia frente a la probabilidad	***Como*** usuario ***quiero*** ingresar el valor de eficacia frente a la probabilidad de la salvaguarda al ser esta implementada.	Alta	5
CS08	Consultar el valor de la eficacia al ser implementada la salvaguarda	***Como*** usuario ***quiero*** consultar el valor de la eficacia al ser implementada la salvaguarda	Alta	3
Total				40

A continuación, en las Tabla 42 a Tabla 49 se detallan las historias de usuario del cuarto Sprint:

Tabla 42 Historia de usuario CS01

Historia de Usuario	**CS01**
Fecha:	28/9/2021
Código:	CS01
Requisito:	Seleccionar una salvaguarda
Puntos estimados:	13
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** seleccionar las salvaguardas para reducir el riesgo de las amenazas.
Justificación:	Reducir el riesgo debido a la degradación de amenazas
Dependencia:	CAM01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco
Criterios de aceptación:	1. El sistema mostrará una tabla con la lista del catálogo de salvaguardas propuesto por la metodología Magerit. Las salvaguardas estarán distribuidas en forma de vista de árbol y cada salvaguarda contará con las siguientes columnas: - Código - Nombre - Acción 2. La columna acción muestra la función de seleccionar, está representado por un icono de más (+) permite abrir un formulario para registrar características adicionales de la salvaguarda seleccionada.

Tabla 43 Historia de usuario CS02

Historia de Usuario	**CS02**
Fecha:	28/9/2021
Código:	CS02
Requisito:	Registrar características de las salvaguardas
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** registrar características adicionales de la salvaguarda seleccionada.
Justificación:	Permite registrar información importante de las salvaguardas.
Dependencia:	CS01
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco

Criterios de aceptación:	1. El sistema permitirá registrar características adicionales de las salvaguardas para lo cual ingresará los siguientes datos: - Tipo de la salvaguarda, - Lista de amenazas, - Descripción de la salvaguarda. El tipo de la salvaguarda pueden ser de tipo: prevención, disuasión, eliminación, minimización o limitación del impacto, corrección, recuperación, monitorización y detección. La lista de amenazas se refiere a la lista de amenazas que puede causar efecto si se aplica esta salvaguarda. 2. Los campos tipo de la salvaguarda, lista de amenazas y descripción de la salvaguarda son campos obligatorios, esto implica que si alguno de estos campos este vacío no se podrá crear la salvaguarda y se mostrará el mensaje de error mencionando “Ingrese [las amenaza, ¡la descripción de la salvaguarda]!"

Tabla 44 Historia de usuario CS03

Historia de Usuario	**CS03**
Fecha:	28/9/2021
Código:	CS03
Requisito:	Consultar datos de las salvaguardas
Puntos estimados:	3
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** consultar datos de los activos ingresados
Justificación:	Permite listar todas las salvaguardas que han sido registrados por el usuario
Dependencia:	CS02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco

Criterios de aceptación:	1. El sistema mostrará una tabla con todas las salvaguardas registradas por el usuario en el sistema, la tabla muestra las siguientes columnas: - Código, - Nombre, - Tipo, - Amenazas, - Descripción, y - Acción 2. La columna acción mostrará la función de editar y/o eliminar. - Editar representado por el icono de lápiz que permitirá abrir un formulario para la edición los campos de las salvaguardas. - Eliminar representado por un ícono de basurero que permitirá abrir un cuadro de confirmación para eliminar una salvaguarda.

Tabla 45 Historia de usuario CS04

Historia de Usuario	**CS04**
Fecha:	28/9/2021
Código:	CS04
Requisito:	Modificar datos de las salvaguardas
Puntos estimados:	3
Prioridad:	Media
Descripción:	***Como*** usuario ***quiero*** modificar los datos anteriormente registrados de las salvaguardas.
Justificación:	El usuario modificará los datos ingresados anteriormente de las salvaguardas.
Dependencia:	CS03
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco
Criterios de aceptación:	1. El sistema permitirá modificar los datos de la salvaguarda registrada previamente, para la cual se muestra un formulario completo con los datos antes registrados, donde se pueden cambiar los siguientes datos: - Tipo de la salvaguarda, - Lista de amenazas, - Descripción de la salvaguarda. 2. Al modificar los datos de los campos tipo de la salvaguarda, lista de amenazas y descripción de la salvaguarda son campos obligatorios, esto implica que si algún campo este vacío no se podrá guardar los cambios y se mostrará el mensaje de error mencionando “Ingrese [las amenaza, ¡la descripción de la salvaguarda]!"

Tabla 46 Historia de usuario CS05

Historia de Usuario	**CS05**
Fecha:	28/9/2021
Código:	CS05
Requisito:	Eliminar una salvaguarda
Puntos estimados:	3
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** eliminar una salvaguarda
Justificación:	El usuario podrá eliminar una salvaguarda de la lista de salvaguardas ya registradas previamente.
Dependencia:	CS03
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco
Criterios de aceptación:	1. El sistema permitirá eliminar una salvaguarda creada previamente por el usuario, antes de eliminar se presentará una notificación de aviso ¿Desea eliminar la salvaguarda [nombre de la salvaguarda]?, si el usuario desea eliminar y da clic en aceptar se eliminará del sistema, caso contrario si da clic en cancelar no se borra la salvaguarda.

Tabla 47 Historia de usuario CS06

Historia de Usuario	**CS06**
Fecha:	28/9/2021
Código:	CS06
Requisito:	Registrar el valor de eficacia frente al impacto
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** ingresar el valor de eficacia frente al impacto de la salvaguarda al ser esta implementada.
Justificación:	El usuario registrará el valor del porcentaje de eficacia frente al impacto de la salvaguarda al ser implementada
Dependencia:	CS02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco
Criterios de aceptación:	1. El sistema permitirá registrar el valor de eficacia frente al impacto al implementar la salvaguarda en un intervalo de 0 a 100 porciento. 2. El campo para registrar el valor de porcentaje únicamente aceptará números de 0 a 100.

Tabla 48 Historia de usuario CS07

Historia de Usuario	**CS07**
Fecha:	28/9/2021
Código:	CS07
Requisito:	Registrar el valor de eficacia frente a la probabilidad
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** ingresar el valor de eficacia frente a la probabilidad de la salvaguarda al ser esta implementada.
Justificación:	El usuario registrará el valor del porcentaje de eficacia frente a la probabilidad de la salvaguarda al ser implementada
Dependencia:	CS02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco
Criterios de aceptación:	1. El sistema permitirá registrar el valor de eficacia frente a la probabilidad al implementar la salvaguarda en un intervalo de 0 a 100 porciento. 2. El campo para registrar el valor de porcentaje únicamente aceptará números de 0 a 100.

Tabla 49 Historia de usuario CS08

Historia de Usuario	**CS08**
Fecha:	28/9/2021
Código:	CS08
Requisito:	Consultar el valor de la eficacia al ser implementada la salvaguarda
Puntos estimados:	3
Prioridad:	Alta
Descripción:	Como usuario quiero consultar el valor de la eficacia al ser implementada la salvaguarda
Justificación:	El usuario visualizará el valor de la eficacia al ser implementada la salvaguarda
Dependencia:	CS02
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo, Marco Parco
Criterios de aceptación:	1. El sistema mostrará el valor de eficacia al implementar la salvaguarda en una escala de porcentaje de un intervalo de o a 100 por ciento.

2.3.5.2 Implementación

A continuación, se describe la implementación de las historias de usuarios de la tercera iteración, además incluye historias de usuario que proceden de la segunda iteración que tuvieron observaciones.

CS01: Seleccionar una salvaguarda

El ingreso de una salvaguarda inicia al dar clic en “Agregar Salvaguarda” donde en consecuente se mostrará una ventana con una lista de salvaguardas (Figura 43), en esa lista de salvaguardas el usuario podrá seleccionar cual salvaguarda desea, una vez identificada la salvaguarda debe dar clic en el icono más (+).

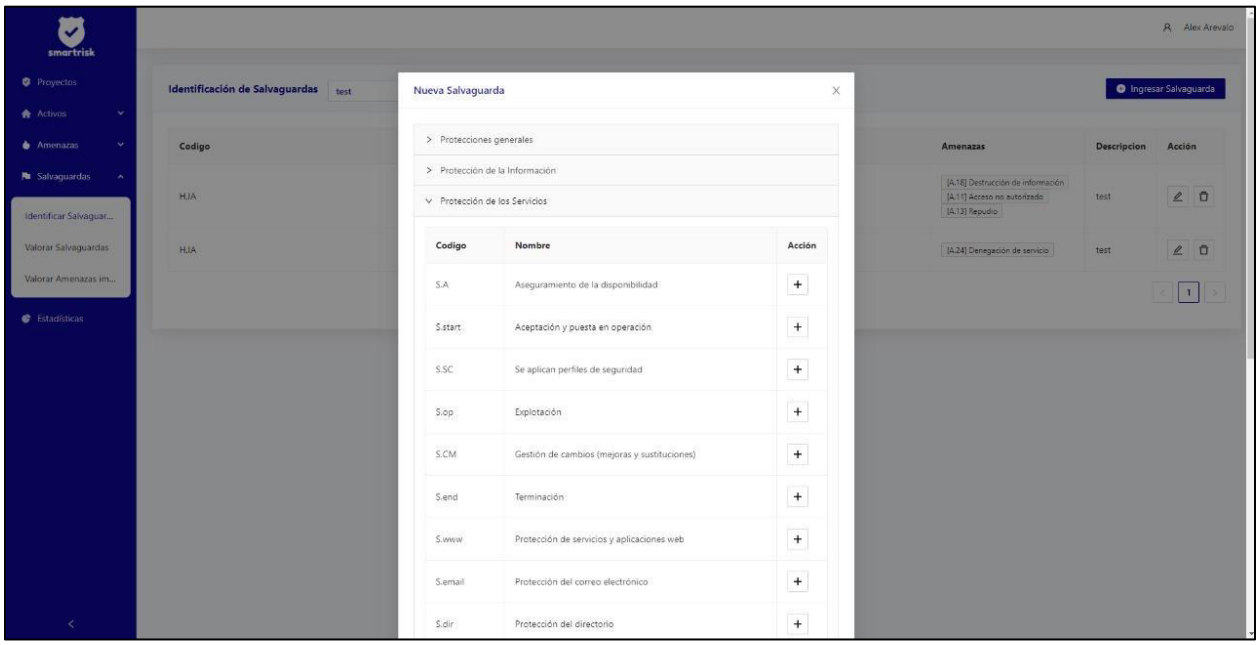


Figura 43 Ventana de lista de salvaguardas

CS02: Registrar características de las salvaguardas

Ya seleccionada la salvaguarda y dado clic en el signo más (+) se despliega un formulario como en la Figura 44 donde se ingresa las características como: el tipo de salvaguarda, lista de amenazas y descripción de la salvaguarda.

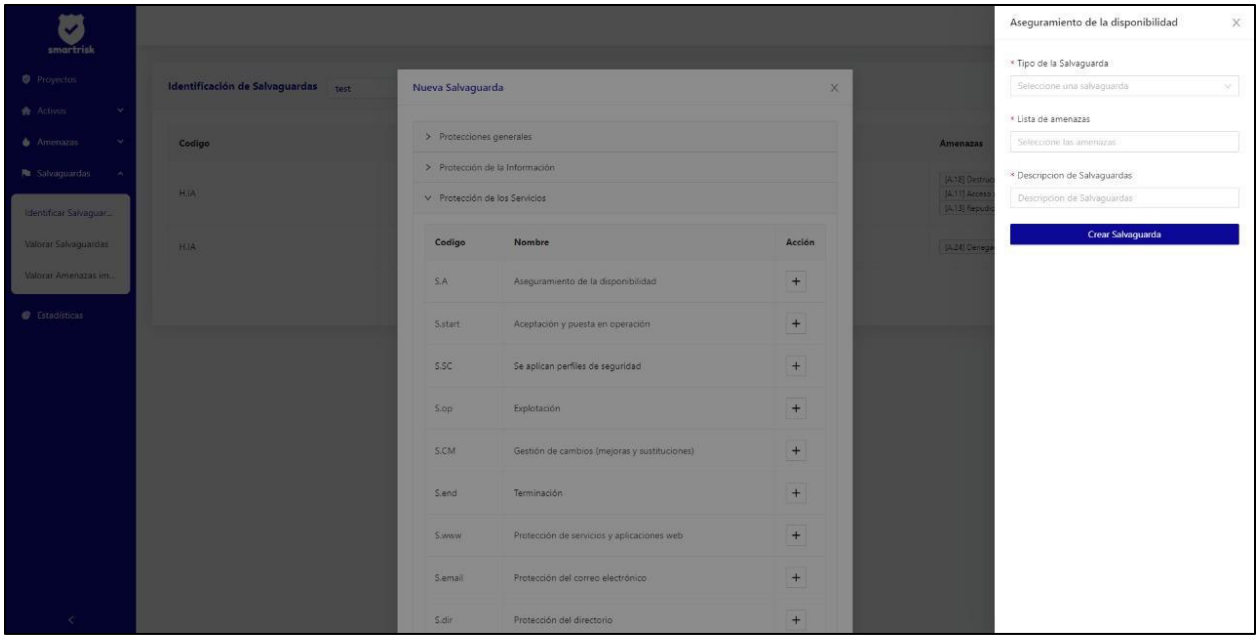


Figura 44 Formulario de registro de características de salvaguardas.

Una vez ingresado las características en el formulario el sistema validará que el tipo de salvaguarda, lista de amenazas y descripción de salvaguarda no estén vacíos debido a que son campos obligatorios si los mismos están vacíos mostrarán un mensaje de error como en la Figura 45.

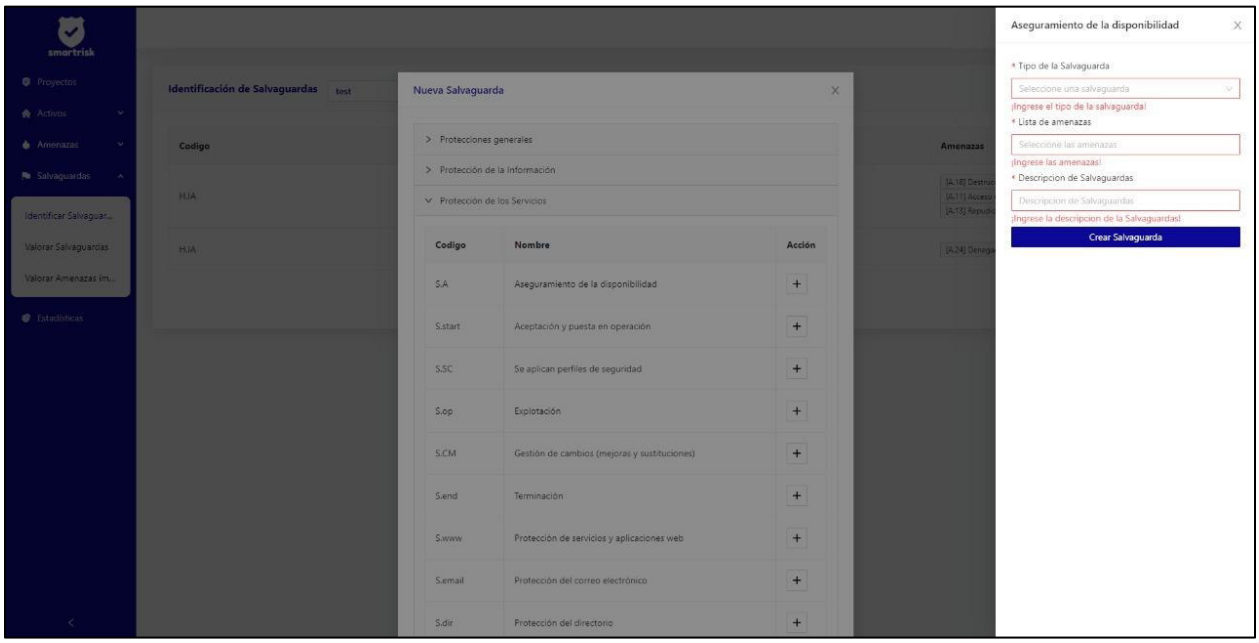


Figura 45 Validación del formulario de registro de características de salvaguardas

CS03: Consultar datos de las salvaguardas

La lista de salvaguardas ingresadas se muestra en una tabla como en la Figura 46, cada una de las salvaguardas están distribuidas en columnas que contienen: código, nombre, tipo, amenazas y acción. La columna acción muestra dos funciones claves que se puede realizar con dicha salvaguarda que son editar (icono lápiz) y eliminar (icono basurero).

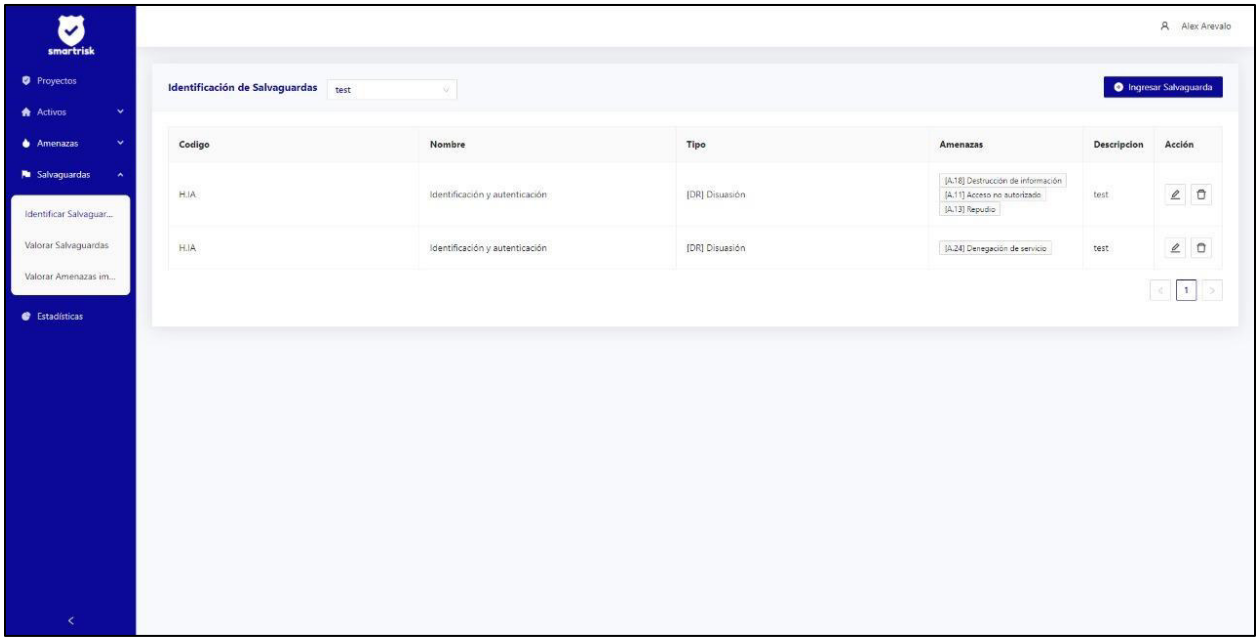


Figura 46 Tabla de la lista de salvaguardas ingresadas.

CS04: Modificar datos de las salvaguardas

Para la actualización de datos de una salvaguarda se debe dar clic en el botón del lápiz de la columna de acción, posterior se despliega un formulario con datos previos ingresados de la salvaguarda (Figura 47) y allí se podrá editar los datos. Es importante considerar que antes de actualizar la salvaguarda el sistema validará si todos los campos no están vacíos, si no están vacíos los datos ingresados se actualizarán y se guardará.

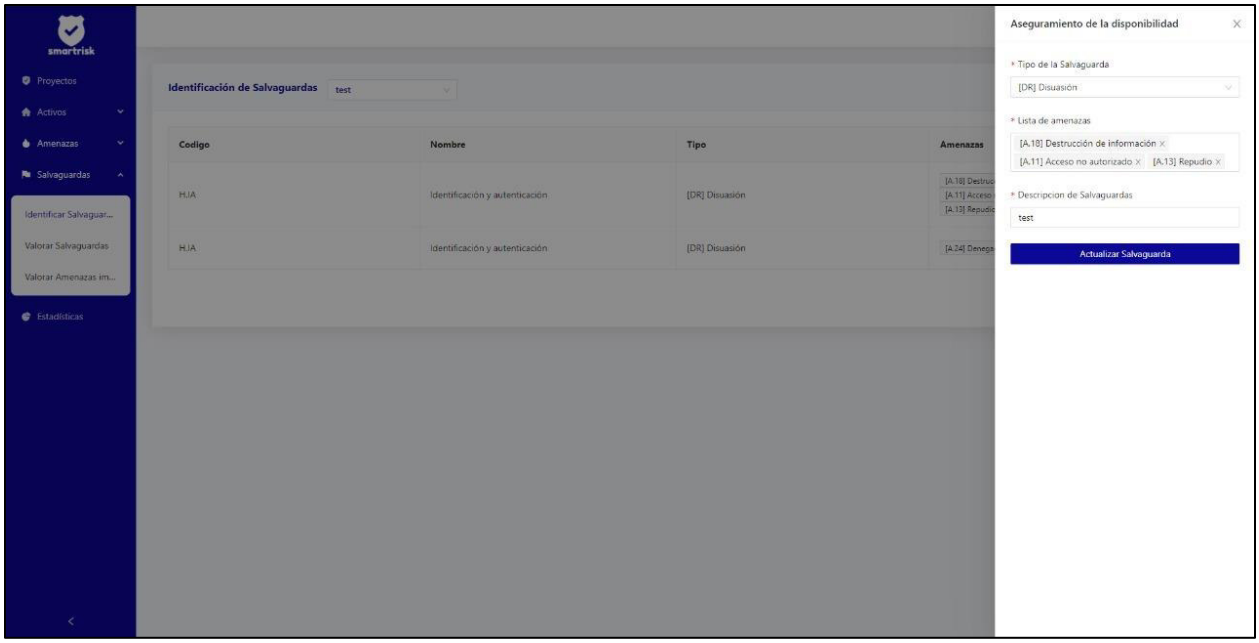


Figura 47 Formulario para modificar datos de la salvaguarda.

CS05: Eliminar una salvaguarda

La eliminación de una salvaguarda inicia al dar clic en el icono de basurero ubicado en la columna acción, posterior se muestra una notificación (Figura 48) en donde se debe confirmar si está seguro de eliminar la salvaguarda, si da clic en aceptar la amenaza se eliminará de la lista de salvaguardas caso contrario si da en cancelar no se eliminará.

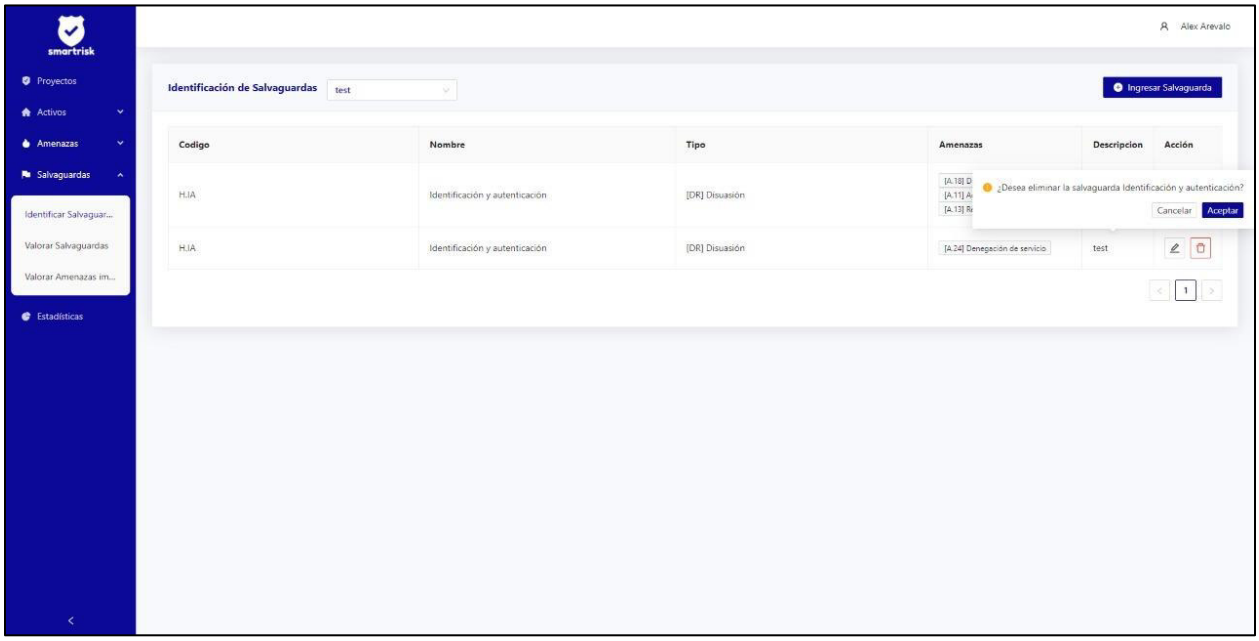


Figura 48 Eliminar una salvaguarda

CS06: Registrar el valor de eficacia frente al impacto

El ingreso del valor de la eficacia frente al impacto se lo realiza dando clic en el botón de lápiz ubicado en la columna de acción, luego se habilitará la celda donde se puede ingresar el valor del porcentaje, columna de eficacia frente al impacto de la Figura 49, este porcentaje de eficacia es un número de 0 a 100 por ciento. El sistema validará automáticamente que los valores se encuentren en el intervalo de 0 a 100 por ciento, si están fuera lo establecerá en un valor dentro del intervalo de forma automática.

CS07: Registrar el valor de eficacia frente a la probabilidad

El ingreso del valor de eficacia frente a la probabilidad se lo realiza de igual forma dando clic en el icono de lápiz ubicado en la columna acción, luego se habilitará la celda donde se puede ingresar el valor del porcentaje, columna eficacia frente a la probabilidad de la Figura 49, este porcentaje de eficacia es un número de 0 a 100 por ciento. El sistema validará automáticamente que los valores se encuentren en el intervalo de 0 a 100 por ciento, si están fuera lo establecerá en un valor dentro del intervalo de forma automática.

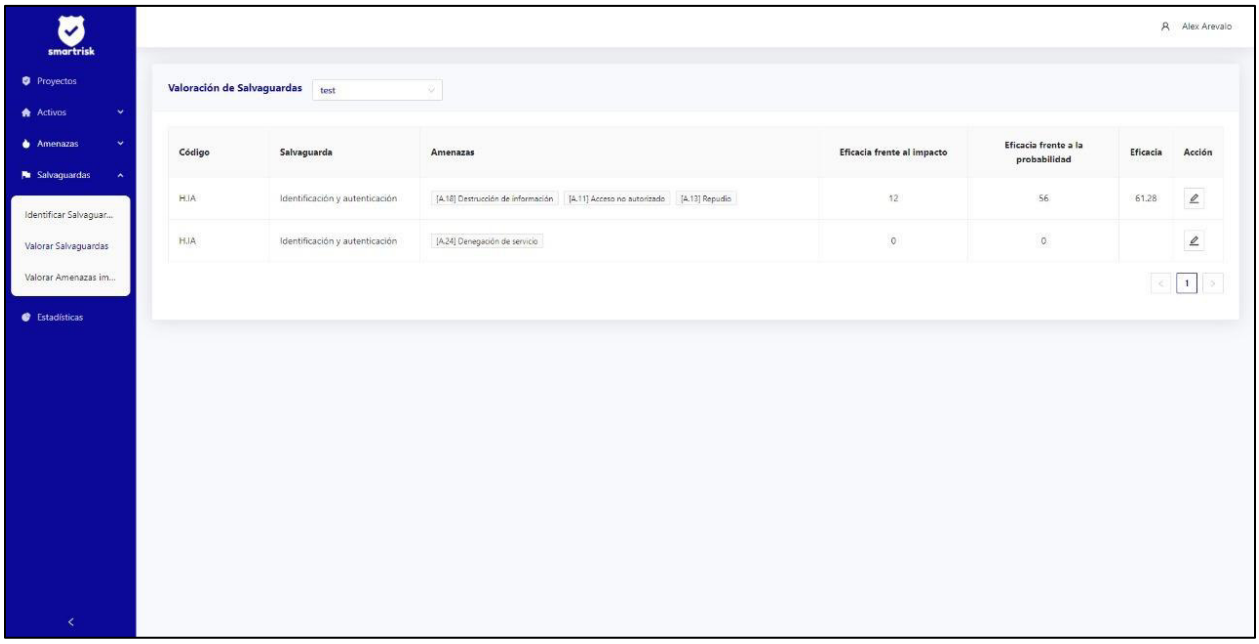


Figura 49 Registro del valor de la eficacia frente al impacto y a la probabilidad.

CS08: Consultar el valor de la eficacia al ser implementada la salvaguarda

El valor de la eficacia se mostrará en la Figura 50 en la columna “Eficacia” allí en cada celda se encontrará un porcentaje entre el intervalo de 0 a 100, el valor de la eficacia es el resultado de la eficacia frente al impacto y la eficacia frente a la probabilidad.

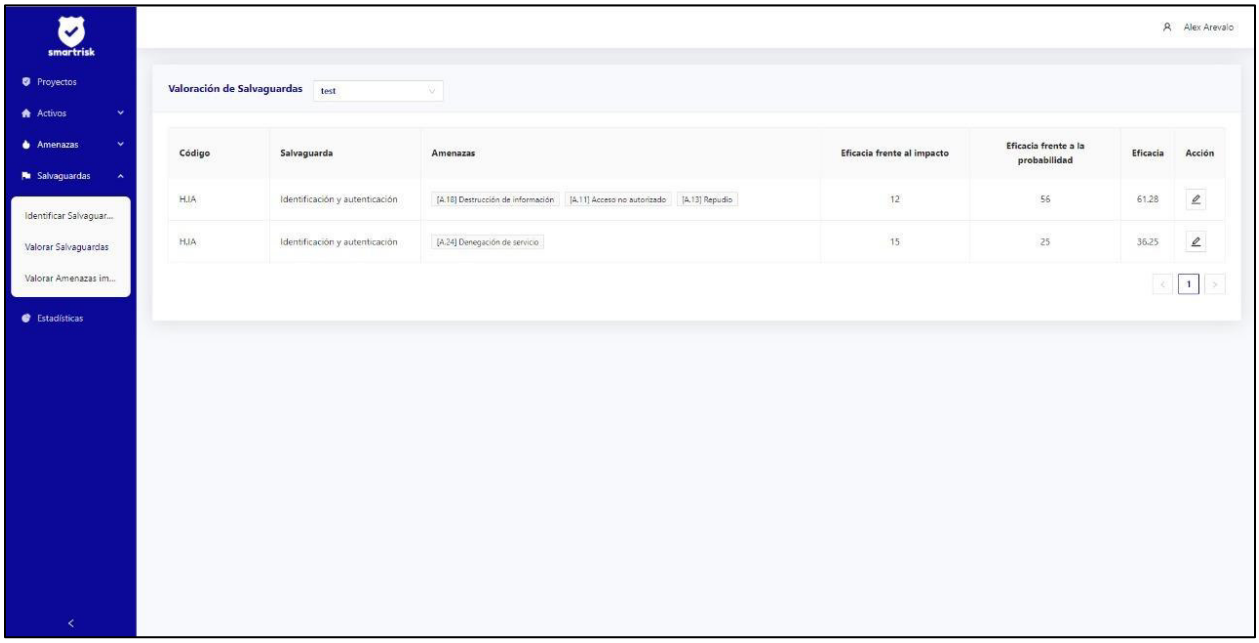


Figura 50 Valor de la eficacia de la salvaguarda.

2.3.5.3 Revisión del Spring

Una vez realizadas las historias de usuario del cuarto Sprint se realiza la presentación del producto funcional, logrando así obtener la retroalimentación de los interesados del producto y siendo esta resumida en la Tabla 50 (*Spring Review*) donde se detallan las observaciones realizadas por los interesados.

Tabla 50 Revisión del Sprint del cuarto Spring

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
CS01	Seleccionar una salvaguarda	Ninguna	13	13	0
CS02	Registrar características	Ninguna	5	5	0

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
	de las salvaguardas				
CS03	Consultar datos de las salvaguardas	Ninguna	3	3	0
CS04	Modificar datos de las salvaguardas	Ninguna	3	3	0
CS05	Eliminar una salvaguarda	Ninguna	3	3	0
CS06	Registrar el valor de eficacia frente al impacto y a la probabilidad.	Ninguna	5	5	0
CS07	Registrar el valor de eficacia frente a la probabilidad	Ninguna	5	5	0
CS08	Consultar el valor de la eficacia al ser implementada la salvaguarda	Ninguna	3	3	0
Total			**40**	**40**	**0**

2.3.5.4 Despliegue

Para el despliegue de esta iteración se utilizó la misma configuración de despliegue continuo que se detalló en el primer Sprint.

2.3.6 Sprint 5

2.3.6.1 Planificación del Sprint

La Tabla 51 muestra la lista de requerimientos a implementar en el quinto Sprint.

Tabla 51 Planificación del Sprint para el quinto Sprint.

Código	**Nombre**	**Descripción**	**Prioridad**	**Estimación** (Story Points)
Estimación de Estado de Riesgo				
ER01	Consultar el valor de la probabilidad y degradación residual.	***Como*** usuario ***quiero*** observar el valor de la probabilidad y degradación residual frente a la eficacia de las salvaguardas.	Alta	8
ER02	Consultar el valor del impacto potencial acumulado y repercutido	***Como*** usuario ***quiero*** observar el impacto potencial acumulado y repercutido del hogar inteligente	Alta	8
ER03	Consultar el valor del impacto residual acumulado y repercutido.	***Como*** usuario ***quiero*** observar el impacto residual acumulado y repercutido del hogar inteligente una vez consideradas las salvaguardas.	Alta	8
ER04	Consultar el valor del riesgo potencial acumulado y repercutido.	***Como*** usuario ***quiero*** observar el riesgo potencial acumulado y repercutido del hogar inteligente.	Alta	5
ER05	Consultar el valor del riesgo residual acumulado y repercutido.	***Como*** usuario ***quiero*** observar el riesgo residual acumulado y repercutido del hogar inteligente una vez considerada las salvaguardas.	Alta	5
Total				**34**

A continuación, en la Tabla 52 hasta la Tabla 56 se detallan las historias de usuario de la quinta iteración:

Tabla 52 Historia de usuario ER01

Historia de Usuario	**ER01**
Fecha:	28/9/2021
Código:	ER01
Requisito:	Consultar el valor de la probabilidad y degradación residual.
Puntos estimados:	8
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** observar el valor de la probabilidad y degradación residual frente a la eficacia de las salvaguardas.
Justificación:	El usuario observará el valor de la probabilidad y degradación residual una vez ya tomado en cuenta las salvaguardas.
Dependencia:	CS08
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema mostrará el valor de la probabilidad y la degradación residual posterior consideradas las salvaguardas. El valor se presentará en una tabla por cada activo, por cada amenaza y por cada dimensión de seguridad. 2. El valor es un número real de 0 a 100 por ciento.

Tabla 53 Historia de usuario ER02

Historia de Usuario	**ER02**
Fecha:	29/9/2021
Código:	ER02
Requisito:	Consultar el valor del impacto potencial acumulado y repercutido
Puntos estimados:	8
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** observar el valor del impacto potencial acumulado y repercutido del hogar inteligente
Justificación:	El usuario observará el valor del impacto potencial acumulado y repercutido del hogar inteligente
Dependencia:	CS08
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema mostrará el valor del impacto potencial acumulado y repercutido en una tabla por cada activo, por cada amenaza y por cada dimensión de seguridad y lo clasificará en dos columnas una para impacto potencial acumulado y otra para el impacto potencial repercutido. 2. El valor es un número real de 0 a 100 por ciento.

Tabla 54 Historia de usuario ER03

Historia de Usuario	**ER03**
Fecha:	30/9/2021
Código:	ER03
Requisito:	Consultar el valor del impacto residual acumulado y repercutido.
Puntos estimados:	8
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** observar el valor del impacto residual acumulado y repercutido del hogar inteligente una vez consideradas las salvaguardas.
Justificación:	El usuario observará el valor del impacto residual acumulado y repercutido del hogar inteligente una vez tomado en cuenta las salvaguardas.
Dependencia:	CS08
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema mostrará el valor del impacto residual acumulado y repercutido en una tabla por cada activo, por cada amenaza y por cada dimensión de seguridad y lo clasificará en dos columnas una para impacto residual acumulado y otra para el impacto residual repercutido. 2. El valor es un número real de 0 a 100 por ciento.

Tabla 55 Historia de usuario ER04

Historia de Usuario	**ER04**
Fecha:	1/10/2021
Código:	ER04
Requisito:	Consultar el valor del riesgo potencial acumulado y repercutido.
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** observar el valor del riesgo potencial acumulado y repercutido del hogar inteligente.
Justificación:	El usuario observará el valor del riesgo potencial acumulado y repercutido del hogar inteligente.
Dependencia:	CS08
Usuario(s):	Usuario que ha iniciado sesión

Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema mostrará el valor del riesgo potencial acumulado y repercutido en una tabla por cada activo, por cada amenaza y por cada dimensión de seguridad y lo clasificará en dos columnas una para riesgo potencial acumulado y otra para el riesgo potencial repercutido. 2. El valor es un número real de 0 a 100 por ciento.

Tabla 56 Historia de usuario ER05

Historia de Usuario	**ER05**
Fecha:	2/10/2021
Código:	ER05
Requisito:	Consultar el valor del riesgo residual acumulado y repercutido.
Puntos estimados:	5
Prioridad:	Alta
Descripción:	***Como*** usuario ***quiero*** observar el valor del riesgo residual acumulado y repercutido del hogar inteligente una vez considerada las salvaguardas.
Justificación:	El usuario observará el valor del riesgo residual acumulado y repercutido del hogar inteligente una vez considerada las salvaguardas.
Dependencia:	CS08
Usuario(s):	Usuario que ha iniciado sesión
Responsable:	Alex Arevalo
Criterios de aceptación:	1. El sistema mostrará el valor del riesgo residual acumulado y repercutido en una tabla por cada activo, por cada amenaza y por cada dimensión de seguridad y lo clasificará en dos columnas una para riesgo residual acumulado y otra para el riesgo residual repercutido. 2. El valor es un número real de 0 a 100 por ciento.

2.3.6.2 Implementación

A continuación, se describe la implementación de las historias de usuarios de la quinta iteración:

ER01: Consultar el valor de la probabilidad y degradación residual.

El valor tanto de la probabilidad y degradación residual se muestra en la Figura 51 cada uno de los activos cuenta con sus respectivas amenazas y las mismas muestran un valor para la probabilidad y el registro del valor de degradación por cada dimensión de seguridad. El valor que se mostrará en cada celda es un número real entre 0 a 100 por ciento.

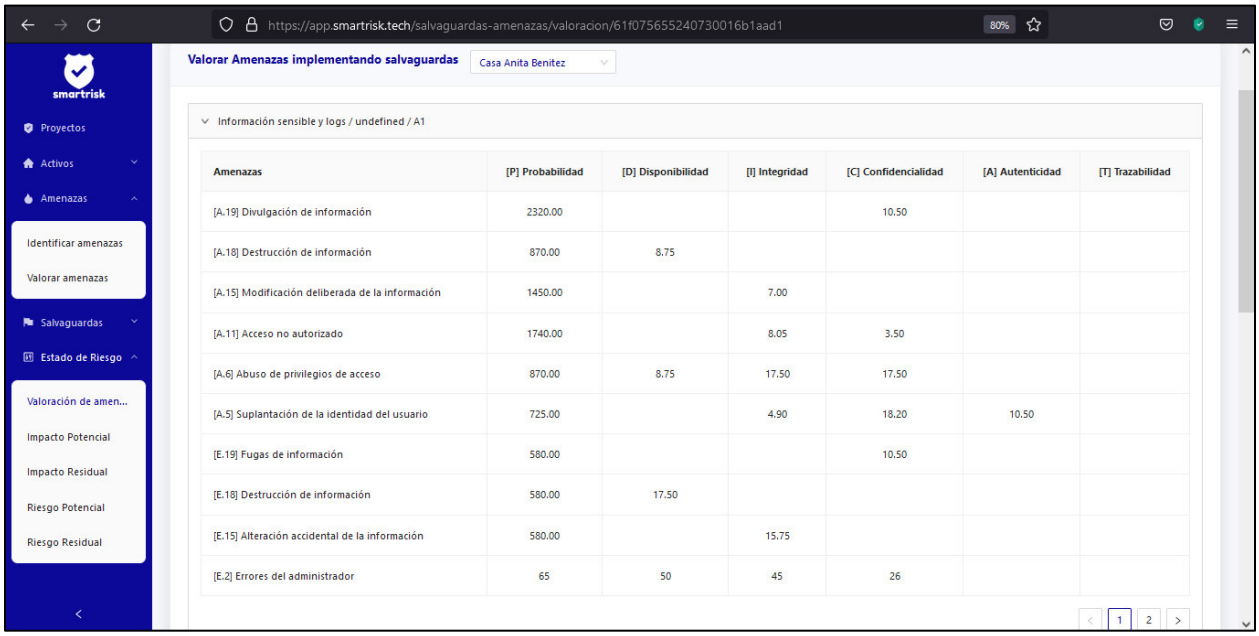


Figura 51 Tabla de resultados de probabilidad y degradación residual.

ER02: Consultar el valor del impacto potencial acumulado y repercutido

El valor del impacto potencial acumulado y repercutido se muestra en la Figura 52, la tabla está distribuida en dos columnas: impacto potencial acumulado e impacto potencial repercutido. Los valores se mostrarán por cada activo, por cada amenaza y por cada dimensión de seguridad. El valor que se mostrará en cada celda es un número real entre 0 a 100 por ciento.

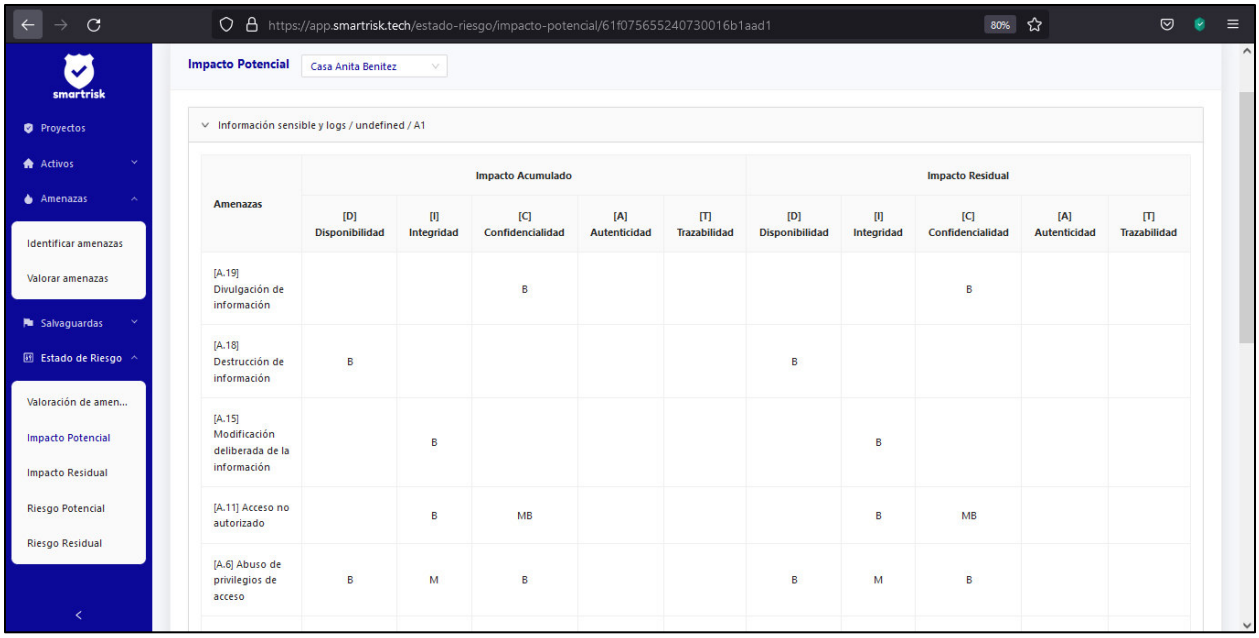


Figura 52 Tabla de resultados del impacto potencial acumulado y repercutido

ER03: Consultar el valor del impacto residual acumulado y repercutido.

El valor del impacto residual acumulado y repercutido se muestra en la Figura 53, la tabla está distribuida en dos columnas: impacto residual acumulado e impacto residual repercutido. Los valores se mostrarán por cada activo, por cada amenaza y por cada dimensión de seguridad. El valor que se mostrará en cada celda es un número real entre 0 a 100 por ciento.

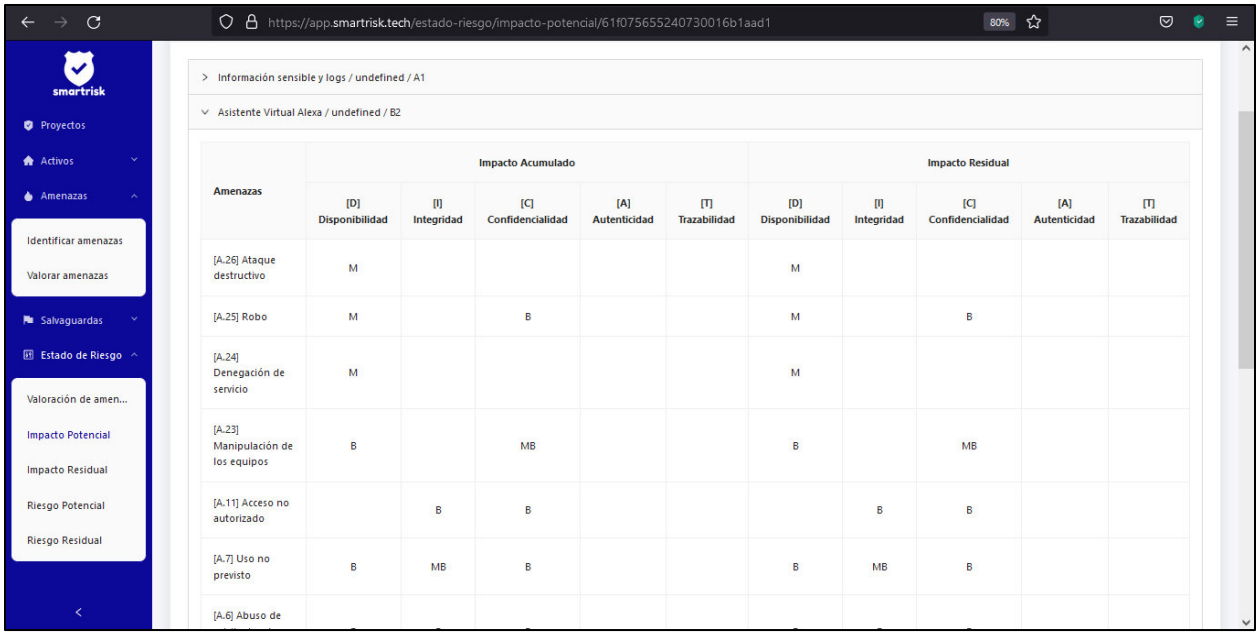


Figura 53 Tabla de resultados de impacto residual acumulado y repercutido

ER04: Consultar el valor del riesgo potencial acumulado y repercutido

El valor del riesgo potencial acumulado y repercutido se muestra en la Figura 54, la tabla está distribuida en dos columnas: riesgo potencial acumulado y riesgo potencial repercutido. Los valores se mostrarán por cada activo, por cada amenaza y por cada dimensión de seguridad. El valor que se mostrará en cada celda es un número real entre 0 a 100 por ciento.

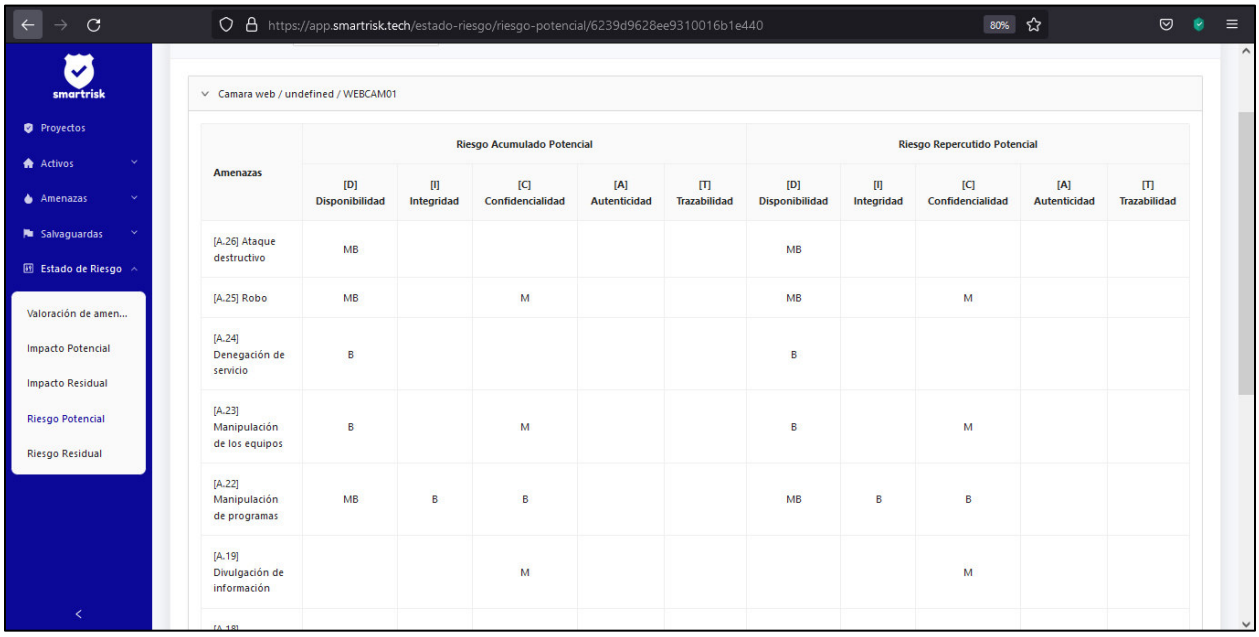
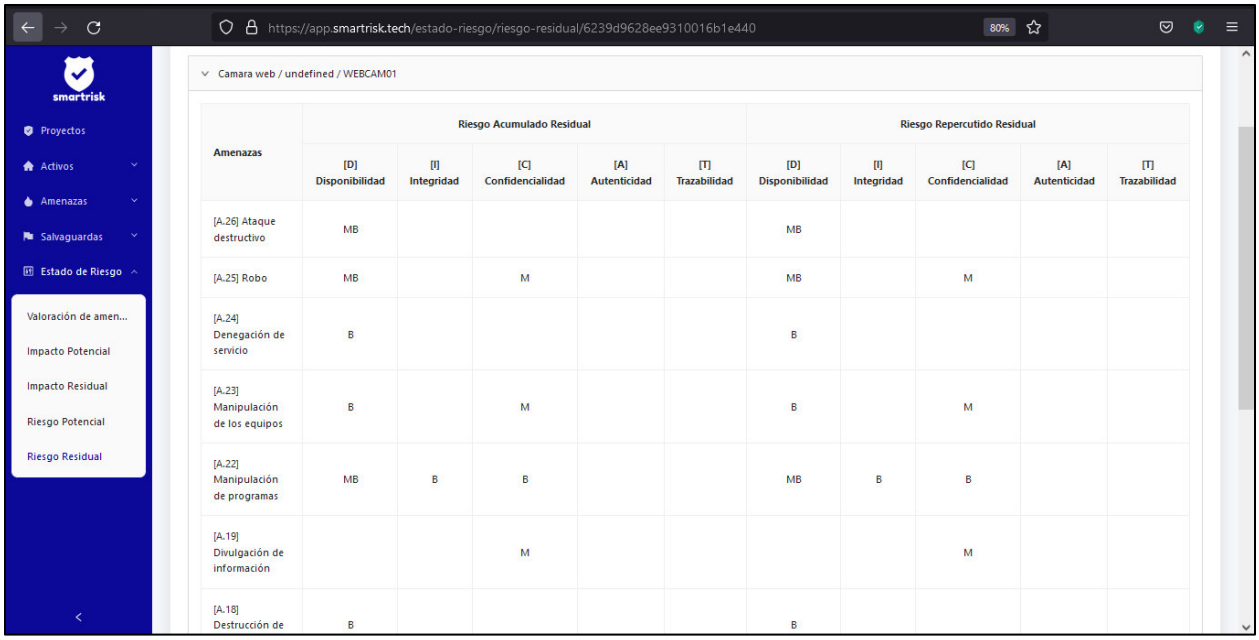


Figura 54 Tabla de resultados del riesgo potencial acumulado y repercutido.

ER05: Consultar el valor del riesgo residual acumulado y repercutido

El valor del riesgo residual acumulado y repercutido se muestra en la Figura 55, la tabla está distribuida en dos columnas: riesgo residual acumulado y riesgo residual repercutido. Los valores se mostrarán por cada activo, por cada amenaza y por cada dimensión de seguridad. El valor que se mostrará en cada celda es un número real entre 0 a 100 por ciento.



Amenazas	Riesgo Acumulado Residual					Riesgo Repercutido Residual				
	[D] Disponibilidad	[I] Integridad	[C] Confidencialidad	[A] Autenticidad	[T] Trazabilidad	[D] Disponibilidad	[I] Integridad	[C] Confidencialidad	[A] Autenticidad	[T] Trazabilidad
[A.26] Ataque destructivo	MB					MB				
[A.25] Robo	MB		M			MB		M		
[A.24] Denegación de servicio	B					B				
[A.23] Manipulación de los equipos	B		M			B		M		
[A.22] Manipulación de programas	MB	B	B			MB	B	B		
[A.19] Divulgación de información			M					M		
[A.18] Destrucción de	B					B				

Figura 55 Tabla de resultados del riesgo residual acumulado y repercutido.

2.3.6.3 Revisión del Spring

Una vez finalizado el desarrollo de las historias de usuario de la quinta y última iteración se procede a entregar al interesado el producto funcional. La retroalimentación del producto funcional se resume en la Tabla 57 (*Spring Review*) aquí se detallan las observaciones con relación al producto del segundo Spring.

Tabla 57 Revisión del Spring del quinto Spring

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
ER01	Consultar el valor de la probabilidad y degradación residual.	Ninguna	8	8	0
ER02	Consultar el valor del impacto potencial acumulado y repercutido	Ninguna	8	8	0

Código	Nombre	Observaciones	Puntos estimados	Puntos finalizados	Puntos pendientes
ER03	Consultar el valor del impacto residual acumulado y repercutido.	Ninguna	8	8	0
ER04	Consultar el valor del riesgo potencial acumulado y repercutido.	Ninguna	5	5	0
ER05	Consultar el valor del riesgo residual acumulado y repercutido.	Ninguna	5	5	0
Total			**34**	**34**	**0**

2.3.6.4 Despliegue

Para el despliegue de esta iteración se utilizó la misma configuración de despliegue continuo que se detalló en el primer Sprint.

3 Análisis de la Metodología – Caso de Estudio Manual

3.1 Caso de estudio simulado manual para dispositivos IoT bajo la metodología Magerit versión 3.0

Situación Actual

El caso de estudio a desarrollar es una pequeña infraestructura IoT básica de un hogar inteligente creada a modo de practica por consenso de varios expertos con la finalidad de poder evaluar en este escenario los principales riesgos a los que se encuentran expuestos los activos del ecosistema IoT que forman un hogar inteligente, se utilizará la metodología Magerit versión 3.0 para el análisis de riesgos.

La infraestructura del hogar inteligente como se puede ver en la Figura 56 cuenta con los siguientes elementos:

- Alexa,
- Google Home,
- Luz inteligente,
- Información,
- Hub y
- Enrutador IoT.

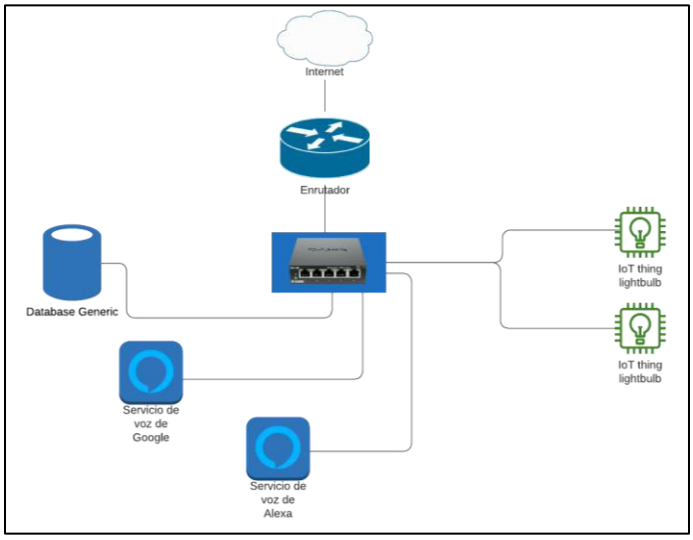


Figura 56 Topología de red

El escenario creado es un hogar inteligente cuenta con varias tecnologías y dispositivos, está equipado con sensores, actuadores con la capacidad de almacenar la información del entorno para realizar tareas automáticamente. Los asistentes virtuales Alexa y Google Home en este caso actuarán como sensores mientras que los dos focos inteligentes como actuadores. Los dispositivos de red utilizados son un enrutador y un concentrador que permitirán la conectividad entre los dispositivos inteligentes y el internet.

El hogar inteligente es un departamento de una sola planta cuenta con una alimentación de energía eléctrica, una conexión de internet a través de un enlace de fibra óptica, el ingreso a la casa cuenta con cerraduras y solo puede acceder el propietario.

Como se puede verificar en la topología de red de la Figura 56 cuenta con un enrutador principal por donde cuenta con acceso a internet, un concentrador encargado en conectar con todos los dispositivos de la red IoT.

El servicio que ofrece el hogar inteligente a las personas que habitan allí es que la luz enciende automáticamente cuando el grado de luminosidad de la casa es baja, e igual forma se apaguen cuando la luminosidad es alta.

Las operaciones que se ejecutan en la infraestructura del hogar inteligente de forma periódica son:

c. Revisión de conexión a internet y a la electricidad.
d. Revisión de logs de los dispositivos.
e. Revisión de funcionamiento de los dispositivos

A diferencia de un sistema de información tradicional cada uno de los dispositivos están a cargo de un responsable en específico, pero como en este caso solo se trata de un ecosistema IoT de un hogar inteligente que pertenece a un solo responsable que en este caso es el dueño de la casa como ejemplo práctico el dueño será Anita Benítez.

El caso de estudio y la aplicación correcta de la metodología de análisis de riesgos al escenario teórico propuesto facilita conocer las actividades a desarrollarse por la metodología con la finalidad de automatizar el proceso manual a un proceso automatizado guiado mediante una aplicación web. El cálculo manual del escenario planteado condiciona la validez y la utilidad de automatizar el análisis de riesgos.

3.1.1 Aplicación de la Metodología Magerit

El caso de estudio presentado en la Figura 56 ayudará a comprender el análisis de riesgos debido a la aplicación de las actividades secuencialmente paso a paso lo que permitirá calcular el nivel de riesgo de forma manual al que se encuentra expuesto el ecosistema IoT del hogar inteligente basando en la metodología Magerit que cuenta con dos enfoques de evaluación cualitativo y cuantitativo. El enfoque cualitativo se desarrollará a continuación:

3.1.2 Caracterización de los activos

3.1.2.1 Identificación de los activos

En la identificación de activos se procede a identificar y registrar los activos del ecosistema IoT del hogar inteligente como se puede ver en la Tabla 58 se recoge información de código, responsable del activo, tipo de activo al que pertenece, subtipo especifico (atributo informativo) y cantidad.

El atributo cantidad se refiere si existe varios activos de características similares en funcionamiento y configuración en este caso como se puede ver la fila de color naranja claro de la Tabla 58 es similar al foco de código E5, esto muestra que no es necesario calcular dos veces el activo sino con solo registrar un foco estaría bien. En casos hipotéticos no podemos ingresar activo por activo si tenemos 50 focos de características similares, por esto facilitaría el registrar uno solo representativo y la cantidad de cuantos existen.

Tabla 58 Identificación de los activos

Código	Responsable	Nombre Activo	Tipo	Subtipo Especifico
A1	Anita B.	Información sensible y logs	[D] Datos / Información	[conf] datos de configuración (1)
B2	Anita B.	Alexa	[Iot] Internet de las cosas	[virass] asistente virtual
C3	Anita B.	Router	[Iot] Internet de las cosas	[iotrouter] Router IoT
D4	Anita B.	Hub	[HW] Equipos informáticos (hardware)	[hub] concentradores
E5	Anita B.	Hue_light3	[Iot] Internet de las cosas	[smartlight] Smart lighting systems
F6	Anita B.	Hue_light1	[Iot] Internet de las cosas	[smartlight] Smart lighting systems
G7	Anita B.	Google home	[Iot] Internet de las cosas	[virass] asistente virtual

Elaborado por: Parco & Arevalo

El atributo tipo y subtipo especifico son características que sirven como criterio para identificar las amenazas potenciales y salvaguardas apropiadas del activo. La metodología para el tipo de activo propone un catálogo donde clasifica a los activos jerárquicamente por grupos y cada activo puede pertenecer a uno o más jerarquías.

La tabla propuesta por la metodología no es exhaustiva, ni válida para siempre como se menciona en el libro de Catálogo de Elementos [48]. A pesar de que la metodología Magerit fue pensada para realizar el análisis de riesgos a tecnologías de información tradicional este estudio

lo adaptará para realizar un análisis de riesgos en ecosistemas IoT, lo que implica añadir cambios a los catálogos de clases de activos y amenazas que tomen en cuenta a dispositivos inteligentes.

La propuesta para adicionar al catálogo de tipos de activos un grupo jerárquico que abarque los dispositivos IoT debido a que en el catálogo de la metodología no abarca tecnologías nuevas por tanto fue necesario mediante entrevistas con profesionales plantear un grupo jerárquico para ecosistemas IoT. El grupo jerárquico planteado se basó en el modelo de referencia de IoT de la ITU, lo cual se divide en cuatro niveles: nivel de aplicación, nivel de soporte de servicio y aplicaciones, nivel de red y nivel de dispositivo. Como resultado se obtuvo la siguiente clasificación donde se muestra el nombre y el código con el que se registró para adjuntarlo al catálogo de tipo de activos propuesto por la metodología:

Nivel de aplicación:

[apphome] smart home

[appbuild] smart building

Nivel de soporte de servicio y aplicaciones se subdivide en dos subgrupos:

- [cspg] Capacidades de soporte genericas
  [prodat] Procesamiento de datos
  [aldat] Almacenamiento de datos
- [cspe] Capacidades de soporte especificas
  [CusDev] Desarrollo personalizado de IoT

Nivel de red esta subdivida en tres subgrupos:

- [capred] Capacidades de red
  [amqp] AMQP
  [coap] Constrained application protocol (CoAP)
  [dds] DDS
  [httpp]HTTP/HTTPS
  [mqtt] MQTT
  [opcua] OPC UA
  [xmpp] XMPP
  [rest] RESTFUL SERVICES
  [websock] WEB SOCKET
- [captran] Capacidades de transporte
  [tcp] TCP

[udp] UDP

- [tipcom] Estandares de comunicación

  [coal] Corto alcance

  [blue] Bluetooth Low-Energy (BLE)

  [nfc] NFC

  [zigbee] Zigbee

  [meal] Mediano alcance

  [wifi] Wifi

  [laal] Largo alcance

  [lpwan] LPWAN

  [loraw] LoraWan

  [sigfox] SigFox

  [nbiot] NB-IoT

  [redcel] Red Celular

  [sateli] Satelital

Nivel de dispositivo esta subdividido en cinco subgrupos:

- [devnet] Equipos de red IoT

  [iotgate] Gateway IoT

  [iotmodem] Modem IoT

  [iotrouter] Router IoT

  [iothub] Hub

- [sen] sensores

  [senlum] Sensor de luminosidad

  [sentem] Sensor de temperatura

  [senpre] Sensor de presencia

  [senhum] Sensor de humedad

  [senpre] Sensor de presión

  [senrad] Sensor de radiación de luz infrarroja

  [senvel] Sensor de velocidad

  [senson]Sensor de sonido

  [sengas] Sensor de Gas

  [camera] Camara

  [recegps] Receptor GPS

[wsn] WSN (red de sensores inalámbricos)

[wsan] WSAN (red de sensores y actuadores)

[mwsn] MWSN (red de sensores inalámbricos móviles)

- [act] actuadores

[luz] Luz

[valvu] Valvula

[motor] Motor

[coma] Comandos (acciones "suaves", distribución de archivos, actualizaciones de firmware)

- [enddev] Dispositivos finales

[smartp] Celular Inteligente

[tablet] Tablet

[mcu] Unidad de microcontrolador (Micro-controller Unit)

[mcuard] Arduino

[sbc] Ordenadores de placa única (Single-board computers)

[raspb] Raspberry Pi

[virass] asistente virtual

[smrtv] Television Inteligente

[werea] Wereables

[game] Video juego

[compc] Computador

- [appliance] accesorios

[tag] tags

[rfid] RFID

[barco] Barcode

[smrter] Termostato inteligente

[nesther] Nest Thermostats

[smrtlig] Sistemas de iluminación inteligente (Smart lighting systems)

[philhue] Philips Hue

[smrtlav] Lavadora inteligente

[smrtcaf] Cafetera inteligente

[smrtref] Refrigeradora inteligente

[smrtmic] Microondas inteligente

[smrtest] Estufa inteligente

3.1.2.2 Dependencias entre activos

Una vez identificados todos los activos esenciales del hogar inteligente se determina las dependencias entre activos, la relación de un activo a otro nace debido a que todos conforman un sistema por tanto si un dispositivo IoT tiene un incidente de una amenaza este puede propagarse a otros debido a que existe dependencia directa o indirecta entre activos.

En la Tabla 59 se muestra las dependencias entre activos y la estimación del grado de dependencia que fue resultado de la consideración de la opinión de expertos, el análisis refleja que el activo esencial que se encuentra en el nivel 1 del árbol de dependencias es [A1] que depende en un 50% directamente de los asistentes virtuales [B2] y [G7], ambos asistentes dependen en un 30% del encaminador (*Router*) y este a su vez depende en un 10% del concentrador [D4] finalmente entre el foco inteligente y el concentrador(Hub) existe un 30% de dependencia.

Tabla 59 Dependencia entre activos

Código	Nombre Activo	Dependencias	Grado de dependencia
A1	Información sensible y logs	B2, G7	50%
B2	Alexa	C3	30%
C3	Router	D4	10%
D4	Hub	E5, F6	30%
E5	Hue_light3		
F6	Hue_light1		
G7	Google home	C3	30%

Elaborado por: Parco & Arevalo

En la Figura 57 se representa un grafo que refleja el árbol de dependencias de la lista de activos de la Tabla 59.

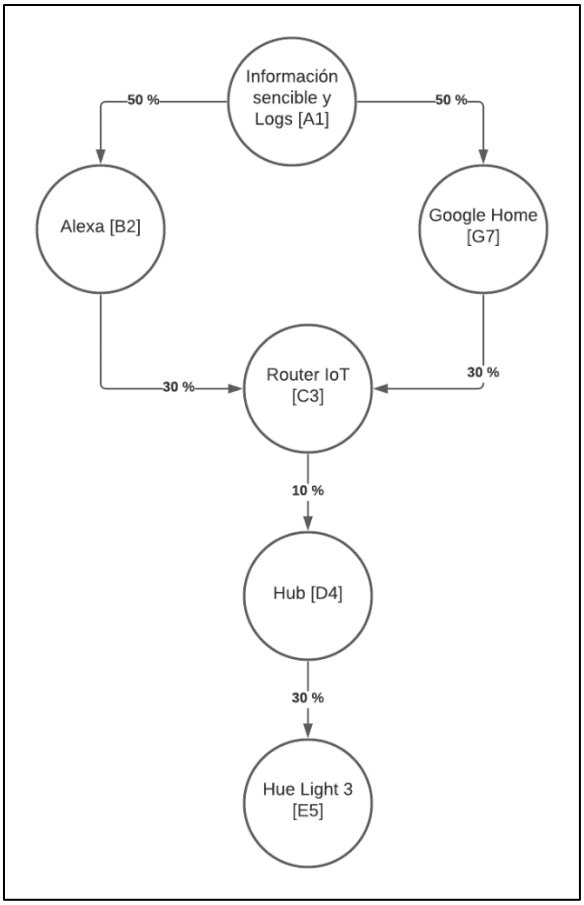


Figura 57 Árbol de dependencia

3.1.2.3 Valoración entre los activos

En esta actividad se estimará un valor en la dimensión que el activo es importante, a pesar de ser una actividad muy subjetiva debido a que depende del consenso del juicio de expertos es importante porque de aquí se derivan los cálculos de los riesgos de cada uno de los activos. La valoración de los activos se lo realiza en cada dimensión de seguridad ([D] Disponibilidad, [I] Integridad, [C] Confidencialidad, [A] Autenticidad, [T] Trazabilidad).

En este caso de estudio se utilizará un enfoque cualitativo por tanto para valorar un activo se utilizó una escala numérica de 0 a 10 como se muestra en la Tabla 60, donde los valores más cercanos a 0 tienen menor valor y pueden causar daños menores mientras que si se acercan a 10 tienen mayor valor y si se ven afectados pueden causar graves daños a la casa inteligente.

Tabla 60 Valoración de activos

Código	Nombre Activo	[D]	[I]	[C]	[A]	[T]
A1	Información sensible y logs	9	7	5	8	8
B2	Alexa	8	5	6	6	5
C3	Router	8	5	4	4	6
D4	Hub	5	4	4	4	4
E5	Hue_light3	6	4	4	4	6
F6	Hue_light1	6	4	4	4	6
G7	Google home	8	6	6	6	5

Elaborado por: Parco & Arevalo

3.1.2.4 Valor acumulado

La estimación de valoración de cada activo y las dependencias facilita el cálculo del valor acumulado de cada activo, es importante considerar primero el valor propio en cada dimensión de seguridad. La Ecuación 1 determinar el valor acumulado de un activo en un enfoque cualitativo.

$$valor\_acumulado(B) = max\,(valor(B), max_i\,\{valor(A_i)\})$$

Ecuación 1 Fórmula de valor acumulado

La ecuación anterior dice que el valor acumulado sobre un activo es el mayor de los valores que soporta, bien propio, bien de alguno de sus superiores. [14]

El cálculo del valor acumulado del ejemplo tratado se deduce mediante árboles de dependencias como en la Figura 58 y Figura 59. En los árboles de dependencia el valor propio del activo se representa mediante el nodo de color naranja claro, el valor acumulado del activo tiene el contorno de color rojo y el conjunto de nodos superiores son de color verde.

Los grafos de (a) hasta (f) calculan el valor acumulado con respecto al nodo de color naranja claro, además únicamente representa el valor acumulado de la dimensión de disponibilidad.

En el árbol (a) en el nodo raíz está situado la información y logs, este nodo no tiene valor acumulado debido a que no cuenta con activos superiores. Los árboles (b) y (c) su valor acumulado es el máximo valor entre sus superiores y su valor, está representado de color rojo su contorno.

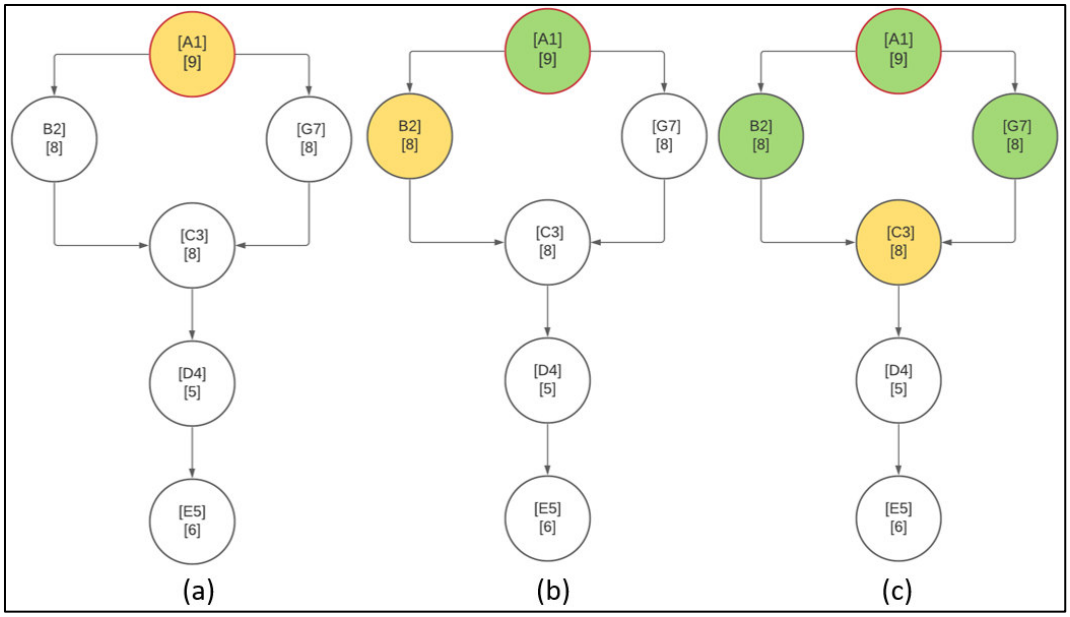


Figura 58 Valor acumulado de [A1], [B2] y [C3] (Disponibilidad)

En la Figura 59 en el grafo (f) se puede constatar que el valor acumulado únicamente es el máximo valor entre sus superiores y el valor propio, en este caso su valor acumulado es [9].

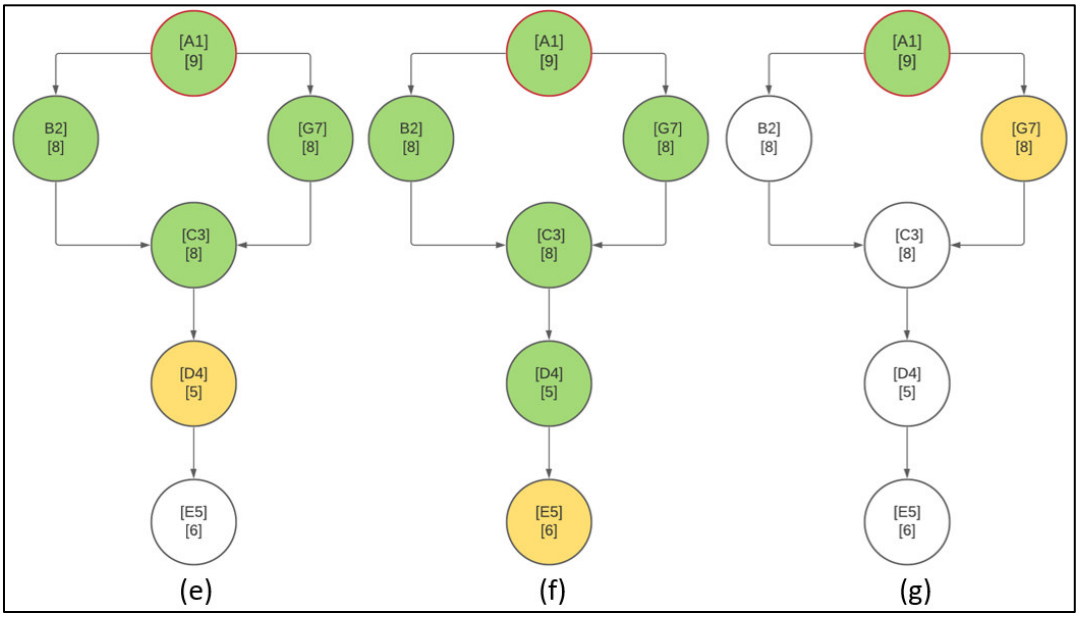


Figura 59 Valor acumulado de [D4], [E5] y [G7] (Disponibilidad)

En la Tabla 61 se muestra el valor acumulado de cada uno de los activos en cada dimensión de seguridad que fue calculado en los árboles de dependencia.

Tabla 61 Valor acumulado

Código	Nombre Activo	[D]	[I]	[C]	[A]	[T]
A1	Información sensible y logs	9	7	5	8	8
B2	Asistente virtual Alexa	9	7	6	8	8
C3	Enrutador (router)	9	7	6	8	8
D4	Concentrador (hub)	9	7	6	8	8
E5	Hue_light3	9	7	6	8	8
F6	Hue_light1	9	7	6	8	8
G7	Asistente virtual Google home	9	7	6	8	8

Elaborado por: Parco & Arevalo

3.1.3 Caracterización de las amenazas

3.1.3.1 Identificación de las amenazas

La identificación de las amenazas del ecosistema inteligente de cada activo se baso en el catálogo de amenazas planteada por la metodología, por cada activo se indetifico que posible amenaza le puede ocurrir y su degradación en cada dimension de seguridad. Las amenzas detectadas del asistente virtual Alexa se muestra en la columna “Amenazas” de la Tabla 64, la identificacion de amenazas para los activos restantes se encuentra en el Anexo 4.

Las dispositivos inteligentes son una nueva clasificación de activos por tanto no se encuentra las amenazas posibles que pueden verse afectados dichos activos, por tal motivo se realizo una encuesta a varios profesionales donde determinaron que amenazas pueden afectar la nueva clasificacion de dispositivos IoT. Los resultados obtenidos en la encuesta determina que las amenazas que afectan a activos de tipo [SW] Aplicaciones (software) y [HW] equipos informáticos (hardware) son amenazas que de igual forma afectan a los dispositivos IoT.

3.1.3.2 Valoracion de las amenzas

Las amenzas identificadas por cada activo deben ser valoradas en dos apectos, la frecuencia de ocurrencia de cada amenaza (probabilidad) y la degradacion que causaria la amenaza en cada dimensión del activo si esta se llevara a cabo.

Las probabilidad de ocurrencia y la degradacion se valoraron siguiendo los siguientes criterios:

- Frecuencia

En la Tabla 62 se muestra las diferentes escalas en las que se puede valorar la probabilidad de ocurrencia de una amenaza como plantea la metodología.

Tabla 62 Escala nominal probabilidad de ocurrencia

Escala alfanumérica	Escala númerica	Periodicidad
MA	100	A diario
A	10	Mesualmente
M	1	Una vez al año
B	1/10	Cada varios años
MB	1/100	Siglos

Tomado de [14]

- Degradación

En la Tabla 63 se muestra la escala nominal de degradación de un activo si la amenza ocurre, la escala númerica fue basada en la valoración del software GlobalSUITE descrita en el trabajo de fin de grado de Martínez [49].

Tabla 63 Escala nominal de degradación del valor

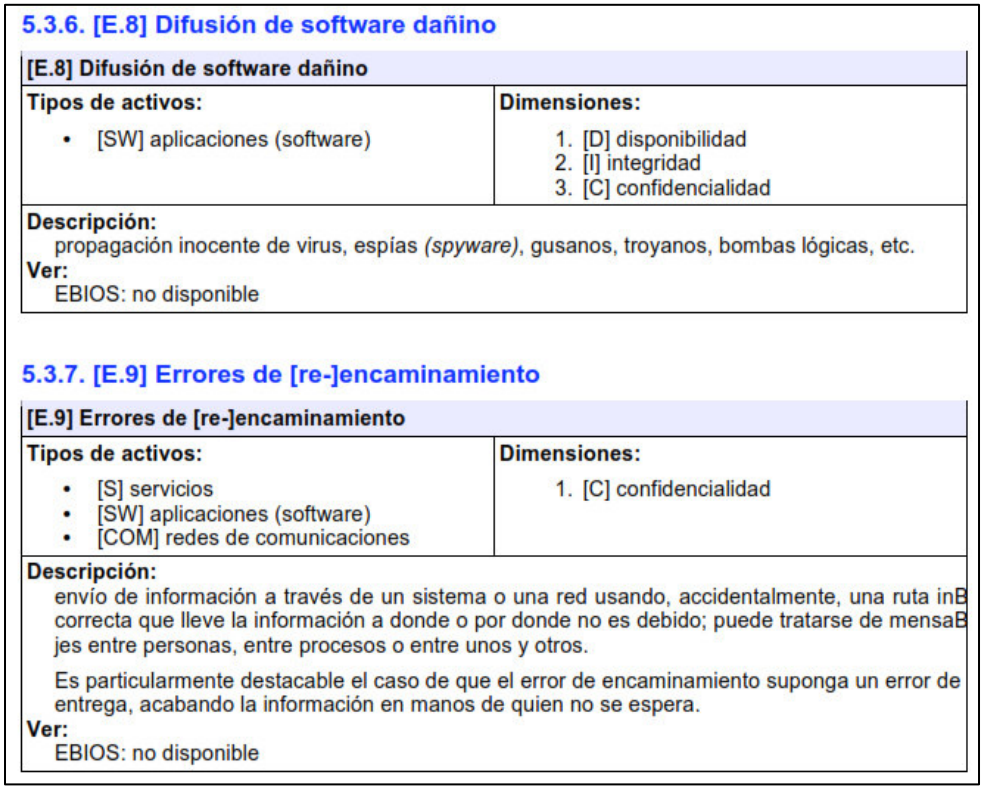
Escala alfanumérica	Escala numérica	Periodicidad
MA	95-100	casi seguro
A	67-94	muy alto
M	22-66	posible
B	3-21	poco probable
MB	0-2	muy raro

Tomado de [14].

La valoración utilizada en la probabilidad es una escala alfanumérica, mientras que en la degradacion en cada dimension es una escala numérica aunque se puede valorar con escalas numéricas o alfanuméricas, en este caso de estudio se utilizará la escala numérica debido a que la metodología cuenta con una tabla referencial en donde la entrada tanto de probabilidad y degradacion son numéricas y será fácil realizar el cálculo del impacto.

El ingreso del valor de degradación de un activo en cada dimensión de seguridad depende del catálogo de amenazas debido a que como muestra la metodología una amenaza puede afectar a uno o varias dimensiones de seguridad esto se puede comprobar en la parte de dimensiones de la Figura 60, en la amenaza [E.8] las dimensiones que se ven afectadas son disponibilidad,

integridad y confidencialidad , mientras que en la amenaza [E.9] unicamente afecta a la confidencialidad. Por tanto el ingreso del valor de degradacion en cada dimensión de seguridad depende de la metodología.



5.3.6. [E.8] Difusión de software dañino

[E.8] Difusión de software dañino	
Tipos de activos: • [SW] aplicaciones (software)	**Dimensiones:** 1. [D] disponibilidad 2. [I] integridad 3. [C] confidencialidad
Descripción: propagación inocente de virus, espías *(spyware)*, gusanos, troyanos, bombas lógicas, etc. **Ver:** EBIOS: no disponible	

5.3.7. [E.9] Errores de [re-]encaminamiento

[E.9] Errores de [re-]encaminamiento	
Tipos de activos: • [S] servicios • [SW] aplicaciones (software) • [COM] redes de comunicaciones	**Dimensiones:** 1. [C] confidencialidad
Descripción: envío de información a través de un sistema o una red usando, accidentalmente, una ruta inB correcta que lleve la información a donde o por donde no es debido; puede tratarse de mensaB jes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera. **Ver:** EBIOS: no disponible	

Figura 60 Captura de parte del catálogo de amenazas

Tomado de [48]

Al realizar la adaptación que abarque dispositivos inteligentes se debio incluir en cada amenaza en la parte de tipos de activos el tipo de activo IoT(Internet de las Cosas) que gracias a encuestas y opinión de expertos menciona que tanto donde incluyan el tipo de activo [SW] aplicaciones (software) y [HW] equipos informáticos (hardware) tambien este afectará al tipo de activo IoT (Internet de las cosas). Finalmente se realizo una hoja de cálculo para evidenciar que se incluya al tipo de activo IoT (Internet de las cosas) como se muestra en la Figura 61, el catálogo de amenazas completo se adjuntará en el Anexo V, en la hoja denominada “Amenazas”.

		Tipos de activos:	Dimensiones:
[N] Desastres naturales			
	[N.1] Fuego	[HW] equipos informáticos (hardware)	[D] disponibilidad
		[Media] soportes de información	
		[AUX] equipamiento auxiliar	
		[L] instalaciones	
		[IoT] Internet de las cosas	
	[N.2] Daños por agua		
		[HW] equipos informáticos (hardware)	[D] disponibilidad
		[Media] soportes de información	
		[AUX] equipamiento auxiliar	
		[L] instalaciones	
		[IoT] Internet de las cosas	
	[N.*] Desastres naturales		
		[HW] equipos informáticos (hardware)	[D] disponibilidad
		[Media] soportes de información	
		[AUX] equipamiento auxiliar	
		[L] instalaciones	
		[IoT] Internet de las cosas	
[I] De origen industrial			
	[I.1] Fuego		
		[HW] equipos informáticos (hardware)	[D] disponibilidad
		[Media] soportes de información	
		[AUX] equipamiento auxiliar	
		[L] instalaciones	
		[IoT] Internet de las cosas	

Figura 61 Captura de la hoja de cálculo del catálogo de amenazas.

El registro de la degradación en este caso de estudio simulado debe ser registrado para cada uno de los activos existententes en el ecosistema inteligente (información sensible y logs, asistente virtual Alexa, conmutador, concentrador, Hue_light3 y asistente virtual Google Home), pero para mayor manejo de este documento unicamente se presentara la tabla del asistente virtual Alexa debido a que las tablas son extensas. Todo el registro de la valoración de cada activo se econtrará en el Anexo 4 en la hoja de identificación de amenazas.

La Tabla 64 muestra el registro del valor de degradación y la probabilidad del asistente virtual Alexa, las celdas de color amarillo muestran las dimensiones de seguridad que afecta dicha amenaza. Las dimensiones de seguridad en las columnas de la tabla unicamente mostrará la inicial de cada dimension [D] Disponibilidad, [I] Integridad, [C] Confidencialida, [A] Autenticidad, [T] Trazabilidad.

Tabla 64 Valoración de amenazas Alexa

Amenazas	Probabilidad	D	I	C	A	T
[N.1] Fuego	MB	80%				
[N.2] Daños por agua	M	80%				
[N.*] Desastres naturales	MB	80%				
[I.1] Fuego	B	80%				
[I.2] Daños por agua	B	70%				
[I.*] Desastres industriales	MB	50%				
[I.3] Contaminación mecánica	B	60%				
[I.4] Contaminación electromagnética	A	60%				
[I.5] Avería de origen físico o lógico	A	70%				
[I.6] Corte del suministro eléctrico	A	50%				
[I.7] Condiciones inadecuadas de temperatura o humedad	A	65%				
[I.8] Fallo de servicios de comunicaciones	M	80%				
[E.1] Errores de los usuarios	B	25%	50%	50%		
[E.2] Errores del administrador	B	75%	80%	80%		
[E.3] Errores de monitorización (log)	M		80%			80%
[E.8] Difusión de software dañino	A	80%	65%	70%		
[E.9] Errores de [re-]encaminamiento	M			80%		
[E.10] Errores de secuencia	M		50%			
[E.15] Alteración accidental de la información	B		85%			
[E.18] Destrucción de información	MB	80%				
[E.19] Fugas de información	M			80%		
[E.20] Vulnerabilidades de los programas (software)	B	60%	80%	80%		
[E.21] Errores de mantenimiento / actualización de programas (software)	M	80%	40%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	80%				
[E.24] Caída del sistema por agotamiento de recursos	M	50%				
[E.25] Pérdida de equipos	B	80%		60%		
[A.5] Suplantación de la identidad del usuario	B		65%	85%	70%	
[A.6] Abuso de privilegios de acceso	B	70%	85%	85%		
[A.7] Uso no previsto	B	30%	30%	30%		
[A.8] Difusión de software dañino	M	90%	80%	80%		
[A.9] [Re-]encaminamiento de mensajes	M			85%		
[A.10] Alteración de secuencia	M		50%			
[A.11] Acceso no autorizado	B		50%	50%		
[A.12] Análisis de tráfico	B			80%		
[A.13] Repudio	M		50%			80%

Amenazas	Probabilidad	D	I	C	A	T
[A.14] Interceptación de información (escucha)	M			80%		
[A.15] Modificación deliberada de la información	M		80%			
[A.18] Destrucción de información	M	75%				
[A.19] Divulgación de información	B			90%		
[A.22] Manipulación de programas	M	85%	60%	60%		
[A.23] Manipulación de los equipos	M	50%		60%		
[A.24] Denegación de servicio	M	90%				
[A.25] Robo	B	90%		75%		
[A.26] Ataque destructivo	B	80%				

3.1.4 Caracterización de Salvaguardas

3.1.4.1 Identificación de las salvaguardas pertinentes

La información conocida tanto con que cuenta el sistema (activos) y cuáles son los incidentes adversos que pueden ocurrir sobre los activos (amenazas) son la parte importante, en la práctica existen sistemas IoT que cuentan con alguna medida de seguridad sea esta física (cerraduras) o lógica (antivirus) que trata de reducir los riesgos es por eso por lo que adicional también se debe considerar las salvaguardas o contramedidas que existen en el ecosistema IoT porque de alguna forma afecta en el cálculo del valor del riesgo.

Las salvaguardas o contramedidas son medidas de protección para que las amenazas no causen daño [14] las conocidas encontramos ya categorizadas en catálogos o en buenas prácticas de protección planteadas por expertos. Este caso de estudio se utilizó el catálogo de salvaguardas propuesto por la metodología Magerit versión 3.0 en el libro de guías técnicas.

Las salvaguardas encontradas en el caso de estudio con el que cuenta el ecosistema IoT simulado se muestra en la Tabla 66 en las cuatro primeras columnas donde registra el tipo de salvaguarda, el nombre de la salvaguarda, y las amenazas sobre las que causan repercusión si son aplicadas. El tipo de salvaguarda pueden ser de tipo: [PR] preventivas, [DR] disuasorias, [EL] eliminatorias, [IM] minimizadoras, [CR] correctivas, [RC] recuperativas, [MN] de monitorización, [DC] de detección, [AW] de concienciación, [AD] administrativas.

3.1.4.2 Valoración de las salvaguardas

Una vez conocida las salvaguardas se procede a valorar las mismas por el grado de eficacia que tiene para reducir el riesgo. La eficacia es un valor entre 0 por ciento (no protege nada) y 100 por ciento (protege y es eficaz), este valor se puede descomponer en una eficacia frente al impacto "e^i" y una eficacia frente a la probabilidad de ocurrencia "e^f". Según la naturaleza de la salvaguarda afectara al impacto, o a la frecuencia o ambas.

En este caso de estudio para calcular la eficacia de la salvaguarda se deberá ingresar el valor de la eficacia frente al impacto y a la frecuencia, para posterior calcular la eficacia de la salvaguarda con la Ecuación 2 propuesta en la metodología en el libro de guías técnicas.

$$\left(1 - e^i\right) \times \left(1 - e^f\right) = 1 - e$$

Ecuación 2 Fórmula de la Eficacia

Tomado de [18].

El valor de la eficacia obtenido es categorizado según la Tabla 65 donde el porcentaje de eficacia determinará en qué nivel de madurez se encuentra la salvaguarda. El valor calculado de la eficacia de la implementación de la salvaguarda de este caso de estudio se muestra en la última columna de la Tabla 66.

Tabla 65 Eficacia y madurez de las salvaguardas

Nivel	Significado	Eficacia
L0	Inexistente	0%
L1	inicial / ad hoc	10%
L2	reproducible pero intuitivo	50%
L3	proceso definido	90%
L4	gestionado y medible	95%
L5	Optimizado	100%

Tomado de [14].

El resultado de la caracterización de las salvaguardas es un informe de las salvaguardas implementadas y caracterizadas por su grado de efectividad como se muestra en la Tabla 66.

Tabla 66 Identificación y valoración de salvaguardas

Tipo	Código	Nombre de la Salvaguarda	Amenazas	e^i	e^f	Eficacia	
[PR]	L.design	Diseño	I.1	40%	70%	82%	L2
[PR]	L.AC	Control de los accesos físicos	I.1, E.25	40%	80%	88%	L2
[IM]	S.A	Aseguramiento de la disponibilidad	I.2	50%	10%	55%	L2
[IM]	HW.start	Puesta en producción	I.4, E.23	50%	10%	55%	L2
[RC]	BC.BIA	Análisis de impacto (BIA)	I.1	60%	5%	62%	L2
[PR]	E.4	Personal subcontratado	I.1	10%	20%	28%	L1
[DR]	AUX.AC	Climatización	I.1, I.7	50%	50%	75%	L2
[PR]	SW.CM	Cambios (actualizaciones y mantenimiento)	E.20, E.21	40%	50%	70%	L2
[DR]	AUX.wires	Protección del cableado	I.4	50%	20%	60%	L2
[PR]	H.AU	Registro y auditoría	E.2, E.25	40%	20%	52%	L2
[RC]	SW.A	Copias de seguridad (backup)	E.8	50%	10%	55%	L2
[PR]	H.tools.LA	Herramienta para análisis de logs	E.2, E.3, E.15, A.13, A.15	60%	50%	80%	L2
[DC]	H.tools.AV	Herramienta contra código dañino	E.8, A.11	0%	10%	10%	L0
[DC]	H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de	E.8	40%	30%	58%	L2
[EL]	HW.SC	Se aplican perfiles de seguridad	A.23, E.20	60%	50%	80%	L2
[DR]	COM.SC	Se aplican perfiles de seguridad	A.6	50%	50%	75%	L2
[DC]	H.tools.VA	Herramienta de análisis de vulnerabilidades	A.11	30%	20%	44%	L1
[IM]	HW.CM	Cambios (actualizaciones y mantenimiento)	I.5, E.23	50%	60%	80%	L2
[RC]	AUX.power	Suministro eléctrico	I.6	50%	10%	55%	L2
[RC]	COM.A	Aseguramiento de la disponibilidad	I.8	50%	5%	53%	L2
[PR]	SW.SC	Se aplican perfiles de seguridad	E.8, A.6	40%	50%	70%	L2
[DR]	H.ST	Segregación de tareas	E.15	30%	30%	51%	L2
[IM]	SW.start	Puesta en producción	E.20	20%	50%	60%	L2
[RC]	D.A	Copias de seguridad de los datos (backup)	A.8, A.18	50%	10%	55%	L2
[PR]	K.IC	Gestión de claves de cifra de información	A.14	50%	2%	51%	L2
[PR]	D.C	Cifrado de la información	A.19	50%	50%	75%	L2
[DR]	S.www	Protección de servicios y aplicaciones web	A.24	50%	60%	80%	L2
[PR]	H.IA	Identificación y autenticación	A.25	70%	70%	91%	L3
[IM]	H.AC	Control de acceso lógico	A.19	60%	40%	76%	L2
[IM]	H.IR	Gestión de incidencias	N.2	40%	5%	43%	L1
[IM]	COM.C	Protección criptográfica de la confidencialidad de los datos intercambiados	A.14	60%	80%	92%	L3
[IM]	MP.IC	Protección criptográfica del contenido	A.14	80%	80%	96%	L4

Tipo	Código	Nombre de la Salvaguarda	Amenazas	e^i	e^f	Eficacia	
[DC]	H.tools.DLP	DLP: Herramienta de monitorización de contenidos	A.19	50%	20%	60%	L2
[RC]	BC.DRP	Plan de Recuperación de Desastres (DRP)	N.2	80%	20%	84%	L2

En el caso que se desplieguen varias salvaguardas en una amenaza se debe calcular la eficacia del paquete de salvaguardas de forma que las salvaguardas aplicadas de forma concurrente la eficacia es la media de ellas, se suman las eficacias y se divide por el número de sumandos. En la Tabla 67 se muestra el cálculo de la eficacia al aplicar el paquete de salvaguardas a la amenaza [I.1] Fuego.

Tabla 67 Eficacia del paquete de salvaguardas aplicadas a la amenaza I.1

I.1	e^i	e^f
L.design	40%	70%
L.AC	40%	80%
BC.BIA	60%	5%
E.4	10%	20%
AUX.AC	50%	50%
Promedio	**40%**	**45%**

Por tanto, el promedio obtenido del paquete de salvaguardas a desplegarse sobre la amenaza [I.1] Fuego es eficacia frente al impacto 40 por ciento y eficacia frente a la probabilidad 45 por ciento. Es importante considerar que se calculó únicamente a modo de ejemplo para el paquete de salvaguardas aplicadas a I.1 y esto se deben hacer con las demás amenazas en donde más de una salvaguarda actúa sobre la amenaza.

3.1.5 Estimación del estado de riesgo

3.1.5.1 Valoración de las amenazas desplegadas las salvaguardas

El despliegue de las salvaguardas modifica el valor de la probabilidad de ocurrencia y la degradación que sufre el activo ante las amenazas, lo que conlleva a valorar nuevamente la degradación y probabilidad de todos los activos del sistema inteligente tomando en cuenta la eficacia que tienen las salvaguardas al ser implementadas.

La degradación residual es el resultado de reducir el porcentaje de eficiencia frente al impacto al valor del porcentaje de degradación antes de implementar las salvaguardas.

$$Degradación\ residual\ =\ Degradación\ -\ (\ Degradación\ x\ e^{i}\ )$$

Ecuación 3 Fórmula de la degradación residual

La probabilidad residual es el resultado de reducir el porcentaje de eficiencia frente a la probabilidad al valor del porcentaje de probabilidad antes de implementar las salvaguardas.

$$Probabilidad\ residual\ =\ Probabilidad\ -\ (\ Probabilidad\ x\ e^{f}\ )$$

Ecuación 4 Fórmula probabilidad residual

La Tabla 68 muestra el valor de la probabilidad y la degradación residual del asistente virtual Alexa, las amenazas que se vieron afectadas al implementar las salvaguardas tienen la celda de color verde, las amenazas que no tienen color son aquellas que no existe implementación de ninguna salvaguarda sobre las mismas.

Tabla 68 Valoración de amenazas residuales del Asistente Virtual Alexa

Amenazas	P	D	I	C	A	T
[N.1] Fuego	MB	80%				
[N.2] Daños por agua	B	48%				
[N.*] Desastres naturales	MB	80%				
[I.1] Fuego	MB	48%				
[I.2] Daños por agua	MB	35%				
[I.*] Desastres industriales	MB	50%				
[I.3] Contaminación mecánica	B	60%				
[I.4] Contaminación electromagnética	M	30%				
[I.5] Avería de origen físico o lógico	M	35%				
[I.6] Corte del suministro eléctrico	M	25%				
[I.7] Condiciones inadecuadas de temperatura o humedad	M	33%				
[I.8] Fallo de servicios de comunicaciones	B	40%				
[E.1] Errores de los usuarios	B	25%	50%	50%		
[E.2] Errores del administrador	MB	49%	52%	52%		
[E.3] Errores de monitorización (log)	B		32%			32%
[E.8] Difusión de software dañino	B	54%	44%	47%		
[E.9] Errores de [re-]encaminamiento	M			80%		
[E.10] Errores de secuencia	M		50%			

Amenazas	P	D	I	C	A	T
[E.15] Alteración accidental de la información	MB		47%			
[E.18] Destrucción de información	MB	80%				
[E.19] Fugas de información	M			80%		
[E.20] Vulnerabilidades de los programas (software)	MB	36%	48%	48%		
[E.21] Errores de mantenimiento / actualización de programas (software)	B	48%	24%			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MB	36%				
[E.24] Caída del sistema por agotamiento de recursos	M	50%				
[E.25] Pérdida de equipos	MB	30%		40%		
[A.5] Suplantación de la identidad del usuario	B		65%	85%	70%	
[A.6] Abuso de privilegios de acceso	MB	38%	47%	47%		
[A.7] Uso no previsto	B	30%	30%	30%		
[A.8] Difusión de software dañino	B	45%	40%	40%		
[A.9] [Re-]encaminamiento de mensajes	M			85%		
[A.10] Alteración de secuencia	M		50%			
[A.11] Acceso no autorizado	MB		42%	42%		
[A.12] Análisis de tráfico	B			80%		
[A.13] Repudio	B		20%			32%
[A.14] Interceptación de información (escucha)	B			30%		
[A.15] Modificación deliberada de la información	B		32%			
[A.18] Destrucción de información	B	38%				
[A.19] Divulgación de información	MB			42%		
[A.22] Manipulación de programas	M	85%	60%	60%		
[A.23] Manipulación de los equipos	B	20%		20%		
[A.24] Denegación de servicio	B	45%				
[A.25] Robo	MB	27%		23%		
[A.26] Ataque destructivo	B	80%				

3.1.5.2 Determinación del impacto potencial

Una vez ya registrado la valoración de los activos en varias dimensiones, la frecuencia de ocurrencia y la degradación de las amenazas se procede a realizar los cálculos de estimación del valor de impacto potencial. La estimación del impacto depende del valor del activo y el valor de degradación de una amenaza.

Existen dos tipos de impacto potencial:

- El **impacto potencial acumulado** de una amenaza sobre un activo es el efecto dañino que causa dicha amenaza considerando la dependencia de todos los activos de los que

depende, se calcula tomando en cuenta el valor acumulado del activo y la degradación de cada amenaza en su respectiva dimensión de seguridad.

- El **impacto potencial repercutido** de una amenaza sobre un activo es el efecto dañino que causa dicha amenaza sin considerar la dependencia entre activos, se calcula tomando en cuenta el valor propio del activo y la degradación de cada amenaza en su respectiva dimensión de seguridad.

La estimación del valor de degradación de impacto potencial acumulado y repercutido se obtiene mediante la matriz de la Tabla 69 propuesta por la metodología Magerit versión 3 en el libro de guías técnicas. La matriz de doble entrada propuesta por la metodología es tal cual, en su diagrama de colores y su interpretación de impacto, lo que varía es en la agregación por parte de nuestro estudio obtenido en la literatura de [49] y [18] son los intervalos de los porcentajes de degradación y el intervalo de valoración numérica del activo.

Tabla 69 Matriz de doble entrada para el determinar el impacto

Impacto			**Degradación**		
			0%-29%	30%-79%	80%-100%
Valor	0	MB	MB	MB	MB
	1-3	B	MB	MB	B
	4-6	M	MB	B	M
	7-9	A	B	M	A
	10	MA	M	A	MA

Tomado de [18].

Una vez identificado la degradación y el valor del activo sea acumulado o propio según el impacto a calcular, se procede a ubicar en la fila y la columna de la matriz de doble entrada donde la intersección es el valor del impacto que soporta el activo ante la amenaza. La Tabla 70 muestra el cálculo del impacto potencial acumulado y repercutido del asistente virtual Alexa a manera de ejemplo, la valoración de los activos restantes lo encontraremos en la hoja “Riesgos e Impacto Residual” del Anexo 4.

Tabla 70 Impacto potencial acumulado y repercutido del Asistente Virtual Alexa

Amenazas	**Impacto Potencial Acumulado**					**Impacto Potencial Repercutido**				
	D	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**
[N.1] Fuego	A					A				
[N.2] Daños por agua	A					A				

Amenazas	Impacto Potencial Acumulado					Impacto Potencial Repercutido				
	D	I	C	A	T	D	I	C	A	T
[N.*] Desastres naturales	A					A				
[I.1] Fuego	A					A				
[I.2] Daños por agua	M					M				
[I.*] Desastres industriales	M					M				
[I.3] Contaminación mecánica	M					M				
[I.4] Contaminación electromagnética	M					M				
[I.5] Avería de origen físico o lógico	M					M				
[I.6] Corte del suministro eléctrico	M					M				
[I.7] Condiciones inadecuadas de temperatura o humedad	M					M				
[I.8] Fallo de servicios de comunicaciones	A					A				
[E.1] Errores de los usuarios	B	M	B			B	B	B		
[E.2] Errores del administrador	M	A	M			M	M	M		
[E.3] Errores de monitorización (log)		A			A		M			M
[E.8] Difusión de software dañino	A	M	B			A	B	B		
[E.9] Errores de [re-]encaminamiento			M					M		
[E.10] Errores de secuencia		M					B			
[E.15] Alteración accidental de la información		A					M			
[E.18] Destrucción de información	A					A				
[E.19] Fugas de información			M					M		
[E.20] Vulnerabilidades de los programas (software)	M	A	M			M	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	A	M				A	B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A					A				
[E.24] Caída del sistema por agotamiento de recursos	M					M				
[E.25] Pérdida de equipos	A		B			A		B		
[A.5] Suplantación de la identidad del usuario		M	M	M			B	M	B	
[A.6] Abuso de privilegios de acceso	M	A	M			M	M	M		
[A.7] Uso no previsto	M	M	B			M	B	B		
[A.8] Difusión de software dañino	A	A	M			A	M	M		
[A.9] [Re-]encaminamiento de mensajes			M					M		
[A.10] Alteración de secuencia		M					B			
[A.11] Acceso no autorizado		M	B				B	B		
[A.12] Análisis de tráfico			M					M		
[A.13] Repudio		M			A		B			M
[A.14] Interceptación de información (escucha)			M					M		

Amenazas	Impacto Potencial Acumulado					Impacto Potencial Repercutido				
	D	I	C	A	T	D	I	C	A	T
[A.15] Modificación deliberada de la información		A					M			
[A.18] Destrucción de información	M					M				
[A.19] Divulgación de información			M					M		
[A.22] Manipulación de programas	A	M	B			A	B	B		
[A.23] Manipulación de los equipos	M		B			M		B		
[A.24] Denegación de servicio	A					A				
[A.25] Robo	A		B			A		B		
[A.26] Ataque destructivo	A					A				

3.1.5.3 Determinación del impacto residual

En esta actividad se determina el impacto residual al que está sometido el ecosistema inteligente tomando en cuenta el valor del activo, la valoración de las amenazas y la eficacia de las salvaguardas desplegadas, ya considerando las medidas de seguridad desplegadas. El impacto residual utiliza la misma matriz de doble entrada (Tabla 69) utilizada para el cálculo del impacto potencial, la diferencia que la degradación residual se calcula como se muestra la Ecuación 5

$$Impacto\ Residual\ =\ Impacto\ (\ valor\ activo, degradacion\ residual\ )$$

Ecuación 5 Fórmula del impacto residual

Tomado de [18].

Existen dos tipos de impacto potencial:

- El **impacto residual acumulado** es el efecto dañino que produce una amenaza sobre el activo luego de aplicar las medidas de seguridad se calcula sobre el valor acumulado del activo y toma en cuenta la relación de todos los activos de los que depende.
- El **impacto residual repercutido** es el efecto dañino que produce una amenaza sobre el activo luego de aplicar las medidas de seguridad se calcula sobre el valor propio del activo y no toma en cuenta la relación de dependencia con los demás activos.

La Tabla 71 muestra el resultado de estimación del impacto residual acumulado y repercutido, el mapa de colores que se visualiza depende de si el impacto es crítico o bajo como se muestra en la tabla referencial de mapa de calor de la Tabla 69.

El análisis de impacto acumulado y repercutido residual comparado con el potencial se puede constatar que una vez consideradas las salvaguardas el valor del impacto residual se ha reducido y varios de valores de muy altos (MA) han pasado a altos (A) en el ejemplo del asistente virtual Alexa. El cálculo del impacto residual del resto de activos se muestra en la hoja “Riesgos e Impacto Residual” del Anexo 4.

Tabla 71 Impacto residual acumulado y repercutido del asistente virtual Alexa.

Amenazas	Impacto residual acumulado					Impacto residual repercutido				
	D	I	C	A	T	D	I	C	A	T
[N.1] Fuego	A					A				
[N.2] Daños por agua	M					M				
[N.*] Desastres naturales	A					A				
[I.1] Fuego	M					M				
[I.2] Daños por agua	M					M				
[I.*] Desastres industriales	M					M				
[I.3] Contaminación mecánica	M					M				
[I.4] Contaminación electromagnética	M					M				
[I.5] Avería de origen físico o lógico	M					M				
[I.6] Corte del suministro eléctrico	B					B				
[I.7] Condiciones inadecuadas de temperatura o humedad	M					M				
[I.8] Fallo de servicios de comunicaciones	M					M				
[E.1] Errores de los usuarios	B	M	B			B	B	B		
[E.2] Errores del administrador	M	M	B			M	B	B		
[E.3] Errores de monitorización (log)		M			M		B			B
[E.8] Difusión de software dañino	M	M	B			M	B	B		
[E.9] Errores de [re-]encaminamiento			M					M		
[E.10] Errores de secuencia		M					B			
[E.15] Alteración accidental de la información		M					B			
[E.18] Destrucción de información	A					A				
[E.19] Fugas de información			M					M		
[E.20] Vulnerabilidades de los programas (software)	M	M	B			M	B	B		
[E.21] Errores de mantenimiento / actualización de programas (software)	M	B				M	MB			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	M					M				
[E.24] Caída del sistema por agotamiento de recursos	M					M				
[E.25] Pérdida de equipos	M		B			M		B		

Amenazas	Impacto residual acumulado					Impacto residual repercutido				
	D	I	C	A	T	D	I	C	A	T
[A.5] Suplantación de la identidad del usuario		M	M	M			B	M	B	
[A.6] Abuso de privilegios de acceso	M	M	B			M	B	B		
[A.7] Uso no previsto	M	M	B			M	B	B		
[A.8] Difusión de software dañino	M	M	B			M	B	B		
[A.9] [Re-]encaminamiento de mensajes			M					M		
[A.10] Alteración de secuencia		M					B			
[A.11] Acceso no autorizado		M	B				B	B		
[A.12] Análisis de tráfico			M					M		
[A.13] Repudio		B			M		MB			B
[A.14] Interceptación de información (escucha)			B					B		
[A.15] Modificación deliberada de la información		M					B			
[A.18] Destrucción de información	M					M				
[A.19] Divulgación de información			B					B		
[A.22] Manipulación de programas	A	M	B			A	B	B		
[A.23] Manipulación de los equipos	B		MB			B		MB		
[A.24] Denegación de servicio	M					M				
[A.25] Robo	B		MB			B		MB		
[A.26] Ataque destructivo	A					A				

3.1.5.4 Determinación del riesgo potencial

Una vez obtenido el impacto potencial de las amenazas sobre los activos se calcula el riesgo que no es más que el producto del impacto y la probabilidad de ocurrencia.

Existen dos tipos de riesgos:

- El **riesgo potencial acumulado** utiliza el impacto acumulado y la probabilidad de ocurrencia de la amenaza. El resultado de este riesgo permite determinar las salvaguardas que deben ser implementadas posteriormente.

- El **riesgo potencial repercutido** utiliza el impacto repercutido y la probabilidad de ocurrencia de la amenaza. El resultado del cálculo de este permite determinar las consecuencias de las incidencias técnicas.

El cálculo del riesgo utiliza una matriz de doble entrada como muestra en la Tabla 72 propuesta por la metodología en el libro de guías técnicas, la intersección entre impacto y probabilidad es el resultado del riesgo. Tanto el riesgo acumulado y repercutido sea este potencial o residual utilizan la misma matriz de doble entrada. El mapa de calor de riesgo planteado por la metodología es MA (rojo), A (tomate), M (amarillo), B (blanco) y MB (gris).

Tabla 72 Matriz de doble entrada para determinar el riesgo

Riesgo		**Probabilidad**				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tomado de [18].

En la Tabla 73 se muestra el cálculo de riesgo potencial acumulado y repercutido del asistente virtual Alexa por cada amenaza y dimensión. El mapa de calor que muestra la tabla indica que la amenaza [E.8] difusión de software dañino en los dos tipos de riesgos demuestra que un incidente puede causar daño y que se debe aplicar alguna medida de seguridad. A modo de ejemplo se realiza para el asistente virtual debido a que muestra un riesgo mayor a diferencia de los otros activos, el cálculo de riesgos de los activos restantes se muestra en la hoja “Riesgos e Impacto Residual” del Anexo 4.

Tabla 73 Riesgo potencial acumulado y repercutido del Asistente Virtual Alexa

Amenazas	**Riesgo Potencial Acumulado**					**Riesgo Potencial Repercutido**				
	D	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**
[N.1] Fuego	M					M				
[N.2] Daños por agua	A					A				
[N.*] Desastres naturales	M					M				
[I.1] Fuego	A					A				
[I.2] Daños por agua	M					M				
[I.*] Desastres industriales	B					B				
[I.3] Contaminación mecánica	M					M				
[I.4] Contaminación electromagnética	A					A				

Amenazas	Riesgo Potencial Acumulado					Riesgo Potencial Repercutido				
	D	I	C	A	T	D	I	C	A	T
[I.5] Avería de origen físico o lógico	A					A				
[I.6] Corte del suministro eléctrico	A					A				
[I.7] Condiciones inadecuadas de temperatura o humedad	A					A				
[I.8] Fallo de servicios de comunicaciones	A					A				
[E.1] Errores de los usuarios	B	M	B			B	B	B		
[E.2] Errores del administrador	M	A	M			M	M	M		
[E.3] Errores de monitorización (log)		A			A		M			M
[E.8] Difusión de software dañino	MA	A	M			MA	M	M		
[E.9] Errores de [re-]encaminamiento			M					M		
[E.10] Errores de secuencia		M					B			
[E.15] Alteración accidental de la información		A					M			
[E.18] Destrucción de información	M					M				
[E.19] Fugas de información			M					M		
[E.20] Vulnerabilidades de los programas (software)	M	A	M			M	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	A	M				A	B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	A					A				
[E.24] Caída del sistema por agotamiento de recursos	M					M				
[E.25] Pérdida de equipos	A		B			A		B		
[A.5] Suplantación de la identidad del usuario		M	M	M			B	M	B	
[A.6] Abuso de privilegios de acceso	M	A	M			M	M	M		
[A.7] Uso no previsto	M	M	B			M	B	B		
[A.8] Difusión de software dañino	A	A	M			A	M	M		
[A.9] [Re-]encaminamiento de mensajes			M					M		
[A.10] Alteración de secuencia		M					B			
[A.11] Acceso no autorizado		M	B				B	B		
[A.12] Análisis de tráfico			M					M		
[A.13] Repudio		M			A		B			M
[A.14] Interceptación de información (escucha)			M					M		
[A.15] Modificación deliberada de la información		A					M			
[A.18] Destrucción de información	M					M				
[A.19] Divulgación de información			M					M		
[A.22] Manipulación de programas	A	M	B			A	B	B		
[A.23] Manipulación de los equipos	M		B			M		B		
[A.24] Denegación de servicio	A					A				
[A.25] Robo	A		B			A		B		

Amenazas	Riesgo Potencial Acumulado					Riesgo Potencial Repercutido				
	D	I	C	A	T	D	I	C	A	T
[A.26] Ataque destructivo	A					A				

3.1.5.5 Estimación del riesgo residual

La estimación del riesgo residual involucra el valor del activo, la valoración de las amenazas y la eficacia de las salvaguardas implementadas. El cálculo del riesgo residual de igual forma utiliza la matriz de doble entrada manejada para calcular el riesgo potencial con la diferencia que el impacto y frecuencia son residuales como muestra la Ecuación 6.

$$Riesgo\ Residual\ = \Re\ (\ Impacto\ Residual\ , Frecuencia\ Residual)$$

Ecuación 6 Fórmula de riesgo residual.

Tomado de [18].

Existen dos tipos de riesgos residuales:

El **riesgo residual acumulado** se calcula con el impacto residual acumulado y la probabilidad residual.

El **riesgo residual repercutido** se calcula mediante el impacto residual repercutido y la probabilidad residual.

La Tabla 74 muestra el riesgo residual acumulado y repercutido únicamente para el activo del asistente virtual Alexa. El color de las celdas en las dimensiones de seguridad muestra que existe una disminución del riesgo al ser implementadas las salvaguardas. La mayoría de las amenazas que ha sido implementadas las salvaguardas tienen un riesgo muy bajo (MB).

Tabla 74 Riesgo residual acumulado y repercutido del asistente virtual Alexa.

Amenazas	Riesgo residual acumulado					Riesgo residual repercutido				
	D	I	C	A	T	D	I	C	A	T
[N.1] Fuego	M					M				
[N.2] Daños por agua	M					M				
[N.*] Desastres naturales	M					M				
[I.1] Fuego	B					B				
[I.2] Daños por agua	B					B				

Amenazas	Riesgo residual acumulado					Riesgo residual repercutido				
	D	I	C	A	T	D	I	C	A	T
[I.*] Desastres industriales	B					B				
[I.3] Contaminación mecánica	M					M				
[I.4] Contaminación electromagnética	M					M				
[I.5] Avería de origen físico o lógico	M					M				
[I.6] Corte del suministro eléctrico	B					B				
[I.7] Condiciones inadecuadas de temperatura o humedad	M					M				
[I.8] Fallo de servicios de comunicaciones	M					M				
[E.1] Errores de los usuarios	B	M	B			B	B	B		
[E.2] Errores del administrador	B	B	MB			B	MB	MB		
[E.3] Errores de monitorización (log)		M			M		B			B
[E.8] Difusión de software dañino	M	M	B			M	B	B		
[E.9] Errores de [re-]encaminamiento			M					M		
[E.10] Errores de secuencia		M					B			
[E.15] Alteración accidental de la información		B					MB			
[E.18] Destrucción de información	M					M				
[E.19] Fugas de información			M					M		
[E.20] Vulnerabilidades de los programas (software)	B	B	MB			B	MB	MB		
[E.21] Errores de mantenimiento / actualización de programas (software)	M	B				M	MB			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B					B				
[E.24] Caída del sistema por agotamiento de recursos	M					M				
[E.25] Pérdida de equipos	B		MB			B		MB		
[A.5] Suplantación de la identidad del usuario		M	M	M			B	M	B	
[A.6] Abuso de privilegios de acceso	B	B	MB			B	MB	MB		
[A.7] Uso no previsto	M	M	B			M	B	B		
[A.8] Difusión de software dañino	M	M	B			M	B	B		
[A.9] [Re-]encaminamiento de mensajes			M					M		
[A.10] Alteración de secuencia		M					B			
[A.11] Acceso no autorizado		B	MB				MB	MB		
[A.12] Análisis de tráfico			M					M		
[A.13] Repudio		B			M		MB			B
[A.14] Interceptación de información (escucha)			B					B		
[A.15] Modificación deliberada de la información		M					B			
[A.18] Destrucción de información	M					M				
[A.19] Divulgación de información			MB					MB		
[A.22] Manipulación de programas	A	M	B			A	B	B		

Amenazas	Riesgo residual acumulado					Riesgo residual repercutido				
	D	I	C	A	T	D	I	C	A	T
[A.23] Manipulación de los equipos	B		MB			B		MB		
[A.24] Denegación de servicio	M					M				
[A.25] Robo	MB		MB			MB		MB		
[A.26] Ataque destructivo	A					A				

4 RESULTADOS Y DISCUSIÓN

En el presente capítulo se muestra las pruebas de funcionalidad, usabilidad y rendimiento realizadas a la aplicación web. Esta sección tiene como objetivo determinar que el sistema cumpla con los requerimientos y un nivel adecuado para su utilización. Finalmente, se realizó una discusión de los resultados obtenidos en las pruebas realizadas.

4.1 Pruebas de funcionalidad

Pruebas funcionales son un tipo de pruebas de software que valida el sistema de software frente a los requerimientos funcionales. El propósito de las pruebas funcionales es probar cada función de la aplicación de software, proporcionando la entrada adecuada y verificando la salida con los requerimientos funcionales [50].

Durante el desarrollo de la aplicación web toda la funcionalidad fue aprobada por los desarrolladores y la parte interesada en cada revisión del Sprint. A continuación, se documenta las pruebas funcionales realizadas por personas externas al proyecto, teniendo como caso de prueba los requerimientos principales de la aplicación.

Los resultados completos de los casos de prueba se encuentran en el Anexo 6.

4.1.1 Resultados Casos de Prueba

Caso de Prueba:

En la Tabla 75 se muestra el caso de prueba para registrar un proyecto en la aplicación.

Tabla 75 Caso de Prueba - Registrar un proyecto

Caso de Prueba			**CP##**
Funcionalidad	Registrar un proyecto		
Descripción	El usuario realizara el registro de un nuevo proyecto de análisis de riesgo.		
Entradas	**Datos de Inicio de Sesión**		
	Correo electrónico		
	Contraseña		
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech		
	2. Iniciar sesión con las credenciales.		
	3. En el menú izquierdo seleccionar “Proyectos”.		
	4. En la pantalla de proyectos seleccionar el botón “Crear nuevo proyecto”.		
	5. Llenar el formulario con los datos del nuevo proyecto y luego seleccionar el botón “Crear Proyecto”.		
	6. Al terminar el proceso de crear proyecto se mostrará su nuevo proyecto en la tabla de proyectos registrados.		
Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se guardaron los datos del proyecto.			
Se mostro los datos del proyecto en la tabla.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para registrar un proyecto fue realizado por 3 usuarios, obteniendo resultados satisfactorios de todos los usuarios. En la Tabla 76 se puede observar los resultados de este caso de prueba.

Tabla 76 Resultados de casos de prueba - Registrar un proyecto

Resultados Esperados	**Resultado Obtenido**			
	Si	**Parcialmente**	**No**	**Total**
Se guardaron los datos del proyecto.	3	0	0	3
Se mostro los datos del proyecto en la tabla.	3	0	0	3
Total	**6**	**0**	**0**	**6**

Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 77 se muestra el caso de prueba para identificar activos en la aplicación.

Tabla 77 Caso de Prueba - Identificar activos

Caso de Prueba			**CP##**
Funcionalidad	Identificar activos		
Descripción	El usuario realizara el ingreso de activos al sistema.		
Entradas	**Datos de Inicio de Sesión**		
	Correo electrónico		
	Contraseña		
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech		
	2. Iniciar sesión con las credenciales.		
	3. En el menú izquierdo dentro del submenú de “Activos” seleccionar “Identificar activos”.		
	4. En la pantalla de identificación de activos seleccionar el botón “Ingresar activo”.		
	5. Llenar el formulario con los datos del nuevo activo y luego seleccionar el botón “Crear Activo”.		
	6. Al terminar el proceso de crear activo el nuevo activo se mostrará en la tabla de activos.		
Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se guardaron los datos del activo.			
Se mostro los datos del activo en la tabla.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para identificar activos fue realizado por 3 usuarios, obteniendo resultados satisfactorios en la identificación de activos dentro de la aplicación. En la Tabla 78 se puede observar los resultados de este caso de prueba.

Tabla 78 Resultados de casos de prueba - Identificar activos

Resultados Esperados	**Resultado Obtenido**			
	Si	**Parcialmente**	**No**	**Total**
Se guardaron los datos del activo.	2	1	0	3
Se mostro los datos del activo en la tabla.	3	0	0	3

Total	5	1	0	6
Total (%)	83,33%	16,67%	0,00%	100,00%

En este caso se obtuvo un resultado con valoración de parcial al momento de guardar los activos y el comentario del usuario fue que no lo dejo guardar ya que este campo es obligatorio y debe ser de tipo numérico pero lo cual se resolvió volviendo a llenar nuevamente sin problemas.

Caso de Prueba:

En la Tabla 79 se muestra el caso de prueba para registrar dependencias en la aplicación.

Tabla 79 Caso de Prueba - Registrar dependencias

Caso de Prueba				CP##
Funcionalidad	Registrar dependencias			
Descripción	El usuario registrar las dependencias que existan entre activos.			
Entradas	**Datos de Inicio de Sesión**			
	Correo electrónico			
	Contraseña			
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech			
	2. Iniciar sesión con las credenciales.			
	3. En el menú izquierdo dentro del submenú de “Activos” seleccionar “Registrar dependencias entre activos”.			
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.			
	5. Dentro de la tabla seleccionar la celda a la cual se le va a dar un valor numérico de dependencia.			
	6. Seleccionar el botón de Guardar.			
	7. Al terminar el proceso el valor de la dependencia se guarda y se muestra en la tabla.			
Resultado Esperado		**Resultado Obtenido**		
		Si	**Parcialmente**	**No**
Se mostraron los activos relacionados al proyecto.				
Se guardo el valor de la dependencia.				
Se mostro el valor de la dependencia en la tabla.				
Observaciones del Resultado Obtenido				

Resultados:

El caso de prueba para registrar dependencias fue realizado por 3 usuarios, obteniendo resultados satisfactorios en el registro dentro de la aplicación. En la Tabla 80 se puede observar los resultados de este caso de prueba.

Tabla 80 Resultados de casos de prueba - Registrar dependencias

Resultados Esperados	Resultado Obtenido			
	Si	Parcialmente	No	Total
Se mostraron los activos relacionados al proyecto.	3	0	0	3
Se guardo el valor de la dependencia.	3	0	0	3
Se mostro el valor de la dependencia en la tabla.	3	0	0	3
Total	**9**	**0**	**0**	**9**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 81 se muestra el caso de prueba para valorar activos en la aplicación.

Tabla 81 Caso de Prueba - Valorar activos

Caso de Prueba			CP##
Funcionalidad	Valorar activos		
Descripción	El usuario valorara los activos en las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad.		
Entradas	**Datos de Inicio de Sesión**		
	Correo electrónico		
	Contraseña		
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech		
	2. Iniciar sesión con las credenciales.		
	3. En el menú izquierdo dentro del submenú de “Activos” seleccionar “Valorar activos”.		
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.		
	5. Dentro de la tabla de valoración de activos seleccionar un activo, la dimensión de disponibilidad y seleccionar el botón de la celda de dicho activo.		
	6. Dentro del menú de valoración que aparece seleccionar el valor “Alto (+)” y luego seleccionar el botón “Guardar”		
	7. Al terminar el proceso el valor de la celda en ese activo y dimensión debe cambiar al número “7”		
Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se abrió el menú de valoración.			
Se guardo el valor de ese activo.			
Se mostro el número 7 en la celda de ese activo			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para valorar activos fue realizado por 3 usuarios, obteniendo resultados satisfactorios en la valoración de cada activo dentro de la aplicación. En la Tabla 82 se puede observar los resultados de este caso de prueba.

Tabla 82 Resultados de casos de prueba - Valorar activos

Resultados Esperados	Resultado Obtenido			
	Si	Parcialmente	No	Total
Se abrió el menú de valoración.	3	0	0	3
Se guardo el valor de ese activo.	3	0	0	3
Se mostro el número 7 en la celda de ese activo	3	0	0	3
Total	**9**	**0**	**0**	**9**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 83 se muestra el caso de prueba para identificar amenazas en la aplicación.

Tabla 83 Caso de Prueba - Identificar amenazas

Caso de Prueba			CP##
Funcionalidad	Identificar amenazas		
Descripción	El usuario podrá identificar amenazas por cada uno de los activos.		
Entradas	**Datos de Inicio de Sesión**		
	Correo electrónico		
	Contraseña		
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech		
	2. Iniciar sesión con las credenciales.		
	3. En el menú izquierdo dentro del submenú de “Amenazas” seleccionar “Identificar amenazas”.		
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.		
	5. Los activos se mostrarán en una lista, seleccionar el primer activo este se deberá colapsar y mostrará un listado de amenazas automáticamente.		
	6. Dentro de la lista de amenazas seleccionar el botón de editar amenaza que tiene el icono de un lápiz y se abrirá un modal con dos entradas.		
	7. En el modal ingresar los datos de vulnerabilidades y un comentario luego seleccionar el botón guardar.		
	8. Al terminar el proceso en la columna de vulnerabilidades se mostrarán las vulnerabilidades ingresadas de dicha amenaza.		
Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se abrió el modal con el menú de la amenaza.			
Se guardaron los datos de vulnerabilidad y comentario.			

Se mostraron las vulnerabilidades ingresadas en la lista.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para identificar amenazas fue realizado por 3 usuarios, obteniendo resultados satisfactorios para este caso de prueba en la aplicación. En la Tabla 84 se puede observar los resultados de este caso de prueba.

Tabla 84 Resultados de casos de prueba - Identificar amenazas

Resultados Esperados	**Resultado Obtenido**			
	Si	**Parcialmente**	**No**	**Total**
Se abrió el modal con el menú de la amenaza.	3	0	0	3
Se guardaron los datos de vulnerabilidad y comentario.	3	0	0	3
Se mostraron las vulnerabilidades ingresadas en la lista.	3	0	0	3
Total	**9**	**0**	**0**	**9**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 85 se muestra el caso de prueba para valorar amenazas en la aplicación.

Tabla 85 Caso de Prueba - Valorar amenazas

Caso de Prueba		**CP##**
Funcionalidad	Valorar amenazas	
Descripción	El usuario podrá valorar las amenazas de cada uno de los activos en las dimensiones de probabilidad, disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad.	
Entradas	**Datos de Inicio de Sesión**	
	Correo electrónico	
	Contraseña	
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech	
	2. Iniciar sesión con las credenciales.	
	3. En el menú izquierdo dentro del submenú de “Amenazas” seleccionar “Valorar amenazas”.	
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.	
	5. Los activos se mostrarán en una lista, seleccionar el primer activo este se deberá colapsar y mostrará un listado de amenazas con sus dimensiones.	

	6. En la primera amenaza seleccionar el botón de la columna de acción y se mostraran entradas de texto en las celdas de la primera fila de dicha amenaza.
	7. Ingresar los valores numéricos para cada una de las dimensiones y luego seleccionar el botón con el icono de guardar.
	8. Al terminar el proceso se mostrará los valores ingresados en cada una de las dimensiones.

Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se mostro las entradas de texto.			
Se guardaron los valores de las amenazas.			
Se mostraron los valores de las amenazas.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para valorar amenazas fue realizado por 3 usuarios, obteniendo resultados satisfactorios en la valoración de amenazas de los activos dentro de la aplicación. En la Tabla 86 se puede observar los resultados de este caso de prueba.

Tabla 86 Resultados de casos de prueba - Valorar amenazas

Resultados Esperados	**Resultado Obtenido**			
	Si	**Parcialmente**	**No**	**Total**
Se mostro las entradas de texto.	3	0	0	3
Se guardaron los valores de las amenazas.	3	0	0	3
Se mostraron los valores de las amenazas.	3	0	0	3
Total	**9**	**0**	**0**	**9**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 87 se muestra el caso de prueba para identificar salvaguardas en la aplicación.

Tabla 87 Caso de Prueba - Identificar salvaguardas

Caso de Prueba		**CP##**
Funcionalidad	Identificar salvaguardas	
Descripción	El usuario podrá identificar salvaguardas para todo el proyecto de análisis de riesgo.	
Entradas	**Datos de Inicio de Sesión**	
	Correo electrónico	
	Contraseña	
Proceso	1. Ingresar a la siguiente dirección en un navegador:	

	https://app.smartrisk.tech
	2. Iniciar sesión con las credenciales.
	3. En el menú izquierdo dentro del submenú de “Salvaguardas” seleccionar “Identificar Salvaguardas”.
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.
	5. En la pantalla de identificación de salvaguardas seleccionar el botón “Ingresar Salvaguarda” el cual abrirá un modal con el listado de salvaguardas.
	6. Dentro del listado seleccionar la primera salvaguarda y luego seleccionar el botón de más “+” el cual abrirá un formulario.
	7. Ingresar los datos del formulario para la identificación de la salvaguarda, luego seleccionar el botón “Crear Salvaguarda”.
	8. Al terminar el proceso en la tabla de identificación de salvaguardas se mostrará la nueva salvaguarda creada.

Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se abrió el modal con el listado de salvaguardas.			
Se abrió el formulario para identificar la salvaguarda.			
Se guardo los datos de la salvaguarda.			
Se mostraron los datos de la salvaguarda en la tabla.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para identificar salvaguardas fue realizado por 3 usuarios, obteniendo resultados satisfactorios en la identificación dentro de la aplicación. En la Tabla 88 se puede observar los resultados de este caso de prueba.

Tabla 88 Resultados de casos de prueba - Identificar salvaguardas

Resultados Esperados	**Resultado Obtenido**			
	Si	**Parcialmente**	**No**	**Total**
Se abrió el modal con el listado de salvaguardas.	3	0	0	3
Se abrió el formulario para identificar la salvaguarda.	3	0	0	3
Se guardo los datos de la salvaguarda.	3	0	0	3
Se mostraron los datos de la salvaguarda en la tabla.	3	0	0	3
Total	**12**	**0**	**0**	**12**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 89 se muestra el caso de prueba para valorar salvaguarda en la aplicación.

Tabla 89 Caso de Prueba - Valorar salvaguarda

Caso de Prueba			**CP##**
Funcionalidad	Valorar salvaguarda		
Descripción	El usuario podrá valorar la salvaguarda en lo que se refiere a la eficacia frente al impacto y la eficacia frente a la probabilidad.		
Entradas	**Datos de Inicio de Sesión**		
	Correo electrónico		
	Contraseña		
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech		
	2. Iniciar sesión con las credenciales.		
	3. En el menú izquierdo dentro del submenú de “Salvaguardas” seleccionar “Valorar Salvaguardas”.		
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.		
	5. En la tabla de valoración de salvaguardas seleccionar la primera salvaguarda y en la columna de acción seleccionar el botón de editar con el icono del lápiz.		
	6. Se mostrará entradas de texto en las columnas de eficacia frente al impacto y eficacia frente a la probabilidad, dentro de dichas columnas ingresar 12 y 56 respectivamente y luego seleccionar el botón de guardar.		
	7. Se calculará la columna de eficacia automáticamente y se mostrará el valor de 61.28.		
	8. Al terminar el proceso en la tabla de valoración de salvaguardas se mostrará los datos ingresados y el dato calculado automáticamente.		
Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se mostraron las entradas de texto para las columnas de eficacia frente al impacto y eficacia frente a la probabilidad.			
Se calculo automáticamente el valor de la columna de eficacia.			
Se mostraron en la tabla los valores guardados.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para valorar salvaguarda fue realizado por 3 usuarios, obteniendo resultados satisfactorios de este caso de prueba dentro de la aplicación. En la Tabla 90 se puede observar los resultados de este caso de prueba.

Tabla 90 Resultados de casos de prueba - Valorar salvaguarda

Resultados Esperados	Resultado Obtenido			
	Si	Parcialmente	No	Total
Se mostraron las entradas de texto para las columnas de eficacia frente al impacto y eficacia frente a la probabilidad.	3	0	0	3
Se calculo automáticamente el valor de la columna de eficacia.	3	0	0	3
Se mostraron en la tabla los valores guardados.	3	0	0	3
Total	**9**	**0**	**0**	**9**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

Caso de Prueba:

En la Tabla 91 se muestra el caso de prueba para mostrar impacto potencial en la aplicación.

Tabla 91 Caso de Prueba - Mostrar impacto potencial

Caso de Prueba			CP##
Funcionalidad	Mostrar impacto potencial		
Descripción	El usuario podrá visualizar los valores de impacto potencial para cada uno de los activos ingresados en el proyecto.		
Entradas	**Datos de Inicio de Sesión**		
	Correo electrónico		
	Contraseña		
Proceso	1. Ingresar a la siguiente dirección en un navegador: https://app.smartrisk.tech		
	2. Iniciar sesión con las credenciales.		
	3. En el menú izquierdo dentro del submenú de “Estado del Riesgo” seleccionar “Impacto Potencial”.		
	4. En la cabecera de la tabla seleccionar el proyecto en el que se va a trabajar y aparecerá los activos relacionados a ese proyecto.		
	5. Se mostrará un listado de activos del proyecto y seleccionar el primer activo.		
	6. Dentro de cada activo se mostrará por cada activo una tabla con 3 columnas una perteneciente a las “Amenazas”, una de “Impacto acumulado” y otra de “Impacto residual” cada una con 5 sub-columnas que contienen las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad.		
	7. Cada una de las amenazas contendrá un valor en cada una de estas dimensiones según el tipo de valoración que se le haya dado a lo largo del proceso.		
Resultado Esperado	**Resultado Obtenido**		
	Si	**Parcialmente**	**No**
Se mostro el listado de activos			

Se mostro la tabla de Impacto potencial con sus respectivas columnas.			
Se mostro el valor de las dimensiones para las amenazas valoradas.			
Observaciones del Resultado Obtenido			

Resultados:

El caso de prueba para mostrar impacto potencial fue realizado por 3 usuarios, obteniendo resultados satisfactorios de este caso de prueba dentro de la aplicación. En la Tabla 92 se puede observar los resultados de este caso de prueba.

Tabla 92 Resultados de casos de prueba - Mostrar impacto potencial

Resultados Esperados	**Resultado Obtenido**			
	Si	**Parcialmente**	**No**	**Total**
Se mostro el listado de activos	3	0	0	3
Se mostro la tabla de Impacto potencial con sus respectivas columnas.	3	0	0	3
Se mostro el valor de las dimensiones para las amenazas valoradas.	3	0	0	3
Total	**9**	**0**	**0**	**9**
Total (%)	**100,00%**	**0,00%**	**0,00%**	**100,00%**

4.2 Pruebas de usabilidad

Las pruebas de usabilidad se refieren a la evaluación de un producto con usuarios que intentarán completar tareas, generalmente utilizando una o más interfaces de usuario específicas. El objetivo es identificar cualquier problema de usabilidad, recopilar datos cualitativos, cuantitativos y determinar la satisfacción del usuario con el producto [50].

Las encuestas realizadas se muestran en el Anexo 7.

4.2.1 Resultados de la Prueba de Usabilidad

Las pruebas de usabilidad se realizaron a 16 personas externas al proyecto de edades entre los 18 – 30 años (Figura 62). La siguiente encuesta permitió recopilar datos cuantitativos acerca de la facilidad con la cual los usuarios pueden navegar a través de las distintas interfaces de usuario de la aplicación web.

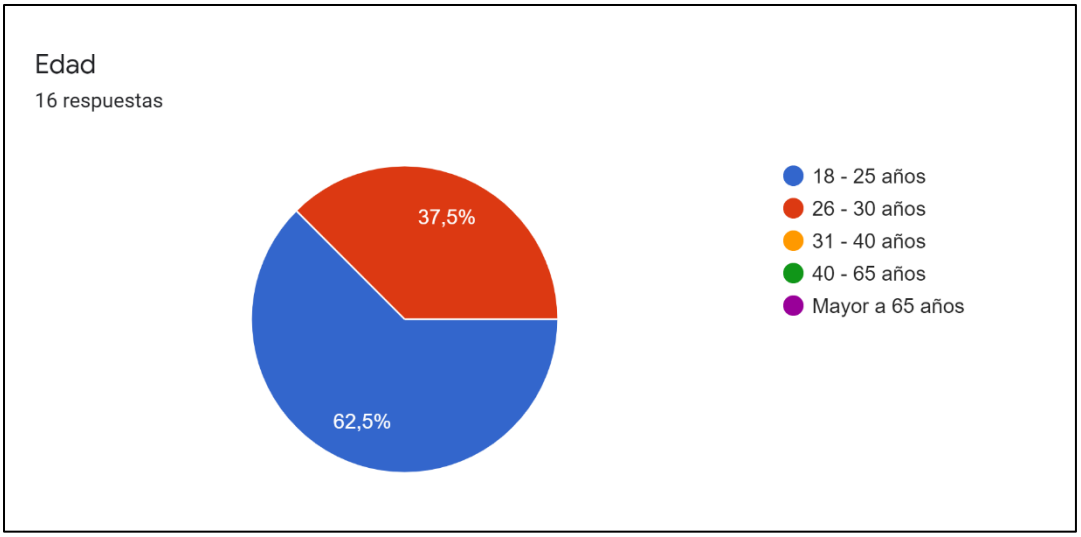


Figura 62 Distribución de edades

La encuesta fue realizada tomando una escala cuantitativa que va de 1 a 5, en donde 1 representa muy difícil y el número 5 representa un nivel muy fácil.

Para la primera pregunta se obtuvieron valoraciones entre 4 y 5 con un total del 100% de la valoración, lo que representa un nivel muy fácil de aceptación para la pantalla del dashboard principal de navegación como se muestra en la Figura 63.

Pregunta 1: ¿Cómo considera la facilidad de navegación en el dashboard principal?

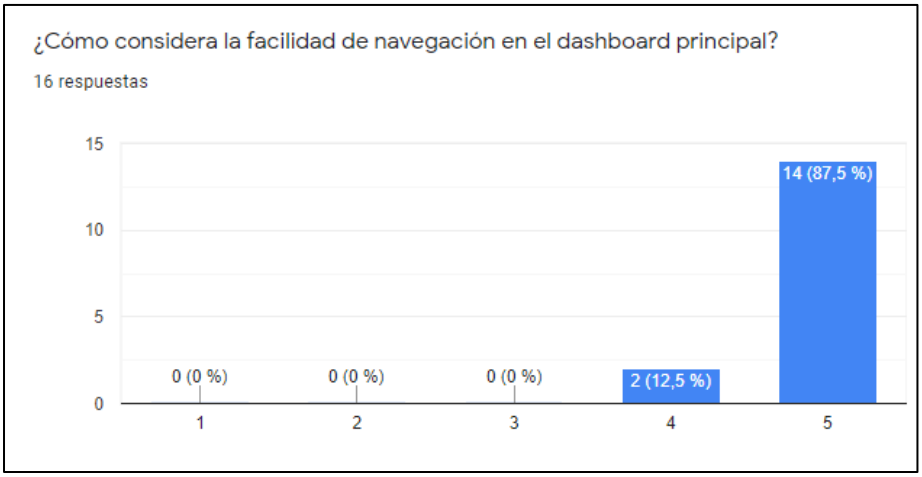


Figura 63 Prueba de Usabilidad – Pregunta 1.

Para la segunda pregunta se obtuvo un 62,5% en un nivel 5 y un 37.5% con un nivel de dificultad de 4 lo cual está dentro de un rango fácil de usabilidad (Figura 64).

Pregunta 2: ¿Cómo considera la facilidad para registrar un nuevo activo?

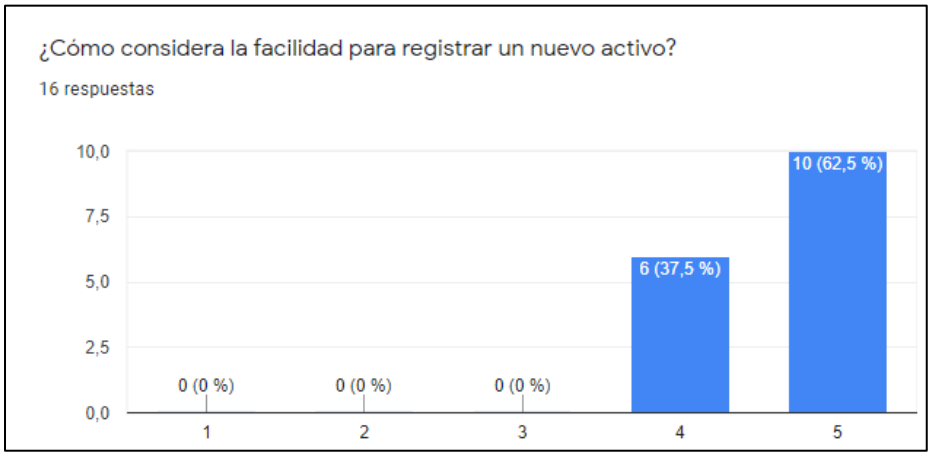


Figura 64 Prueba de Usabilidad – Pregunta 2.

Para la tercera pregunta se obtuvo un 68,8% en un nivel 5 y un 31.3% con un nivel de dificultad de 4 lo cual se encuentra dentro de un rango fácil de usabilidad para la pantalla de valorar un activo (Figura 65).

Pregunta 3: ¿Cómo considera la facilidad para valorar un activo?

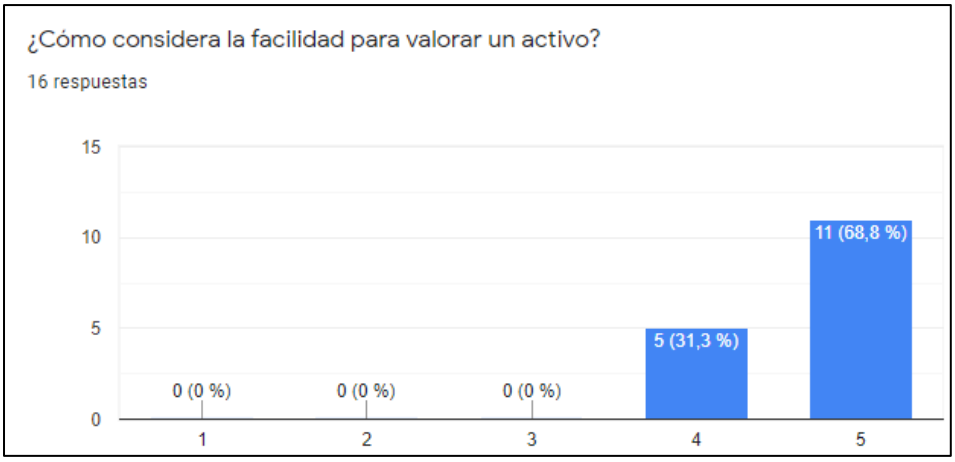


Figura 65 Prueba de Usabilidad – Pregunta 3.

Con la cuarta pregunta se obtuvo un 81,3% en un nivel 5 y un 18.8% con un nivel de dificultad de 4 lo cual está dentro de un rango muy fácil de usabilidad para la pantalla de valorar una amenaza (Figura 66).

Pregunta 4: ¿Cómo considera la facilidad para valorar una amenaza?

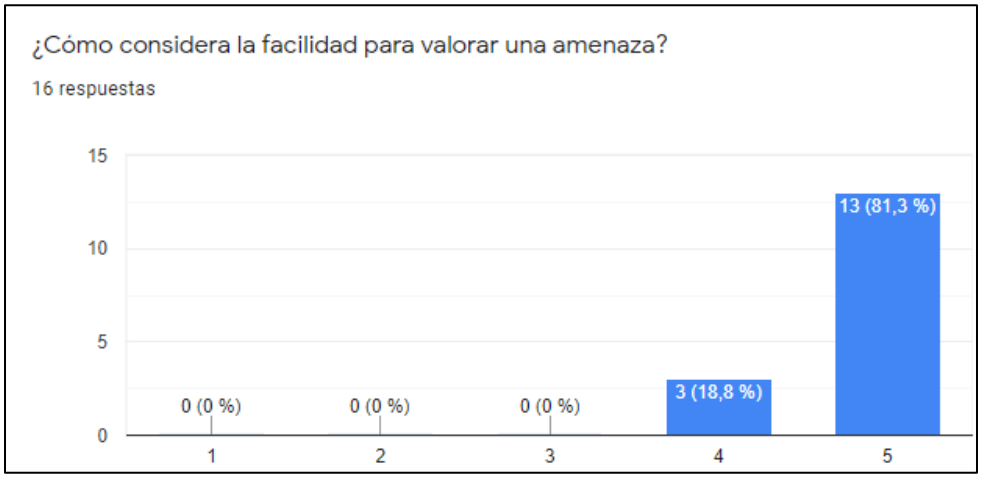


Figura 66 Prueba de Usabilidad – Pregunta 4.

Para la quinta pregunta se obtuvo un 75% en un nivel 5 y un 25% con un nivel de dificultad de 4 lo cual está dentro de un rango muy fácil de usabilidad para la pantalla de valorar una salvaguarda (Figura 67).

Pregunta 5: ¿Cómo considera la facilidad para valorar una salvaguarda?

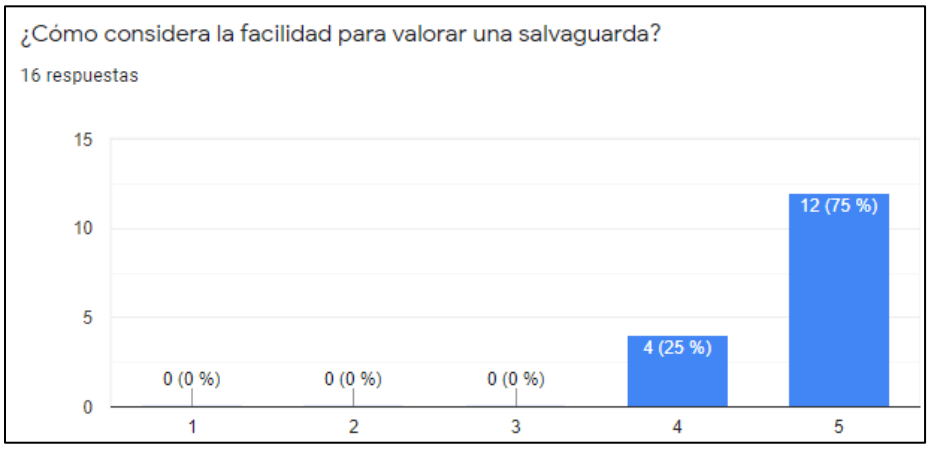


Figura 67 Prueba de Usabilidad – Pregunta 5.

Para la sexta pregunta se obtuvo un 87,5% en un nivel 5 y un 12,5% con un nivel de dificultad de 4 lo cual está dentro de un rango muy fácil de usabilidad para la pantalla de impacto potencial (Figura 68).

Pregunta 6: ¿Cómo considera la facilidad para visualizar la tabla con el impacto potencial?

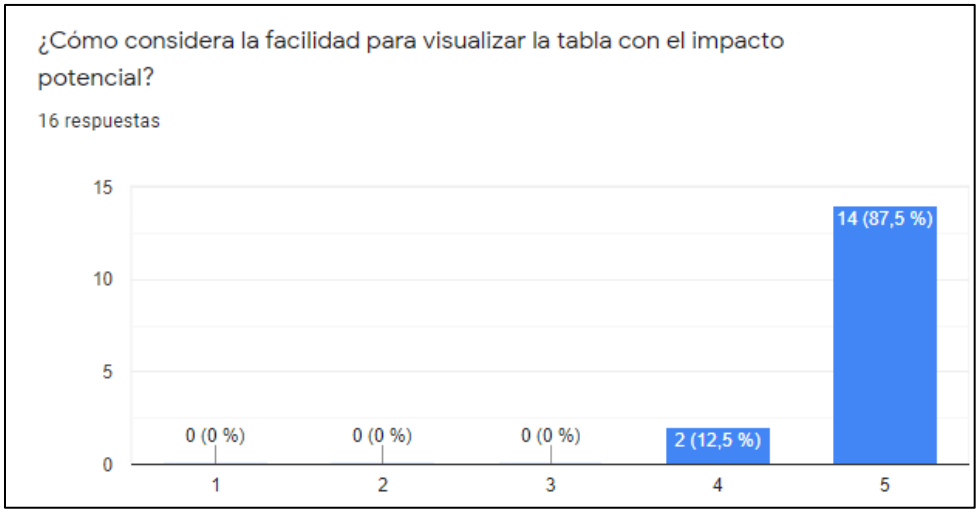


Figura 68 Prueba de Usabilidad – Pregunta 6.

4.3 Pruebas de rendimiento

ISTQB (*International Software Testing Qualifications Board*) define al rendimiento de una aplicación como un factor importante para proporcionar una buena experiencia a los usuarios que hacen uso de dicha aplicación [50].

Las pruebas de rendimiento constan de un análisis estático del código fuente y un análisis de carga a la aplicación web. Para realizar las pruebas, se utilizó las herramientas: SonarQube y JMeter respectivamente.

4.3.1 Análisis de Código Fuente

SonarQube es una herramienta de código abierto (*Open-Source*) desarrollada por SonarSource para la inspección continua de la calidad del código. Sonar realiza un análisis de código estático, que proporciona un informe detallado de errores, fallas de codificación (*code smells*), vulnerabilidades y duplicidad de código [51].

En la Figura 69 se observan los resultados obtenidos al realizar el análisis de código estático.

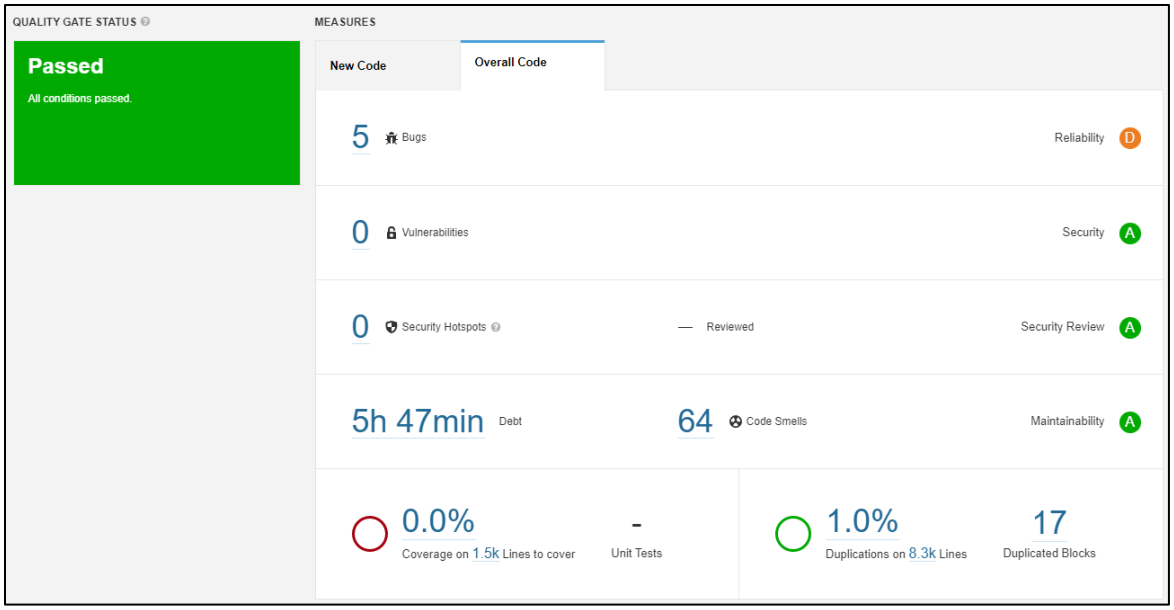


Figura 69 Resultados del análisis con SonarQube.

Se encontraron 5 bugs o errores los cuales hacen referencia a que el código debe ser refactorizado para tener un correcto funcionamiento. Se analizo cada uno de ellos y logramos encontrar que corresponden a conflictos de nombres dentro de las hojas de estilos los cuales utilizan una abreviación para acceder a sus propiedades en este caso el color del background en algunos componentes y por lo cual no representan un posible fallo en la aplicación, su funcionamiento o visualización (Figura 70).

Figura 70 Análisis de bugs encontrados.

SonarQube no ha logrado encontrar vulnerabilidades de seguridad dentro del código fuente. Sin embargo, se han obtenido 64 fallas de codificación, los cuales no representan deficiencias en el código y no son técnicamente incorrectos, pero pueden incurrir en un complejo mantenimiento del código [52]. Se analizo cada una de estas fallas de codificación y se pudo observar que en su mayoría son recomendaciones de nombramiento de variables y recomendaciones en funciones algorítmicamente complejas que pueden ser mejoradas (Figura 71), sin embargo, dichas funciones cumplen correctamente con su proceso, por lo tanto, la aplicación no se verá afectada en su correcto funcionamiento.

Figura 71 Análisis de fallas de codificación (Code smells).

También se ha obtenido un valor de mantenibilidad de código de 5.47 horas que tomaría refactorizar todo el código de la aplicación web, lo cual está dentro de los estándares pero que puede ser mejorado con una refactorización más profunda del código. Finalmente, el análisis obtenido a través de SonarQube nos indica que la aplicación web paso todas las pruebas sometidas por SonarQube y cumple en su mayoría con los estándares y buenas prácticas de desarrollo de software.

4.3.2 Análisis de Rendimiento

Apache JMeter es una herramienta de código abierto (*Open Source*) diseñada para simular pruebas de carga de un servidor HTTP, probar el comportamiento funcional y medir el rendimiento. Originalmente fue diseñado para probar aplicaciones web, pero desde entonces se ha expandido a otras funciones de prueba [53].

Se realizaron dos pruebas de carga de usuarios al servidor de la aplicación web. La primera prueba que se realizo fue hacia la página **home** cargando 20 usuarios por segundo, aumentando el valor de usuarios progresivamente, hasta llegar a un total de 1000 usuarios por segundo. Y se obtuvo como resultado un 100% de peticiones aceptadas lo cual significa que el servidor puede aceptar alrededor de 1000 peticiones de usuarios por segundo sin presentar errores (Figura 72).

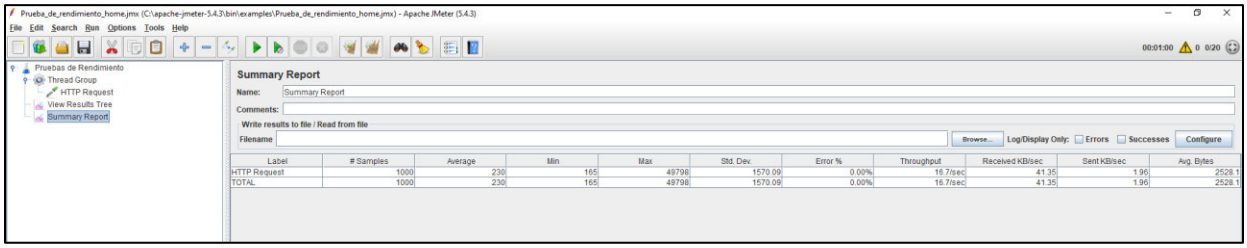


Figura 72 Resultados de prueba de carga a la página home.

La segunda prueba de carga que se realizo fue hacia la página de **proyectos** del sistema. La carga se realizó de igual manera con 20 usuarios por segundo hasta alcanzar los 1000 usuarios por segundo. En este caso se obtuvo un 100% de las peticiones recibidas por el servidor (Figura 73).

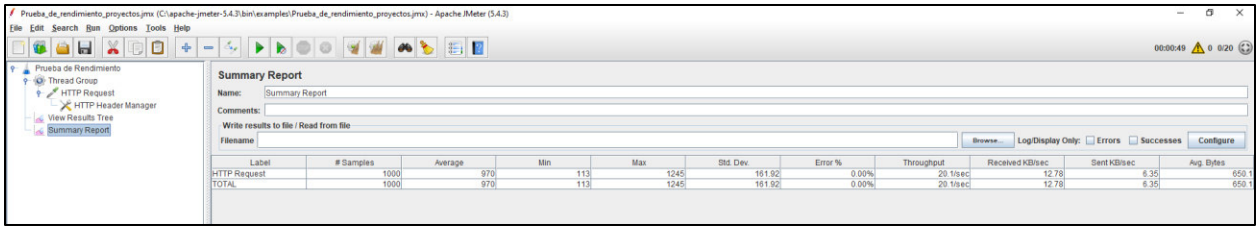


Figura 73 Resultados de prueba de carga a la página proyectos

A continuación, se muestra la Tabla 93 con los resultados resumidos de las pruebas de carga realizadas, en donde tenemos el número de peticiones realizadas, peticiones aceptadas y peticiones rechazadas.

Tabla 93 Resultados de pruebas de rendimiento.

Resultados de Pruebas de Rendimiento					
Ruta de la prueba	Número de peticiones	Peticiones aceptadas		Peticiones rechazadas	
		Valor	%	Valor	%
/home	1000	1000	100%	0	0%
/proyectos	1000	1000	100%	0	0%

En conclusión, se puede decir que el servidor en el cual está corriendo la aplicación web puede soportar gran capacidad de carga de manera concurrente aceptando un 100% de las peticiones de usuarios con un mínimo porcentaje de errores.

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- La revisión y análisis de la metodología Magerit versión 3.0 ayudo a comprender que es una metodología fácil de aplicar para realizar el análisis de riesgos derivados del uso de tecnología de la información y comunicación, debido a que cuenta con un proceso bien definido para establecer el riesgo. El procedimiento es sistemático toma en cuenta secuencialmente activos, amenazas, salvaguardas para posterior determinar el estado del riesgo. Al ser un proceso sistemático y con la ayuda de modelado de procesos se pudo automatizar e identificar cuatro módulos: caracterización de activos, caracterización de amenazas, caracterización de salvaguardas y estado del riesgo.

- Al realizar una búsqueda de aplicaciones web presentes en el mercado que realicen el análisis de riesgos y determine el riesgo mediante la metodología Magerit únicamente se encontró tres softwares. A pesar de basarse en la metodología Magerit los tres softwares encontrados son de uso comercial que contienen más metodologías y estándares lo que hace inmanejable e incompresible el análisis de riesgos llevando a confusión al determinar el estado del riesgo. Lo que conlleva que a pesar de tener un proceso de análisis de riesgos se basan en varias metodologías lo que hace inmanejable a una persona técnica llevar a cabo el proceso de análisis de riesgos.

- La adaptación de la metodología Magerit de análisis de riesgos a ecosistemas de internet de las cosas (IoT) en hogares inteligentes fue llevada a cabo debido a que el análisis de riesgos a tecnologías de información tradicional se basa en el mismo principio

que los dispositivos inteligentes ya que los mismos se encuentran dentro de las tecnologías de la información y comunicación. La tarea que se realizó para incluir los dispositivos IoT a la metodología fue agregar en los catálogos una clasificación de activos que abarque dispositivos inteligentes y en el catálogo de amenazas también tome en cuenta que amenazas pueden causar algún tipo de incidente a tecnología de internet de las cosas.

- La compresión de la metodología Magerit y el proceso de cada una de las actividades para determinar el estado del riesgo en ecosistemas inteligentes es fundamental para el desarrollo de la aplicación web debido a que sin haber antes realizado el caso de estudio simulado de forma manual era casi imposible únicamente con los requisitos del usuario desarrollar la aplicación web.

- La identificación de los módulos de la aplicación se logró gracias a: la comprensión de las actividades del proceso de análisis de riesgos, al modelado del proceso en BPMN, recolección de requisitos por parte de los interesados y al diseño de Mockups de la aplicación. Con todas las actividades realizadas se identificó cinco módulos siguientes: Autenticación, Proyectos, Caracterización de Activos, Caracterización de Amenazas, Caracterización de Salvaguardas y Estado de Riesgo. Las actividades realizadas conllevaron a ser más llevadero y ordenado el desarrollo de una aplicación web de análisis de riesgos en ecosistemas de Internet de las Cosas a pesar de iniciar el proyecto con requisitos poco definidos por parte de los interesados.

- La elaboración del caso de estudio realizado de forma manual el proceso de análisis de riesgos en hogares inteligentes con ecosistemas de Internet de las Cosas facilito a la comprensión de como adaptar la Metodología Magerit a ecosistemas IoT debido a que durante las actividades en los catálogos propuestos también se les añadía a los dispositivos de Internet de las cosas que no estaban tomados en cuenta en la metodología, esto también iba de mano de la opinión de varios profesionales. Una vez ya comprendido como incluir a dispositivos inteligentes en los catálogos fue sencillo en el desarrollo modificar los catálogos y que estos ya sean tomados en cuenta en el desarrollo de la aplicación web.

- Al utilizar una arquitectura de Modelo-Vista-Controlado (MVC) en conjunto con tecnologías web (React, NodeJS, MongoDB) se logró desarrollar una aplicación modular de fácil integración de nuevas funcionalidades durante cada iteración debido a tener separado cada uno de los módulos bien identificados. Esto ayuda a que el desarrollo sea sencillo y ordenado al implementar cada una de las características de la aplicación web.

- El uso del estándar ISO/IEC 29110 con el marco de trabajo Scrum en el desarrollo de la aplicación web permitió llevar a cabo el proyecto de forma ordenada y documentada con la finalidad de entregar un producto de software de calidad. La administración llevada a cabo por el estándar del desarrollo de toda la aplicación web fue divida en dos actividades principales: gestión del proyecto e implementación de software, la primera se encargó de la planificación y cronograma del proyecto mientras que la segunda actividad se encargó del desarrollo de la aplicación y de su respectiva documentación en cada ciclo de vida del software. La administración facilitó que cada actividad sea llevada a cabo cumpliendo con los requisitos de los interesados del proyecto.

- Una vez finalizada la implementación de todos los requerimientos de la aplicación web se realizó la ejecución de pruebas de funcionalidad, usabilidad y rendimiento las cuales permitieron determinar que la aplicación cumple con los requerimientos definidos y se encuentra en un nivel adecuado para su utilización. Para estos tres tipos de pruebas se obtuvieron el 95 por ciento de satisfacción tomando como referencia los resultados de los casos de prueba de funcionalidad, las encuestas de usabilidad y los resultados de las pruebas de rendimiento.

5.2 Recomendaciones

- Se recomienda verificar que el servidor en el cual se va a desplegar el backend de la aplicación cuente con las mejores especificaciones de disco duro, memoria RAM entre otras prestaciones de hardware ya que esto permitirá un correcto funcionamiento de la aplicación web y facilitara la escalabilidad cuando se tenga una alta demanda de peticiones al servidor.

- Al momento de configurar la base de datos se recomienda activar la opción de respaldos que provee MongoDB Atlas y de esta manera obtenemos respaldos de la base de datos en la nube cada día y de esta manera evitar posibles pérdidas de información.

- Se recomienda tener en cuenta que al utilizar los Workflows de GitHub Actions cuando se requiera conectarse con servicios de terceros como MongoDB Atlas para cargar la base de datos se debe con figurar el sistema de nombres de dominio (DNS) dentro del archivo main.yml para que en este caso el servidor pueda encontrar y conectarse al dominio de MongoDB Atlas en donde está desplegada la base de datos.

- Finalmente se recomienda tener activada la autenticación de doble factor dentro de los servicios de Netlify y Heroku para añadir una segunda capa de protección a los servidores en los cuales está desplegada la aplicación web.

BIBLIOGRAFÍA

[1] R. Pérez Colón, S. Navajas y E. Terry, «IoT en ALC 2019: Tomando el pulso al Internet de las Cosas en América Latina y el Caribe,» BID Lab, 2019.

[2] S. Nagarkar y V. Prasad, «Risk Analysis of Smart home IoT-Devices,» *CLIO An Annual Interdisciplinary Journal of History,* vol. VI, nº 1, pp. 488-493, 2020.

[3] D. Rawat y K. Z. Ghafoor, Smart Cities Cybersecurity and Privacy, Washington: Elseiver Inc., 2019.

[4] P. Radanliev, D. C. De Roure, R. Nicolescu, M. Huth, R. Mantilla Montalvo, S. Cannady y P. Burnap, «Future developments in cyber risk assessment for the internet of things,» *Computers in Industry,* vol. 102, nº 1, pp. 14-22, 2018.

[5] L. Gantiva Henao, «Universidad Piloto de Colombia,» 27 Enero 2020. [En línea]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6868/Risk%20management%20IoT_LAGH%20V5.pdf?sequence=1. [Último acceso: 27 06 2020].

[6] A. Vorster y L. Labuschagne, «A framework for comparing different information security risk analysis methodologies,» de *Conference of the South African institute of computer scientists and information technologists on IT research in developing countries*, South Africa, 2005.

[7] Kaspersky, «Internet of Things Security Threats,» Kaspersky Lab., [En línea]. Available: https://www.kaspersky.com/resource-center/threats/internet-of-things-security-risks. [Último acceso: 27 06 2020].

[8] B. Ali y I. Awad, «Cyber and Physical Security Vulnerability Assessment for IoT-Based Smart Homes,» Researchgate, Marzo 2018. [En línea]. Available: https://www.researchgate.net/publication/323649445_Cyber_and_Physical_Security_Vulnerability_Assessment_for_IoT-Based_Smart_Homes. [Último acceso: 1 Julio 2020].

[9] O. Q. Gao, «Risk Assessment for IoT : a system evaluation of the smart home and its cybersecurity imperative,» MIT, Junio 2016. [En línea]. Available: https://dspace.mit.edu/handle/1721.1/106247. [Último acceso: 30 Junio 2020].

[10] P. Siddhanti, P. M. Asprion y B. Schneider, «Cybersecurity by Design for Smart Home Environments,» Scitepress, 2019. [En línea]. Available:

https://www.scitepress.org/Papers/2019/77092/77092.pdf. [Último acceso: 02 Julio 2020].

[11] L. Teixeira da Costa, . J. . P. Corrêa Barros y M. Tavares, «Vulnerabilities in IoT Devices for Smart Home Environment,» de *ICISSP 2019*, 2019.

[12] V. Malik y S. Singh, «Internet of Things: Risk Management,» *Smart Innovation, Systems and Technologies,* vol. 141, pp. 419-426, 2019.

[13] S. Islam y W. Dong, «Human factors in software security risk management,» ACM, Mayo 2008. [En línea]. Available: https://dl.acm.org/doi/pdf/10.1145/1373307.1373312. [Último acceso: 13 Mayo 2020].

[14] Consejo Superior de Administración Electrónica del Gobierno de España, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[15] d. Mkpong-Ruffin, D. Umphress, J. Hamilton y J. Gilbert, «Quantitative software security risk assessment model,» ACM, Octubre 2007. [En línea]. Available: https://dl.acm.org/doi/abs/10.1145/1314257.1314267. [Último acceso: 13 Abril 2020].

[16] A. Kohli, K. H. Reierson y A. M. Anderson, «Converting desktop applications to web applications,» Google Patents, 3 Noviembre 2015. [En línea]. [Último acceso: 13 Mayo 2020].

[17] S. Hoque, Full-Stack React Projects 2018, Packt Publishing Ltd, 2018.

[18] Consejo Superior de Administración Electrónica del Gobierno de España, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[19] EAR PILAR, «AR TOOLS,» [En línea]. Available: https://www.ar-tools.com/es/tools/pilar_basic/v20211/index.html. [Último acceso: 08 07 2021].

[20] INCIBE Instituto Nacional de Ciberseguridad, «INCIBE,» [En línea]. Available: https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/listado-soluciones/gxsgsi. [Último acceso: 08 07 2021].

[21] Platinum Ciber-Seguridad, «R BOX,» [En línea]. Available: https://www.r-box.com.ar/ . [Último acceso: 08 07 2021].

[22] Check Point Software Technologies Ltd., 2021. [En línea]. Available: https://www.checkpoint.com/es/products/iot-security/. [Último acceso: 08 07 2021].

[23] ISO/IEC, «ISO/IEC Informe Técnico 29110-1:2016,» ISO, Suiza, 2016.

[24] ISO/IEC, « ISO/IEC Informe Técnico 29110-5-1-1,» ISO/IEC, Suiza, 2012.

[25] K. Schwaber y J. Sutherland, La Guía de Scrum, © 1991-2016 Ken Schwaber y Jeff Sutherland, 2016.

[26] R. Morales-Chaparo, M. Linaje, J. C. Preciado y Sánchez-Figueroa, «MVC Web design patterns and Rich Internet Applications,» Researchgate, 2005. [En línea]. [Último acceso: 01 Diciembre 2020].

[27] A. Kumar, «Sencha MVC Architecture,» Packt Publishing, Noviembre 2012. [En línea]. [Último acceso: 01 Diciembre 2020].

[28] E. R. Zulian, «Implementación de un framework para el desarrollo de aplicaciones web utilizando patrones de diseño y arquitectura MVC/REST,» Universidad de Belgrado, 2010. [En línea]. Available: http://190.221.29.250/bitstream/handle/123456789/640/354_Tesina_Zulian.pdf?seq. [Último acceso: 01 Diciembre 2020].

[29] D. Mircea, A. Virgil, A. Pelcz y I. Truican, «MVC Architecture In Web Applications Development,» 2005. [En línea]. Available: http://ecad.tu-sofia.bg/et/2005/pdf/Paper138-D_Kristaly.pdf. [Último acceso: 01 Diciembre 2020].

[30] Figma, «Figma,» 2020. [En línea]. Available: https://www.figma.com/blog/. [Último acceso: 10 Diciembre 2020].

[31] Mozilla, «JavaScript,» Mozilla, Diciembre 2019. [En línea]. Available: https://developer.mozilla.org/en-US/docs/Web/JavaScript. [Último acceso: 20 Diciembre 2020].

[32] Mozilla, «HTML,» Mozilla, 02 Diciembre 2020. [En línea]. Available: https://developer.mozilla.org/en-US/docs/Web/HTML. [Último acceso: 20 Diciembre 2020].

[33] W. W. W. Consortium, «Cascading Style Sheets,» W3C, 12 Diciembre 2020. [En línea]. Available: https://www.w3.org/Style/CSS/Overview.en.html. [Último acceso: 20 Diciembre 2020].

[34] ReactJS, «ReactJS,» ReactJS, 2020. [En línea]. Available: https://reactjs.org/. [Último acceso: 20 Diciembre 2020].

[35] A. Design, «Ant Design,» Ant Design, 2020. [En línea]. Available: https://ant.design/. [Último acceso: 20 Diciembre 2020].

[36] NodeJS, «NodeJS,» NodeJS, 2020. [En línea]. Available: https://nodejs.org/en/. [Último acceso: 20 Diciembre 2020].

[37] ExpressJS, «ExpressJS,» ExpressJS, 2020. [En línea]. Available: https://expressjs.com/. [Último acceso: 20 Diciembre 2020].

[38] Mongodb, «Mongodb,» Mongodb, 2020. [En línea]. Available: https://www.mongodb.com/what-is-mongodb. [Último acceso: 20 Diciembre 2020].

[39] Robomongo, «Robo 3T,» Robomongo, 2020. [En línea]. Available: https://robomongo.org/. [Último acceso: 20 Diciembre 2020].

[40] Mongoose, «Mongoose,» Mongoose, 2020. [En línea]. Available: https://mongoosejs.com/. [Último acceso: 20 Diciembre 2020].

[41] V. Code, «What is AXIOS and How To Use it!,» DEV, 07 Abril 2020. [En línea]. Available: https://dev.to/veewebcode/what-is-axios-and-how-to-use-it-4an1. [Último acceso: 20 Diciembre 2020].

[42] RedHat, «What is an API?,» RedHat, 2020. [En línea]. Available: https://www.redhat.com/en/topics/api/what-are-application-programming-interfaces. [Último acceso: 20 Diciembre 2020].

[43] codecademy, «What is REST?,» codecademy, 2020. [En línea]. Available: https://www.codecademy.com/articles/what-is-rest. [Último acceso: 20 Diciembre 2020].

[44] JSON, «Introducing JSON,» JSON, 2020. [En línea]. Available: https://www.json.org/json-en.html. [Último acceso: 20 Diciembre 2020].

[45] VisualStudio, «VisualStudio,» VisualStudio, 2020. [En línea]. Available: https://code.visualstudio.com/. [Último acceso: 20 Diciembre 2020].

[46] GitHub, «GitHub,» GitHub, 2020. [En línea]. Available: https://guides.github.com/activities/hello-world/. [Último acceso: 20 Diciembre 2020].

[47] Sourcetreeapp, «Sourcetreeapp,» Sourcetreeapp, 2020. [En línea]. Available: https://www.sourcetreeapp.com/. [Último acceso: 20 Diciembre 2020].

[48] Consejo Superior de Administración Electrónica del Gobierno de España, MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos, Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

[49] I. Martínez, Herramientas para la gestión de riesgos de la seguridad de la información. Aplicación de GlobalSUITE al método Magerit., Madrid: Universidad Politécnica de Madrid, 2018.

[50] ISTQB, «Foundation Level Specialist Syllabus Performance Testing,» 2018. [En línea]. Available: https://www.istqb.org/downloads.html. [Último acceso: 10 Diciembre 2021].

[51] SonarSource, «SonarQube,» 2021. [En línea]. Available: https://www.sonarqube.org/. [Último acceso: 10 Enero 2022].

[52] SonarQube, «Concepts. Code Smell,» 2021. [En línea]. Available: https://docs.sonarqube.org/latest/user-guide/concepts/. [Último acceso: 10 Enero 2022].

[53] T. A. S. Foundation, «Apache JMeter,» 2021. [En línea]. Available: https://jmeter.apache.org/. [Último acceso: 10 Enero 2022].

ANEXOS

Anexo 1: Declaración del Trabajo

Documento adjunto en formato digital:

https://tinyurl.com/AnexoITesisArevaloParco

Anexo 2: Plan de Proyecto

Documento adjunto en formato digital:

https://tinyurl.com/AnexoIITesisArevaloParco

Anexo 3: Diseño de Interfaz de Usuario

Diseño de interfaz de usuario en Figma herramienta utilizada para el diseño:

https://www.figma.com/file/KrIaUwu8svJzGn08p8aNTl/Mockups-AppWeb_AnalisisDeRiesgos

Documento adjunto en formato digital:

https://tinyurl.com/AnexoIIITesisArevaloParco

Anexo 4: Caso de Estudio del Análisis Cualitativo de Riesgos IoT

Documento adjunto en formato digital:

https://tinyurl.com/AnexoIVTesisArevaloParco

Anexo 5: Catálogos de la Metodología Magerit Incluido Dispositivos de Internet de las Cosas.

Documento en formato digital:

https://tinyurl.com/AnexoVTesisArevaloParco

Anexo 6: Casos de Prueba.

Documento en formato digital:

https://tinyurl.com/AnexoVITesisArevaloParco

Anexo 7: Encuesta de Usabilidad:

Documento en formato digital:

https://tinyurl.com/AnexoVIITesisArevaloParco